

eSoft

Simply better network security.™

InstaGate®

VPN Manager 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 VPN Manager

eSoft VPN Manager is a global VPN management tool that allows a central administrator to configure multiple InstaGate IPsec VPNs from a single console. Policies defined in VPN Manager are automatically distributed to participating InstaGates, eliminating the need to configure each device. VPN Manager supports both star (central office) and meshed (fully connected) VPN topologies. Sites with dynamic IP addresses are also supported.

VPN Manager consists of the following components:

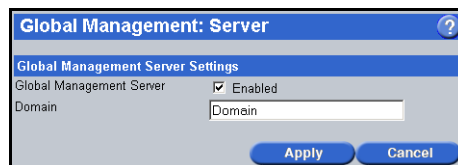
- **Global Management Server** — Installed on an InstaGate with VPN Manager, this server is the central repository for VPN policies.
- **eSoft InstaGate Devices** — When managed by VPN Manager, InstaGates use the Global Management Client to contact the Global Management Server for policy updates.
- **eSoft VPN Clients** — Optional SoftPak for remote user VPN access, allows mobile remote clients to contact the Global Management Server for policy updates.

Enabling the Global Management Server

Before creating VPN policies or adding devices, you must first enable the Global Management Server.

To enable the Global Management Server:

1. Select *Server* from the *Global Management* menu.



2. Check the *Global Management Server Enabled* check box.

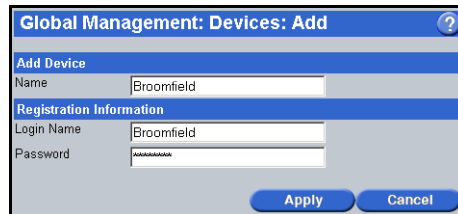
-
3. Enter the *Domain* for management. The domain name is used to identify and group the devices managed by the Global Management Server.
 4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Adding VPN Devices

After enabling the Global Management Server, set up the devices to manage.

To add a VPN device:

1. Select *Devices* from the *Global Management* menu.
2. Click *Add* to add a new device. To modify an existing device, select the device you wish to modify and click *Modify* (see “Modifying Devices” on page 7). To delete a device, select the device you wish to delete and click *Delete*.



The screenshot shows a dialog box titled "Global Management: Devices: Add". It has a blue header bar with a question mark icon on the right. Below the header, there are two sections. The first section is "Add Device" and contains a "Name" field with the text "Broomfield". The second section is "Registration Information" and contains two fields: "Login Name" with the text "Broomfield" and "Password" with masked characters "*****". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

3. Enter a unique *Name* to identify the device in VPN Manager.
4. Enter a *Login Name* and *Password* for the device. The name and password specified are used to register the device with VPN Manager.
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

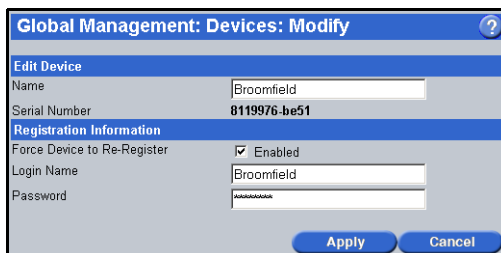
Note In order to manage the InstaGate hosting VPN Manager using VPN Manager, you must add a device for the hosting InstaGate.

Modifying Devices

The Modify page allows you to change a device's name and registration information.

To modify a device:

1. Select *Devices* from the *Global Management* menu.
2. Select the device you want to modify, and click *Modify*.



3. Edit the device *Name* if necessary.
4. Select the *Force Device to Re-Register Enabled* check box to force the device's global management client to re-register with the global management server before connecting to the VPN. You can also change the *Login Name* and *Password* used to register the device.

Note After selecting the *Force Device to Re-Register* check box, you must manually re-register the device by selecting *Global Management* from the client InstaGate's *System* menu, and clicking *Apply*. See "Registering VPN Devices" on page 8 for further information.

