

VISUAL
messagecenter
powered by **thinkserver**

Cisco PIX/ASA Security

User Guide

ThinkServer **1.6**

tango04
Computing Group
Solutions for Advancing People

Cisco PIX/ASA Security User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2010 Tango/04. All rights reserved.

First Printing: June 2010

Document version: 1.01

Product version: 1.6

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Tango/04.

Trademarks

Any references to trademarked product names are owned by their respective companies.

Technical Support

For technical support visit our web site at www.tango04.com.

Tango/04 Computing Group S.L.

Avda. Meridiana 358, 5 A-B

08027 Barcelona

Spain

Phone: +34 93 274 0051

Table of Contents

Table of Contents iii

How to Use this Guidev

Chapter 1

Introduction 1

1.1. What you will find in this document.....1

Chapter 2

Before You Begin 3

Chapter 3

Cisco PIX/ASA logging configuration 4

3.1. Configure firewall logging.....4

3.1.1. Entering privileged mode4

3.1.2. Entering configuration mode4

3.1.3. Enabling logging.....4

3.1.4. Configuring syslog logging output.....5

3.1.5. Adding timestamp to messages5

3.1.6. Adding Device ID to messages6

3.1.7. Viewing logging configuration6

3.1.8. Logging queue6

3.1.9. Filtering messages using message ID7

3.1.10. Filtering messages using message class.....7

3.1.11. Defining custom messages list.....9

3.1.12. Further information9

Chapter 4

Security Package Configuration 10

4.1. General Parameters 10

4.2. Scopes 11

4.3. Event Categories 12

4.4. Event Exclusion Filters 14

Chapter 5

Common Configuration 15

5.1. Data source configuration 15

5.2. Monitor configuration 16

5.2.1. General settings 17

5.2.2. Filters 17

5.2.3. Default health settings 18

5.2.4. Additional Parameters 19

5.2.5. Default message templates 19

5.2.6. Variables list for Cisco PIX/ASA Security ThinAgent 19

5.2.7. Field Map SmartConsole – ThinkServer 20

5.3. Advanced Monitor Configuration 21

Appendices

Appendix A: Further Information 23

A.1. Using Tango/04 PDF Documentation 23

A.2. Tango/04 University 23

A.3. Contacting Tango/04 25

About Tango/04 Computing Group 26





Legal notice 27

How to Use this Guide

This chapter explains how to use Tango/04 User Guides and understand the typographical conventions used in all Tango/04 documentation.

Typographical Conventions

The following conventional terms, text formats, and symbols are used throughout Tango/04 printed documentation:

Convention	Description
Boldface	Commands, on-screen buttons and menu options.
<i>Blue Italic</i>	References and links to other sections in the manual or further documentation containing relevant information.
<i>Italic</i>	Text displayed on screen, or variables where the user must substitute their own details.
Monospace	Input commands such as System i commands or code, or text that users must type in.
UPPERCASE	Keyboard keys, such as CTRL for the Control key and F5 for the function key that is labeled F5.
	Notes and useful additional information.
	Tips and hints that will improve the users experience of working with this product.
	Important additional information that the user is strongly advised to note.
	Warning information. Failure to take note of this information could potentially lead to serious problems.

Network security is a very important aspect of the overall security of an enterprise. Most businesses today protect their networks using firewalls. Cisco Systems is one of the leaders in networking devices. Among their networking products, are the PIX and ASA firewalls.

Tango/04 has developed a ThinAgent specifically for monitoring these Cisco firewalls. The Cisco PIX/ASA Security ThinAgent monitors each event on your Cisco firewall devices categorizing them and providing detailed information.

The Cisco PIX/ASA Security ThinAgent is based on the syslog ThinAgent and retrieves information via syslog. Syslog is a network protocol that allows a machine to send event notification messages across IP networks to event message collectors - also known as syslog servers or syslog saemons. In other words, a machine or a device can be configured in such a way that it generates a Syslog Message and forwards it to a specific syslog daemon (server) running in another computer. The Cisco PIX/ASA Security ThinAgent is an example of such a service. It processes the incoming UDP messages forwarded by a remote syslog daemon.

Some important features provided with this ThinAgent are:

- Parsed message information
- Custom categorization for messages
- Advanced event filtering
- Full Cisco message explanation
- Cisco suggestion for each message
- Cisco class name and class description for each message

This ThinAgent is compatible with Cisco PIX and ASA devices running software version 7.0, 7.1, 7.2, 8.0 or 8.1. The ThinAgent may also work with devices not running those software versions, but additional features provided by the ThinAgent will not be available.

1.1 What you will find in this document

This User Guide describes the purpose of the Cisco PIX/ASA Security ThinAgent and all variables that come pre-configured. It also explains the minimum configuration settings required to get important security information from your firewalls. For a full description of VISUAL Message Center ThinkServer functionality see the [VISUAL Message Center ThinkServer User Guide](#).

The Cisco PIX/ASA configuration chapter covers the basic configuration you should set on your firewalls, but also explains some other aspects you should take into account for advanced monitoring.

The Cisco Security Package Configuration chapter explains how to configure your filters to reduce the amount of information displayed and how to configure and customize the event categories. This helps to specify the information delivery based on your particular requirements.

The Common Configuration chapter covers the common configuration of data sources and monitors.

The following chapters give a detailed description of the ThinAgent, the default configuration and the variables. You can use these variables to set health conditions, configure actions, create templates, and send messages to VISUAL Message Center SmartConsole. There are also a number of generic variables available to all ThinAgents, which are described in the [VISUAL Message Center ThinkServer User Guide](#).

Furthermore you will find a field map for the ThinAgent describing the values as they appear in the SmartConsole and ThinkServer.

This document only describes the ThinAgents specific to Cisco PIX/ASA. However there are a number of ThinAgents that are also useful when monitoring network devices. For example the Networking ThinAgents include monitors for SNMP and Network. These ThinAgent monitors should also be considered for full monitoring of your networking devices. For details see the [Network ThinAgents User Guide](#).

Chapter 2

Before You Begin

The Cisco PIX/ASA Security ThinAgent relies on the Cisco PIX/ASA security logging. Before using this ThinAgent, make sure your Cisco device is configured to log security information and to send it via syslog to the machine where VISUAL Message Center ThinkServer is running.

The next chapter explains how to configure your firewall to meet the minimum requirements for using the Cisco PIX/ASA Security ThinAgent.

Cisco PIX/ASA logging configuration

Cisco PIX/ASA firewalls have a logging feature. There are different types of logging output, but we will only need to enable the logging output to syslog. In this chapter we will introduce some of the most commonly used commands.

3.1 Configure firewall logging

Configuring the firewall logging is made up of three important steps:

- Step 1.** Enter configuration mode.
- Step 2.** Enable logging.
- Step 3.** Enable and configure the syslog output.

