1. Overview
1.1 Deployment Options
1.1.1 Virtual Deployment
1.1.1.1 How to Deploy the Barracuda Application Security Control Center Vx image
1.1.1.2 Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx
1.1.1.3 Barracuda Application Security Control Center Vx Quick Start Guide
1.1.1.4 Backing Up Your Virtual Machine System State
1.2 Getting Started
1.3 Accounts and Roles
1.4 Barracuda Application Security Control Center as an Administrator
1.5 Barracuda Application Security Control Center as an Account Admin
1.5.1 Account Management
1.5.2 Centralized Management
1.5.2.1 Shared Configuration
1.5.2.2 Templates
1.5.2.3 Update the Firmware and Definitions (Attack, Virus, Security and GeoIP)
1.5.3 Appliance/Instance Management
1.6 Limited Warranty and License

Overview

Error rendering macro 'jira' : The JIRA server returned a trusted apps error: USER_UNKNOWN; Unknown User: {0}; ["pdfcreator"]

> The Barracuda Web Application Firewall version 8.1.1 and above can be connected to the Barracuda Application Security Control Center. The Barracuda Web Application Firewall version below 8.1.1 is not supported.

The Barracuda Application Security Control Center (BASCC) is a comprehensive centralized management system that allows administrators to manage multiple Barracuda Web Application Firewalls with varying configurations from a single console. The Barracuda Application Security Control Center web interface allows you to view all connected devices, both as an aggregate view and as simple devices through a Proxy view.

The Barracuda Application Security Control Center allows you to customize configuration templates and selectively apply those templates to connected devices. Templates are defined based on the configuration of a single connected device, and stored on the Barracuda Application Security Control Center. From here, the template can be pushed to one or more devices selected by you.

You can configure the security policy settings and share it with the connected devices. For more information on sharing the configuration, see Shared Configuration. The Barracuda Application Security Control Center provides role based administration feature to restrict access to system resources based on the roles assigned to users. A user can be assigned different permissions in different groups, along with a different permission assigned to the same user. In such cases, the Barracuda Application Security Control Center chooses the maximum permission role assigned to the user and grants access to the selected devices i.e., the lower level user role will be overridden by the higher-level user role.

This guide walks you through installation and initial configuration of your Barracuda Application Security Control Center with the Barracuda Web Application Firewall, and provides concepts and examples to help you understand how to manage Barracuda Web Application Firewalls through the web interface according to your organization's deployment needs and security policies.

The Barracuda Application Security Control Center with the Barracuda Web Application Firewall is a valuable tool for large enterprises, MSSP's and others with multi-WAF deployments. Some common use cases include:

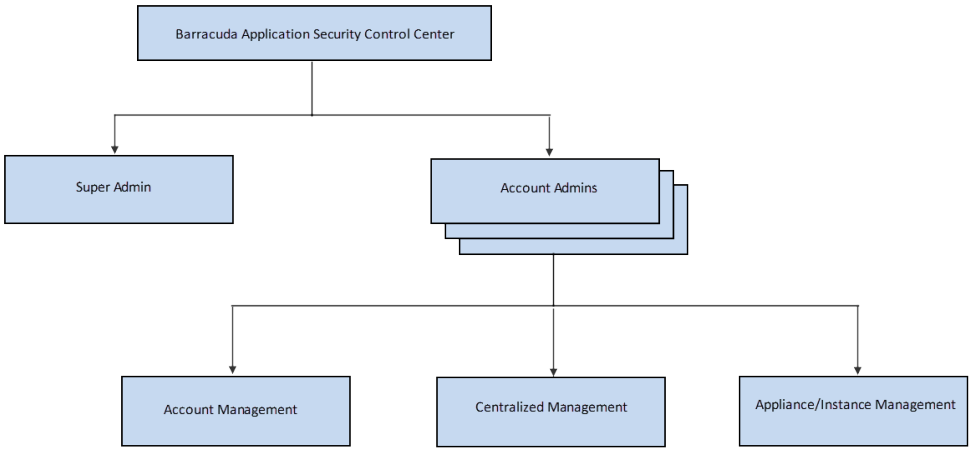
- **Shared infrastructure** – In this scenario, multiple or varying applications and services are configured on the connected Barracuda Web Application Firewalls. Each system has a custom configuration but uses the same set of security policies. In this scenario, the administrator configures security policies once and pushes them to all connected devices without modifying custom configuration settings.
- **Dedicated infrastructure** – In this scenario, the application deployed on a system has sufficient resource requirements that this entire appliance is dedicated. Through the Barracuda Application Security Control Center, dedicated Barracuda Web Application Firewalls completely isolate your server environment from the public cloud.
- **Multi DC infrastructure** – In this scenario, the application may be critical enough that it is hosted in different data centers either for scalability or for disaster recovery purposes. In this situation, the same service exists on multiple systems but is really the same application, so it is like a 'super service' hosted on multiple systems. It may have different IP addresses on different clusters but all the configurations elements for the services are the same.
- **Hybrid Deployments** – Deployments which have both on-prem (Hardware or Virtual) and cloud Barracuda Web Application Firewalls serving multiple applications are easily managed using the Barracuda Application Security Control Center in a single location.

The Barracuda Application Security Control Center web interface allows administrators to configure and monitor multiple Barracuda Web Application Firewall devices running firmware version xxxx from a single console, including:

- Monitor connected device health;
- Access security, service traffic, server traffic, client traffic, and aggregated system traffic reports across all connected devices;
- Manage certificates for all connected devices;
- Create and manage templates to create and import object type backups such as services, URL profiles, and URL policies;
- View firmware and definition version for each connected device;
- Create and manage users and groups, and assign permission-based roles.

The Barracuda Application Security Control Center supports two different administrator accounts, one to manage and configure the Barracuda Application Security Control Center including IP configuration and SNMP management, and one to create users and connect and manage connected Barracuda Web Application Firewall devices:

- **Barracuda Application Security Control Center Administrator Account** – Manage and configure the Barracuda Application Security Control Center.
- **Barracuda Application Security Control Center Account Admin** – Create users and manage and connect products through the Barracuda Application Security Control Center web interface.



Deployment Options

Currently, the Barracuda Application Security Control Center supports only virtual deployment.

In This Section:

- Virtual Deployment

Virtual Deployment

The Barracuda Application Security Control Center Vx is a comprehensive centralized appliance management system that allows administrators to manage multiple Barracuda Web Application Firewalls with varying configurations from a single console.

Deploying Your Barracuda Application Security Control Center Vx

Complete the following steps to deploy your Barracuda Application Security Control Center Vx:

- Deploy the Barracuda Application Security Control Center Vx image
- Allocate the cores, RAM, and hard disk space for your Barracuda Application Security Control Center Vx
- Set up the Barracuda Application Security Control Center Vx with the Vx Quick Start Guide
- Configure the Barracuda Application Security Control Center from the Web Interface

Managing Your Virtual Machine

- Backing Up Your Virtual Machine System State

How to Deploy the Barracuda Application Security Control Center Vx image

Barracuda offers the following types of images for the Barracuda Application Security Control Center Vx deployment. Follow the instructions for your hypervisor to deploy the Barracuda Application Security Control Center Vx appliance.

Image Type	Supported Hypervisors
OVF	• VMware ESX and ESXi (vSphere Hypervisor) versions 4.x • VMware ESX and ESXi (vSphere Hypervisor) versions 5.x and 6.x • Sun/Oracle VirtualBox and VirtualBox OSE version 3.2
VMX	• VMware Server 2.x • VMware Workstation 6.x, Player 3.x, and Fusion 3.x
XVA	• Citrix XenServer 5.5+
VHD	• Microsoft Hyper-V 2008 • Microsoft Hyper-V 8, 8.1, 2012, 2012 R2, 10

You can download these images from the Barracuda Virtual Appliance Download page. After the download is complete, extract the files from the ZIP folder.

Deploy OVF Images

VMware ESX and ESXi 4.x

Use the OVF file ending in **-4x. ovf** for this hypervisor .

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.
3. Select **Import from file**, navigate to the extracted folder, and locate the Barracuda Application Security Control Center Vx OVF file. Click **Next**.
4. Set the network to point to the target network for this virtual appliance.
5. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**.
6. Right-click your virtual appliance, select **Open Console**, and click the green arrow to power it on.
7. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to provision your virtual appliance.

VMware ESX, ESXi 5.x, and ESXi 6.x

Use the OVF file ending in **-5x.ovf** for the ESXi 5.x hypervisor and use the OVF file ending in **-6x.ovf** for the ESXi 6.x hypervisor.

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. Launch vSphere Client and select the appropriate resource pool.
3. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.
4. Click **Browse**, navigate to the extracted folder, and locate the Barracuda Application Security Control Center Vx OVF file.
5. Click **Next**. Verify that you are installing the correct Barracuda virtual appliance. Click **Next** again.
6. Enter a name for the virtual appliance. Click **Next**.
7. Select the destination storage for the virtual machine. Click **Next**.
8. Select a disk format. To ensure maximum stability when deploying your Barracuda Vx appliance, specify the disk format as **Thick Provision Eager Zeroed**. Click **Next** .
9. Map the network to the target network for this virtual appliance. Click **Next**.
10. Review the deployment options. Click **Finish** to deploy the virtual appliance.
11. Click **Finish** to deploy the appliance.
12. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**.
13. Locate the appliance within the appropriate virtual machine and resource pool. Select it and power it on by clicking the green arrow.
14. Click the **Console** tab. You can monitor the appliance as it is prepared for use.
15. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

Sun/Oracle VirtualBox and VirtualBox OSE 3.2

Use the OVF file ending in -4x. ovf for this hypervisor .

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. From the **File** menu in the VirtualBox client, select **Import Appliance**.

3. Navigate to the extracted folder and locate the Barracuda Application Security Control Center Vx OVF file.
4. Select the file and click **Next**.
5. On the **Import Settings** screen, follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx** . Click **Finish**.
6. Start the appliance.
7. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

Deploy VMX Images

VMware Server 2.x

Use the **.vmx** and **.vmdk** files for this hypervisor .

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. Navigate to the extracted folder and move the files ending in **.vmx** and **.vmdk** into a folder in your datastore (which you can locate from the **Datastores** list on your server's summary page).
3. From the VMware Infrastructure Web Access client's **Virtual Machine** menu, select **Add Virtual Machine to Inventory**.
4. Navigate to the folder in your datastore used in step 2 and select the file ending in **.vmx**. Click **OK**.
5. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**.
6. Start the appliance.
7. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

VMware Workstation 6.x, Player 3.x, and Fusion 3.x

Use the **.vmx** file for this hypervisor .

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. From the **File** menu, select **Open a Virtual Machine**.
3. Navigate to the extracted folder and select the file ending in **.vmx**.
4. Use the default settings and click **Finish**.
5. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**.
6. Start the appliance.
7. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

Deploy XVA Images

Citrix XEN Server 5.5+

Use the **.xva** file for this hypervisor. For XEN Server, you first import the virtual appliance template and then create a new virtual appliance based on that template.
Step 1. Import the virtual appliance template:

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. From the **File** menu in the XenCenter client, select **Import**.
3. Click **Browse**, navigate to the extracted folder, and select the file ending in **.xva**. Click **Next**.
4. Select a server for the template. Click **Next**.
5. Select a storage repository for the template. Click **Import**.
6. Select a virtual network interface for the template. Click **Next**.
7. Review the template settings. Click **Finish** to import the template.