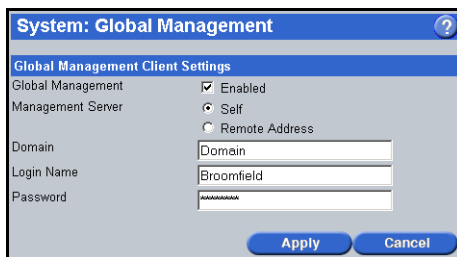
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Registering VPN Devices

After adding a device in VPN Manager, the device must then be configured to talk to VPN Manager. Participating InstaGates use the Global Management Client to connect to VPN Manager's Global Management Server. The first time a device contacts VPN Manager, the device registers itself by authenticating using the domain, login name and password defined in VPN Manager. Once registered, a device continually exchanges configuration information with the Global Management Server and reconfigures as necessary.

To register a device:

1. Select *Global Management* from the *System* menu.



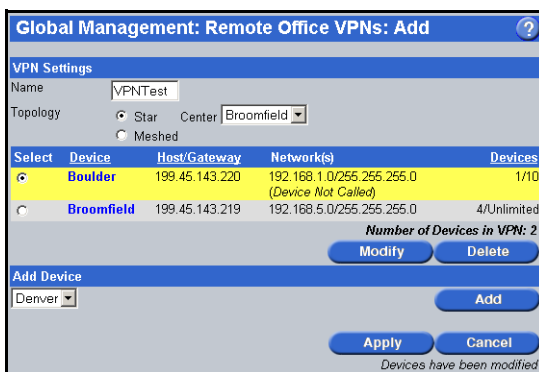
2. Select the *Global Management Enabled* check box. This enables the device's Global Management Client, allowing it to connect to VPN Manager's Global Management Server.
3. Enter the IP address or host name of the *Management Server*.
If the InstaGate itself is the management server, click the *Self* radio button.
4. Enter the *Domain* for management. The domain name is used to identify and group the devices managed by VPN Manager. The domain specified must match the domain entered when enabling the Global Management Server (see "Enabling the Global Management Server" on page 5).
5. Enter the device's *Login Name* and *Password*. The name and password specified must match the name and password entered when adding the device in VPN Manager (see "Adding VPN Devices" on page 6).
6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring Remote Office VPNs

Once you have added and registered devices in VPN Manager, create VPNs between the devices.

To add a remote office VPN:

1. Select *Remote Office VPNs* from the *Global Management* menu.
2. Click *Add* to add a new VPN. To modify an existing VPN, select the VPN you wish to modify and click *Modify*. To delete a VPN, select the VPN you wish to delete and click *Delete*.



3. Enter a unique *Name* to identify the VPN in VPN Manager.
4. Select the VPN *Topology*:
 - **Star** — In a Star topology, all devices connect to a central device, but not to each other. For example, if you have several branch offices that need to connect to a central office, but not to other branch offices, select *Star*.
 - **Meshed** — In a Meshed topology, all devices connect to all other devices. For example, if you have several offices that all need to connect to each other, select *Meshed*.
5. Select the *Devices* you wish to add to the VPN from the drop-down list, and click *Add*.
6. To specify the network routes on a device that are available to the VPN, select the device and click *Modify*. See “Configuring Network Routing” on page 10 for more information.
7. If you selected a Star VPN topology, select the central device in the VPN from the *Center* drop-down list.
8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring Network Routing

To determine the network routes available to the VPN for the selected device:

1. Select a device and click *Modify* in the Remote Office VPN page.

The screenshot shows a dialog box titled "Global Management: Remote Office VPNs: Edit: Modify: Boulder". The main heading is "Routes Available for this VPN". There are three radio button options: "None (Host only)", "All Registered", and "Selected". The "Selected" option is selected. Below it is a dropdown menu with "Other" selected. To the right of the dropdown are "Add >" and "< Remove" buttons. Below the dropdown are two input fields: "Network" with the value "199.54.137.6" and "Netmask" with the value "255.255.255.0". To the right of these fields is a list box containing "192.168.1.0/255.255.255.0". At the bottom of the dialog are "Apply" and "Cancel" buttons.

