



SecurityCluster 2.5

HOW-TO GUIDELINES

Setting up SecurityCluster 2.5 for eTrust Intrusion Detection

HWTO1SBSC.2.5 - 28/3/02

Purpose of this Document

This document describes the configuration steps of StoneBeat® SecurityCluster™ 2.5 for use with Computer Associates™ eTrust™ Intrusion Detection™ system.

The structure of the document is as follows:

- Section *“Installation Overview”* on page 3 presents an overview of the required steps for configuring StoneBeat SecurityCluster for use with eTrust Intrusion Detection.
- Section *“Configuring StoneBeat SecurityCluster”* on page 4 explains the configuration steps for StoneBeat SecurityCluster installation.
- Section *“Configuring Network Interface Bindings”* on page 10 describes the necessary check of the network interface bindings after StoneBeat SecurityCluster installation.

For more information on StoneBeat SecurityCluster installation, configuration, and operation, see *StoneBeat SecurityCluster 2.5 Manual* and the *StoneBeat SecurityCluster Release Notes*.

For the latest product information, documents, and news, visit Stonesoft Web site at <http://www.stonesoft.com>.

For more information on eTrust Intrusion Detection, see the Computer Associates Web site at <http://www.ca.com>.

Installation Overview

To install and configure StoneBeat SecurityCluster for use with eTrust Intrusion Detection:

1. Install eTrust Intrusion Detection according to the product documentation.



.....
Note: eTrust Intrusion Detection must be installed before StoneBeat SecurityCluster.
.....

2. Install StoneBeat SecurityCluster according to Chapter 3 of the *StoneBeat SecurityCluster Manual*.
3. Configure StoneBeat SecurityCluster as described in section [“Configuring StoneBeat SecurityCluster” on page 4](#) of this document. Note that eTrust Intrusion Detection limits the number of the IP addresses on the operational interface to one. This results to the following issues:
 - Only one IP address can be configured for each operational interface and the configured IP address must be the Cluster IP.
 - Because the operational interface has only the Cluster IP address defined, the operational interfaces cannot be used for connections originating from the security server itself. For example, you cannot use ping from the security server through the operational interface because the return packets will be load balanced between the nodes and may be returned to a wrong node.
 - Because the operational interface has only the Cluster IP address defined, a separate Administrator NIC is needed if other than standalone installation is used.
4. Configure the network interface bindings as described in section [“Configuring Network Interface Bindings” on page 10](#) of this document.

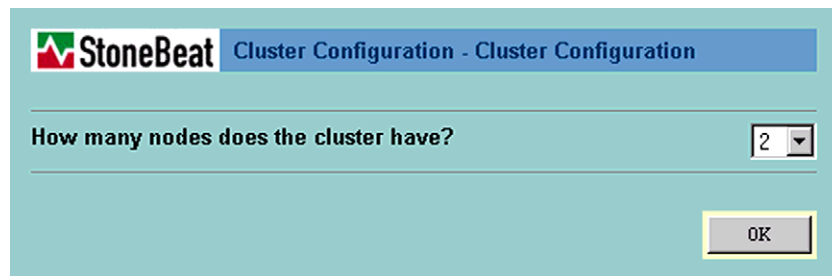
Configuring StoneBeat SecurityCluster

This section describes the necessary steps for configuring StoneBeat SecurityCluster for use with eTrust Intrusion Detection.