Additionally you can configure other settings, such as create filtering conditions or custom message lists, change facility settings, etc. However, these additional settings are not a requirement for using the Cisco PIX/ASA Security ThinAgent.

3.1.1 Entering privileged mode

To enter the privileged mode, run the `enable` command as per the following example:

```
firewall> enable
Password: *****
firewall#
```

After running the command, the command prompt will change from `>` to `#`.

3.1.2 Entering configuration mode

To enter the configuration mode you must already be in privileged mode and run the `configure terminal` command:

```
firewall# configure terminal
```

After running this command, the command prompt will change from `>` to `(config)`:

```
firewall(config)#
```

3.1.3 Enabling logging

To enable logging on the Cisco Firewall enter privileged mode and run the `logging enable` command:

```
firewall(config)# logging enable
```

To disable logging run the `no logging enable` command:

```
firewall(config)# no logging enable
```

3.1.4 Configuring syslog logging output

To enable logging output to syslog the following actions have to be performed:

Step 1. Set logging level by running the `logging trap` command:

```
firewall(config)# logging trap informational
```



Note

Available levels for syslog logging output are as follows:

- 0 - emergencies - System is unusable
- 1 - alerts - Immediate action is needed
- 2 - critical - Critical conditions exist
- 3 - errors - Error conditions exist
- 4 - warnings - Warning conditions exist
- 5 - notification - Normal, but significant, conditions exist
- 6 - informational - Informational messages
- 7 - debugging - Debugging messages

If a particular syslog level is set, all lower levels are also included. So if you were to set the level in step one as informational, levels 0-5 would also be included.

Step 2. Configure the host to which messages will be sent.

```
firewall(config)# logging host inside 10.1.1.2
```

Step 3. Set the facility number for syslog messages. This step is optional.

```
firewall(config)# logging facility 16
```

The default facility used to send messages is set to 20.



Important

The keyword to enable the syslog output is `trap` as shown in the first command.

By default, port 514 is used to send messages to the syslog server. The port can be changed by using this syntax:

```
logging host interface_name ip_address [tcp[/port] | udp[/port]]
```

To disable the syslog logging output, run:

```
firewall(config)# no logging trap
```

3.1.5 Adding timestamp to messages

Adding a timestamp to messages is very useful to know the exact moment an event occurs on the firewall device. Although this is an optional step, it is highly recommended.

To add the timestamp to messages run the following command:

```
firewall(config)# logging timestamp
```

3.1.6 Adding Device ID to messages

If you are monitoring several devices it might be useful to add the device ID to messages. This helps to determine the host name of the firewall on each message. Although this is an optional step, it is highly recommended.

To add the device id to messages run the following command:

```
firewall(config)# logging device-id hostname
```

You could also set other kind of device id instead of the name. For example you could set any other word as device id by running this:

```
firewall(config)# logging device-id string MyPIXFirewall
```

The example above defines MyPIXFirewall as device id.

3.1.7 Viewing logging configuration

To see the whole logging configuration you can run the `show logging` command:

```
pixfirewall(config)# show logging
```

An example output can be seen below:

```
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Standby logging: disabled
Deny Conn when Queue Full: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level informational, facility 20, 96 messages logged
Logging to inside 10.1.1.2 errors: 2 dropped: 5
History logging: disabled
Device ID: hostname "firewall"
Mail logging: disabled
ASDM logging: level informational, 96 messages logged
```

As you can see, the output gives you all the details about each logging configuration.

3.1.8 Logging queue

Another very important parameter is logging queue. Although this is an optional step, it is highly recommended. The default value for the logging queue is 512 messages.

The queue size can be checked by running the `show logging queue` command:

```
firewall# show logging queue
```

An example output can be seen below:

```
Logging Queue length limit : 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 23 msg(s) most on queue
```

In this example the average number of messages generated by the system is 23 and there is no problem sending them. However, if the value of `xxx msg(s) most on queue` is equal or higher than 512, that means the firewall will have dropped some messages.

You can adjust the queue size manually by running the following command:

```
firewall(config)# logging queue 1024
```

The queue size can range from 0 to 8192 messages. Setting this parameter to 0 means the queue size has no limit (up to available memory).



Warning

If messages are generated faster than they are sent to the syslog server, the firewall starts dropping messages. In order to avoid this the logging queue should be adjusted to a higher value.

3.1.9 Filtering messages using message ID

This is an optional configuration in case you know which messages you want to exclude from syslog logging.

Although the ThinAgent has a filtering configuration (see [section 4.4 - Event Exclusion Filters](#) on [page 14](#)), the filtering explained here in this section, is done in the firewall device, so messages don't ever appear in the syslog. Using this filtering feature could substantially reduce the syslog traffic and ThinAgent resources usage.

In order to filter for specific messages run the `no logging message msg_number` command:

```
firewall(config)# no logging message msg_number
```

To check if a specific message is being logged you can run the following command:

```
firewall(config)# show logging message msg_number
```



Note

This filtering configuration will exclude the message from all logging outputs, not just the syslog output. If you want to filter a particular message from syslog output but log it in another output, you'll have to use the Cisco Security Package filter options. Refer to [section 4.3 - Event Categories](#) on [page 12](#) for further information.

3.1.10 Filtering messages using message class

Besides filtering by message ID number, you can use the message classes as filters. Message classes group several ID numbers together, so if you exclude a class you'll be excluding all message IDs in it. Successfully implementing this filtering method can substantially reduce syslog traffic resulting in better ThinAgent performance and resource usage. The classes are all defined in Cisco's documentation. This step is not required for the general configuration.

For example, classes for software version 8.1 are:

Class	Definition	Message ID (that start with these digits)
auth	User Authentication	109, 113
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
config	Command Interface	111, 112, 208, 308
dap	Dynamic Access Policies	734
e-mail	E-mail Proxy	719
ha	High Availability (Failover)	101, 102, 103, 104, 210, 211, 709
ip	IP Stack	209, 215, 313, 317, 408
ips	Intrusion Protection Service	400, 401, 415
np	Network Processor	319
npssl	NP SSL	725
ospf	OSPF Routing	318, 409, 503, 613
rip	RIP Routing	107, 312
rm	Resource Manager	321
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPSEC	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
webvpn	Web-based VPN	716

Please review the Cisco documentation for your particular software version, since some classes may be different between software versions.

In order to filter a particular message *class* run the following command:

```
firewall(config)# no logging class msg_class
```

3.1.11 Defining custom messages list

To define a list, for example to include all messages with severity 3 (error), and also messages from 611101 to 611323, run the following commands:

```
firewall(config)# logging list my_message_list level 3  
firewall(config)# logging list my_message_list message 611101-611323
```

To send your custom list to syslog output, run the following command:

```
firewall(config)# logging trap my_message_list
```

This step is not required for the general configuration.



Note

The logging list command is only available in software versions 7.2 and later.