Step 2. Create a new virtual appliance:

1. Right-click the virtual appliance template and select **New VM wizard**.
2. Select the virtual appliance template. Click **Next**.
3. Enter a name for the virtual appliance. Click **Next**.
4. For the DVD drive, select **<empty>**. Click **Next**.
5. Select a home server. Click **Next**.
6. Specify the number of virtual CPUs and memory for the virtual appliance. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx** . Click **Next**.
7. Select a virtual disk. Click **Next**.
8. Select a virtual network interface. Click **Next**.
9. Review the virtual appliance settings. Click **Create Now**.
10. When the virtual appliance is ready, right-click it and then click **Start**.
11. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

Deploy VHD Images

Microsoft Hyper-V 2008

Use the **.vhd** file for this hypervisor.

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. Navigate to the extracted folder and verify that the **HyperV** folder contains the following sub-folders:
   - **Snapshots**
   - **Virtual Hard Disks**
   - **Virtual Machines**
3. In Hyper-V Manager, right-click the VM host and select **Import Virtual Machine**.
4. Navigate to the extracted folder, select the **HyperV** folder, and click **Select Folder**.
5. Select **Copy the virtual machine** and **Duplicate all files**. Click **Import**.
6. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx** .
7. Start the Barracuda Application Security Control Center Vx by right-clicking the virtual machine and selecting **Start**.
8. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

Microsoft Hyper-V 8, 8.1, 2012, 2012 R2, and 10

Use the **.vhd** file for this hypervisor.

1. Download and expand the Barracuda Application Security Control Center Vx ZIP folder.
2. Launch the *WinServerSetup.bat* file located in the extracted folder. This batch file corrects a compatibility issue and takes less than a minute to run.
3. Navigate to the extracted folder and verify that the **HyperV** folder contains the following sub-folders:
   - **Snapshots**
   - **Virtual Hard Disks**
   - **Virtual Machines**
4. In Hyper-V Manager, right-click the VM host and select **Import Virtual Machine**.
5. On the **Before You Begin** page of the **Import Virtual Machine** wizard, click **Next**.
6. On the **Locate Folder** page:
   a. Click **Browse**, navigate to the extracted folder, and select the **HyperV** folder. Click **Select Folder**.
   b. Click **Next**.
7. On the **Select Virtual Machine** page, click **Next**.
8. On the **Choose Import Type** page, select **Copy the virtual machine (created a new unique ID)**. Click **Next**.
9. On the **Choose Destination: Choose Folders for Virtual Machine Files** page, click **Browse** to search for the location where you want to store the VM files. Click **Next**.
10. On the **Choose Storage Folders: Choose Folders to Store Virtual Hard Disks** page, click **Browse** to search for the location where you want to store the virtual hard disks for the VM. Click **Next**.
11. For Microsoft Windows 10, you can modify the RAM and Hard Disk space allocations after completing step **12**.
    On the **Configure Memory** page, enter a size for the **Startup RAM** that meets the requirements at **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**. Keep the default settings for the other fields. Click **Next.**
12. On the **Connect Network** page, select the network interface that you want to use for management access of the VM. Click **Next**.
13. On the **Summary** page, verify that all the settings are correct. Click **Finish**.
14. For Microsoft Windows 10, go to the **Actions** pane and click on **Settings** under **Barracuda Application Security Control Center**. Under Hardware, ensure that their is enough memory and hard disk space as specified in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx**.
15. Start your virtual appliance.
16. Follow the **Barracuda Application Security Control Center Vx Quick Start Guide** instructions to set up your virtual appliance.

To take advantage of Microsoft's VHDX support on Hyper-V 2012, 2012 R2 and 10, follow the instructions in How to Convert and Replace a Barracuda Virtual Appliance VHD File with a VHDX Format File.

Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Application Security Control Center Vx

Barracuda recommends the following sizing for initial deployment of your virtual appliance, or upgrading existing installations.

Cores, RAM, and Hard Disk Space for the Barracuda Application Security Control Center Vx

Model	Minimum Cores	RAM - Recommended Minimum	Hard Disk - Recommended Minimum
V400 Vx	2	4 GB	50 GB

Note:

(1) To increase the performance of this model, you should plan on adding 1 GB of RAM for each additional core. Also plan to add additional hard disk space. To purchase licenses for additional cores, contact your Barracuda sales representative.

Allocating Cores

In your hypervisor, specify the number of cores to be used by the Barracuda Application Security Control Center Vx. Each Barracuda Application Security Control Center Vx model can use only the number of cores specified in the table above. For example, if you assign 4 cores to the Barracuda Application Security Control Center V400 Vx (which supports only 2 cores), the hypervisor disables the 2 extra cores that cannot be used.

To add cores to your appliance:

1. Shut down the Barracuda Application Security Control Center Vx in your hypervisor.
2. In the virtual machine CPU settings, add cores.

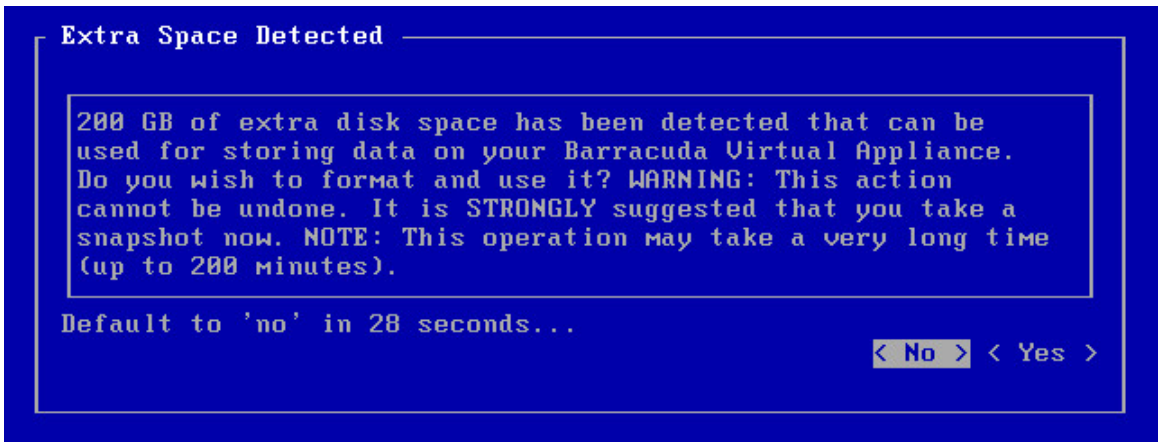
Your hypervisor license and version might limit the number of cores that you can specify for your appliance. In some cases, you must add cores in multiples of two.

Allocating Hard Disk Space

Barracuda requires a minimum of 50 GB of hard disk space to run your Barracuda Application Security Control Center Vx. From your hypervisor, you can specify the size of the hard disk or add a hard disk.

To specify the allocated hard disk space or add a hard disk to your appliance:

1. Shut down the Barracuda Application Security Control Center Vx in your hypervisor.
2. Take a snapshot of the virtual machine.
3. In the virtual machine settings, specify the new size for the hard disk or add a new hard disk.
4. Restart the virtual machine. As the appliance is booting up, view the console for Barracuda Application Security Control Center Vx. When the blue Barracuda console screen appears and asks if you want to use the additional hard disk space, enter **Yes.**



If you do not respond to the prompt in 30 seconds, the answer defaults to No. Resizing can take several minutes, depending on the amount of hard disk space specified.

Next Step

For instructions on how to set up the Barracuda Application Security Control Center Vx, see the **Barracuda Application Security Control**

Center Vx Quick Start Guide.

Barracuda Application Security Control Center Vx Quick Start Guide

To setup your Barracuda Application Security Control Center Vx, complete the following steps:

Before You Begin

Deploy the Barracuda Application Security Control Center Vx on your hypervisor. When the Barracuda Application Security Control Center Vx is deployed, by default it has only one Network Interface Card (NIC) associated with it. If you want to deploy the Barracuda Application Security Control Center Vx in the One-Arm Proxy mode, then skip ahead to the Step 1. Enter the License Code section.

Continue with Step 1. Enter the License Code.

⚠ You cannot add a **Management interface** without adding a **LAN interface**.

Step 1. Open Network Address Ranges on Firewall

If your Barracuda Application Security Control Center Vx is located behind a corporate firewall, open the following Barracuda network address ranges for the ports shown in the table below on your firewall to ensure proper operation:

- 64.235.144.0/20
- 198.207.200.0/22
- 209.222.80.0/21

Port	Direction	TCP	UDP	Usage
22	Out	Yes	No	Technical Support connections
25	In/Out	Yes	No	Email alerts
53	Out	Yes	Yes	Domain Name Service (DNS)
80/8000	Out	Yes	No	Virus/attack/security definition and firmware updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	Out	Yes	No	Initial VM Provisioning *
* The initial provisioning port can be disabled once the initial provisioning process is complete.				

Step 2. Start the Virtual Appliance, Configure Networking, and Enter the License

You should have received your Barracuda Vx license token via email or from the website when you downloaded the Barracuda Application Security Control Center Vx package. If not, you can request an evaluation on the Barracuda website at https://www.barracuda.com/purchase/evaluation or purchase one from https://www.barracuda.com/purchase/index. The license token looks similar to the following: 01234-56789-ACEFG.

1. In your hypervisor client, start the virtual appliance and allow it to boot up.
2. From the console, log in as **admin** with the password **admin**.
3. In the **System Configuration** window, use the down arrow key and select **TCP/IP Configuration**. Configure the following:
    a. WAN IP Address
    b. WAN Netmask
    c. Gateway Address
    d. Primary DNS Server
    e. Secondary DNS Server
4. If the Internet can be accessed only through an explicit proxy, configure the proxy server using **Proxy Server Configuration (Optional)**, so that it reaches the Internet for provisioning.
5. Under **Licensing** enter your Barracuda License **Token** and **Default Domain** to complete provisioning. The appliance will reboot as a part of the provisioning process.

Step 3. Accept the End User License Agreement and Verify Configuration

1. Go to **https://<your ip>** to access the web interface.
2. Read through the End User License Agreement. Scroll down to the end of the agreement.
3. Enter the required information: **Name**, **Email Address**, and **Company (if applicable)**. Click **Accept**. You are redirected to the Login

page.

4. Log into the Barracuda Application Security Control Center Vx web interface as the administrator:
   Username: *admin* **Password**: *admin*
5. Go to the **BASIC > IP Configuration** page and configure the following:
   a. Configure **TCP/IP Configuration**.
   b. Verify that the Primary and Secondary DNS servers are correct in the **DNS Configuration** section.
   c. Enter **Default Hostname** and **Default Domain** (for example, <yourcompanydomain.com>) in the **Domain Configuration**. The **Hostname** will be used in reporting and the **Default Domain** is the domain for the system.

If you are planning to put the Barracuda Application Security Control Center Vx in **Offline** mode, ensure you check the following:

- All definitions are updated on the **ADVANCED > Energize Updates** page.
- The Barracuda Application Security Control Center Vx is on the latest Firmware Version on the **ADVANCED > Firmware Update** page.