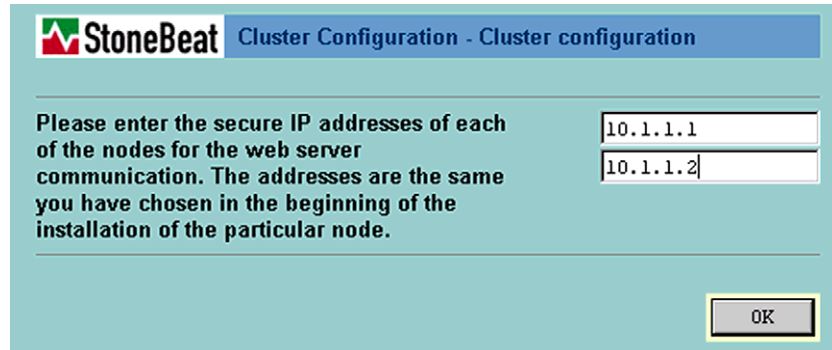
To configure StoneBeat SecurityCluster:

1. After installing eTrust Intrusion Detection and StoneBeat SecurityCluster, start the SecurityCluster Web configuration GUI by selecting **Start>Programs>SecurityCluster>Web Configuration GUI** or by browsing to the address <http://localhost:3003/install/>.
2. Prepare the SecurityCluster nodes for Web configuration as instructed in Chapter 4 on page 60 of the *StoneBeat SecurityCluster Manual*.
3. Start the configuration of the SecurityCluster nodes as instructed in Chapter 4 on page 62 of the *StoneBeat SecurityCluster Manual*. On configuration step 9 on page 66 of the *StoneBeat SecurityCluster Manual*, continue as instructed in this document.

ILLUSTRATION 1.1 *Defining the number of nodes*



4. Select the number of nodes in the cluster from the dropdown menu and click **OK** to continue.

ILLUSTRATION 1.2 *Defining the node IP addresses for configuration*

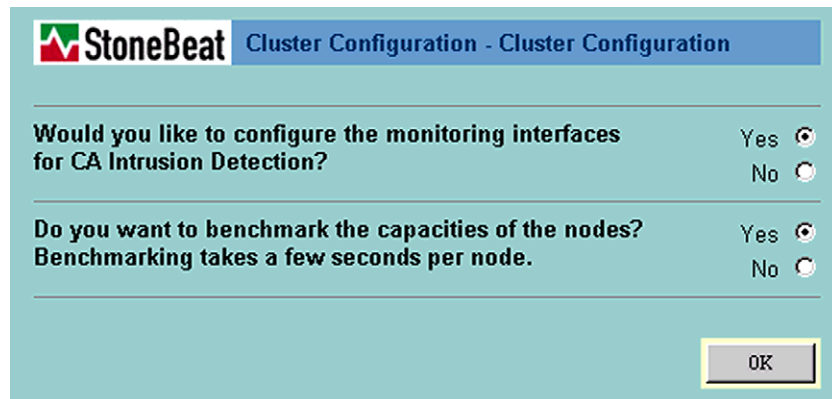
StoneBeat Cluster Configuration - Cluster configuration

Please enter the secure IP addresses of each of the nodes for the web server communication. The addresses are the same you have chosen in the beginning of the installation of the particular node.

10.1.1.1
10.1.1.2

OK

5. Enter the configuration Web server IP addresses for communication with the nodes.
6. Click **OK** to continue.

ILLUSTRATION 1.3 *Selecting monitoring interface configuration and benchmarking*

StoneBeat Cluster Configuration - Cluster Configuration

Would you like to configure the monitoring interfaces for CA Intrusion Detection? Yes No

Do you want to benchmark the capacities of the nodes? Benchmarking takes a few seconds per node. Yes No

OK

7. For configuring the monitoring interfaces for eTrust Intrusion Detection, select **Yes**.
8. For automatic benchmarking of the node capacities, select **Yes**. The benchmark value describes a node's capacity for handling traffic load and is used in the load balancing calculations.
9. Click **OK** to continue.

