

WatchGuard® Firebox Vclass High Availability Guide

High Availability for Vcontroller 4.0 and CPM 4.1



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.

AppLock®, AppLock®/Web, Designing peace of mind®, Firebox®, Firebox® 1000, Firebox® 2500, Firebox® 4500, Firebox® II, Firebox® II Plus, Firebox® II FastVPN, Firebox® III, Firebox® SOHO, Firebox® SOHO 6, Firebox® SOHO 6tc, Firebox® SOHO|tc, Firebox® V100, Firebox® V80, Firebox® V60, Firebox® V10, LiveSecurity®, LockSolid®, RapidStream®, RapidCore®, ServerLock®, WatchGuard®, WatchGuard® Technologies, Inc., DVCP™ technology,, Enforcer/MUVPN™, FireChip™, HackAdmin™, HostWatch™, Make Security Your Strength™, RapidCare™, SchoolMate™, ServiceWatch™, Smart Security. Simply Done.™, Vcontroller™, VPNforce™ are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2000 The OpenSSL Project. 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.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``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 OpenSSL PROJECT 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.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim

Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. 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 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.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS 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 AUTHOR OR 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.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. 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.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."
4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``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 RALF S. ENGELSCHALL OR HIS 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.

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. 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.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).¹ Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

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 APACHE SOFTWARE FOUNDATION 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.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Part No: 1035-000

Contents

CHAPTER 1 Firebox Vclass High Availability	1
How High Availability Works	2
High Availability Modes	2
Prerequisites for a High Availability System	3
Connecting the appliances	4
Installing High Availability	4
Configuring High Availability Active/Active in Vcontroller ...	7
Managing High Availability	13
Setting and Responding to Alarms	14
CHAPTER 2 Firebox Vclass High Availability with CPM	17
Configuring High Availability in CPM	17
Setting and Responding to Alarms	19
High Availability CPM Scenarios	20

WatchGuard® Firebox Vclass High Availability

In a WatchGuard Firebox Vclass High Availability (HA), two Firebox Vclass appliances are connected so that one serves as a ready backup to the other if the main appliance fails while managing network traffic. This chapter guides you through connecting, linking, and running a High Availability (HA) Active/Active system using two Firebox Vclass appliances in a primary and secondary relationship.

This chapter discusses the following topics:

- “How High Availability Works” on page 2
- “High Availability Modes” on page 2
- “Prerequisites for a High Availability System” on page 3
- “Connecting the appliances” on page 4
- “Installing High Availability” on page 4
- “Configuring High Availability Active/Active in Vcontroller” on page 7
- “Managing High Availability” on page 13
- “Setting and Responding to Alarms” on page 14

How High Availability Works

When High Availability is active, a Primary appliance sends a “heartbeat” to a Secondary appliance. This heartbeat tells the Secondary appliance that the primary appliance is still “alive,” or up. If the primary appliance fails, the heartbeat ceases. When the Secondary appliance detects three consecutive missed heartbeats, it assumes all processing tasks.

High Availability Modes

There are two High Availability modes: *Active/Standby* and *Active/Active*.

Active/Standby

In Active/Standby mode, when a primary appliance fails the passive appliance comes online with a full copy of the state table and VPN tunnels, to provide maximum uptime and network availability. Active/Standby is available for all models that have an HA interface. In this mode, both appliances are configured with the same system name, IP address, and configuration information.

Active/Active

In Active/Active mode, the paired appliances process traffic in parallel, and use transparent state failover. In the case of a failure, all processing and traffic transitions seamlessly to the appliance that is still working. System configuration, security policies, active connections, and VPN tunnels are shared between the two active appliances. Both appliances are sending and receiving packets, so processing throughput is potentially doubled. If one appliance fails, the other is fully aware of the state of all connections and can continue carrying the load without dropping any packets. Active/Active mode requires the purchase of an upgraded software license.