The Barracuda Application Security Control Center periodically connects to Barracuda Central to check for the availability of new Energize Updates. To receive new Energize Updates, ensure your Barracuda Application Security Control Center is able to connect to internet to reach Barracuda Central.

Step 4. Update the Firmware

Click on the **ADVANCED > Firmware Update** page. If there is a new *Latest General Release* available, perform the following steps to update the system firmware:

1. Click on the **Download Now** button located next to the firmware version that you wish to install. To view download progress, click on the **Refresh** button. When the download is complete, the **Refresh** button will be replaced by an **Apply Now** button.
2. Click on the **Apply Now** button to install the firmware. This will take a few minutes to complete.
3. After the firmware has been applied, the Barracuda Application Security Control Center Vx will automatically reboot, displaying the login page when the system has come back up.
4. Log back into the web interface again and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings you may have already entered, as new features may have been included with the firmware update.

Step 5. Change the Administrator Password

To avoid unauthorized use, we recommend you change the default administrator password to a more secure password. You can only change the administrator password for the web interface. Go to the **BASIC > Administration** page and enter your old and new passwords, then click on **Save Password**.

Backing Up Your Virtual Machine System State

Virtual machine environments generally provide a *snapshot* capability, which captures the state of a system as it's running. Once a snapshot is created, you can perform additional operations on the system and *revert* to the snapshot in the case of disaster recovery (or for any other reason). Because this feature is so powerful, Barracuda strongly recommends performing a snapshot at certain points in time:

- Before upgrading the Barracuda product firmware.
- Before making major changes to your configuration (this makes taking a snapshot a convenient *undo* mechanism).
- After completing and confirming a large set of changes, such as initial configuration.
- As a periodic backup mechanism.

Before taking a snapshot, Barracuda strongly recommends powering off the virtual machine. This step is particularly important if you are using Microsoft Hyper-V as your virtual machine environment.

Barracuda Networks recommends that you review your virtual environment documentation regarding the snapshot capabilities and be familiar with their features and limitations.

Getting Started

This section refers to Barracuda Application Security Control Center firmware version xxxx with the Barracuda Web Application Firewall firmware version 8.1.x.

- Step 1 - Configure the Barracuda Application Security Control Center Vx Web Interface
- Step 2 - Create the Barracuda Application Security Control Center Account Administrator
- Step 3 - Connect Devices to the Barracuda Application Security Control Center Vx

Step 1 - Configure the Barracuda Application Security Control Center Vx Web Interface

Before configuring the web interface, ensure you have completed the steps mentioned in ***Allocating Cores, RAM and Hard Disk Space for your Barracuda Application Security Control Center***.in the **Virtual Deployment** article.

In this Section:

- Configure the Barracuda Application Security Control Center from the Web Interface
- Activate Subscriptions
- Update the Barracuda Application Security Control Center Firmware
- Update Definitions

Configure the Barracuda Application Security Control Center from the Web Interface

Verify the system accessing the web interface is connected to the same network as the Barracuda Application Security Control Center, and that the appropriate routing is in place to allow connection to the IP address of the Barracuda Application Security Control Center via a web browser.

To configure administrative settings on the Barracuda Application Security Control Center:

1. From a web browser, enter *http://* followed by the IP address of the Barracuda Application Security Control Center. For example: *http://192.168.200.200*
2. Log into the Barracuda Application Security Control Center using the Barracuda Application Security Control Center Administrator Account (**admin**/**admin**).
3. Go to the **BASIC > IP Configuration** page, and perform the following steps:
    a. In the **TCP/IP** Configuration section, verify the IP address, netmask, and default gateway for your Barracuda Application Security Control Center.
    b. In the **DNS Configuration** section, verify the primary and secondary DNS servers for your Barracuda Application Security Control Center.
    c. If you want to configure a proxy server to allow access to the internet, enter the proxy server details in the **Proxy Server Configuration** section.
    d. Enter the **Default Domain**, for example: mydomain.com
    e. Enter an externally resolvable system name (FQDN) for the Barracuda Application Security Control Center in the **External System Name** field.
    f. Click **Save**.

Whenever your Barracuda Application Security Control Center IP address is changed on the **IP Configuration** page, you are disconnected from the administration interface. You must log in using the new IP address.

Activate Subscriptions

After you install the Barracuda Application Security Control Center, activate Barracuda Energize Updates and other applicable subscriptions to fully enable the appliance and let it continue to receive the latest updates to all virus, attack, and security definitions from Barracuda Central. The Barracuda Energize Updates service downloads these updates to your Barracuda Application Security Control Center on an hourly basis.

Proxy Server Configuration

Internet access is required to download Firmware and Energize Updates from the Barracuda Central servers; enter the Proxy Server IP address and port number on the **BASIC > IP Configuration** page to access the Internet.

To activate your subscription status:

1. Log into the Barracuda Application Security Control Center using the Barracuda Application Security Control Center Administrator Account (**admin** / **admin**).
2. Go to the **BASIC > Dashboard** page. Under **Subscription Status**, verify the **Energize Updates** status is *Current*.
3. Click on the designated link to open up the **Product Activation** page in a new browser window.
4. On the **Product Activation** page, fill in the required fields, and then click **Activate**. A confirmation page opens and displays the terms of your subscription.
5. If the **Energize Updates** status is *Not Activated*, click the activation link to go to the **Barracuda Networks Product Activation** page and complete activation of your subscriptions.

6. If your Barracuda Application Security Control Center cannot communicate directly to the Barracuda Central servers, an **Activation Code** displays; enter this code in the **Activation Code** area, and then click **Save** to activate your Barracuda Application Security Control Center.
7. Return to the Barracuda Application Security Control Center administration interface and navigate to the **BASIC > Dashboard** page. In the **Subscription Status** section, verify the **Energize Updates** status is Current.
8. There may be a slight delay of a few minutes for the display to reflect your updated subscription status. If the status continues to display as Not Activated, click **Refresh** in the **Subscription Status** section.

If your subscription status does not change to *Current* within an hour, or if you have trouble filling out the **Product Activation** page, contact your Barracuda Networks sales representative.

Update the Barracuda Application Security Control Center Firmware

Use the following steps to update the firmware.

1. Log in to the Barracuda Application Security Control Center using the Barracuda Application Security Control Center Administrator Account (**admin** / **admin**).
2. Go to the **ADVANCED > Firmware Update** page. Verify that the installed version matches the **Latest General Release**. The **Download Now** button next to the **Latest General Release** is disabled if the Barracuda Application Security Control Center is already up-to-date with the latest firmware.
3. If the installed version does not match the **Latest General Release**: read the release notes to learn about the latest features and fixes provided in the new firmware version, and click **Download Now** to begin the download. Updating the firmware may take several minutes; *do not turn off the unit during this process*. Click **Refresh** next to the firmware download progress to view the download status. A "Firmware downloaded" message displays once the download is complete.
4. Click **Apply Now** when the download is complete, and then click **OK** when prompted to reboot the Barracuda Application Security Control Center. A **Status** page displays the progress of the reboot. Once the reboot is complete, the login page appears.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Log into the Barracuda Application Security Control Center using the ***Barracuda Application Security Control Center*** Administrator Account (**admin** / **admin**).
2. Go to the **ADVANCED > Energize Updates** page.
3. Select **On** for **Automatic Updates**; the recommended setting is **On** for all available definitions.
4. Verify the current version is the same as the latest general release. If the rules are not up-to-date, continue to the next step, otherwise definition update is complete.
5. Click **Update** to download and install the latest available definitions onto the Barracuda Application Security Control Center.

Step 2 - Create the Barracuda Application Security Control Center Account Admin

Before creating the Barracuda Application Security Control Center Account Admin, complete **Step 1 - Configure the Barracuda Application Security Control Center Web Interface**.

The Barracuda Application Security Control Center Account Admin creates users and connects devices.

To create the Barracuda Application Security Control Center Account Admin, you must first log in to the web interface using the Barracuda Application Security Control Center Administrator Account (**admin**/**admin**), and complete the following steps:

1. Go to the **BASIC > Account Management** page, and in the **Account Creation** section, enter the **Account Name**, **Administrator Email Address**, and select the **Preferred Time Zone** for the new account.
2. Click **Create Account**. The account displays in the **Account View** table at the top of the page.
3. A confirmation email containing the login credentials is sent to the administrator email address entered in step **1** above. Use these credentials to log in to the web interface to create users and assign permissions, connect devices, and view device status.

Step 3 - Connect Devices to the Barracuda Application Security Control Center

Use the following steps to connect one or more Barracuda Web Application Firewall devices to the Barracuda Application Security Control Center:

1. Log into the Barracuda Application Security Control Center web interface as the Barracuda Application Security Control Center Account Admin.
2. The **BASIC > Connect Products** page is displayed as no devices are connected to the Barracuda Application Security Control Center.
3. Copy the **Validation Token** displayed under **Connecting Products to the Barracuda Application Security Control Center**.
4. In another browser window, log into the Barracuda Web Application Firewall you want to connect as the administrator. From the product **ADVANCED > Firmware Upgrade** page, check to make sure you have the latest firmware installed on the device. If not, download and install it before proceeding.
5. Go to the **ADVANCED > Cloud Control** page on the product, and do the following:
    a. Set **Connect to Barracuda Application Security Control Center** to *Yes*.

b. Enter the username and password of the Barracuda Application Security Control Center Account Admin.
c. In the **Barracuda Application Security Control Center** field, enter the IP address or hostname of the Barracuda Application Security Control Center.
d. In the **Validation Token** field, paste the Barracuda Application Security Control Center validation token you copied in step **3** above.
e. Click **Save**. Note that your device can connect with only one Barracuda Application Security Control Center at a time.
f. In the Barracuda Application Security Control Center web interface, refresh your browser page. The connected device should now display in the left pane.
g. By default, statistics are presented for that product. Click on the product link to configure using the web interface for that device.

Accounts and Roles

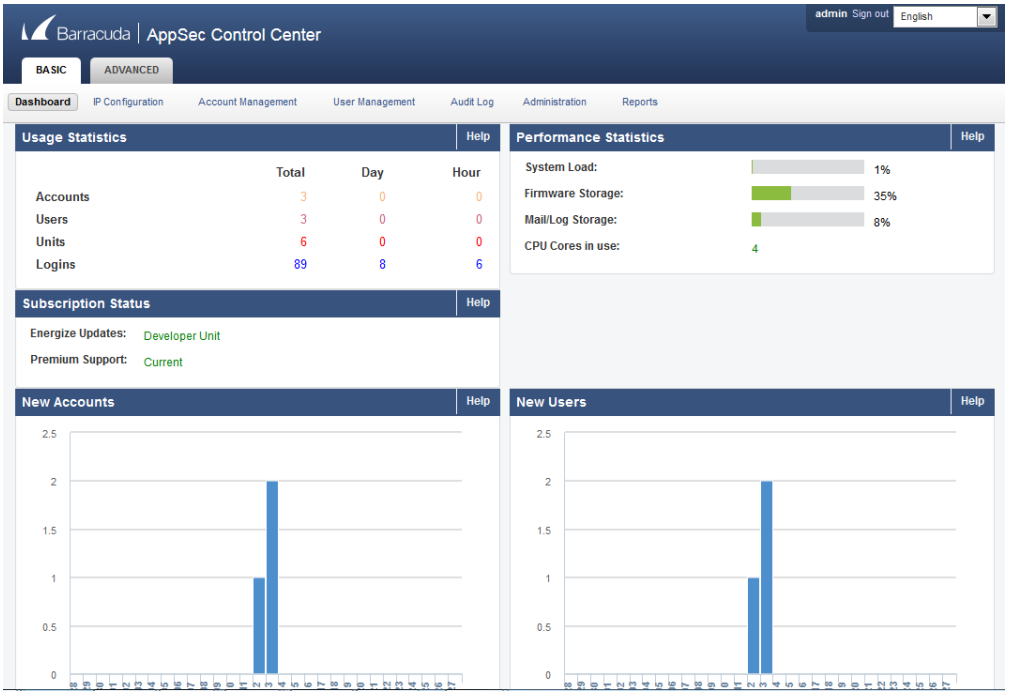
Administrator Accounts

There are two different administrator accounts, one to manage and configure the Barracuda Application Security Control Center including IP configuration and SNMP management, and one to create users and connect and manage connected Barracuda Web Application Firewall devices:

- **Barracuda Application Security Control Center Administrator Account** – Manage and configure the Barracuda Application Security Control Center.
- **Barracuda Application Security Control Center Account Admin** – Create users and manage and connect products through the Barracuda Application Security Control Center web interface.

