Viewing Entity Information

Introduction

The Info page provides information about how an aggregate (or host) is behaving. This page shows the services the aggregate is a client and a server of, as well as the number of events the aggregate is involved in. The system presents this information in both a table format and as a pie graph.

Info page layout

The Info page displays a traffic graph that shows the total traffic the aggregate or host has been involved in for the selected time frame and pie charts that show how the entity is being used. These include the following:

<table>
<thead>
<tr>
<th>Chart Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Server Services</td>
<td>The top services the host is a server of.</td>
</tr>
<tr>
<td>Top Client Services</td>
<td>The top services the host is a client of.</td>
</tr>
<tr>
<td>Top Servers Used</td>
<td>The top servers the host is using.</td>
</tr>
<tr>
<td>Top Clients Served</td>
<td>The top clients the host is serving.</td>
</tr>
<tr>
<td>Top Events</td>
<td>The ongoing events the host is involved in.</td>
</tr>
<tr>
<td>Top Vulnerabilities</td>
<td>The hosts that SiteProtector determines are vulnerable.</td>
</tr>
</tbody>
</table>

Reference: See “Additional SiteProtector information” on page 138 for a complete description.

Table 47: Entity information pie charts

Navigating on the Info page

Standard navigation and time controls apply on the Info page.

Reference: See “Navigating the Proventia Network ADS Web User Interface” on page 12.

Updating the entity information shown

The system displays the aggregate or host address at the top of the page and lists any groups they contain or are members of. The system displays the information using the default Last time frame that covers the most recent 24 hours. You can update the information by changing the timeframe.

Changing the timeframe

To change the timeframe for the entity information displayed:

1. Click the clock icon to toggle to the desired time frame.

   Reference: See “Selecting the timeframe” on page 17.

2. Type or select the period for which you want to see information.

3. Click UPDATE.

Viewing the entity info tables

The tables below the graphs show these top entities with additional details, appropriate to the type of table. The Other rows include a Show all link that you can click to expand the table to see the other services that weren’t active enough to be in the top number shown. The tables display the client, server, and service names as a link that you can click to navigate to either another Info page or the Explore page that shows the host information.

Note: You can only expand one Other row at a time. When you expand a new row, the current row collapses.
If you have SiteProtector configured, the Info page provides additional entity information. This includes SiteProtector information incorporated into the Events graph and table, and an additional table that shows SiteProtector vulnerabilities for that host. The Events table incorporates SiteProtector data in the display of ongoing events the host is involved in. It shows the number of times that host has been involved in the violating traffic for that event. You can click the event name to navigate to its Event Details page.

The Vulnerability table shows any hosts that SiteProtector considers vulnerable. It scans hosts to find which types of attacks a host is vulnerable to on certain services. When a host uses that service, SiteProtector tags it as a vulnerable host. Hosts listed on this page might require further investigation.

Important: SiteProtector information is not displayed when the query contains more than 255 IP addresses. The system displays a message when this occurs.
Chapter 18

Creating and Viewing Reports

Overview

Introduction
Proventia Network ADS continually collects detailed host-to-host traffic data. The Reports pages allow you to generate reports from this traffic data to help you monitor how your network is being used. You can either create one-time reports or report templates that you can use to generate standard reports at specifically scheduled times.

Reports pages
The Reports menu contains three pages:

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a report or report template.</td>
</tr>
<tr>
<td>List</td>
<td>View or delete existing reports.</td>
</tr>
<tr>
<td>Manage</td>
<td>Update existing report templates or recreate a report.</td>
</tr>
</tbody>
</table>

Table 48: Report pages

User access on the Reports pages
Administrators and analysts can perform all actions described in this chapter. Users can create and view reports, but they can only delete reports they create.

In this chapter
This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Reports:Create Page</td>
<td>140</td>
</tr>
<tr>
<td>Types of Reports</td>
<td>141</td>
</tr>
<tr>
<td>Creating Reports</td>
<td>142</td>
</tr>
<tr>
<td>Viewing Listed Reports</td>
<td>144</td>
</tr>
<tr>
<td>Viewing Reports</td>
<td>146</td>
</tr>
<tr>
<td>Managing Scheduled Reports</td>
<td>148</td>
</tr>
</tbody>
</table>
Chapter 18: Creating and Viewing Reports

About the Reports: Create Page

Introduction
The Reports: Create page allows you to create a one-time report or a report template that you can schedule to run on a regular basis.