3.1.12 Further information

This chapter is not intended to be a full firewall logging configuration guide.

For further information about logging configuration please consult the Cisco documentation for your particular device or software version:

- Cisco Security Appliance System Log Messages, Version 7.0 - Configuring Logging on the Security Appliance:

<http://www.cisco.com/en/US/docs/security/asa/asa70/system/message/logconf.html>

- Cisco Security Appliance System Log Messages, Version 7.1 - Configuring Logging on the Security Appliance:

<http://www.cisco.com/en/US/docs/security/asa/asa71/system/message/logconf.html>

- Cisco Security Appliance System Log Messages, Version 7.2 - Configuring Logging and SNMP:

<http://www.cisco.com/en/US/docs/security/asa/asa72/system/message/logconf.html>

- Cisco Security Appliance Command Line Configuration Guide, Version 8.0 - Monitoring the Security Appliance:

<http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/monitor.html>

- Cisco Security Appliance Command Line Configuration Guide, Version 8.1 - Monitoring the Security Appliance:

<http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html>

- PIX/ASA 7.x and later with Syslog Configuration Example (Cisco Document ID: 63884):

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00805a2e04.shtml

Security Package Configuration

In order to take advantage of all Cisco PIX/ASA Security ThinAgent features you have to configure some parameters for the Cisco Security Package. This is a Python module that adds advanced logic to the ThinAgent. The Security Packages Configurator is used to configure the parameters of the package. To run this tool go to **Start > Programs > Tango04 > VISUAL Message Center ThinkServer > Tools > Security Packages Configurator**.

The tool allows you to configure other security packages as well, but you should only use the options available in the *Cisco Pix & Asa Security* tab.

**Important**

The Security Packages Configurator requires the Windows .NET framework version 2.0 or later to be installed.

4.1 General Parameters

In this tab you can configure the logging feature of the Cisco Security module. These options should only be used in case errors or incorrect behavior occur in order to determine the underlying reason.

There are 2 different trace options:

- **General Trace:** logs all information related to the Python Cisco Security module and all its activities.
- **Garbage Collector:** logs information related to objects in memory just for profiling and internal debugging.

For each trace option, the level of detail and method of output can be selected.

There are 3 possible output methods:

- **File:** writes logging information to the following file:

```
%ThinkServerDir%\PythonLib\Lib\TSExtensions\CiscoSecurity\CiscoSecurityTrace.log
```

- **Windows Debugging Service:** uses the OutputDebugString to write information. You can capture this information with tools such as Sysinternals DebugView.
- **Both:** uses both of the above mentioned output methods.

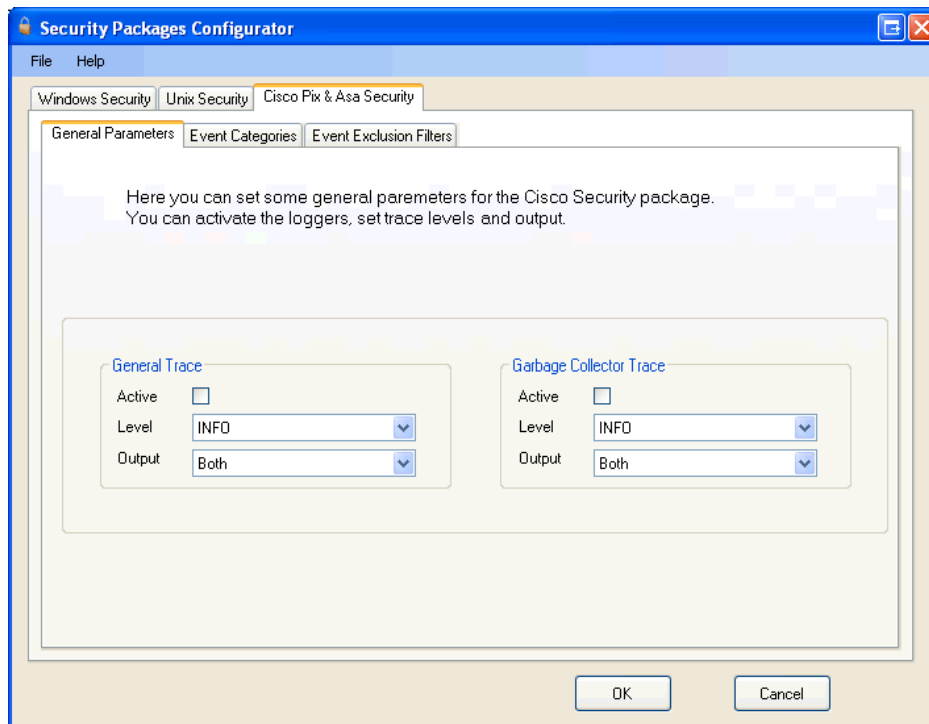


Figure 1 – Security Packages Configurator: Cisco Pix & Asa Security tab



Warning

Do not activate these traces unless a Tango/04 Technical Consultant asks for it. These traces can generate a lot of information and in some cases might reduce the performance of the ThinAgent.

4.2 Scopes

Before explaining the other settings in the Security Packages Configurator, you should first understand the *scope* concept used with this ThinAgent.

Imagine this is the network layout you are monitoring:

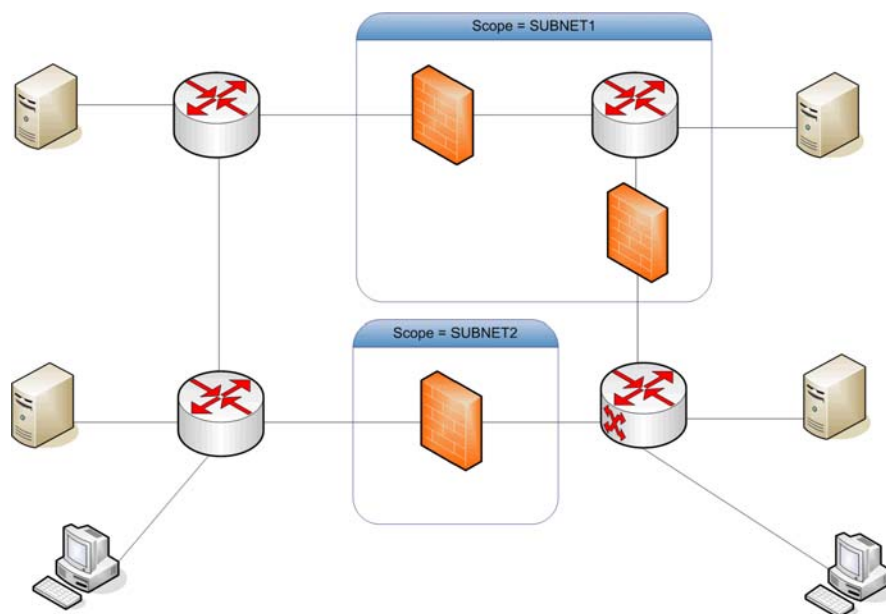


Figure 2 – An example network layout containing 2 scopes

In this case, the network has 3 firewall devices. Two of the devices have been defined to belong to a scope named `SUBNET1` and the other to the scope `SUBNET2`.