Barracuda Application Security Control Center Administrator Account

The Barracuda Application Security Control Center Administrator Account is a super admin account that gives the privilege to configure and manage the Barracuda Application Security Control Center. Log in to the device using the Barracuda Application Security Control Center Administrator Account (**admin**/**admin**). Once logged in, you can view and manage connected devices, update security definitions, manage the images displayed in the web interface, troubleshoot the device, view tasks and task errors, and create the Barracuda Application Security Control Center Account Admin(s).



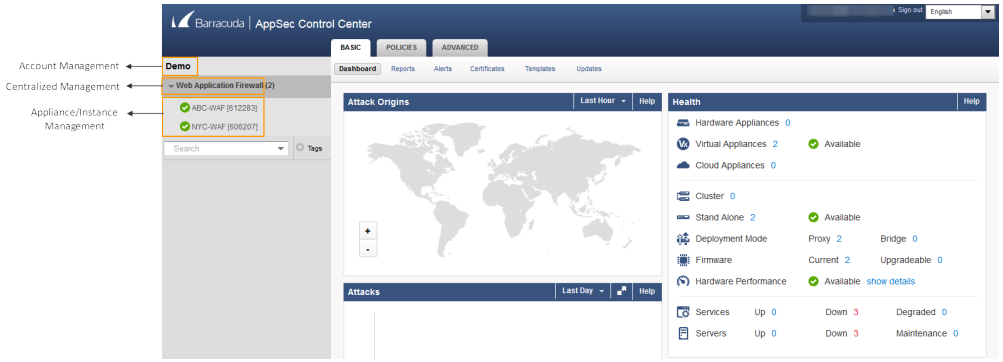
It is recommended to change the administrator account password (**admin**/**admin**) to a secured password by using the **Password Change** section on the **BASIC > My Account** page.

To know more about Barracuda Application Security Control Center Administrator, refer to the Barracuda Application Security Control Center as an Administrator.

Barracuda Application Security Control Center Account Admin

Through the Barracuda Application Security Control Center web interface, you create users and assign various permissions to each user to access the Barracuda Application Security Control Center, connect devices, manage device certificates, create templates based on object types, view connected device status, create/modify security policies and synchronize it with the connected devices.

When you log into the Barracuda Application Security Control Center as an account admin, the web interface provides Account Management, Centralized Management and the Appliance/Instance Management.



- Account Management allows you to:
  - Manage connected devices
  - Manage your Barracuda Application Security Control Center Account Admin settings
  - Configure LDAP and add users and user groups
  - View all activities related to the Barracuda Application Security Control Center
  - Generate Barracuda Application Security Control Center-related reports
  - View Barracuda Application Security Control Center running tasks and task errors
- Centralized Management allows you to:
  - Access security and traffic reports across connected appliances
  - Manage connected appliance certificates
  - Create and manage templates based on connected appliances
  - Check for firmware and virus definition updates
  - Create, associate, edit and synchronize security policies
  - Set association mode for security policies to automatic or manual
- Appliance/Instance Management allows you configure specific appliances.

To view the tabs and pages displayed in each context, click on each context name in the left pane.

To know more about Barracuda Application Security Control Center Account Admin, refer to the Barracuda Application Security Control Center as an Account Admin.

Barracuda Application Security Control Center as an Administrator

Use the Barracuda Application Security Control Center Administrator Account to set up and manage the Barracuda Application Security Control Center, and to create the Barracuda Application Security Control Center Admin Account. When you log in using this account, the **BASIC > Dashboard** displays the current operating status of the Barracuda Application Security Control Center. You cannot access connected devices when logged in using this account.

From the **BASIC** tab:

- **IP Configuration** – Configure administrative settings on the Barracuda Application Security Control Center. For more information, refer to ***Step 3 - How to Configure the Web Interface***.
- **Account Management** – View and activate/deactivate users on the account, and set up the Barracuda Application Security Control Center Admin Account.
- **User Management** – View users on the selected account associated with the Barracuda Application Security Control Center.
- **Audit Log** – Monitor all changes to the Barracuda Application Security Control Center initiated by a system administrator.
- **Administration** – Configure additional administrative settings on the Barracuda Application Security Control Center.
- **Reports** – Generate individual reports on a one-time basis.

From the **ADVANCED** tab:

- **Backup** – Save automated backups of various configuration settings for your Barracuda Application Security Control Center to one of three types of servers. Configurations can be entered for all Destination server types, but only the one selected at the time of the backup is used for scheduled backups.
- **Energize Updates** – View information for each type of update.
- **Firmware Update** – View the current version of the firmware installed on the Barracuda Application Security Control Center, and update with newer firmware versions as appropriate.
- **Appearance** – Enter a name to identify this Barracuda Application Security Control Center, and customize the image that appears in the web interface.
- **Troubleshooting** – Establish a connection to Barracuda Support and access tools to help diagnose potential network problems.
- **Advanced Networking** – Add Network Time Protocol (NTP) servers.
- **Task Manager** – View running tasks and any task errors encountered during a process.

To create the Barracuda Application Security Control Center Account Admin, log in to the web interface using the Barracuda Application Security Control Center Administrator Account, and complete the following steps:

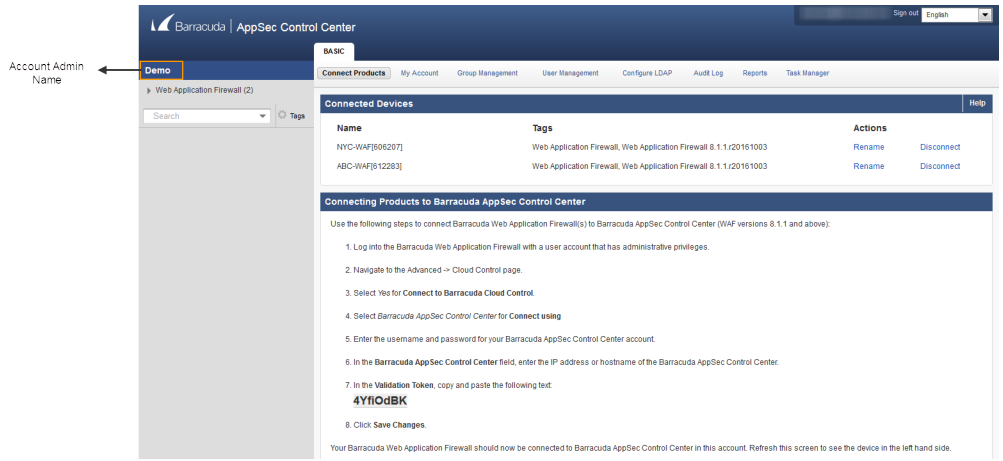
1. Go to the **BASIC > Account Management** page, and in the **Account Creation** section, enter the **Account Name**, **Administrator Email Address**, and select the **Preferred Time Zone** for the Barracuda Application Security Control Center Account Admin.
2. Click **Create Account**. The account displays in the **Account View** section.
3. A confirmation email containing the login credentials is sent to the email address entered in step 1 above. Use these credentials to log into the web interface to create users and assign permissions, connect Barracuda Web Application Firewall devices, and view device status.

Barracuda Application Security Control Center as an Account Admin

When you log in to the Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin, the Centralized Management and the **BASIC > Dashboard** page of the Barracuda Application Security Control Center web interface displays. In this, you view a summary of all devices connected to your Barracuda Application Security Control Center. All the Barracuda Web Application Firewall devices that are connected are listed in the left pane. The central portion of the page displays aggregated performance and traffic statistics for all connected devices. To switch to the proxy, or device mode, click on a device name in the left pane.

For all connected devices, the **BASIC > Dashboard** page displays detected attack types across all connected Barracuda Web Application Firewall devices, current operating state of the connected devices, subscription status, and total traffic passed through the WAN interface of the connected devices.

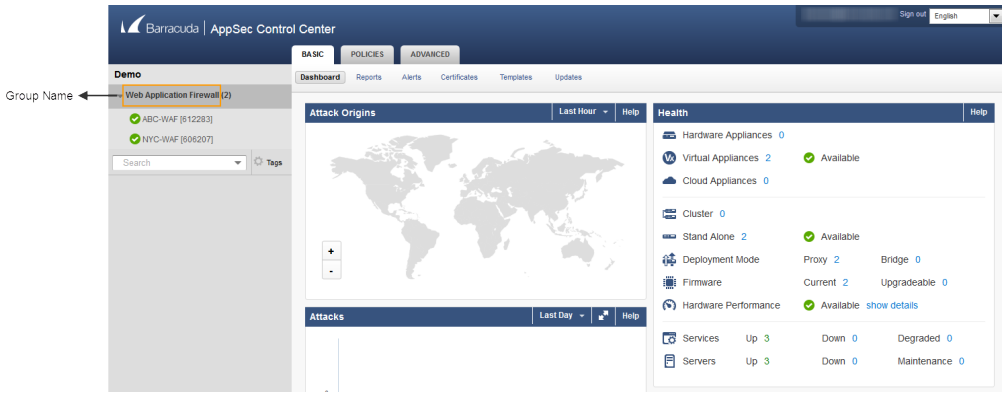
When you log in to the Barracuda Application Security Control Center as an account admin, the web interface provides account admin view, centralized management view and the device view. To view the tabs and pages displayed for account admin, click on the account admin name in the left pane. You can perform the following configuration in the account admin view:



From the **BASIC** tab:

- **Connect Products** page – Connect/disconnect Barracuda Web Application Firewall devices to/from the Barracuda Application Security Control Center.
- **My Account** page – Reset your password (unless your system is set up to use LDAP), update the Time Zone where the Barracuda Application Security Control Center resides, and make any necessary changes to your account information.
- **Group Management** page – Create and manage local and LDAP user groups.
- **User Management** page – Create and manage users including user role permissions.
- **Configure LDAP** page – Set up your Active Directory server to allow the Barracuda Application Security Control Center to authenticate individual users and to verify user group membership.
- **Audit Log** page – Monitor all changes to connected devices initiated by a system administrator.
- **Reports** page – Generate individual reports on a one-time basis for connected devices.
- **Task Manager** page – Monitor system tasks and task errors. View tasks in progress and any errors encountered when tasks are performed.