Create page layout
Proventia Network ADS displays the name of each report type as a button along the left side of the page. Some report types are menus that contain a list of reports. When you choose a report type, the system displays the corresponding pane for you to complete that includes the information appropriate to the report type.

Note: By default, if you do not select a page when you select the Reports tab, the system displays the List page.

Pane sections
Each report pane has three sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>Use to customize the data you want the system to include in the report.</td>
</tr>
<tr>
<td>Filter</td>
<td>Use to choose filter options to limit the report results to specific entities (host, services, etc.)</td>
</tr>
<tr>
<td>Schedule</td>
<td>Use to choose the time and frequency Proventia Network ADS generates reports (report or template).</td>
</tr>
</tbody>
</table>

Table 49: Report pane sections

Using the report panes to customize data
Use the report form to customize the report. You can generate higher-level, overview types of reports, or very specific reports that include the type of entity, how many entities you want to see, and a corresponding time period in which to see the data.

The following examples show how you can build upon a basic report to include more specific data and to generate a recurring report:

- To create a basic version of a host Traffic report, choose the top ten hosts for the last 24 hours.
- To create a more advanced version of the same Traffic report, add a filter that limits the results to hosts within a specific group object.
- To schedule the Traffic report, set it to generate daily and email the report to your system administrator.

About report templates
Templates allow you to create recurring reports that your network users can re-run. They also allow you to schedule how often you want the system to automatically generate them and who you want the system to email the reports to.
Types of Reports

Introduction
This topic provides a description of the types of reports you can generate to monitor your network activity and to help you understand how it is being used.

Report types
You can create many types of reports from the traffic that Proventia Network ADS collects:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recent Templates</td>
<td>The most recently generated reports or used templates. When you select a recent template, the system creates the report.</td>
</tr>
<tr>
<td>Traffic</td>
<td>A traffic report with the specified top entities, counts, and traffic over a specific time period.</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>The top x number of hosts, users, TCP services, or UDP services, and destination ports on your network.</td>
</tr>
<tr>
<td>Drilldown Summary</td>
<td>The network's top traffic contributors. This report shows the top three services on the network, then the top three servers of those services, then the top three clients of each of the servers (for those services).</td>
</tr>
<tr>
<td>Details</td>
<td>The detailed traffic information for either a host, service, or group object for a specified time period.</td>
</tr>
<tr>
<td>Entity to Entity</td>
<td>The traffic between two entities (host addresses, groups, IP addresses, or CIDRs) for the specified time period.</td>
</tr>
</tbody>
</table>

Table 50: Types of reports

How Proventia ADS matches traffic for entity-to-entity reports
For entity-to-entity reports, when the system looks for matching traffic in the database, it tries to match traffic in the following order:

1. IP addresses
2. CIDR blocks
3. hostnames
4. group names

If the system does not recognize the value you enter in one of the fields as an existing IP, CIDR, or host name, it assumes it is a group. If it is not a group, but the system does not recognize what you entered, it displays an "invalid group" error message.
Chapter 18: Creating and Viewing Reports

Creating Reports

Introduction

This topic describes options for creating reports, and gives the procedures for creating reports and report templates.

Limiting results

When limiting results to a specific entity or to traffic between specific entities, you can add multiple filter entries. The system combines each filter entry in an AND (not OR) fashion. You can select the entities from the displayed lists or use the free-form option to enter your own.