As you can see, a scope is just a logical way to group your firewall devices in your network. Scopes can be assigned any name which fits the monitoring structure but the name is limited to one word only. Later in this user guide you'll see how to define different scopes on your network for assigning firewalls to.

So, why should you use scopes?

Custom scopes can be used to provide different categories and subcategories for different devices or groups of devices. Furthermore, creating different exclusion lists for different scopes allows for more powerful filtering. Finally, scopes allow you to create a more descriptive set of BusinessViews in the VISUAL Message Center SmartConsole by using filters with the scope name variable in order to clearly group devices. Scopes are also very useful for implementations in networks with a large number of firewall devices.

The default scope in the Cisco Security package is named `GENERAL`. This default scope is used if there aren't any other scopes configured. Furthermore, Tango/04 gives you some standard categories and subcategories for this default scope. However, using the default scope means that devices are not being grouped in any way.

4.3 Event Categories

The Event Categories tab allows you to create and configure different categories and subcategories for each defined scope. The categories and subcategories are used to group message IDs. If the default scope is selected, the monitor will automatically make all categories and subcategories default as well.

To configure scope and categories for message IDs:

- Step 1.** From the Scope drop down list pick a predefined scope.
- Step 2.** From the Category drop down list pick a predefined category.
- Step 3.** From the SubCategory drop down list pick a predefined subcategory.
- Step 4.** In the Version drop down list, either pick a version number or select *all* to include all available version numbers.

Step 5. Finally add Message IDs in the ID List section for the messages to be included.

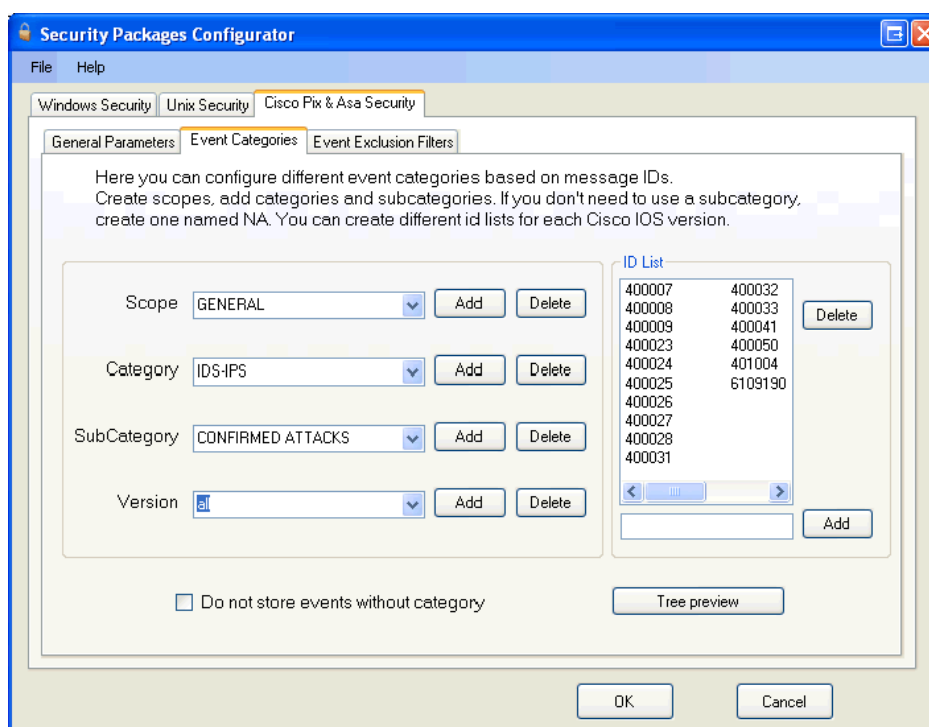


Figure 3 – Security Packages Configurator: Event Categories tab

Alternatively, new entries can be added by simply typing a new name in the drop down list field and clicking the Add button. In the same manner, changes to predefined properties can be made using the Delete button.

When all four options have been defined message IDs can be added to the ID List section to the right. To add IDs simply enter the ID number in the input field and click the Add button. Likewise, message IDs can easily be removed from a scope by clicking the Delete button.

There might be an instance where a message only belongs to a category but no subcategories. In such a case, the proper category should be assigned but the subcategory NA should be used (i.e. not available).

Categories can be applied to any of the available software versions and to specific ones as well. For example, you might want to have a different list of message IDs for an older software version than the latest one. To do this you would simply assign the same scope, category and subcategory to the IDs but then assign separate versions.

A particular message might not have a category or a subcategory, likely because it would not be in any list. Such messages will be assigned category NA and subcategory NA. You can easily exclude all those messages by selecting the *Do not store events without category* checkbox.



Note

Using this quick exclusion filter can decrease the amount of messages in the solution. But be careful, because important messages could be excluded, simply because you didn't assign the IDs to any category or subcategory or didn't know they existed.

To get a better overview of the event categories another view is provided. This view can be accessed by clicking the **Tree Preview** button. The *Tree Preview* window will appear, displaying the complete list of categories and subcategories with their complete list of IDs as seen in [Figure 4](#). A hierarchical view of

the tree is displayed in the window. Items can be expanded to view the complete message list of each criteria.

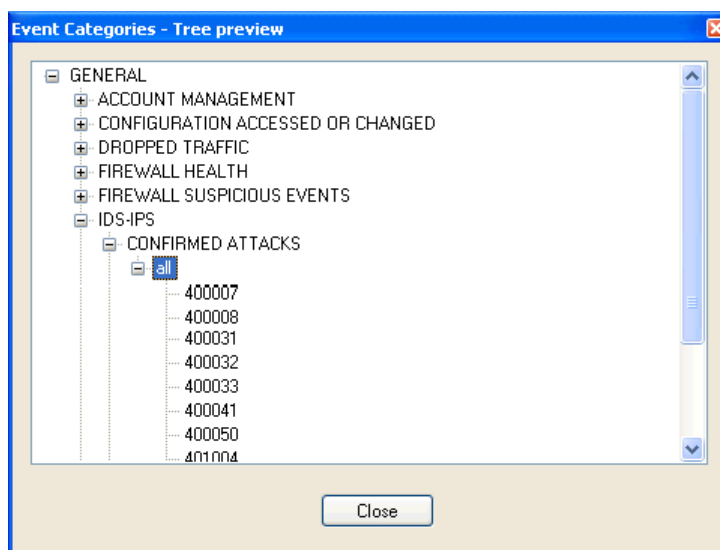


Figure 4 – Security Packages Configurator: Tree Preview

4.4 Event Exclusion Filters

Cisco firewall devices can generate a large amount of messages in a short period. Because of this it is very important to carefully filter messages. As seen in [Chapter 3 - Cisco PIX/ASA logging configuration](#) on [page 4](#), messages can be filtered directly in the firewall device. Additionally, the Cisco Security Package lets you add more specific filters for each scope and software version. Filters can be set up by using the message ID or severity.