Configuration Comparison Between Active/Standby and Active/Active Mode

Configuration Item	Active/Standby Mode	Active/Active Mode
Host Name	Same for primary and secondary appliances.	Different for primary and secondary appliances.
IP addresses	Same for primary and secondary appliances.	Different for primary and secondary appliances.
MAC address	Same for primary and secondary appliances. Uses VRRP defined MAC addresses.	Different for primary and secondary appliances. Use the devices' factory MAC addresses.
Sending/Receiving Packets	Only the Active appliance can send and receive packets.	Both Active appliances can send and receive packets, potentially doubling system throughput.

In This Guide

*This guide discusses High Availability Active/Active mode for both Vcontroller and CPM. To learn about High Availability Active/Standby mode, see the *Vclass User Guide* and the *CPM User Guide*.*

Prerequisites for a High Availability System

To set up the High Availability feature, you need the following:

- Two Firebox Vclass appliances. For HA Active/Active mode, the appliances must be the same model. Only V80 and V100 appliances are supported for HA Active/Active.
- The appliance you use as the Secondary or backup device must be reset to the factory default configuration.
- Software upgrade licenses for the High Availability feature. You obtain these licenses from the WatchGuard LiveSecurity web site, after you register your appliances.
- Crossover cables to connect the appliance HA ports.

Connecting the appliances

To set up a High Availability system, you must connect two Firebox Vclass appliances through the HA port. For Active/Active mode, both appliances must be the same model.

- Connect the Private interface (0) of the Primary appliance to a hub or switch.
- Connect the Private interface (0) of the Secondary appliance to the same hub or switch.
- Connect all other interfaces that are being used in the same way. Every interface connection from the Primary appliance to a hub or switch must be matched with a connection from the Secondary appliance to the same hub or switch.
- Connect the HA interfaces with crossover cables.
- Connect the management station to a hub that is connected to interface 0 (private) on both appliances. The management station can also be connected to an HA2 port.

Installing High Availability

Your purchase of the WatchGuard High Availability Active/Active software upgrade includes a license key certificate. You enter this license key at the LiveSecurity Web site. The LiveSecurity web site will then generate a feature key for you.

Import the High Availability license to your Appliances

To use two appliances in a High Availability configuration, you must import separate High Availability licenses into both appliances.

Generate a Feature Key

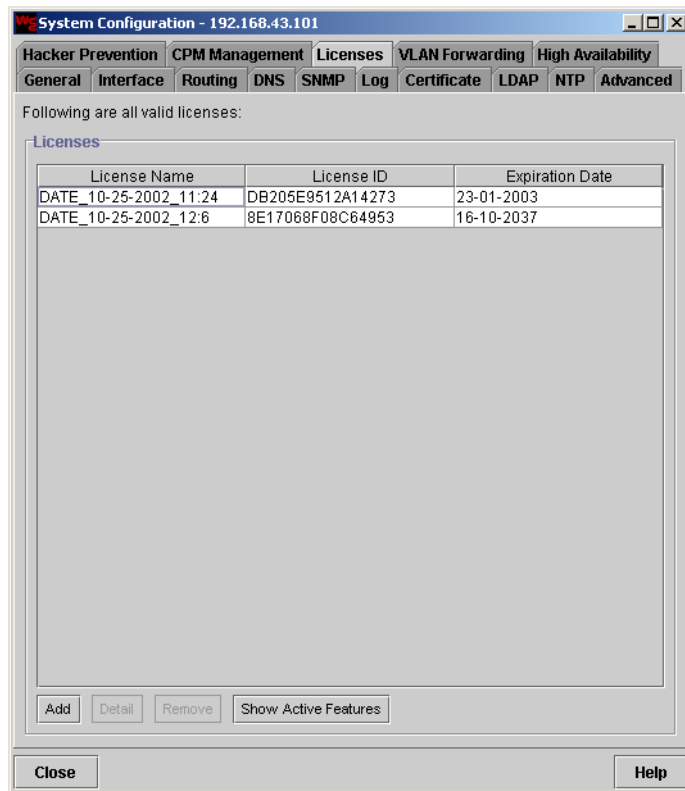
- 1 Generate the feature key at the LiveSecurity web site. You must register and log in.
Once you are logged in, you must activate your products if they are not already activated.