Procedure

To create a report:

1. Select Report ➔ Create.
   The Reports: Create page appears.
2. Select the type of report or report name you want to create from the list.
   The corresponding pane appears.
3. In the Setup section, select one of the following from the Show list:
   - Top to see the highest traffic generators, and then select the number of top entities to include.
   - Bottom to see the lowest traffic generators, and then select the number of bottom entities to include.
4. Verify the correct entity is selected from the list.
5. Select the time period you want to use from the During list.
6. In the Filter section, select the type of entity you want to limit the results to from the Limit to list.
7. Type the corresponding values in the box.
8. For Traffic Between filters, do one of the following:
   - Select two entities from the lists.
   - Select Freeform, and then type in the value.
   - Enter the value as any valid IP address, CIDR, host name, or group name.
   - Click the form icon to redisplay the list of entities.
9. Do one of the following:
   - Click the plus sign (+) to add additional filters.
   - Click the minus sign (-) to remove an existing filter.
10. In the Schedule section, choose one of the following from the Create as list:
    - report to generate a one-time report, and then move to Step 15.
    - template to generate a recurring report.
11. For a template, type a unique name for the template in the Named box.
    Caution: If you create a report and assign it the same name as an existing template, the new report replaces the template.
    You can include spaces in report names, but you cannot include the underscore character (_).
12. Select how often you want the system to create the report from the Repeat list.
13. Select the time you want the report created from the At (times) lists.

14. Type the report recipients email addresses in the Email to box.
   
   Tip: Enter multiple addresses as a comma-separated list of email addresses.

15. Click CREATE.

   The system displays the report status sheet to show when your report is complete.

   Reference: See “Viewing Listed Reports” on page 144 for a description of the report status sheet.
Chapter 18: Creating and Viewing Reports

Viewing Listed Reports

Introduction

This topic describes the status sheet, the Reports List page, and it provides the instructions for reviewing and exporting report data.

Viewing the List Page

The Reports List page shows a table that lists all reports in the system including completed reports, queued reports, and those other users have created.

Report maximums

Proventia Network ADS saves and displays the most recent 500 reports, 50 per page. These include any reports you set up as a template to run on a recurring schedule. Once your list exceeds 500, it deletes the oldest reports. The system also deletes reports once they are six months old. The table lists each report as a row that includes an option button, the system-generated ID number, a description of the report, the status, and (for administrative users) a delete icon.

Report status

The system displays the status as either Completed (with the time it was completed), Executing, or Queued.

Reference: See Table 51, below, for information about what each status means.

Status sheet

When you run a report, Proventia Network ADS returns you to the List page and displays the status sheet. The status sheet displays a table that shows the following:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The system-assigned number for this report.</td>
</tr>
<tr>
<td>Description</td>
<td>The system-generated description or the user-assigned template name for the report. The description is displayed as bold text if it has not been viewed.*</td>
</tr>
<tr>
<td>Status</td>
<td>Shows one of the following:</td>
</tr>
<tr>
<td></td>
<td>* Executing for those currently running.</td>
</tr>
<tr>
<td></td>
<td>* Queued for those waiting to be run.</td>
</tr>
<tr>
<td></td>
<td>* Completed with the completion time for reports that have finished running and are available for viewing.</td>
</tr>
<tr>
<td>Selection check box</td>
<td>Use to stop or cancel a running or queued report.</td>
</tr>
</tbody>
</table>

Table 51: Report status

Viewing the Report

Once the report is completed, you can view it.

To view the report:

- Click the description link.

Reference: See “Viewing Reports” on page 146.
Navigating on the Reports: List page

When the amount of reports exceeds the amount that the system can display on one page, Proventia Network ADS displays the page navigational tools in the upper-right corner of the page that you can use to page forward and backward or navigate to a particular page.

Reference: See “Navigating the Proventia Network ADS Web User Interface” on page 12.

Deleting or canceling a report

To delete a completed report or cancel a report that is running:

1. Select the check box on the report row.
2. Click DELETE.
Viewing Reports

Introduction

The View page displays a selected report’s content with its corresponding tables and graphs.

About report icons

This page displays sheet icons next to some of the table entries. These icons link to additional report data for that entry.

Example: If you are viewing a top services graph and HTTP is listed in the table below the graph, then you can click the form icon next to HTTP to see the top servers of HTTP traffic.

Important: Any time you create a sub report by clicking the report icon, Proventia Network ADS displays the most recent data that corresponds to the report period. For example, if you are looking at a report for the top services for the last 15 minutes that is 3 hours old (was run 3 hours ago), and you click the form icon for the top servers of HTTP, the system displays the top HTTP servers for the past 15 minutes, not for the original time period (3 hours ago).