If you want to create global filters, not just for a particular scope or version, use the combination of scope GENERAL and version ALL. All the IDs and severities you add to these will be used as global filters.

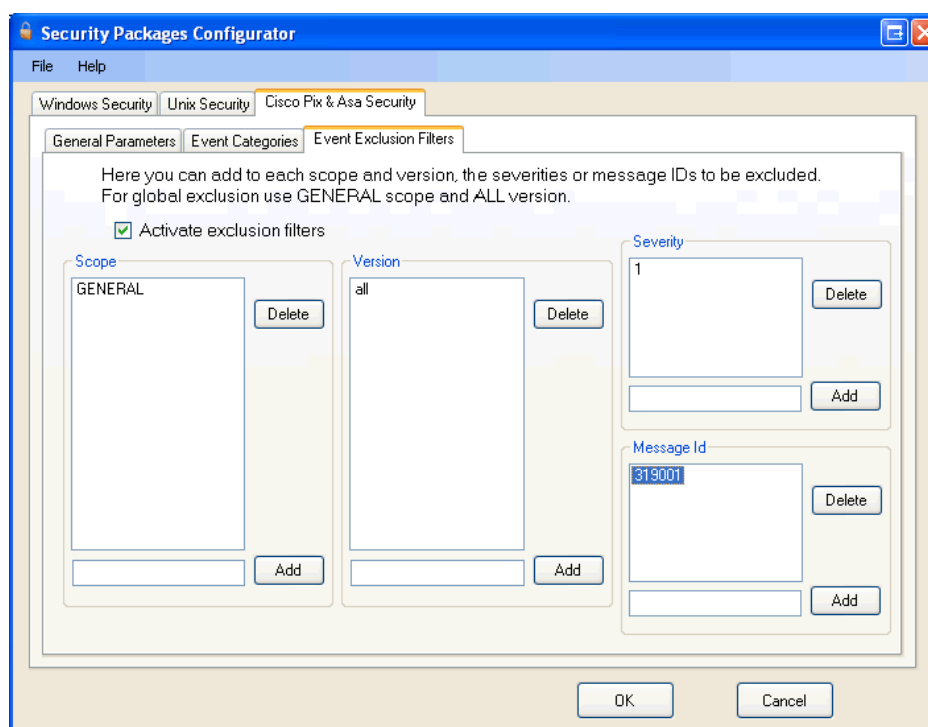
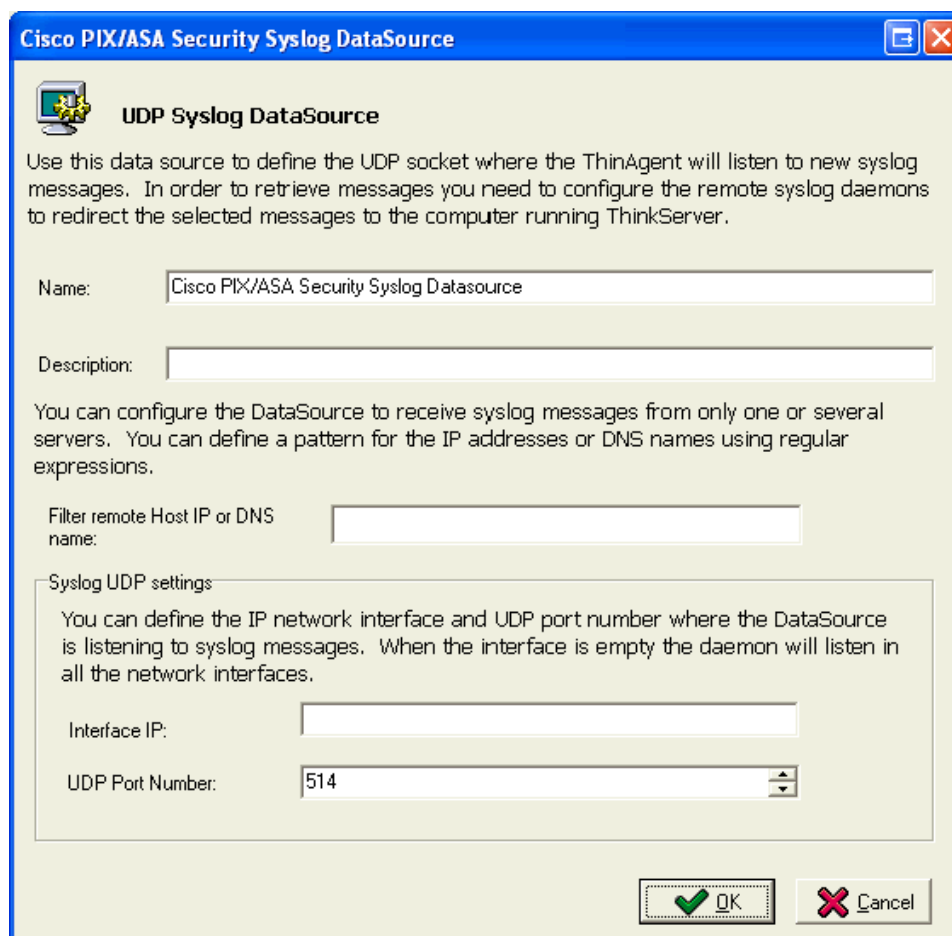


Figure 5 – Cisco Pix & Asa Security: Event Exclusion Filters tab

Now that the firewall device is set up properly and security packages have been configured the ThinAgent itself needs to be configured. How about an intro here? About the ThinAgent?

5.1 Data source configuration

A few parameters need to be set to properly configure the Cisco PIX/ASA Security Syslog DataSource. This data source works the same way the Linux / Unix data source does (to see more details about this please refer to the *Unix / Linux Security Agent User Guide*).



The screenshot shows a dialog box titled "Cisco PIX/ASA Security Syslog DataSource". The main heading is "UDP Syslog DataSource". Below the heading is a paragraph of text: "Use this data source to define the UDP socket where the ThinAgent will listen to new syslog messages. In order to retrieve messages you need to configure the remote syslog daemons to redirect the selected messages to the computer running ThinkServer." There are two input fields: "Name:" with the value "Cisco PIX/ASA Security Syslog Datasource" and "Description:" which is empty. Below this is another paragraph: "You can configure the DataSource to receive syslog messages from only one or several servers. You can define a pattern for the IP addresses or DNS names using regular expressions." There is an input field for "Filter remote Host IP or DNS name:". Below that is a section titled "Syslog UDP settings" with a paragraph: "You can define the IP network interface and UDP port number where the DataSource is listening to syslog messages. When the interface is empty the daemon will listen in all the network interfaces." There are two input fields: "Interface IP:" which is empty and "UDP Port Number:" with the value "514". At the bottom right are "OK" and "Cancel" buttons.