- 2 Generate a feature key.
More information here, pending further info...

Import the Feature Key to the Vclass appliances

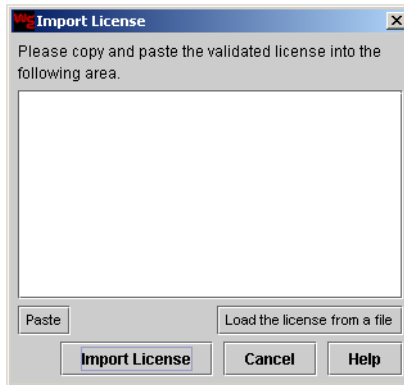
To add the new license for the High Availability feature, follow these steps:

- 1 Click the **License** tab.
The Licences list is displayed.



To import a new license, follow these steps:

- 2 Click **Add**.
The Import License window appears.

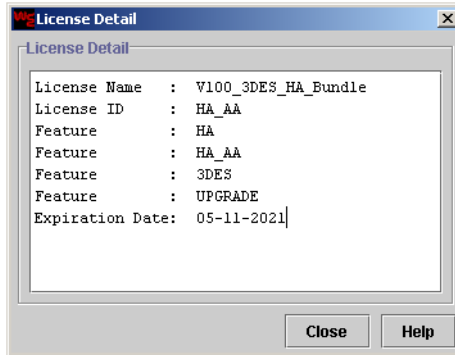


- 3 Click **Load the license from a file**.
- 4 Locate and select the license file.

NOTE

If you prefer, you can also use a text editor to open the file. Then copy and paste the text. You can also copy and paste the license text directly from the WatchGuard LiveSecurity Web site.

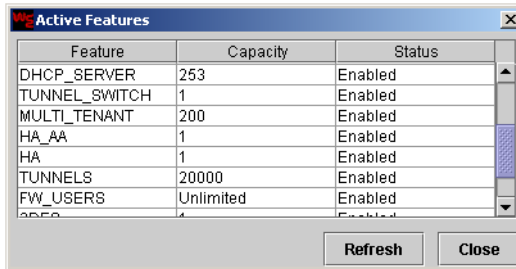
- 5 When the license text is displayed, click **Import License**.
This imports the license into the Firebox Vclass appliance. After the import is complete, the window closes and the newly imported license appears in the license list.
 - 6 Repeat this process to import any other certificates into the Firebox Vclass appliance.
 - 7 To remove a license, select the entry and click **Remove**.
A confirmation dialog box appears.
 - 8 Click **OK**.
The entry is removed from the **License** list.
- To view the details of a particular license, follow these steps:
- 1 Select an entry from the **Licenses** list.
 - 2 Click **Detail**.
The License Detail window appears.



- 3 Review the license information.
- 4 When you are finished, click **Close**.

To see which features are currently active, follow these steps:

- 1 Click **Show Active Features**.
The Active Features window appears.



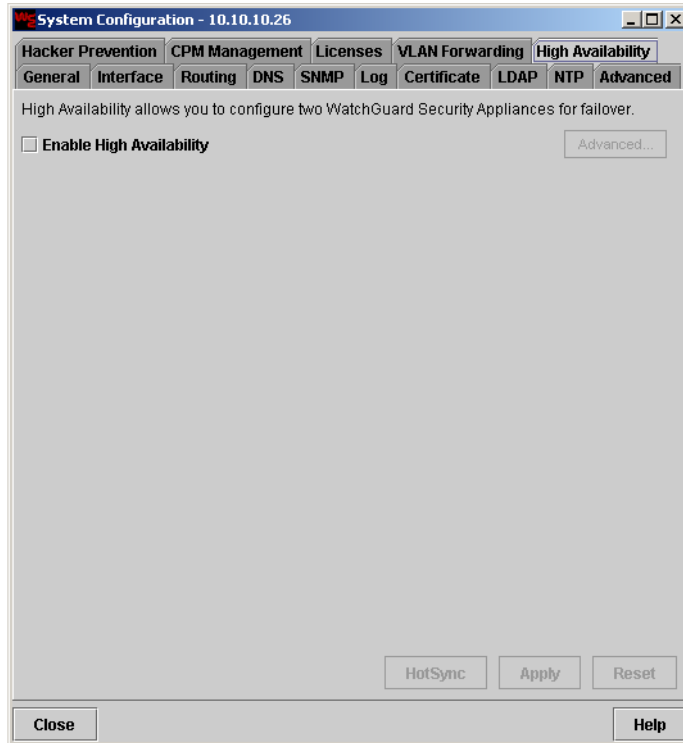
- 2 Review the active features along with their capacity and status.
- 3 Click **Refresh** to update the feature list.
- 4 When you are finished, click **Close**.