Using the report icons

The report icons at the bottom of the Reports: View page allow you to use report data in a number of ways:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detach</td>
<td>Opens and displays the report in a new browser window.</td>
</tr>
<tr>
<td>Email</td>
<td>Sends the report and any comments you enter to the designated recipients.</td>
</tr>
<tr>
<td>Print</td>
<td>Opens the print window for you to specify the print properties and print the report.</td>
</tr>
<tr>
<td>Recreate</td>
<td>Allows you to change the report’s settings, and then generate the report.</td>
</tr>
<tr>
<td>Export icons</td>
<td>Exports the report data in the selected format.</td>
</tr>
</tbody>
</table>

Table 52: Report icons

Using report pop-up menus

If there are multiple types of drill-down data for one table entry, the system displays a pop-up menu that lists the different types of data for you to choose from. Choose the type of information from the pop-up menu (for example, Top Hosts) to creates the report with the additional data.

Reference: “Status sheet” on page 144 for information about that page.

About monthly data in reports

When you are looking at reports that show data for monthly time periods, the date range the system displays might not always correspond to the time period the data shows. The system stores monthly data in one month boundaries that correspond to how long you have been using Proventia Network ADS.

Example: If you initialized your system on Jan. 13, today is May 15, and you run a report for the “last six months,” the report Proventia Network ADS generates shows the date range as Jan. 1 - May 14. However, since the system has no data from before January 13, it really shows data for the period of Jan. 13 - May 14.
Viewing Reports

Emailing a report

To email reports, you must have an SMTP server set.

To email a report:

1. Click the Email report icon.
   The email window opens.
2. Type the recipients email address in the Email to box.
   Tip: Enter multiple recipients as a comma-separated list of email addresses.
3. Type any comments you want to send in the Comments box.
4. Click SEND.

Recreating a report

Recreating reports allows you change the report settings. This includes renaming, further defining, or scheduling a report.

To recreate a report:

1. Click the Recreate report icon.
   The Create page appears with the report pane prepopulated with the current information.
2. Update any report settings, and then click CREATE.
   Reference: See "Creating Reports" on page 142 for these instructions.

Exporting reports

To export a report:

1. Do one of the following:
   - Click the CSV icon to export the report data in a CSV file.
   - Click the PDF icon to export the report data in a PDF file
   - Click the XML icon to export the report data in an XML file.
2. Save the file according to the choices your browser displays.
   In some cases, a new window might open that displays the data.
Chapter 18: Creating and Viewing Reports

Managing Scheduled Reports

Introduction
This topic describes the Reports: Manage page and the actions you can perform.

About the Reports: Manage page
Templates allow you to define a report and set it up to automatically run at specified times. The Manage page shows all existing report templates and allows you to change a template's settings.

Reference: See “Creating Reports” on page 142 for instructions to run a report template without making changes to the current settings.

Navigating on the Reports: Manage page
When the number of report templates exceeds the amount that the system can display on one page, use the page navigational tools in the upper-right corner of the page to page forward and backward or navigate to a particular page.

Reference: See “Navigating the Proventia Network ADS Web User Interface” on page 12 for additional information.

Report templates table
The table shows the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Shows the system-assigned ID number of the report.</td>
</tr>
<tr>
<td>Description</td>
<td>The user-assigned report name or system-assigned name.</td>
</tr>
<tr>
<td>Period</td>
<td>How often the system creates the report.</td>
</tr>
<tr>
<td>Email</td>
<td>The email addresses for all recipients scheduled to receive the report.</td>
</tr>
<tr>
<td>Selection check box</td>
<td>Use to delete reports.</td>
</tr>
</tbody>
</table>

Table 53: Report templates table

Changing report template settings
To change a report's settings:
1. Click the template Description link.
   The Create page appears with the report pane prepopulated with the current information.
2. Update any report settings.
   Reference: See “Creating Reports” on page 142 for these instructions.
3. Click CREATE.