2. Select one of the following routing options:
 - **None (Host Only)** — Only the host (the InstaGate itself) is available to the VPN.
 - **All Registered** — All routes on the device's LAN interface are available to the VPN. As new routes are added, they are made available to the VPN (registered) the next time the device contacts VPN Manager (every five minutes).
 - **Selected** — Only the selected routes are available to the VPN. This allows you to completely control the routes that are allowed. For example, to add a registered network or static route, simply select the network from the drop-down list, and click *Add*. To add a network that hasn't yet registered with VPN Manager, or an individual IP address or group of IP addresses, select *Other* from the drop-down list, and enter the address and subnet mask.
3. Click *Apply* to save your settings, or *Cancel* to exit without saving.

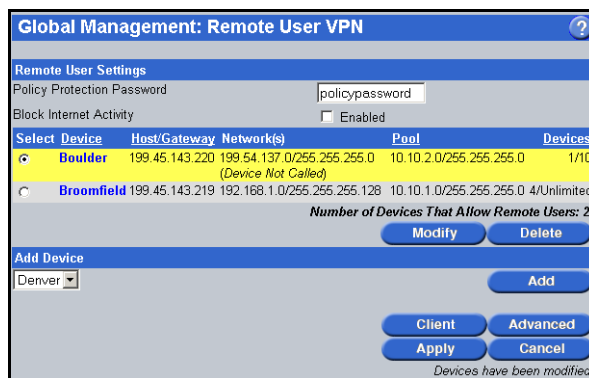
Configuring Remote User VPN

If you have installed the eSoft VPN Client SoftPak, mobile and remote user VPNs can be created and managed using VPN Manager. VPN Manager allows a central administrator to create and manage VPN policies for multiple remote clients. Policies are defined once on InstaGate and then propagated to the remote clients, eliminating the need to individually configure each client. Clients continue to automatically contact the Remote User Policy Server every five minutes to update their configuration settings.

Note In order to connect to VPNs, remote users must have a valid InstaGate account with remote access privileges (specified in the *Add Users* page). If you do not want to create an account for each user, you can use a RADIUS server for remote authentication.

To add a remote user VPN:

1. Select *Remote User VPN* from the *Global Management* menu.



2. Enter the *Policy Protection Password*. This password is used by remote users to access the VPN policy and must be at least 8 characters.
3. Select the *Block Internet Activity Enabled* check box to prevent users from accessing the Internet while connected to the VPN.
4. Select the *Devices* you wish to add to the VPN from the drop-down list, and click *Add*. The devices selected are not connected to each other through the VPN, they simply allow remote user VPN access.
5. To specify the network routes on a device that are available to remote users, select the device and click *Modify*. The *Modify* page also allows you to specify the range of IP addresses dynamically assigned to remote clients that connect to the device. See “Configuring Network Routing” on page 12 for more information.
6. To download the eSoft VPN Client software for distribution to remote users, click *Client*. Refer to the documentation included with the eSoft VPN Client SoftPak for information on installing and using the client software.

-
7. To disable the Remote User Policy Server and prevent clients from automatically downloading the VPN policy, click *Advanced* (see “Disabling the Remote User VPN Policy Server” on page 12). You can then download the policy for manual distribution to clients by clicking *Policy*.
 8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring Network Routing

To modify the remote user settings for the selected device:

1. Select a device and click *Modify* in the Remote User VPN page.
2. Enter a network IP address and subnet mask in the *IP Address Pool* fields. Addresses from this pool are dynamically allocated to clients that connect to the device. The addresses specified cannot be included in any static routes or other networks defined on InstaGate.
3. Select the routes on the device that are available to remote users:
 - **None (Host Only)** — Only the host (the InstaGate itself) is available to remote users.
 - **Selected** — Only the selected routes are available to remote users. This allows you to completely control remote access. For example, to allow access to a registered network or static route, simply select the network from the drop-down list, and click *Add*. To allow access to a network that hasn’t yet registered with VPN Manager, or to an individual IP address or group of IP addresses, select *Other* from the drop-down list, and enter the address and subnet mask.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Disabling the Remote User VPN Policy Server

To disable the Remote User Policy Server and prevent clients from automatically downloading the remote user VPN policy:

1. Click *Advanced* in the Remote User VPN page.
2. Select *Manage Manually*. This allows you to enable and disable the Remote User Policy Server.

If *Manage Automatically* is selected, the Remote User Policy Server is always enabled.

3. Click *Apply* to save your settings, or *Cancel* to exit without saving.