ILLUSTRATION 1.4 Defining the cluster properties

Cluster Configuration - Interfaces	
Cluster ID	1
Cluster properties:	
Load measurement interval:	15 s
Control port:	3002
Heartbeat protocol multicast MAC address:	01:02:03:04:05:06
2nd heartbeat protocol multicast MAC address: (optional)	
Cluster mode:	<input checked="" type="radio"/> balancing <input type="radio"/> standby
Other features:	CA Intrusion Detection in use

10. In the **Cluster ID** field, enter an identifier for the cluster. The allowed range of values is 1–65535.
11. In the **Load measurement interval** field, enter a value between 15 and 150 seconds or leave the field blank to use the default value of 15 seconds. The value defines how often a node measures the load of the traffic that it is handling.
 - A short measurement interval ensures that the cluster reacts more rapidly when a node is overloaded. On the other hand, brief load spikes may cause unwanted load balancing transitions thus affecting the cluster performance.
12. In the **Control port** field, specify a port number for control connections. This is the port number which is used for Stonesoft ClusterManager management connections.
13. In the **Heartbeat protocol multicast MAC address** field, enter a multicast MAC address for the heartbeat protocol. The address has to be a multicast MAC address, meaning that the first byte of the MAC address is an odd number. It is recommended to use the default heartbeat multicast MAC address generated by the configuration wizard.

- You can also specify a second heartbeat address. The heartbeat connection is operational as long as either of the heartbeat connections is operating. The address has to be a multicast MAC address, meaning that the first byte of the MAC address is an odd number.
14. For **Cluster mode**, select whether a load balancing or hot standby configuration is to be used:
- **balancing** mode enables load balancing between the nodes in the cluster.
 - **standby** mode enables a hot-standby configuration where no more than one node is online at a time and the remaining nodes stand ready to take over if the online node fails.
15. In the **Other features** field, the text **CA Intrusion Detection in use** indicates that the monitoring interfaces for eTrust Intrusion Detection were enabled in Illustration 1.3.

ILLUSTRATION 1.5 *Configuring the node properties*

Node ID (must be unique for each node)

Capacity:	<input type="text" value="394"/>
Protocol message period: (leave blank to use the default value)	<input type="text"/> ms
Failover time: (leave blank to use the default value)	<input type="text"/> ms
Boot delay: (leave blank to use the default value)	<input type="text"/> s
Start-up mode:	<input checked="" type="radio"/> offline <input type="radio"/> standby
StoneBeat home:	C:/Program Files/SecurityCluster

Interface		Heartbeat				Not used or
Name	Dedicated IP	1st	2nd	Monitoring	Control	control IP only
SBIMP5	10.1.4.102	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SBIMP6	10.0.4.102	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SBIMP7	192.168.4.102	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SBIMP8	172.16.2.55	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

16. From the **Node ID** dropdown menu, select an identifier for the node. This value must be unique for each cluster node.
17. In the **Capacity** field, the automatically calculated benchmark value is presented if benchmarking was selected in Illustration 1.3. To ensure efficient load balancing calculations, the capacity value should not be edited manually for other than testing and troubleshooting purposes.
18. In the **Protocol message period** field, enter the number of milliseconds you want the node to wait between sending heartbeat protocol messages. The default value of 500 milliseconds (0.5 seconds) is automatically assigned if you leave this field blank.
19. In the **Failover time** field, enter the number of milliseconds the cluster will wait to receive heartbeat protocol messages from the node before considering the node failed. The default value of 5000 milliseconds (5 seconds) is automatically assigned if you leave this field blank.

20. In the **Boot delay** field, enter the number of seconds the node will wait before trying to go online from standby start-up mode. The default value of 60 seconds is automatically assigned if you leave this field blank.
21. In the **Start-up mode** box, select the start-up mode for this node.
 - **offline** mode keeps the node offline until it is commanded to do otherwise.
 - **standby** mode directs the node to go online after successful self-testing period.
22. The **StoneBeat home** field indicates the path of the StoneBeat SecurityCluster installation.
23. On the **Interface** table, choose an interface type for each of the node's interfaces.
24. Repeat the node properties configuration steps 16–23 for each cluster node.
25. Ensure that the monitoring interfaces configured in eTrust Intrusion Detection match those selected in this configuration.
26. Click **Next** to continue.
27. Continue the configuration as instructed in Chapter 4 on page 72 of the *StoneBeat SecurityCluster Manual*.