To view the tabs and pages displayed for a device group, click on the group name (example: Web Application Firewall).



From the **BASIC** tab:

- **Dashboard** page - View detected attack types across all connected Barracuda Web Application Firewall devices, current operating state

of the connected devices, subscription status, and total traffic passed through the WAN interface of the connected devices.
- **Reports** page – Access security and traffic reports across all connected devices.
- **Alerts** page - View system events generated by all connected devices.
- **Certificates** page – Manage certificates, including expired certificates, across all connected appliances.
- **Templates** page – Create new templates based on a connected appliance.

A template is a collection of configuration fragments arranged serially in a file. Use templates to create and import certain object types including Services, URL profiles, URL Policies, so that its configurations can be exported to other Barracuda Web Application Firewall devices from the Barracuda Application Security Control Center centralized management service. For example: Copy configuration of one particular object (example, Service, URL Profile, Security Policy, etc.) from one connected Barracuda Web Application Firewall to another connected Barracuda Web Application Firewall.

- **Updates** page – View and manage Barracuda Application Security Control Center and connected device firmware versions and definition versions.

From the **POLICIES** tab:

- **Security Policies** – Create new policies in addition to the default policies provided in the **Policy Manager** section, and associate the Barracuda Application Security Control Center security policies with the connected devices security policies.

From the **ADVANCED** tab:

- **Settings** - Set the mode to associate the Barracuda Application Security Control Center security policies with the connected devices security policies.

Account Management

User Management

An user can perform the following configurations:

- Create a Tag
- Add a User
- Assign a Role to the User
- Add a Group
- Configure LDAP
- View Audit Logs

Creating a Tag

You can use “Tags” to group the appliances on the Barracuda Application Security Control Center. When a device is connected to the Barracuda Application Security Control Center, by default, the device is added to the “Web Application Firewall” tag and the appropriate firmware tag. Click “Tags” in the left pane to manage the tags or create a new tag. For more information on how to manage and create tags, refer the online help.

Adding a User

To create a new user, log into the Barracuda Application Security Control Center web interface as the Barracuda Application Security Control Center Account Admin, and then complete the following steps:

1. Click on the account admin name in the left pane.
2. Go to the **BASIC > User Management** page, and click **Add User**; the **Add User** page appears.
3. Enter the following details for the new user:
    a. **Email Address** – Enter the user's login email address.
    b. **Full Name** – Enter the user's first and last name.
    c. **Preferred Time Zone** – Select the default time zone used to display stats and report data for this user.
4. In the **User Permissions** section:
5. Assign permission to the user by selecting a role from the **User Role** drop-down list. The following options are available in the **User Role** list:
    a. **View Dashboard only** – User can view connected device statistics based on Access settings on the **BASIC > Dashboard** page .
    b. **View Reports**, **Logs**, and **Dashboard only** – User can view connected device statistics on the **BASIC > Dashboard** page, and track events such as login, connecting, or disconnecting specific devices by user, account, name, and date/time on the **BASIC > Audit Log** page. You may wish to assign this role to a support person or office manager to provide performance and traffic reports for each product type.
    c. **All Actions** – Use this role to create a Barracuda Application Security Control Center administrator account; user can create users and assign permissions, connect/disconnect devices, view device Dashboard, and view tasks and task errors based on **Ac cess** settings.
    d. **Account Admin** – Use this role to create a Barracuda Application Security Control Center account admin; user can configure and manage the Barracuda Application Security Control Center, update security definitions, and view tasks and task errors. **Not e**: See ***Permissions by Role*** for additional details on user roles.
6. After selecting the user role, all Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center gets displayed under the account admin name. Select the units to which the user needs to be granted permission. When a unit is selected, the user gains access to that unit, and granted permission selected in **User Role**. If the check box next to the account admin name is selected, the user gains access to all the Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center. Note that the **Account Admin** role always has access to all connected devices.
7. If you have defined user groups, you can select group membership for this user. Use the **BASIC > Group Management** page to set group permissions and specify unit access for each group. By using **Groups**, you can easily set the same permissions for multiple users without having to manage each user individually.
8. Configured LDAP user groups displays in the **LDAP Permissions** section.
9. Click **Add User** to add the new user. An email is sent to the user’s email address with their login username and password. Once added, the user account displays in the **Users** table on the **BASIC> User Management** page.

Once logged into the Barracuda Application Security Control Center, users can manage their own account information using the **BASIC > My Account** page.

Administrator Actions

Once you create a user, the user account details display in the **Users** table on the **BASIC > User Management** page. From this table, the **Accou nt Admin** can perform the following actions:

- **Reset Password** – Resets the user’s password; a new password is automatically generated and sent to the user’s email address.
- **Edit User** – Modify the user’s time zone, role, and device access.

- **Deactivate/Activate** – Suspend or restart a Barracuda Application Security Control Center user account. Deactivated users can no longer log into the Barracuda Application Security Control Center.

If you attempt to deactivate the last **Account Admin** on the account, a warning displays noting that by deactivating the only Account Admin you will deactivate the account for all users. If necessary, the Barracuda Application Security Control Center Account Administrator can recover the account.

Assigning a Role to the User

When you add new users, you assign a user role, which specifies their level of permissions. The following table lists permissions by role:

Role	Permissions
View Dashboard Only	Users with this role can: • View status including asset reports in the **BASIC > Dashboard** page. • View existing reports in the **BASIC > Reports** page. The user cannot generate custom reports.
View Reports, Logs and Dashboard Only	Users with this role can: • View status including asset reports in the **BASIC > Dashboard** page. • View and generate reports in the **BASIC > Reports** page. • View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode. • Generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode. • View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors.
All Actions	Users with this role can: • View status including asset reports in the **BASIC > Dashboard** page. • View and generate reports in the **BASIC > Reports** page. • View all certificates in the **BASIC > Certificates** page. • Create, import, use, download, edit, and delete templates in the **BASIC > Templates** page. • View and check updates in the **BASIC > Updates** page. • Connect/disconnect devices, and resolve identifier conflicts in the **BASIC > Connect Products** page. • Modify their password, update the time zone, and change the account information in the **BASIC > My Account** page. • Configure Active Directory server details, test LDAP settings, and add user groups in the **BASIC > Configure LDAP** page. • View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode. • Generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode. • View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors.

Account Admin	Users with this role can: • View status including asset reports in the **BASIC > Dashboard** page. • View and generate reports in the **BASIC > Reports** page. This page is unavailable if the system is in proxy mode. • View all certificates in the **BASIC > Certificates** page. • Create, import, use, download, edit, and delete templates in the **BASIC > Templates** page. • View and check updates in the **BASIC > Updates** page. • Connect/disconnect devices, and resolve identifier conflicts in the **BASIC > Connect Products** page. • Modify their password, update the time zone, and change the account information in the **BASIC > My Account** page. • Add, edit, and delete users groups, and import LDAP users from a selected group for synchronization in the **BASIC > Group Management** page. • Add, edit, and deactivate users on the account, reset user passwords, and import LDAP users from a selected group for synchronization in the **BASIC > User Management** page. • Configure Active Directory server details, test LDAP settings, and add user groups in the **BASIC > Configure LDAP** page. • View audit logs in the **BASIC > Audit Log** page. This page is unavailable if the system is in proxy mode. • View tasks and errors in the **BASIC > Task Manager** page. The user can also clear errors.

Effective Permissions

A user can be assigned different permissions in different groups, along with a different permission assigned to the same user under **User Management**. In such cases, the Barracuda Application Security Control Center chooses the maximum permission role assigned to the user and grants access to the selected devices i.e., the lower level user role will be overridden by the higher-level user role. For example, consider a user is assigned:

- “View Dashboard Only” in ***Group1*** for the devices WAF1 and WAF2,
- “Account Admin” in ***Group2*** for the devices WAF2 and WAF3
- “View Reports, Logs and Dashboard Only” permission for the user in the **BASIC > User Management** page. The devices selected for the user are WAF1 and WAF3.

Here:

- In WAF1, the user is assigned with “View Reports, Logs and Dashboard Only” role and “View Dashboard Only” role in ***Group1***. The maximum permission assigned to the user is “View Reports, Logs and Dashboard Only”, so the user gains access to WAF1 with View Reports, Logs and Dashboard Only permission.
- In WAF2, the user is assigned with “View Dashboard Only” and “Account Admin” roles in ***Group1*** and ***Group2*** respectively. In this case, the “Account Admin” role is granted the maximum permission than the other role (“View Dashboard Only”), so the user gains access to WAF2 with “Account Admin” permissions.
- In WAF3, the user is assigned with “View Reports, Logs and Dashboard Only” role and “Account Admin” role in ***Group2***. The Account Admin role is granted with the maximum permission than the other role (“View Reports, Logs and Dashboard Only”), so the user gains access to WAF2 with “Account Admin” permissions.

Adding a Group

Use the **BASIC > Group Management** page to set group permissions and specify unit access for each group. By using **Groups**, you can easily set the same permissions for multiple users without having to manage each user individually. When you log in to the Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin, the **Groups** table on the **BASIC > Group Management** page displays details for all local and LDAP user groups for the account. Note that LDAP must be enabled on the **BASIC > Configure LDAP** page before you can create an LDAP user group.

To add a group, log into the Barracuda Application Security Control Center web interface as the Barracuda Application Security Control Center Account Admin, and then complete the following steps:

1. Click on the account admin name in the left pane.
2. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
3. In the **Add Group** section, do the following:
    a. Enter a name to identify the group in the **Group Name** field.
    b. From the **Role** drop-down list, select a permission for the group.
        i. **View Dashboard only** – Users can view connected device statistics based on Access settings on the **BASIC >**

Dashboard page

ii. **View Reports**, **Logs**, and **Dashboard only** – Users can view connected device statistics on the **BASIC > Dashboard** page, and track events such as login, connecting, or disconnecting specific devices by user, account, name, and date/time on the **BASIC > Audit Log** page. You may wish to assign this role to a support person or office manager to provide performance and traffic reports for each product type.

iii. **All Actions** – Use this role to create a Group with Barracuda Application Security Control Center administrator account permissions; users in this group can create users and assign permissions, connect devices, view device Dashboard, and view tasks and task errors based on **Access** settings.

iv. **Account Admin** – Use this role to create a Group with Barracuda Application Security Control Center account admin permissions; users in this group can configure and manage the Barracuda Application Security Control Center, update security definitions, view tasks and task errors. See **Permissions by Role** for additional details on selecting group roles.

4. The **Access** list displays all Barracuda Web Application Firewall devices currently connected to the Barracuda Application Security Control Center by group. Select the units to which the group user(s) needs to be granted permission. When a unit is selected, the user gains access to that unit, and granted permission selected in **Role**. If the check box next to the account admin name is selected, the user(s) gains access to all the Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center. Note that the **Account Admin** role always has access to all connected devices.
5. All users on the account display in the **Members** section. Select the members you wish to add to the group, and then click **Add Group**.

Once logged into the Barracuda Application Security Control Center, users can manage their own account information using the **BASIC > My Account** page.