Deleting a template
To delete a template:
1. Select the check box on the template row.
2. Click DELETE.
   ADS removes the template, but saves all reports already generated from the template.
Appendixes
Appendix A

Using PFCAP Expressions

Overview

Introduction

Some of the Web user interface pages allow you to search by entering PFCAP expressions for the system to use to match traffic. You can enter the traffic values, such as a specific type of traffic (TCP), the name of a group object, or a specific host that you want to search for in the Search text box, and the system returns all matching traffic. The system displays the expression it uses to match traffic at the top of the page, similar to a page title.

In this appendix

This appendix contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searching by Using PFCAP Expressions</td>
<td>152</td>
</tr>
<tr>
<td>Example Expressions</td>
<td>155</td>
</tr>
</tbody>
</table>
Appendix A: Using PFcap Expressions

Searching by Using PFcap Expressions

Introduction

This topic describes how to construct a PFcap expression and how Proventia Network ADS evaluates them.

Pages that allow PFcap searching

You can search by entering PFcap expressions on the following pages:

- Explore
- Policy
- Host Detail
- Alert Detail
- Flows

You can also use the search boxes on these pages to further filter the matching results, adding to the existing search expression. When you enter an additional value in the text box and click SEARCH, the system appends and updates the existing expression and shows the new matching traffic. In addition to adding Search expressions, you can CLEAR the Search text box to enter a new PFcap expression and start again.

Joining expressions

When entering PFcap expressions that specify the traffic you want Proventia Network ADS to match, use the following to join or describe expressions:

- OR—joins expressions together, either can be true. You can also enter multiple search values as a comma-separated list.
- AND—joins expressions together, both are true.
- NOT—negates an expression.
- (parentheses)—establishes precedence for complicated expressions.

How Proventia ADS evaluates expressions

Proventia Network ADS evaluates rules with ANDs and ORs with equal precedence, and it evaluates them from left to right. If you are using a combination of adjacent objects with AND and OR conjunctions, use parentheses so the system knows the explicit order.

If you have not specified an AND or an OR conjunction, Proventia Network ADS uses an OR if the objects are the same type and an AND if they are different types. This is called merging.

How ADS evaluates objects

Table 54 shows the types of objects. Objects that appear in the same row would be ORd together, and objects on different rows would be ANDd together.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>IP address, group object</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address, group object</td>
</tr>
<tr>
<td>Both source and destination</td>
<td>IP address, group object</td>
</tr>
<tr>
<td>Source</td>
<td>Port, port object</td>
</tr>
<tr>
<td>Destination</td>
<td>Port, port object</td>
</tr>
</tbody>
</table>

Table 54: How objects are merged
Case 1:04-cv-01199-SLR     Document 381-6      Filed 07/10/2006     Page 17 of 36

Searching by Using PFCAP Expressions

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Protocol</td>
</tr>
<tr>
<td>None</td>
<td>TCP Flags</td>
</tr>
<tr>
<td>None</td>
<td>ICMP type</td>
</tr>
<tr>
<td>None</td>
<td>ICMP code</td>
</tr>
</tbody>
</table>

Table 54: How objects are merged (Continued)

Examples

Proventia Network ADS would interpret this expression:

```
port 22 1.1.1.1 2.2.2.2 port 333
```

as this:

```
(port 22 or port 333) and (1.1.1.1 or 2.2.2.2)
```

and it would interpret this expression:

```
group webservers portgroup www-ports port 333 1.1.1.1
```

as this:

```
(portgroup 1.1.1.1 or port 333) and (group webservers or 1.1.1.1)
```

Expressing direction

You can also use a variety of synonyms to express direction for IPs, groups (host and port), ports, and users.

To specify a source, you can enter any of the following specifiers:

- `src`
- `source`
- `from`
- `client`

Direction examples

The following examples show how to express directions.

Entering “src 1.2.3.4” is equal to entering “from 1.2.3.4”.

To specify a destination, you can enter any of the following specifiers:

- `dst`
- `dest`
- `destination`
- `to`
- `target`
- `server`

If you do not set a direction for IP addresses, host groups, or users, Proventia Network ADS uses both source and destination.
Appendix A: Using PF_RING Expressions

Example: If you entered IP address "1.2.3.4", the system interprets it as:

(src 1.2.3.4) or (dst 1.2.3.4)

If you do not set a direction for ports or port groups, Proventia Network ADS uses the destination.

