

eSoft

Simply better network security.™

# **InstaGate®**

## High Availability SoftPak

---

## Copyright Notices

©eSoft, Inc. 2003. eSoft and InstaGate are registered trademarks, and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of InstaGate’s software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of InstaGate’s software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California.

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. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution 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 University of California, Berkeley and its contributors.”
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

---

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “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 REGENTS 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.

Portions of InstaGate’s software are Copyright © The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. 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 Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

5. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”





## InstaGate SoftPak High Availability

eSoft's High Availability SoftPak provides automatic failover from your company InstaGate to an online backup InstaGate, also known as a *hot standby*. The backup InstaGate monitors the health of the primary InstaGate and activates when it detects failure, ensuring that your network remains connected to the Internet and protected by the firewall. Once activated, the backup InstaGate continues to monitor the health of the primary InstaGate and reverts to backup status when the primary InstaGate becomes available.

The two InstaGate's can communicate using your existing LAN and WAN connections, linked DMZ ports (if available), and linked synchronous serial ports (Serial Port 1).

### Connecting the High Availability InstaGates

Connect the primary and backup InstaGate appliances to your network and the Internet (LAN and WAN) using the instructions found in the *InstaGate Quick Start Guide*. The primary and backup InstaGates must be installed on the same network. If you only intend to pass High Availability traffic through the LAN and/or WAN ports (in-band connection), this is the only physical setup required.

To pass High Availability traffic through the DMZ ports (if available), connect the two ports using a crossover Ethernet cable (out-of-band connection). If your primary InstaGate is currently connected to a DMZ network, connect the backup InstaGate to a hub or switch on the same DMZ network using a straight through Ethernet cable (in-band connection).

To pass High Availability traffic through the synchronous serial ports, connect Serial Port 1 on the primary InstaGate to Serial Port 1 on the backup InstaGate using a DB-9 to DB-9 null modem cable (out-of-band connection).

---

## Installing the InstaGates

After physically connecting the primary and backup InstaGates, refer to the *InstaGate Quick Start Guide* and the *InstaGate User Guide* for information about installing and configuring each appliance. While the primary InstaGate requires full configuration (user accounts, firewall policies, VPN policies, etc.) simply configuring the LAN and WAN interfaces is sufficient for the backup InstaGate. The backup InstaGate's LAN and WAN IP addresses must be on the same LAN and WAN subnets as the primary InstaGate. The remainder of the backup InstaGate's configuration settings are automatically obtained from the primary InstaGate using High Availability.

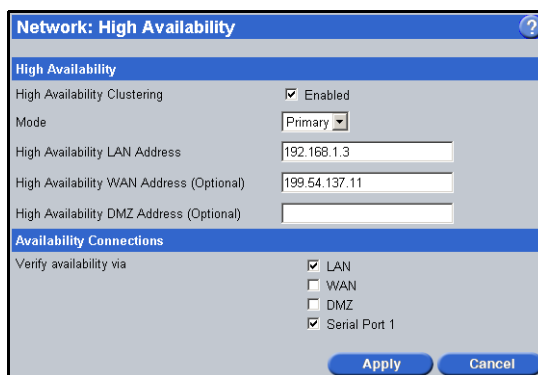
## Configuring High Availability

Once both InstaGates are up and running, you must configure the High Availability settings on each appliance.

### Configuring the Primary InstaGate

The primary InstaGate must be subscribed to the High Availability SoftPak. To configure the primary InstaGate's High Availability settings:

1. Select *High Availability* from the *Network* menu.



The screenshot shows a configuration window titled "Network: High Availability". It is divided into two main sections: "High Availability" and "Availability Connections".

**High Availability Section:**

- High Availability Clustering:** A checkbox labeled "Enabled" is checked.
- Mode:** A drop-down menu is set to "Primary".
- High Availability LAN Address:** A text box contains the IP address "192.168.1.3".
- High Availability WAN Address (Optional):** A text box contains the IP address "199.54.137.11".
- High Availability DMZ Address (Optional):** An empty text box.

**Availability Connections Section:**

- Verify availability via:** A group of checkboxes where "LAN" is checked, and "WAN", "DMZ", and "Serial Port 1" are unchecked.

At the bottom right of the window are two buttons: "Apply" and "Cancel".