Administrator Actions

Once you create a group, the group details display in the **Groups** table on the **BASIC > Group Management** page. From this table, the **Account Admin** can perform the following actions:

- **Edit Group** – Modify the group role, device access, and members.
- **Delete Group** – Delete the group from the Barracuda Control Server.

Configuring Lightweight Directory Access Protocol (LDAP)

- Understanding LDAP Authentication
- Configure the Active Directory Server
- Creating a LDAP Group
- Adding a Local User Group

Understanding LDAP Authentication

The Barracuda Application Security Control Center xxx supports Active Directory (AD) for role based access control. For additional information, log into the web interface as the Barracuda Application Security Control Center Account Admin, and click Help on the **BASIC > Configure LDAP** page.

Use LDAP authentication to store and administer Barracuda Application Security Control Center user accounts and verify user group membership via your organization's LDAP servers; you must have a verified domain to use LDAP. All users for the verified domain are required to use their LDAP credentials to access the Barracuda Application Security Control Center.

Once LDAP authentication is set up and enabled, users added to Barracuda Application Security Control Center by the Barracuda Application Security Control Center Account Admin are automatically set up to use LDAP authentication, replacing the current user Barracuda Application Security Control Center login credentials with their LDAP credentials. New users log in to the Barracuda Application Security Control Center using their LDAP credentials and follow the onscreen instructions to join the appropriate account.

You can add multiple email domains to a single LDAP profile. In scenarios where multiple companies are merged and each retain their email domain; the Barracuda Application Security Control Center can work with multiple email domains.

Configure the Active Directory Server

To configure the Barracuda Application Security Control Center to use your AD server for authentication:

1. Log into Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin.
2. Click on the account admin name in the left pane.
3. Go to the **BASIC > Configure LDAP** page and do the following configuration in the **LDAP Configuration** section:
    a. Set **Enable LDAP** to *Yes*.
    b. In the **Server Alias** field, enter a short name or alias to identify the server.
    c. In the **Server Name/IP** field, enter the IP address or hostname of your Active Directory (AD) server.
    d. In the **LDAP Port** field, enter the port used by your Active Directory (AD) server; the default port number is 389. Ensure that you enter appropriate port number. Example: 636 for SSL port.
    e. In the **Bind DN (Username)** field, enter the distinguished name (DN) of a user in your LDAP directory that has read access to all users in LDAP.

f. In the **Bind Password** field, enter the password associated with the username specified in the **Bind DN** field.
g. In the **LDAP Search Base** field, enter the base distinguished name (DN) for the directory. For example, if your domain is test.com, your base DN might be *dc=test,dc=com*.
h. In the **Username Attribute** field, enter he attribute that contains the user's ID. This is mapped to the mail attribute for use with AD LDAP environments.
i. From the **LDAP Encryption** drop-down menu, select the type of encryption used by your Active Directory (AD) server.
j. Click **Test LDAP** to test your LDAP configuration settings.

4. Click **Save** to save your LDAP settings.

Creating a LDAP Group

To create a LDAP group, perform the following steps:

1. Log into Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin.
2. Click on the account admin name in the left pane.
3. Go to the **BASIC > Configure LDAP** page, and verify **Enable LDAP** is set to *Yes*.
4. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
5. In the **Add Group** section, select **LDAP**.
6. Click **LDAP Browser**, and navigate to and select the new LDAP user group.
7. Click **Add Group**.
8. In the **Groups** table, click **Edit Group**.
9. In the **Role** field, specify the level of permissions:
    a. i. **ViewDashboardOnly** – The users in this group can only view existing reports.
    ii. **View Reports**, **Logs**, and **Dashboard Only** – The users in this group can create and view reports, and view logs and statistics.
    iii. **All Actions** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
    iv. **Account Admin** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
10. From the **Access** list, select the devices that the members of the group can access; you must select at least one device.
11. Click **Save**.

Adding a Local User Group

To add a local user group, perform the following steps:

1. Log into Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin.
2. Click on the account admin name in the left pane.
3. Go to the **BASIC > Group Management** page, and click **Add Group**. The **Add Group** window appears.
4. In the **Add Group** section, select **Local**. The **Local User Group** section appears.
5. In the **Local User Group** section, specify values for the following:
    a. **Group Name** - Enter a name for the local user group.
    b. **Role** - specify the level of permissions:
        i. **ViewDashboardOnly** – The users in this group can only view existing reports.
        ii. **View Reports**, **Logs**, and **Dashboard Only** – The users in this group can create and view reports, and view logs and statistics.
        iii. **All Actions** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
        iv. **Account Admin** – The members of this group have unrestricted access to all other users as well as all systems connected to this account.
    c. **Access** - select the devices that the members of the group can access; you must select at least one device.
    d. **Members** – Select the group members you want to add to the group.
6. Click **Add Group**.

View Audit Logs

Audit logs are generated whenever users log in or log out of the web interface of the Barracuda Application Security Control Center, except in a few rare cases. They are:

The **Login** action is not logged, when:

- Maintenance command is executed by a user or by the Barracuda Application Security Control Center, a new login session will be created in maintenance mode, but it won't be logged.

The **Logout** action is not logged, when:

- The Barracuda Application Security Control Center is restarted because critical processes have crashed, in which case the current existing sessions won't be logged out.
- The Maintenance command is executed by a user or by the Barracuda Application Security Control Center, in which case the current

existing sessions won't be logged out.

Managing Connected Devices

You must have the following login rights to connect and disconnect the Barracuda Web Application Firewall devices to the Barracuda Application Security Control Center:

- Barracuda Application Security Control Center Account Admin login credentials; and
- Admin login credentials for each Barracuda Web Application Firewall you want to connect to, or disconnect from, the Barracuda Application Security Control Center.

Connect a Device

To connect the Barracuda Web Application Firewall to the Barracuda Application Security Control Center, refer to the steps mentioned in **Step 6 - How to Connect Devices to the Barracuda Application Security Control Center**.

Disconnect a Device

To disconnect the Barracuda Web Application Firewall from the Barracuda Application Security Control Center:

1. Log into the Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin, and go to the **BASIC> Connect Products** page.
2. In the **Connected Devices** section:
3. Identify the device you want to disconnect.
4. Click **Disconnect** next to the device under **Actions**. The **Remove Device** pop-up window appears.
5. Click **Remove** to confirm.
6. The device no longer displays in the table or in the left pane.

Task Manager

Use the **BASIC > Task Manager** page to monitor system tasks. This page provides a list of tasks that are in the process of being performed, and displays any errors encountered when performing these tasks.

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy. The **Task Errors** section lists an error until you manually remove it from the list; errors are not automatically phased out over time.

Centralized Management

Devices Statistics

The **BASIC > Dashboard** page provides an overview of the performance and health of all the Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center. In this view, the traffic and performance statistics available in the **BASIC > Dashboard** page of your Barracuda Web Application Firewall will be displayed. If multiple Barracuda Web Application Firewall devices are connected, the aggregated statistics of all the connected devices is displayed.

Security and Traffic Reports

The **BASIC > Reports** page provides an aggregated report of all the Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center. You can view the security reports, service traffic, server traffic, client traffic, and aggregated system traffic reports on this page. For detailed information on reporting, refer to the Reporting article.

Alerts

The **BASIC > Alerts** page displays the alerts generated by the Barracuda Web Application Firewall devices connected to the Barracuda Application Security Control Center. You can customize the display of alerts and configure the threshold for email alerts by using **Preferences**. To receive email notifications from the Barracuda Application Security Control Center,

Managing Certificates

The **BASIC > Certificates** page allows the users to manage certificates, including expired certificates, across all connected devices. For more information on certificates, refer to the Certificate Management article.

Shared Configuration

Overview

The Barracuda Application Security Control Center enables you to configure settings and share it with the connected devices. To share the configuration, you must first associate the object on the Barracuda Application Security Control Center with the object on the Barracuda Web Application Firewall device.

Understanding How the Shared Configuration Works

In this section, we use the object “Security Policy” as an example to explain how the configuration is shared between the Barracuda Application Security Control Center and the connected devices.

Initial Connect to the Barracuda Application Security Control Center

The Barracuda Application Security Control Center includes a predefined set of security policies. When the Barracuda Web Application Firewall is connected to the Barracuda Application Security Control Center, the configuration settings of the security policies on the connected device will automatically be overridden with the Barracuda Application Security Control Center configuration. This configuration synchronization happens because the **Association Mode** for the connecting devices is set to **Automatic** by default on the **ADVANCED > Settings** page. If you intend to manually associate the Barracuda Application Security Control Center security policies with the connected device, set the **Association Mode** to **Manual** before connecting the device.

For information on how to connect a device to the Barracuda Application Security Control Center, see **Connect a Device** section in the **Connecting and Disconnecting Devices** article.

Association Mode

The **Association Mode** determines whether to synchronize the configuration settings automatically or manually with the connected devices at the time the device is first connected to the Barracuda Application Security Control Center.

- **Automatic** – The security policies on the Barracuda Application Security Control Center will automatically be associated with the security policies of the connected device, and the Barracuda Application Security Control Center overrides the configuration of the security policies on the device with its configuration
- **Manual** – You should select the security policies and the devices to which the configuration needs to be synchronized.

Association Mode setting is used ONLY when the device is first connected to the Barracuda Application Security Control Center.

Creating a New Security Policy

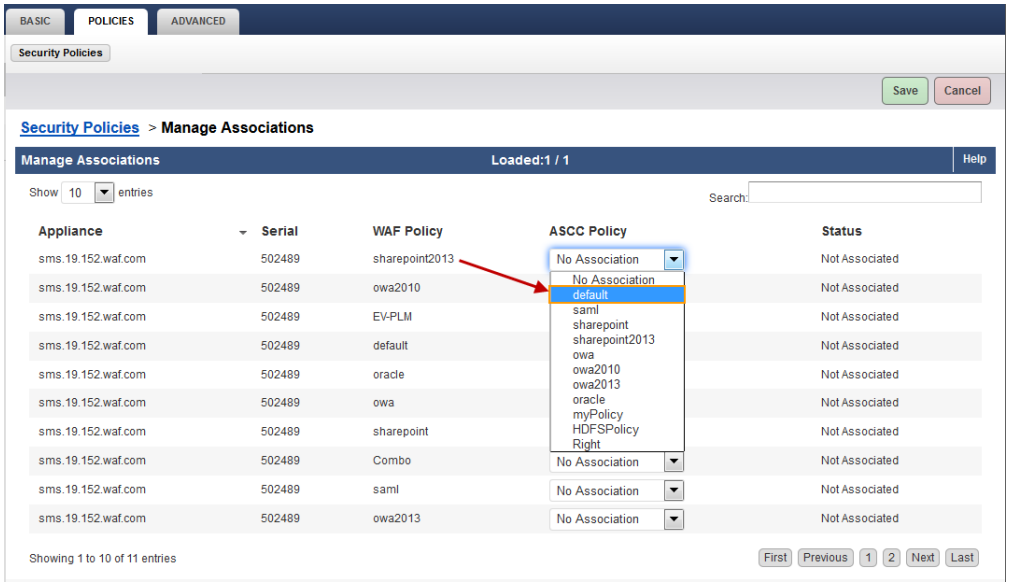
The Barracuda Application Security Control Center provides a predefined set of policies that can be modified and applied to the connected devices. Additionally, you can create a new security policy and synchronize it with all connected devices, or associate the policy with the specific device(s) and synchronize the configuration. Perform the following steps to create and associate a new security policy:

1. Log into the Barracuda Application Security Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Create New Policy** section, do the following:
    a. **Policy Name**: Enter a name for the policy.
    b. **Based On**: Select an existing security policy based on which you want to create a new security policy, or select **Create New** to create a new security policy with custom settings.
    c. **Sync to All**: Specify whether or not to push the policy to the connected devices.
        i. **Yes** – The policy gets created and associates with all connected devices.
        ii. **No** – The policy gets created and will be listed in the **Policy Manager** section. In this case, you should manually associate the policy with the device(s) to synchronize the configuration.
    d. Click **Add**.