Example: If you entered "port 33", the system interprets it as:

(dst port 33)

Example: If you entered "portgroup www-ports" the system interprets it as:

(dst portgroup www-ports)
Example Expressions

Introduction
This topic provides examples of the types of PFCAP expressions you can enter to search the Proventia Network ADS traffic database and to create rules.

Group objects
For groups, enter the group name, or you can enter the group specifier, followed by the group name. To search for a group whose name contains spaces, you must surround the group name in quotation marks (for example, "web servers").

To search for a group called webservers, enter one of the following:

webservers

group webservers

In this case, the system matches any source or destination that is part of the webservers group.

Note: If you use the "group" specifier but the system cannot find a valid group by that name, it looks for that name as a port group.

Port objects
For port groups, enter either the port group name, or you can enter the portgroup or group specifiers, followed by the port group name.

To search for a port group called www-ports, enter one of the following:

- www-ports
- portgroup www-ports
- group www-ports

In this case, the system matches any source or destination that is part of the www-ports port group.

Hosts or CIDRs
For hosts, enter either the IP address, the group name, or specify whether it is the source or destination by typing any of the source or destination specifiers listed in the section "Expressing Direction," followed by the IP address or group name. You can also enter networks in CIDR notation (IP / (slash) number) or by specifying that it is a host IP by entering the keyword host.

To search for a network, enter:

198.168.1.0/24

The system matches any source or destination that is part of the 198.168.1.0/24 network.

To further filter the results to only show the network as a source, you can enter the src specifier before the network in the Search text box:

src 198.168.1.0/24
Appendix A: Using PFCAP Expressions

Ports

Enter ports with the keyword port followed by the port name or number. You can enter a port range by entering port followed by the beginning port number, .. (dot dot) and the port at the end of the range.

You can also specify whether you want the system to match ICMP types and ICMP codes as either numbers or ranges, by entering the icmptype or icmpcode specifiers, and then following with either a number or a number range.

To search for port 22, enter:

```
port 22
```

To specify destination port 22, enter:

```
dst port 22
```

To search for port ranges 0-1024, enter:

```
port 0..1024
```

You can also enter descriptions such as ssh as a quick search for TCP and port 22, or you can enter the same search as:

```
TCP and port ssh
```

To search for web traffic on IP address 1.2.3.4, port 22, enter:

```
1.2.3.4 port 22
```

To search for any traffic with a destination IP address of 1.2.3.4 and a destination port of either 22 or 80, enter:

```
dst 1.2.3.4 port 22, www
```

To match either source 1.2.3.4 or source 1.2.3.5 and destination group accounting on port 80, enter:

```
(src 1.2.3.4 or src 1.2.3.5) and dst accounting port 80
```

The system matches any traffic from either 1.2.3.4 or 1.2.3.5 with a destination port of 80 in the accounting group.

To search for ICMP Echo Request traffic, enter:

```
icmp type 8
```

Protocols

Enter protocols by entering the keyword proto followed by the protocol name or number.

To search for protocol 6 traffic, enter one of the following:

- `tcp`
- `proto tcp`
- `proto 6`
Example Expressions

Using Specifiers for Duplicate Values

If you enter a value in the search text box that is ambiguous (could match multiple types of traffic), the system displays a message to inform you of this and includes all traffic for the values and adds the appropriate specifiers.

Example:

If you have a group named “webservers” and you also have a port group named “webservers,” and you enter “webservers” in the Search box without specifying whether you want results for the group or the port group, the system returns traffic for both and inserts the specifiers (group and portgroup) in the results. In this case, it would display:

“group webservers” or “portgroup webservers”

You can then delete whichever value you do not want and click SEARCH and Proventia Network ADS updates the page to show only the requested matching traffic.
Appendix A: Using PFCAP Expressions
Glossary

ACL (Access Control List)—A list composed of rules and filters stored in a router to allow, deny, or otherwise regulate network traffic based upon network parameters such as IP addresses, protocol types, and port numbers.

address—A coded representation that uniquely identifies a particular network identity.