Figure 6 – Edit data source: Cisco PIX/ASA Security Syslog DataSource

Main information

By default the ThinAgent name is used as the name of the data source, but it can be changed to suit your monitoring needs. Additionally, a more detailed description of the data source can be added if required.

The data source can be configured to receive message only from one or several servers using the IP address or DNS filter. The default data source configuration however will receive all the events and send them to every monitor attached to it.

Configuration variables and default settings		Description
Name	Cisco PIX/ASA Security Syslog DataSource	Use the default name provided or enter a new name for the data source. It is very useful to add the device name you are monitoring to help quickly identifying where problems occur.
Description		Enter a description of the data source
Filter Remote Host IP or DNS name		Optional value to filter the host you want to receive messages from. This filter should be a regular expression, for example: 192.168\.\1\1

Syslog UDP Settings

You can configure the IP network interface where the UDP service is going to listen for messages (only if you want to use a specific interface for this task) and the UDP port. In the default configuration the *Interface IP* field is left blank, indicating that the daemon will listen on all the available IP interfaces.

Configuration variables and default settings		Description
Interface IP		IP network interface where the UDP service is going to listen.
UDP port number	514	Port number used to bind service.

Several data sources can be configured to use the same interface IP and UDP ports, but only one socket will be opened for each configured UDP port. The messages will be redirected to all the data sources depending on the IP Address/DNS Name filter defined in its configuration.

5.2 Monitor configuration

Once you have selected a data source, the monitor configuration window opens.



Figure 7 – Cisco PIX/ASA Security Monitor configuration

5.2.1 General settings

First, enter a name for the monitor and add a description. By default the monitor uses the ThinAgent name, but the name can be changed to better suit your monitoring needs.

Configuration variables and default settings		Description
Name	Cisco PIX/ASA Security Monitor	Enter a name for your monitor
Description		Enter a description for your monitor

To change to another data source click the **Select Data Source** button and select a data source from the list that appears. To edit the currently selected data source click the **Edit Data Source** button.

5.2.2 Filters

There are four filters available: Facility, Severity, Source IP/Name and Message Filter. All of the filters use the regular expression format.

**Warning**

We don't recommend changing the Message Filter. The filter is prepared to get only PIX or ASA messages. If the filter is changed, you might lose messages or receive messages coming from other, non PIX/ASA devices. This could unnecessarily increase the load on your network and devices.

The Source IP/Name filter should be used to filter messages coming from a particular device. For example to only get messages coming from IP 192.168.1.10, you have to set the expression as 192\.168\.1\.10.

5.2.3 Default health settings

By default Health is set to:

- **Critical** if message severity is *emergency*, *alert*, *critical* or *error*, or if message category is IDS-IPS and subcategory is CONFIRMED ATTACK.
- **Warning** if message severity is *warning*.
- **Minor** if message severity is *notice*.
- **Success** in all other cases.

The default health rules can be changed to better meet your monitoring needs. Any of the defined categories and/or subcategories can be used with the Security Packages Configurator or any other variable to change health conditions.

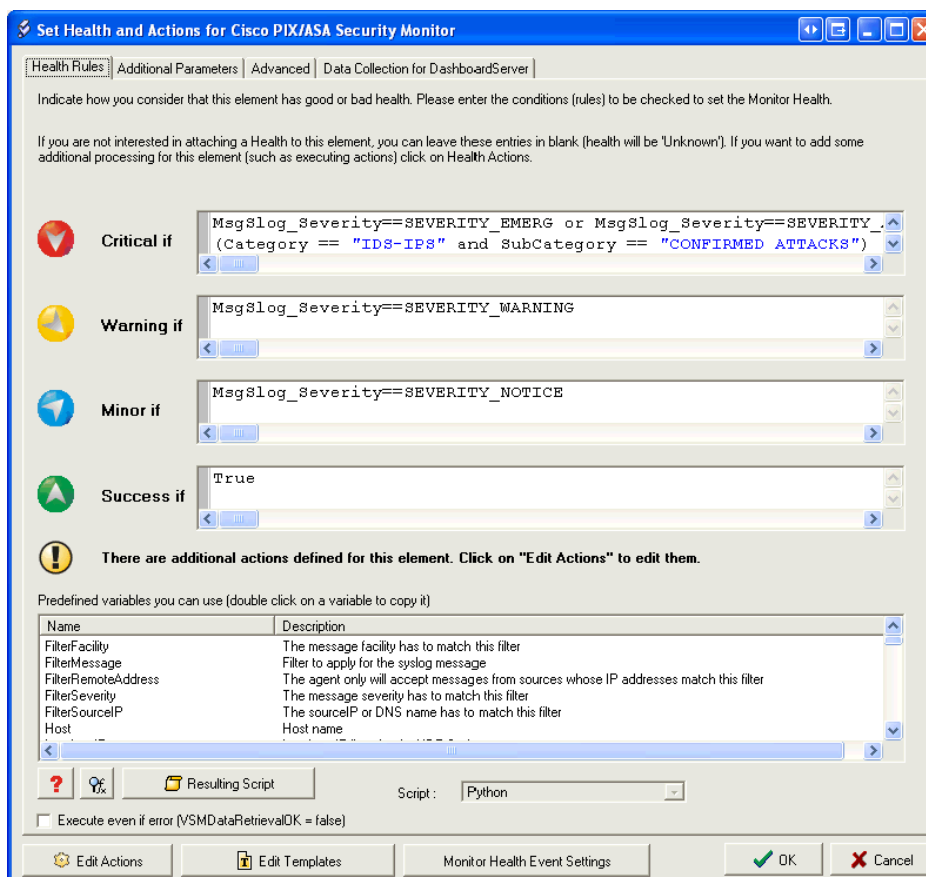


Figure 8 – Set Health and Actions: Health Rules

5.2.4 Additional Parameters

The Additional Parameters tab allows you to set an initial value for the variables that are passed to the monitor script. There are two very important parameters you need to configure: Scope and SoftwareVersion.

By default every monitor uses the GENERAL scope and software version 7.1. If you are grouping devices using scopes (see [section 4.2 - Scopes](#) on [page 11](#)), put the value of the scope the device belongs to.

The software version in the value field should be the version of the firewall device being monitored. It is important that this value is correct because additional information provided by the ThinAgent to the messages depends on the device software version. If the SoftwareVersion parameter is deleted, version ALL will be used. This allows the monitor to assign categories and subcategories to the events, but additional information (explanation and suggestion) will not be provided.