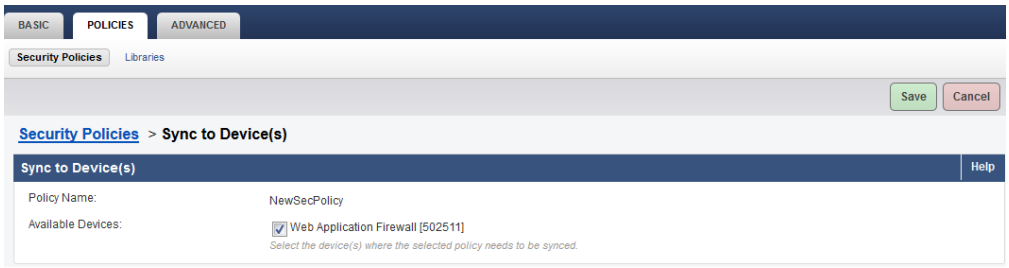
Synchronizing a Custom Policy with the Connected Devices

Perform the following steps to synchronize a custom policy with the connected devices:

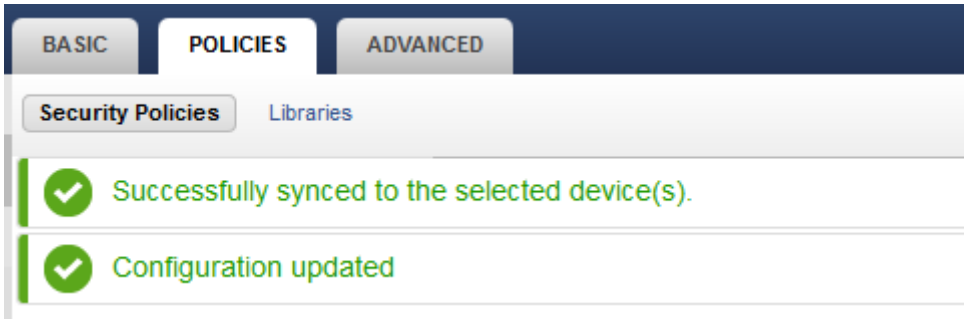
1. Log into the Barracuda Application Security Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Policy Manager** section, identify the policy that needs to be synchronized with the device.
4. Select **Sync to Device(s)** from the **Actions** drop-down list next to the policy. The **Sync to Device(s)** page appears.



5. In the **Sync to Device(s)** section, select the device to which you want to associate the policy and click **Save**.



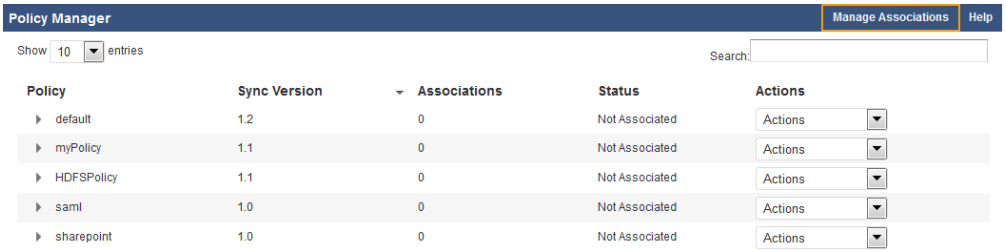
6. The policy gets synchronized with the selected devices.



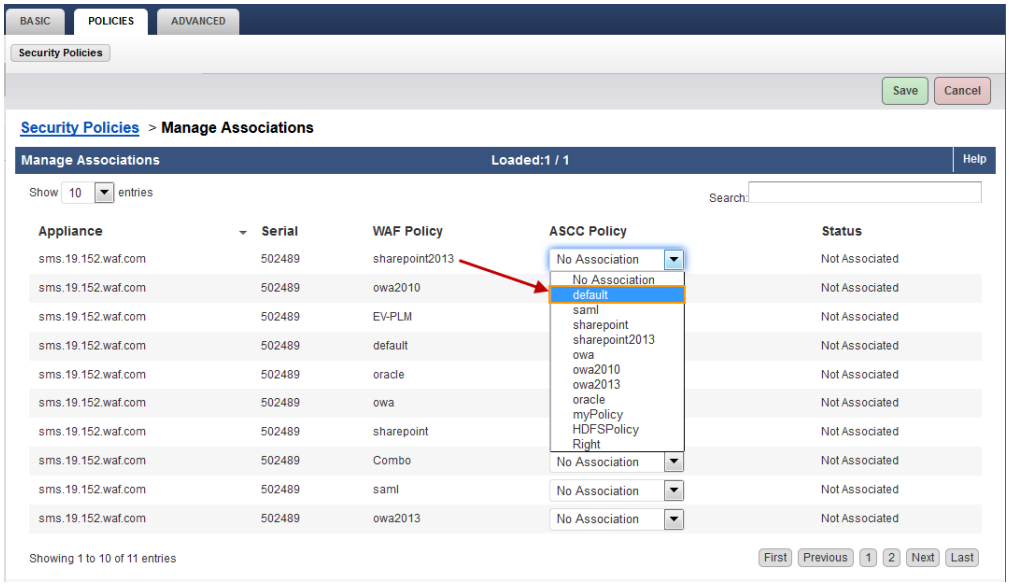
Steps to Manually Associate an Existing Policy on the Barracuda Web Application Firewall with the Policy on the Barracuda Application Security Control Center

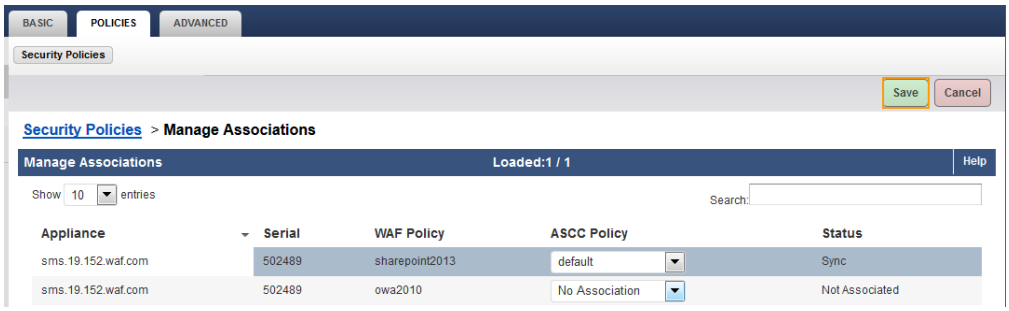
Perform the following steps to manually associate an existing security policy on the Barracuda Web Application Firewall with the Policy on the Barracuda Application Security Control Center:

1. Log into the Barracuda Application Security Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Policy Manager** section, click **Manage Associations**. The **Manage Associations** page appears.

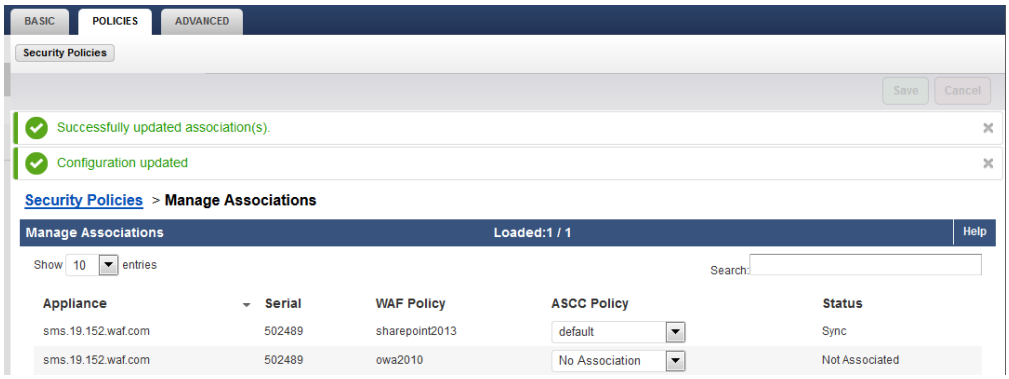


4. In the **Manage Associations** section, identify the WAF policy that needs to be associated with the policy on the Barracuda Application Security Control Center.
5. Select a policy from the **ASCC Policy** drop-down list next to the WAF policy, and click **Save**.





6. After successful association, the **Manage Associations** section displays the ASCC policy that you associated with the WAF policy.



Modifying an Existing Security Policy

When an existing security policy on the Barracuda Application Security Control Center is modified, the configuration is automatically synchronized with the associated security policy(s) on the connected device(s). If the security policy is not associated with the connected device(s), the policy will be saved in the **Policy Manager** section until it is manually synchronized with the connected device(s).

To modify an existing security policy on the Barracuda Application Security Control Center, perform the following steps:

1. Go to the **POLICIES > Security Policies** page on the Barracuda Application Control Center web interface.
2. In the **Policy Manager** section, identify the policy that you want to modify, and select **Edit** from the **Actions** drop-down list next to the policy. The selected policy page appears with all the sub-policies associated with it.
3. In the selected policy page, do the following:
    a. **Revision Control:** Mark the configuration changes as Major/Minor based on the number of changes/severity of changes. This will basically reflect on the sync version associated with the policy. For example, selecting **Minor** and modifying the request limit policy parameters would change the **Sync Version** from 1.0 to 1.1. If the same modification is done by setting the **Revision Control** to **Major**, the **Sync Version** changes from 1.0 to 2.0.
    b. **Request Limits:** The **Request Limits** policy defines the validation criterion for incoming requests by enforcing size limits on HTTP requests. The requests that exceed the defined length/limit are denied or allowed to pass through based on the **Mode** (**Passive** or **Active**) set for a Service. Modify the values if required and click **Save**. For more information, refer the Online Help.
    c. **Cookie Security**: The **Cookie Security** policy guarantees confidentiality of the cookie and avoids tampering of the cookie value. A shorter timeout interval can be configured for cookies to help minimize the chances of cookie stealing. This policy does not

prevent cookie replay attacks. Modify the values if required and click **Save**. For more information, refer the Online Help.

d. **URL Protection:** The **URL Protection** policy protects the service against web attacks. Modify the values if required and click **Save**. For more information, refer to the Online Help.
e. **Parameter Protection:** The **Parameter Protection** policy protects the service against attacks based on parameter values. Modify the values if required and click **Save**. For more information, refer to the Online Help.
f. **Cloaking:** The **Cloaking** policy prevents leakage of information about a Web site or service that is vulnerable for Web attacks. The HTTP headers and return codes are concealed before sending a response to a client. The response headers are filtered based on the headers defined in the **Headers to Filter** field. Modify the values if required and click **Save**. For more information, refer to the Online Help.
g. **URL Normalization:** This **URL Normalization** policy secures the websites from path traversal attacks, and specifies canonicalization policies for URLs found in the requests. Modify the values if required and click **Save**. For more information, refer to the Online Help.
h. **Protected Data Types:** The **Data Theft Protection** policy protects the sensitive information/data sent in responses from being exposed to unauthorized users. Modify the values if required and click **Save**. For more information, refer to the Online Help.
i. **Global ACLs:** The **Global ACL** policy defines the strict access control rules. You can add a new URL ACL or modify the existing URL ACL. Modify the values if required and click **Save**. For more information, refer to the Online Help.
j. **Action Policy:** The **Action Policy** is a collection of settings that determines the action to be enforced when a violation is detected. Modify the default attack action settings if required and click **Save**. For more information, refer to the Online Help.