Configuring High Availability Active/Active in Vcontroller

After you have connected the appliances, you can configure the Secondary appliance with the WatchGuard Vcontroller.

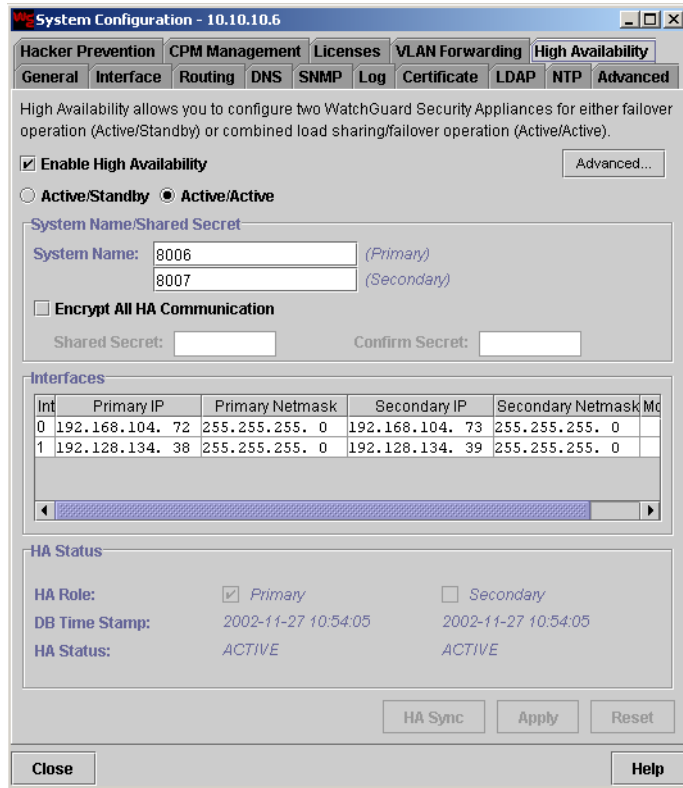
- 1 Make sure you are currently logged in to the Primary appliance.

- 2 After starting the WatchGuard Vcontroller, click the **System Configuration** button.
- 3 When the System Configuration window appears, click the **High Availability** tab.



4 Select **Enable High Availability**.

The following HA options appear in the tab. Select the Active/Active checkbox..



The default HA settings include the following:

- All of the appliance’s interfaces will be monitored. If any interface is detected as “LINK-DOWN,” the Secondary appliance will take over.
- The HA heartbeat interval is set to one beat every second.
- The HA Group ID, which uniquely identifies this group (pair) of Firebox Vclass appliances currently backing each other up, is recorded as 3.
- The HA heartbeat is sent through the HA1 interface.
- The appliance you are currently logged into will be configured as the primary.

NOTE

Make sure that the connection links both HA1 ports on the primary and secondary appliances, and that you are using a crossover cable. If the appliance cannot detect the secondary appliance, check the connection and restart the secondary appliance. When this is done, click the Refresh button to redetect the secondary appliance.

- 5 Type the **System Name** of the primary and secondary appliance.
- 6 If desired, click **Encrypt all HA Communication**, and type and confirm a **Shared Secret**.