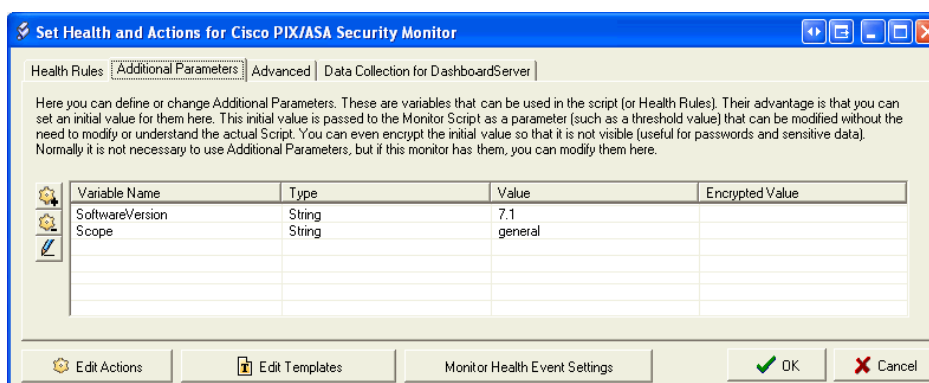


Figure 9 – Set Health and Actions: Additional Parameters

5.2.5 Default message templates

With the Cisco PIX/ASA Security ThinAgent the message templates health wizard is not used at all. Messages are sent by the ThinAgent exactly like they are received as any changes made to the template are ignored.

If you wish to change the received messages those changes should be made using Python in the Advanced tab in Health and Actions settings. Furthermore, variables should not be changed if predefined VISUAL Message Center SmartConsole configuration and reports are to be used.

5.2.6 Variables list for Cisco PIX/ASA Security ThinAgent

Here you can see a list of most important variables for Cisco PIX/ASA Security ThinAgent. These variables can be used for example for setting health values.

Variable	Description
Host	Hostname
IPAddress	Host IP Address
MsgSlog_DateTime	Message Date and Time
MsgSlog_Facility	Message Facility
MsgSlog_FacilityDescription	Message Facility Description
MsgSlog_Severity	Message severity

Variable	Description
MsgSlog_SeverityDescription	Message severity description
MsgSlog_FullMessage	Full raw message
Category	Message Category
SubCategory	Message Subcategory
MsgExplanation	Message explanation (from Cisco System Messages documentation)
MsgSuggestion	Message suggestion (from Cisco System Messages documentation)
CiscoSevertyDesc	Cisco Message severity description
CiscoTimeStamp	Cisco Message date and time
CiscoClass	Cisco Message Class
CiscoClassDesc	Cisco Message Class Description
CiscoFacility	Cisco Message Facility
CiscoSeverityNum	Cisco Message severity
MsgID	Cisco Message ID
CiscoMessage	Cisco Message (parsed message text)

5.2.7 Field Map SmartConsole – ThinkServer

The ThinkServer sends a message to the SmartConsole using the following default variables order:

SmartConsole	ThinkServer	Description
VAR01	VSMScriptID	Script name
VAR02	Host	Hostname
VAR03	IPAddress	Host IP Address
VAR04	MsgSlog_DateTime	Message Date and Time
VAR05	MsgSlog_Facility	Message Facility
VAR06	MsgSlog_FacilityDescription	Message Facility Description
VAR07	MsgSlog_Severity	Message severity
VAR08	MsgSlog_SeverityDescription	Message severity description
VAR09	MsgSlog_FullMessage	Full raw message
VAR10	Category	Message Category
VAR11	SubCategory	Message Subcategory

SmartConsole	ThinkServer	Description
VAR12	MsgExplanation	Message explanation (from Cisco System Messages documentation)
VAR13	MsgSuggestion	Message suggestion (from Cisco System Messages documentation)
VAR14	CiscoSevertyDesc	Cisco Message severity description
VAR15	CiscoTimeStamp	Cisco Message date and time (DD/MM/YYYY hh:mm:ss format. This variable may not appear depending on the message format)
VAR16	CiscoClass	Cisco Message Class
VAR17	CiscoClassDesc	Cisco Message Class Description
VAR18	CiscoFacility	Cisco Message Facility
VAR19	CiscoSeverityNum	Cisco Message severity
VAR20	MsgID	Cisco Message ID
VAR21	CiscoMessage	Cisco Message (parsed message text)
VAR22	----	Cisco Message date and time (with syslog format)
VAR23	----	Cisco Device ID

**Note**

Variable 1 cannot be changed, but all others can. Keep in mind that changing this default variables order can affect the SmartConsole Cisco PIX/ASA default configuration.

5.3 Advanced Monitor Configuration

The ThinAgent uses a Python module named Cisco Security. This module gives the ThinAgent advanced features in order to parse Cisco PIX and ASA messages, add useful information, categorize messages, etc.

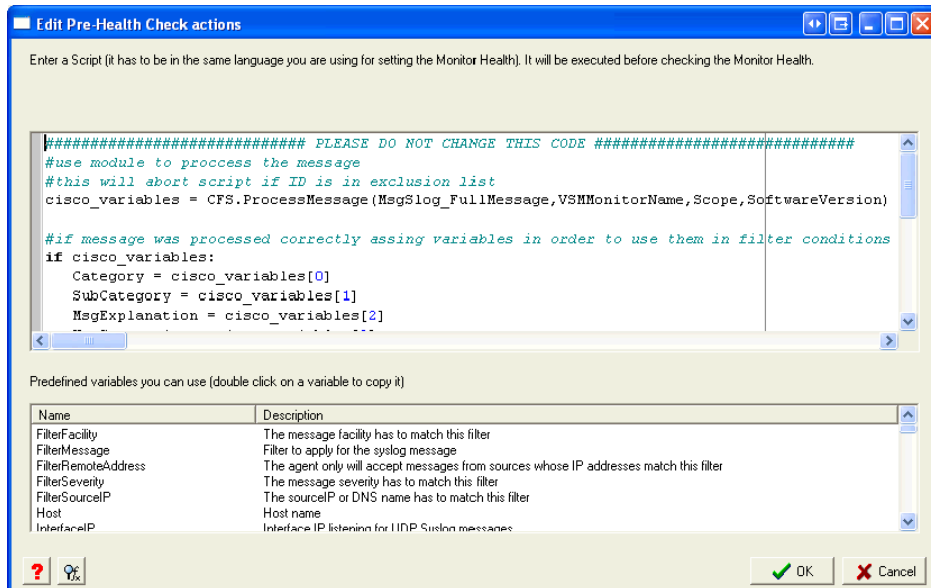


Figure 10 – Editing Pre-Health Check actions

The ThinAgent comes by default with entries made with Python code. These entries can not be changed as it will affect monitor performance. However, new code can be added to the existing one to enhance the actions or to accomplish more advanced functions with the monitor.