Reconnecting to the Barracuda Application Security Control Center after Connection Failure

If the Barracuda Web Application Firewall disconnects from the Barracuda Application Security Control Center due to connection failure and reconnects to the Barracuda Application Security Control Center, the Barracuda Application Security Control Center validates the **Sync Version** with the connected device. If **the Sync Version** in the connected device is different, the Barracuda Application Security Control Center overrides the configuration on the connected device with its configuration. If the **Sync Version** is same, then the configuration is not synchronized with the connected device.

Disconnecting the Device Manually

When a device is disconnected manually, the Barracuda Application Security Control Center removes all the associations made with the device. If the same device is connected again with the Barracuda Application Security Control Center, it is treated as a new device and configuration synchronization happens based on the Association Mode (Automatic or Manual).

Templates

Understanding Templates

A template is a reusable configuration file. It represents parts of your Barracuda Web Application Firewall's existing configuration. You can create three types of templates:

- **Full** – A Full template represents a configuration object. You can create a new object with the desired settings using the Full template option. For example, a 'Service' template would include all (selected) URL Profiles, Parameter Profiles, Rule Groups, URL ACLs, etc., associated with the service. Typically, a full template includes all the relevant information pertaining to an object. You can edit the values of the parameters if required when creating this template. See Tables 1 and 2 below for more information.
- **Partial** – A Partial template represents parts of configuration of an object. With the Partial template, you can update the configuration of existing objects. Applying a partial template can be considered analogous to perform a "Bulk Edit" operation. For example, consider you want to update the Session Timeout value for multiple services. You can create a template with only Session Timeout value modified. When this template is applied on service(s), it only updates the Session Timeout value keeping other parameter values intact.
- **Composite** – A Composite template is a group of full templates of the same type of objects. It can be used when you want to migrate multiple objects of the same type from the QA environment to the production environment. For example, you want to copy URL profiles of an application to another application. You can create a template with selected URL profiles and apply it on the application for which these URL profiles needs to be configured. This will create URL profiles for the selected application on the WEBSITES > Website Profiles page.

Note that you cannot edit the values of parameters when creating a Composite template. If you wish to edit the values of certain parameters, download the template, open the XML file and edit the values before importing it.

Object Type and Dependency Objects

A template only contains a reference to "dependency objects". This means that when the template is downloaded and imported on another Barracuda Web Application Firewall, the dependencies are not imported. While using such a template, all dependencies appear as "key" parameters in the "Use Template" wizard and thus the appropriate dependencies can be referenced before applying the template. For example, when importing a template of a HTTPS service, the certificate is not imported. While applying the template, the certificate appears as a "key" parameter in the wizard and one of the existing certificates on the unit can be associated with the service.

Table 1 lists each object type and Objects on which the Object Type is dependent.

Object Type	Dependency Object
Service	• Rate Control Pool • Authentication Service • Trusted Hosts Group • Session Identifiers • Web Firewall Policy • Certificate • Geo Pool
Server	• Client Certificate
URL Profile	• Custom Blocked Attack Types
Parameter Profile	• Custom Parameter Class
Rule Group Server	• Client Certificate
URL Policy	• Rate Control Pool
Secure Browsing Policy	• Credential Server
URL ACL	• Response Page
Header ACL	• Custom Blocked Attack Types
Security Policy	• Custom Blocked Attack Types
Global ACL	• Response Page
Data Theft Protection	• Custom Identity Theft Type
Custom Parameter Class	• Custom Blocked Attack Types • Custom Input Type Validation

Table 2. List of Dependency Objects.

Dependency Object Name	Description
Rate Control Pool	A rate control pool can be created on the ADVANCED > Libraries page.
Authentication Service	An authentication service can be created on the ACCESS CONTROL > Authentication Services page.
Trusted Hosts Group	A trusted hosts group can be created on the WEBSITES > Trusted Hosts page.
Session Identifiers	A session identifier can be created on the ADVANCED > Libraries page.
Web Firewall Policy	A web firewall policy can be created on the SECURITY POLICIES > Policy Manager page.
Certificate	A certificate can be created on the BASIC > Certificates page.
Client Certificate	A client certificate can be associated on the ACCESS CONTROL > Client Certificates page.
Custom Blocked Attack Types	A custom blocked attack type can be created on the ADVANCED > Libraries page.
Custom Parameter Class	A custom parameter class can be created on the ADVANCED > Libraries page.
Credential Server	A credential server can be created on the WEBSITES > Secure Browsing page.
Response Page	A response page can be created on the ADVANCED > Libraries page.
Custom Identity Theft Type	A custom identity theft type can be created on the ADVANCED > Libraries page.
Custom Input Type Validation	A custom input type validation can be created on the ADVANCED > Libraries page.

Creating Templates

You can create service, security policy, and configuration templates and selectively apply (or reset) those templates to connected Barracuda Web Application Firewall devices in the Cloud Control Context view. This allows you to store your templates in a repository and synchronize data as needed. The BASIC > Templates page displays all defined templates in the Template Repository table.

Create a Template

Use the following steps to create a template.

1. Log into the Barracuda Application Security Control Center as the Barracuda Application Security Control Center Account Admin, and go to the **BASIC > Templates** page.
2. From the **Create From Appliance** drop-down menu, select the appliance, and then click Create Template; the Create Template wizard displays.
3. click on the Barracuda Web Application Firewall in the left pane that you want to use to create the source object for your template. The view changes to the Proxy (Product) context display the Barracuda Web Application Firewall web interface for the selected device.
4. Define your source object for the template. Go to the **ADVANCED > Templates** page. Note: You can also define services and policies within the web interface, for example BASIC > Services, and then click Import Template to add a new template of that particular object type.
5. Click **Create Template** to define a new template. The template created is a self-contained object. For example, a 'Service' template would include all (selected) URL Profiles created for that service, Parameter Profiles, Rule Groups, URL ACLs etc. In short, a template would include all the relevant information pertaining to that object and not just the primary values. For information on object type and dependency objects, see Object Type and Dependency Objects and List of Dependency Objects.
6. In the **Create Template** window, enter a unique Name to represent the template. The name can include alphanumeric characters and underscores (_). Any other special characters such as space, semicolon, asterisk, periods (.), hyphens (-), etc. are not allowed.
7. Select the **Template Format**:
    a. **Full** - Creates a template for an object, which includes all configuration under that object. For example, a 'Service' template would include all (selected) URL Profiles created for that service, Parameter Profiles, Rule Groups, URL ACLs etc. In short, a template would include all the relevant information pertaining to that object and not just the primary values. You can edit the

values of the parameters if required when creating this template.

b. **Composite** - Creates a template for a particular object type. Composite template is useful when you want multiple instances of the same object type in a single template. For example, consider "Server" as your "Template Type". This will list all servers configured under each service. Select the servers which you want to include in the template and click Create. Note that you cannot edit the values of configuration parameters when creating a Composite template. If you wish to edit the values of certain parameters, download the template, open the XML file and edit the values before importing it. For more information on how to edit a composite template, see Edit Template.

c. **Template Type** - Select an object type for which you want to create a template. For example, Service, Server, URL Profile, Parameter Profile.

d. **Based On** - Select the object for which you want to create a template. For example, service1.

8. Click **Create**. The new template is added to the list of **Available Templates**.
9. Click on your user name in the left pane to switch back to the **Cloud Control Context**:
10. In the Barracuda Application Security Control Center web interface, go to **BASIC > Templates**.
11. From the **Import** drop-down menu, select the device where you created the source object; all source objects available on the selected device display:
12. Select the source object you want to import, and then click **Import**. The table populates with your selections.
13. In the **Actions** column for the new service, click **Use**; the available destinations display in a new window. The **Use** operation allows you to apply a template to selected destinations. For example, if you are applying a URL Profile template, the destination option can be a 'Service', because a URL Profile logically exists within a Service. If you are using a "Full" template, the Use template wizard displays different key parameters for each object. For a Composite template, the Use template wizard displays only the Destination field.

Expand the available options to select those devices to which to push the template:

Update the Firmware and Definitions (Attack, Virus, Security and GeoIP)

The **BASIC > Updates** page displays the current version of the firmware installed on each connected appliance, including device name and current firmware version, as well as current virus, attack, security, and GeoIP definitions. If an update is available, a warning icon displays.

Click **Check for Updates** to determine whether updates are available for any of the connected devices. Updates display in the **Update Repository** table.

If you are managing your appliances through a Barracuda Application Security Control Center without direct internet connectivity, you can check for and apply updates to connected devices as well as the Barracuda Application Security Control Center using the following steps:

1. Click **Check for Updates** to populate the table with any additional updates.
2. Click **Download Manifest File** to download firmware and definitions to your local system as a .zip file.
3. Click **Import File** to upload the manifest to your Barracuda Cloud Control account, and update connected systems.

Appliance/Instance Management

The Appliance/Instance Management is the Proxy/Device view in the Barracuda Application Security Control Center. In the proxy view, you can view the configuration of the selected device, and modify the settings (if required). The configuration changes made will be applied immediately, and the requests and responses are treated based on the configured settings. For more information on configuring the Barracuda Web Application Firewall, refer to the Barracuda Web Application Firewall documentation.

Limited Warranty and License

Limited Warranty

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., (“Barracuda Networks”) warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization (“RMA”) procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as “sample” or “beta,” (b) loaned or provided to you at no cost, (c) sold “as is,” (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS PRODUCTS AND THE SOFTWARE IS PROVIDED “AS IS” AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR-FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively “Barracuda Software”) is licensed, not sold, to you by Barracuda Networks, Inc. (“Barracuda”) for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.

2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT

INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.

3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.

4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED “AS IS” WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTIBILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate “click-on” license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively “Barracuda Networks”), grants to the end-user (“Customer”) a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the “Energize Update Software”). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

1. a.
   i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;
   ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
   iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, “Energize Update Software” shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, “Upgrades”) or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customers expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph “(c)” of the “Commercial Computer Software - Restricted Rights” clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the “Technical Data-Commercial Items” clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the Energize Update Software or any equipment, system or network on which

the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other “open source” license agreements. The GNU license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

GNU GENERAL PUBLIC LICENSE, (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means

either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for

copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the

Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License:

"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000

Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu .Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda products may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License.

You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Source Code Availability

Per the GPL and other “open source” license agreements the complete machine readable source code for programs covered by the GPL or other “open source” license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of $100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We mail the packaged source code for any program covered under the GPL or other "open source" license.