Analyzer—A centralized device that accepts event messages from one or more Collectors and performs second-order traffic analysis in order to identify and visualize potential attacks.

anomaly—An event or condition in the network that is identified as an abnormality when compared to a predefined illegal traffic pattern.

API (Application Programming Interface)—A well-defined set of function calls providing high-level controls for underlying services.

ARP (Address Resolution Protocol)—A protocol for mapping an IP address to a physical machine address.

ADOS (Anomaly Detection System)—The Proventia Network ADS Operating System. ADOS manages many of the low-level system processes and communication facilities.

ASCII (American Standard Code for Information Interchange)—A coded representation for standard alphabetic, numeric, and punctuation characters.

Authentication—An identity verification process.

Behavior—Who hosts on your network talk to and how they talk to them. When Proventia Network ADS sees behavior that does not match existing rules, it sends event notifications to the operator for action.

Block hole routing—A technique to route traffic to null interfaces that can never forward the traffic.

CAR (Committed Access Rate)—A tool for managing bandwidth that provides the same control as ACL with the additional property that traffic can be regulated based on bandwidth usage rates in bits per second.

CIDR (Classless Inter-Domain Routing)—Method for classifying and grouping Internet addresses.

cflowd—Developed to collect and analyze the information available from NetFlow. It allows the user to store the information and enables several views of the data. It produces port matrices, AS matrices, network matrices, and pure flow structures.
Collector—A device that gathers network information from adjacent routers via NetFlow™ and performs first-order traffic analysis. Anomalous events are compressed into event messages that are then sent to the listening Analyzer.

customer—An ISP, ASP, or enterprise user of ISS technology.

d
Dark IP—Regions of the IP address space that are reserved or known to be unused.

DNS (Domain Name System)—A system that translates numeric IP addresses into meaningful, human-consumable names and vice-versa.

DoS (Denial of Service)—An interruption of network availability typically caused by malicious sources.

e
encryption—The process by which plain text is scrambled in such a way as to hide its content.

exploit—Tools intended to take advantage of security holes or inherent flaws in the design of network applications, devices, or infrastructures.

f

firewall—A security measure that monitors and controls the types of packets allowed in and out of a network, based on a set of configured rules and filters.

i

ICMP (Internet Control Message Protocol)—An IP protocol that delivers error and control messages between TCP/IP enabled network devices, for example, ping packets.

IP (Internet Protocol)—A connectionless network layer protocol used for packet delivery between hosts and devices on a TCP/IP network.

IP Address—A unique identifier for a host or device on a TCP/IP network.

L

LAN (Local Area Network)—A typically small network that is confined to a small geographic space.

m

MAC (Media Access Control) Address—A unique hardware number associated with a networking device.

MPLS (Multiprotocol Label Switching)—A packet-switching protocol developed by the Internet Engineering Task Force (IETF) initially to improve switching speeds, but other benefits are now seen as being more important.

NetFlow—A technology developed by Cisco Systems, Inc. that allows routers and other network devices to periodically export information about current network conditions and traffic volumes.
NTP (Network Time Protocol)—A protocol that is used to synchronize clock times in a network of computers.

P

PFCAP (Flow Capture) Filter—A string-based, regular expression used to filter traffic on your Proventia Network ADS Analyzer appliance.

packet—A unit of data transmitted across the network that includes control information along with actual content.

class—A secret code used to gain access to a computer system.

policy—The set of behaviors that network operators determine to be acceptable or unacceptable for their network and are the standard that Proventia Network ADS measures host behaviors against.

protocol—a well-defined language used by networking entities to communicate with one another.

R

RADIUS (Remote Authentication Dial In User Service)—A client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

refinement—the process of continually gathering information about prior anomalous activity seen.

report—a periodic summary of anomalous activity on the network.

router—a device that connects one network to another. Packets are forwarded from one router to another until they reach their ultimate destination.

rules—the traffic flows that are either allowed or denied that serve as the standards Proventia Network ADS uses to determine when behavior matches the current policy.