Appendix A

Further Information

A.1 Using Tango/04 PDF Documentation

Tango/04 documentation is available directly from the Tango/04 solutions DVD.

To open the Tango/04 documentation that is provided in PDF files use Adobe Acrobat Reader. Acrobat Reader lets you view, search, and print the documentation. You can download Acrobat Reader for free from the Adobe Web site (<http://www.adobe.com>).



Tip

We advise printing PDF documentation for easy reference. Please ensure you familiarize yourself with a products user guide before attempting to use the product.

To access PDF documents on the DVD:

- Step 1.** Navigate to a *product suite* (VISUAL Message Center for example) and click on the **Product Documentation** link to open a list of all the User Guides available for that product suite. The list contains direct links to the documents in PDF format.
- Step 2.** Alternatively, you can navigate within the DVD menu to a particular *product* and click on the **Product Documentation** link to open the User Guide in PDF format for that product.

A.2 Tango/04 University

In a continuous effort to provide all users of Tango/04 technologies with high quality training and education, Tango/04 Computing Group presents the new training program open to partners and users worldwide.

Tango/04 University is aimed at providing Tango/04 users and partners with the most effective tools and knowledge to manage Tango/04 technologies and products and use them at their highest potential.

Attendance of the training course and passing the related exams is mandatory in order to qualify as Tango/04 Business Partner for the technology area covered by the course, and will offer you important benefits such as:

- Tango/04 Official Certifications - Tango/04 partners will be required to have a number of certified consultants, depending on the Business Partner Level

- Exploit the full potential of Tango/04 technologies - Solutions such as VISUAL Message Center and VISUAL Security Suite are very broad solutions that feature much functionality. Knowing all these functions and how to use them is key to getting the most out of the product
- Integration with other solutions - Tango/04 is constantly growing: knowing the new products and agents may allow you to integrate other parts of the IT infrastructure into Tango/04 Solutions
- Tango/04 Business Partners will learn how to effectively deploy a monitoring project in order to obtain the maximum effectiveness and customer satisfaction.

Participants' profile: Consultants, System Administrators, operators and technical staff, with knowledge of Windows, iSeries, Linux and Unix systems who will be involved in managing or deploying Tango/04 technology.

Pre-requisites: Being Tango/04 Business Partner or Tango/04 Customer.

A.3 Contacting Tango/04

North America

Tango/04 North America
One Phoenix Mill Lane - Suite 201
NH 03458 Peterborough
USA

Phone: 1-800-304-6872 / 603-924-7391
Fax: 858-428-2864
sales@tango04.net
www.tango04.com

Italy

Tango/04 Italy
Viale Garibaldi 51/53
13100 Vercelli
Italy

Phone: +39 0161 56922
Fax: +39 0161 259277
Contact: Ferdinando Caccianotti
info@tango04.it
www.tango04.it

Sales Office in Switzerland

Tango/04 Switzerland
18, Avenue Louis Casañ
CH-1209 Genève
Switzerland

Phone: +41 (0)22 747 7866
Fax: +41 (0)22 747 7999
Contact: Mr. Jean-Philippe Fourche
contact@tango04.net
www.tango04.fr

Sales Office in Peru

Barcelona/04 PERÚ
Centro Empresarial Real
Av. Víctor A. Belaúnde 147, Vía Principal 140
Edificio Real Seis, Piso 6
L 27 Lima
Perú

Phone: +51 1 211-2690
Fax: +51 1 211-2526
info@barcelona04.net
www.barcelona04.com

EMEA

Tango/04 Computing Group S.L.
Avda. Meridiana 358, 5 A-B
08027 Barcelona
Spain

Phone: +34 93 274 0051
Fax: +34 93 345 1329
info@tango04.net
www.tango04.com

Sales Office in France

Tango/04 France
La Grande Arche
Paroi Nord 15ème étage
92044 Paris La Défense
France

Phone: +33 01 40 90 34 49
Fax: +33 01 40 90 31 01
Contact: Mr. Jean-Philippe Fourche
contact@tango04.net
www.tango04.fr

Latin American Headquarters

Barcelona/04 Computing Group SRL (Argentina)
Avda. Federico Lacroze 2252, Piso 6
1426 Buenos Aires Capital Federal
Argentina

Phone: +54 11 4774-0112
Fax: +54 11 4773-9163
info@barcelona04.net
www.barcelona04.com

Sales Office in Chile

Barcelona/04 Chile
Nueva de Lyon 096 Oficina 702,
Providencia
Santiago
Chile

Phone: +56 2 234-0898
Fax: +56 2 2340865
info@barcelona04.net
www.barcelona04.com

About Tango/04 Computing Group

Tango/04 Computing Group is one of the leading developers of systems management and automation software. Tango/04 software helps companies maintain the operating health of all their business processes, improve service levels, increase productivity, and reduce costs through intelligent management of their IT infrastructure.

Founded in 1991 in Barcelona, Spain, Tango/04 is an IBM Business Partner and a key member of IBM's Autonomic Computing initiative. Tango/04 has more than a thousand customers who are served by over 35 authorized Business Partners around the world.

Alliances



Partnerships

IBM Business Partner

IBM Autonomic Computing Business Partner

IBM PartnerWorld for Developers Advanced Membership

IBM ISV Advantage Agreement

IBM Early code release

IBM Direct Technical Liaison

Microsoft Developer Network

Microsoft Early Code Release

Awards



The information in this document was created using certain specific equipment and environments, and it is limited in application to those specific hardware and software products and version and releases levels.

Any references in this document regarding Tango/04 Computing Group products, software or services do not mean that Tango/04 Computing Group intends to make these available in all countries in which Tango/04 Computing Group operates. Any reference to a Tango/04 Computing Group product, software, or service may be used. Any functionally equivalent product that does not infringe any of Tango/04 Computing Group's intellectual property rights may be used instead of the Tango/04 Computing Group product, software or service

Tango/04 Computing Group may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

The information contained in this document has not been submitted to any formal Tango/04 Computing Group test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility, and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. Despite the fact that Tango/04 Computing Group could have reviewed each item for accurateness in a specific situation, there is no guarantee that the same or similar results will be obtained somewhere else. Customers attempting to adapt these techniques to their own environments do so at their own risk. Tango/04 Computing Group shall not be liable for any damages arising out of your use of the techniques depicted on this document, even if they have been advised of the possibility of such damages. This document could contain technical inaccuracies or typographical errors.

Any pointers in this publication to external web sites are provided for your convenience only and do not, in any manner, serve as an endorsement of these web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: iSeries, iSeriese, iSeries, i5, DB2, e (logo)@Server IBM ®, Operating System/400, OS/400, i5/OS.

Microsoft, SQL Server, Windows, Windows NT, Windows XP and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries. UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group. Oracle is a registered trade mark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of other companies.