This feature is optional, and can be left blank if you do not need to encrypt information sent between these appliances during normal operation. Encryption is not necessary if the HA1 interfaces are connected directly with a crossover cable.

NOTE

For better performance, leave the **HA secret** blank. This shared secret is used to encrypt HA state-sync information. VPN tunnel information is always encrypted even if this encryption is disabled.

- 7 Change the secondary system IP addresses and masks so they are different from those for the primary system.
- 8 Click the **Monitor** checkboxes to activate monitoring on specific interfaces.
- 9 Click **Apply** to apply the default HA configuration to the current (Primary) appliance.

The system restarts.
- 10 After the system has restarted, log in to the primary appliance again. Open the System Configuration window, and click on the High Availability tab.

The HA status should show that the current appliance is Primary and Takeover.
- 11 Click **HASync** to copy the entire configuration and policy database from the Primary appliance to the Secondary appliance.

NOTE

The Secondary appliance must be set (or reset) to the factory default configuration for HASync to work. The HASync button will not be

available otherwise. After the initial HASync, all configuration changes are automatically synced between appliances.

- 12 The secondary appliance restarts. Your system is now synced and operating in High Availability Active/Active mode.

You can check HA status from the High Availability tab in the System Configuration window.

Customizing Advanced HA System Parameters

You can customize a number of HA parameters using the **Advanced HA Parameters** dialog box. At this level, you can configure the following:

- Send the HA heartbeat to the secondary appliance's HA2 management interface.
- Change the HA group ID.

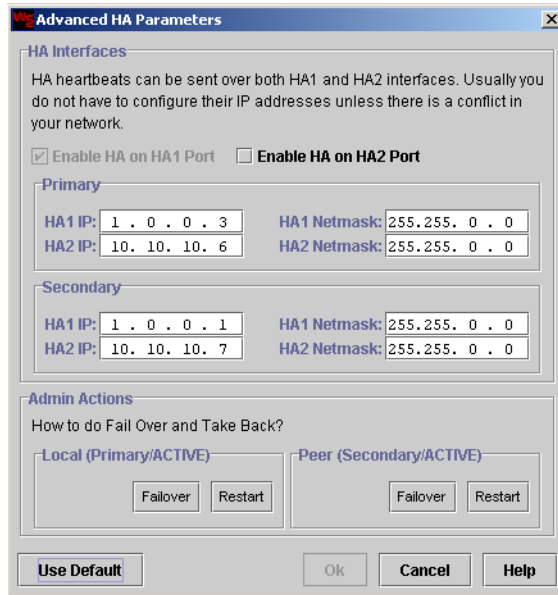
In addition, you can manually trigger a Failover or Restart event on the Primary or Secondary appliance.

To change any of these settings, follow these steps:

- 1 After starting the WatchGuard Vcontroller, click the **System Configuration** button.
- 2 When the System Configuration window appears, click the **High Availability** tab.
- 3 Click to select the checkbox marked **Enable High Availability and Active/Active**.

4 Click the **Advanced** button.

The Advanced HA Parameters dialog box appears.



5 To activate monitoring through the HA ports, click to select the checkbox marked **Enable HA on HA1 Port** and/or **Enable HA on HA2 Port**.

Note that if HA is enabled on the HA2 interface, that interface cannot be used for management access.

6 If specific IP addresses have been assigned to the HA ports, type the IP addresses and Netmasks in each of the two HA Interface fields—Primary and Secondary. Otherwise the default addresses will be adequate.

You can enter different IP addresses so that they can be accessed through your local area network.

7 When you have finished, click **OK** to save the parameter entries and close the **Advanced HA Parameters** dialog box.

Managing High Availability

Configuring Policies

Changes to the policy configuration and other system settings in the Active appliance are automatically synchronized to the secondary system, provided that the secondary appliance has not failed.

A failed appliance will automatically retrieve the new policy configuration from the active appliance when it recovers from the failure.

In rare situations, configurations can get out of sync, and one appliance may be left in the ADMIN state. You can perform a manual HASync to sync the two appliances again.