Configuring Network Interface Bindings

After installing and configuring StoneBeat SecurityCluster, the network interface bindings on the cluster nodes needs to be checked.

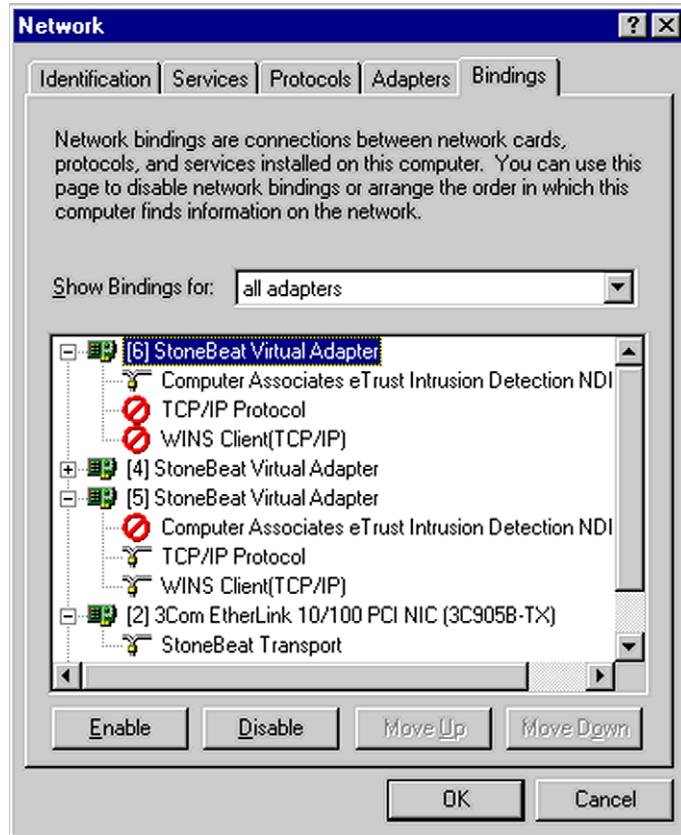
Bindings on Windows NT

The network interface bindings need to be changed after StoneBeat SecurityCluster installation.

To change the network interface bindings:

1. Open the network bindings by selecting **Start>Settings>Control Panel>Network>Bindings**.

ILLUSTRATION 1.6 Network interface bindings on Windows NT



2. From the **Show Bindings for:** dropdown menu, select **all adapters**.
3. Select the StoneBeat Virtual Adapter that is used as the monitoring interface (the adapter [6] in Illustration 1.6).
 - 3.1 Ensure that the eTrust Intrusion Detection binding is enabled. If it is not, select the binding and click **Enable**.
 - 3.2 Disable all the other protocol bindings for this interface by selecting a binding and clicking **Disable**.
4. For all the other adapters, disable the eTrust Intrusion Detection binding by selecting the binding and clicking **Disable**.