2. Select the *High Availability Clustering Enabled* check box.
3. Select *Primary* from the *Mode* drop-down box.
4. Enter the *High Availability LAN Address*. This address must be a unique IP address on the same LAN subnet as the primary and backup InstaGates. The High Availability LAN address is a virtual IP address shared by the primary and backup InstaGates, so that failover is transparent to network devices. The network devices (such as, workstations and servers) must then be configured to use the High Availability address as their proxy and/or default gateway for failover to work properly.

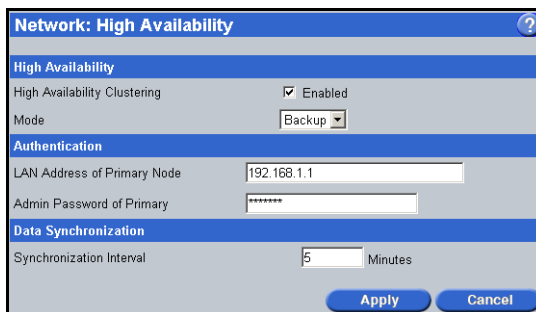
- 
- If necessary, enter the *High Availability WAN Address*. This address must be a unique IP address on the same WAN subnet as the primary and backup InstaGates. The High Availability WAN address is a virtual IP address shared by the primary and backup InstaGates, so that failover is transparent to external devices. By specifying a High Availability WAN address, IPSec VPNs and firewall passthrough rules/policies continue to function after failover.
  - If necessary, enter the *High Availability DMZ Address*. This address must be a unique address on the DMZ network.
  - Select the port(s) to use for verifying availability (*LAN, WAN, DMZ, and Serial Port 1*). High Availability uses a heartbeat protocol between the selected ports on the primary and backup InstaGates to detect failure. Failure (including hardware, switches, hubs, or cables) between all of the selected ports on the InstaGates causes failover to occur. However, if you are using more than one port to verify availability, and failure is detected on some but not all of the ports, failover does not occur. Instead, an email notification message is sent to the system administrators. After failover, the backup InstaGate continues to monitor the health of the primary InstaGate and returns to backup status when the primary InstaGate becomes available.  
  
In addition, if at any time the primary InstaGate detects failure in the backup InstaGate, an email alert is sent to the system administrator.
  - Click *Apply* to save your settings, or *Cancel* to exit without saving.

## Configuring the Backup InstaGate

The backup InstaGate must be the same model (for example, xSP Branch Office, xSP Business, or PRO) as the primary InstaGate. SoftPak subscriptions are only required on the primary InstaGate, with the backup InstaGate automatically mirroring the SoftPak subscriptions of the primary. High Availability is compatible with all eSoft SoftPaks.

To configure the backup InstaGate's High Availability settings:

- Select *High Availability* from the *Network* menu.



The screenshot shows a configuration window titled "Network: High Availability". It is divided into several sections:

- High Availability**:
  - High Availability Clustering:  Enabled
  - Mode: Backup (dropdown menu)
- Authentication**:
  - LAN Address of Primary Node: 192.168.1.1
  - Admin Password of Primary: [masked]
- Data Synchronization**:
  - Synchronization Interval: 5 Minutes

At the bottom right, there are "Apply" and "Cancel" buttons.

- 
2. Select the *High Availability Clustering Enabled* check box.
  3. Select *Backup* from the *Mode* drop-down box.
  4. Enter the primary InstaGate's LAN IP address in the *LAN Address of Primary Node* text box.
  5. Enter the *Administrative Password of the Primary InstaGate*.
  6. Enter the *Synchronization Interval*. At the specified interval, all of the primary InstaGate's configuration information (except its IP address) is automatically synchronized on the backup InstaGate. While user accounts (including passwords and access settings) are synchronized, no user data (such as, personal Web sites, mailboxes, and log files) is transferred.
  7. Click *Apply* to save your settings, or *Cancel* to exit without saving. Upon clicking *Apply*, the backup InstaGate immediately contacts SoftPak Director to download any necessary software.

---

**Note** After the backup InstaGate has finished downloading software, an *Install Now* button appears at the top of the administrative interface. You must click the *Install Now* button to install the backup InstaGate's software (including SoftPaks) and to synchronize its configuration with the primary InstaGate.

---

Once High Availability is enabled, manual configuration changes are not allowed on the backup InstaGate.