Analyzing System Failures

When an appliance fails, the other active appliance takes over processing. When you log into the active appliance using Vcontroller, check the System Status in the lower left corner to determine which appliance you are connecting to. Note that in Active/Active mode, you will be connected to the secondary appliance if the primary appliance has failed, even if you connect via the IP address of the private interface on the Primary appliance.

Checking HA system status

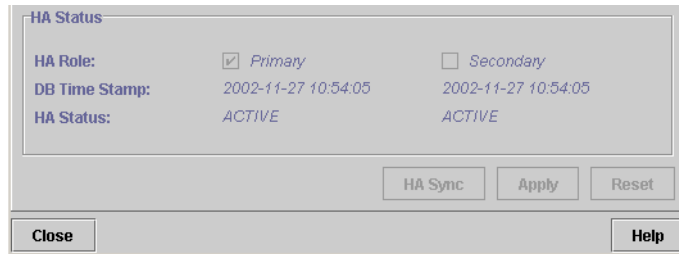
The WatchGuard Vcontroller provides a quick-check feature that tells you, at a glance, the status of your HA system. Look in the lower-left corner of the WatchGuard Vcontroller for the system indicator.

The “HA” monitor tells you which appliance you are logged into, whether it is Primary or Secondary, and whether it is Active or Failover..

2026		◆
0 (Private)	192.168.104.64	●
1 (Public)	192.128.134.32	●
2 (DMZ)	30.0.0.1	●
3 (DMZ2)	40.0.0.1	●
HA/AS	Primary/ACTIVE	
Total Tunnel...	0	
Sys Up Time:	5d, 2h, 9m	

Detailed System Status

Detailed HA system status is shown in the System Configuration/High Availability window. This status includes the HA role, status, DB timestamp, and failure reason (if one exists) for both systems.



To view detailed system status, open the System Configuration window and click on the High Availability tab. You can view the HA status of both the primary and secondary appliances at the same time. The following list describes the possible Status messages you might see.

Active	The current appliance is active
Failed	The current appliance has failed (for example, the link is down)
Takeover	The peer appliance has failed and the current system takes over.
Admin	Administration mode.
Unavailable	When the current appliance cannot detect its peer appliance, it shows this state in the peer HA status.

Setting and Responding to Alarms

When a system fails, an Event alarm is generated and the failover process is logged in the event log. You can check the alarms and the event log to determine when the failover occurred.

Make sure that you open and edit the existing Event Alarm definition so that you are notified by an SNMP trap, email alert, or both. You should also make sure that all SNMP stations have been registered in the appliances, as can be done in the System Configuration window SNMP tab.

For more information on defining alarms, see the *Firebox Vclass User Guide* and *CPM User Guide*.

WatchGuard® Firebox Vclass High Availability with CPM

This chapter describes how to use High Availability with a CPM system.

This chapter discusses the following topics:

- “Configuring High Availability in CPM” on page 17
- “High Availability CPM Scenarios” on page 20