5. Click **OK** to activate the settings.

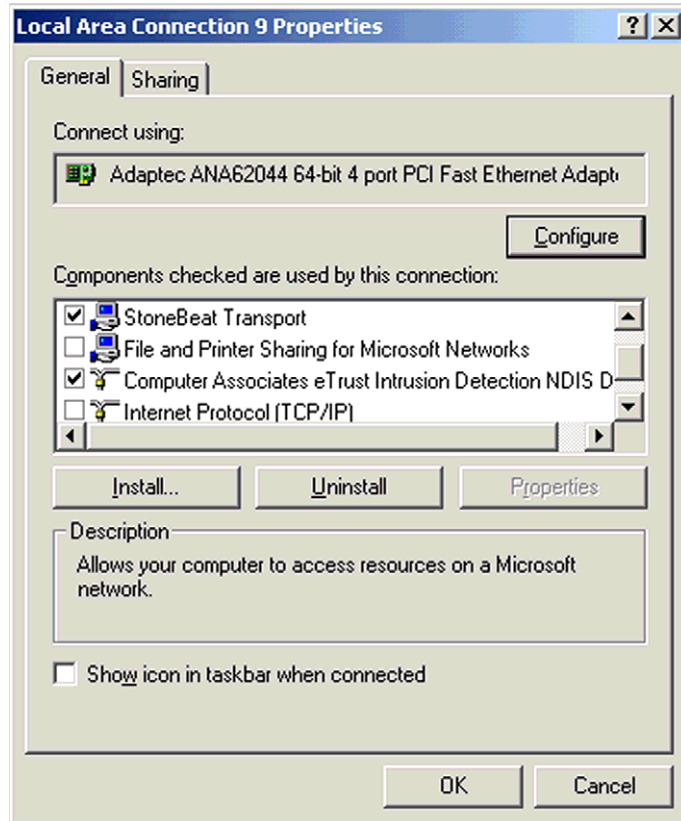
Bindings on Windows 2000

The network interface bindings need to be changed after StoneBeat SecurityCluster installation.

To change the network interface bindings:

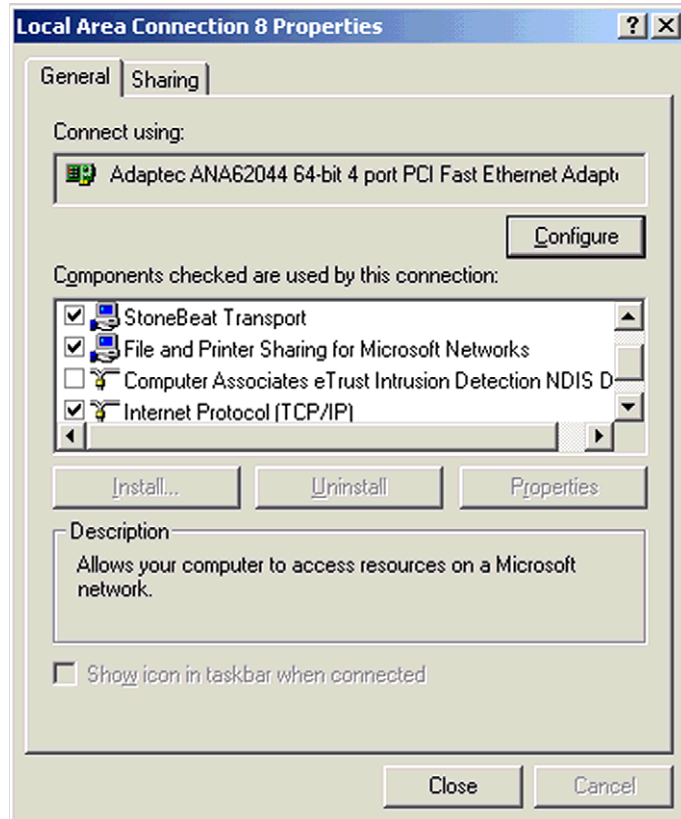
1. Open the interface properties for the monitoring interface by selecting **Start>Settings>Network and Dial-up connections**.
2. Right-click on the **Local Area Connection** icon of the monitoring interface.

ILLUSTRATION 1.7 Properties of the monitoring interface on Windows 2000



3. Ensure that **StoneBeat Transport** and the **Computer Associates eTrust Intrusion Detection** components are selected for this interface.
4. Ensure that the other components are not selected for this interface.
5. Click **OK** to activate the settings.
6. For the other interfaces than the monitoring interface, Right-click on the **Local Area Connection** icon the interface.

ILLUSTRATION 1.8 Other interfaces than the monitoring interface on Windows 2000



7. Ensure that the **Computer Associates eTrust Intrusion Detection** component is not selected. Deselect this component if it is selected.
8. Click **Close** to activate the settings.
9. Repeat the steps 6–8 for all the other interfaces than the monitoring interface.