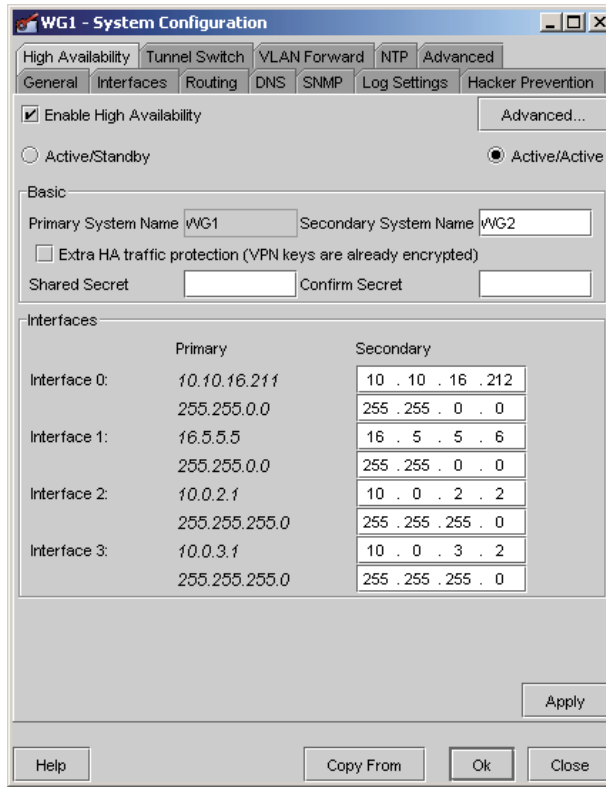
Configuring High Availability in CPM

To set up the CPM Client to manage an HA Active/Active connection:

- 1 Log on to the CPM Client.
- 2 Click **Configuration Editor**.
The Configuration Editor window appears.
- 3 Right-click an appliance record (in the Appliances/Addresses list) and select **Edit/View**.
The System Configuration dialog box appears, displaying the General tab.
- 4 Click the **HA** tab.
- 5 Click to select the checkbox marked **Enable High Availability** if you want to enable this feature.
The Active/Standby, Active/Active, and Advanced button become available.

6 Click the **Active/Active** checkbox.

The following options appear.



7 Enter the **Secondary System Name**.

8 If desired, click **Encrypt all HA Communication**, and type and confirm a **Shared Secret**.

This feature is optional, and can be left blank if you do not need to encrypt information sent between these appliances during normal operation. Encryption is not necessary if the HA1 interfaces are connected directly with a crossover cable.

NOTE

For better performance, leave the **HA secret** blank. This shared secret is used to encrypt HA state-sync information. VPN tunnel information is always encrypted even if this encryption is disabled.

9 Enter the IP addresses and Netmasks for the secondary appliance.

10 Click **Advanced**

The Advanced HA Settings dialog box appears.

11 Click the checkbox of each port you want the backup appliance to monitor.

12 Click the checkbox to select the HA interface you want to enable and send HA heartbeats over and type the Primary IP address, Secondary IP address, and Netmask of the HA interface you enabled.

13 Click **OK**.

Setting and Responding to Alarms

When a system has failed, an Event alarm is generated and the failover process is logged in the event log. You can check the alarms and the event log to determine when the failover occurred.

Make sure that you open and edit the existing Event Alarm definition so that you are notified by an SNMP trap, email alert, or both. You should also make sure that all SNMP stations have been registered in the appliances, as can be done in the System Configuration window SNMP tab.

For more information on defining alarms, see the *Firebox Vclass User Guide* and *CPM User Guide*.

High Availability CPM Scenarios

The following High Availability scenarios are provided:

- “Both appliances are new” on page 20.
- “One appliance is already in service without HA. Add another appliance and set up system for HA Active/Active” on page 20

Both appliances are new

- 1 Add HA licenses to both appliances.
- 2 Reset both appliances to the factory default configuration.
- 3 Add an appliance record for the primary appliance, and set up the system with the proper HA configuration. Compile this profile.
- 4 Connect the HA1 ports of both appliances with a crossover cable. Connect the Private ports of both appliances to the same network as the CPM server.
- 5 Run Discovery on both appliances. Choose the one that will be the primary interface, and deploy the profile to it.
- 6 Both appliances should enter AA mode.
- 7 If necessary, power off, disconnect, and ship the two appliances to their destination if needed.

One appliance is already in service without HA. Add another appliance and set up system for HA Active/Active

In this scenario, one appliance is already in service without HA. We are going to add another appliance, and set the two appliances to work in

HA- Active/Active mode. The appliance that is currently in service will be designated as the primary appliance, and the new appliance will be designated as the secondary appliance.

- 1 Add HA licenses to both appliances.
- 2 Reset the new (secondary) appliance to factory defaults.
- 3 Modify the system configuration of the primary appliance to enable HA, and recompile the profile.
- 4 Connect the HA1 port of both appliances using a crossover cable. Connect the other interfaces as necessary.
- 5 Deploy the profile of the primary appliance
- 6 Both appliances should enter AA mode.