S

SNMP (Simple Network Management Protocol)—A standard protocol that allows routers and other network devices to export information about their routing tables and other state information.

SSH (Secure Shell)—A command line interface and protocol for securely getting access to a remote computer. SSH is also known as Secure Socket Shell.

T

TACACS+ (Terminal Access Controller Access Control System +)—An authentication protocol common to Unix networks that allows a remote access server to forward a user’s logon password to an authentication server to determine whether that user is allowed to access a given system.

Target—a victim host or network of a worm or other malicious denial of service (DoS) attacks.

TCP (Transmission Control Protocol)—A connection-based, transport protocol that provides reliable delivery of packets across the Internet.

TCP/IP—a suite of protocols that controls the delivery of messages across the Internet.
UDP [User Datagram Protocol]—An unreliable, connectionless, communication protocol.

UNC [Universal Naming Convention]—A standard which originated from the UNIX for identifying servers, printers, and other resources in a network. A UNC path precedes the name of the computer with double slashes or backslashes. The path within the computer are separated with a single slash or backslash, as follows:

in UNIX, //servername/path
in Windows and DOS, \\servername\path

Index

symbols 108

numerics 1 151

a

about
  Activity page 112
  built-in behaviors 20
  configuring alerts 21
  Explore page 96
  group contents 51
  Group Objects Configuration page 50
  Notification Objects Configuration page 38
  notification types 40
  Policy page 58
  Services page 90
  severity settings 60
accepting
  alerts 136
Accounts
  table 28
ACLs
  editing numbers 122
  generating 115
  viewing 122
Activity
  table 112
Activity page
  about 112
adding
  email notifications 41
  group objects 51
  notification objects 41
  port objects 81
  services 91
  SNMP notifications 41
  syslog notifications 42
  time objects 47
  user accounts 29
ADS
  how determines severity 80
  status messages 129
ADS status
  viewing 128
aggregated data
  example 103
  searching 102
  viewing 102
alert
  maximums 112
  types of 22
alert details
  exporting 136
  viewing 135
alert types
  severity 60
alerting
  built-in behaviors 64
  icons 22
  maximums 125
  table 84, 114
alerting terms
  definitions 20
Alerts
  table 125
alerts
  accepting 136
  clearing 115, 136
  exporting 116
Summary page 125
Analyzers
  defined 5
  appliance 128
ATF
  configuring alerting 87
  ATF behavior rules
    how ADS generates 58
  ATF settings
    configuring 71
behavior
  tables 58
behaviors
deleting 113
Between
timeframe 100
breadcrumb trail
  using 14
built-in behaviors
  about 20
  alerting 64
  configuring alerting 65
descriptions 62
canceling
  enforcement 121
  reports 145
choosing
  passwords 29
clearing
  alerts 115, 136
Collectors
defined 5
configuring
  alerts 21
  ATF settings 71
  general settings 86
  group objects 49
Microsoft SQL 34
  passive host discovery 36
policy settings 57
rate alerting 69
  services 89
SiteProtector communication 35
  SQL settings 34
time objects 45
configuring alerting
  ATF 87
  built-in behaviors 65
  user-defined rules 67
controls
  navigation 14
collections, typographical
  in commands ix
  in procedures ix
  in this manual ix
  creating
  group objects 108
  port objects 108
  reports 142
  rules 117
definitions
  alerting terms 20
deleting
  behaviors 113
  group objects 55
  port objects 84
  reports 145
  services 91
  templates 148
  time objects 48
  users 31
descriptions
  built-in behaviors 62
  links 100
Details
  host table 133
details
  hosts 133
  services 133
Duration
timeframe 99
editing
  ACL numbers 122
  group objects 51
  notification objects 41
  port objects 81
  rules 117, 119
time objects 47
  user accounts 29
email
  notifications 40
  reports 147
  email notifications
    adding 41
  enforcement
    canceling 121
  enforcing
    worms 121
  event details
    viewing 114
example
aggregated data 103
Explore page 
about 98
exporting 
alert details 136
alerts 115
flows 107
group objects 53
host relationships 105
port objects 82
reports 147
services 91
system configuration 87

f
flood descriptions 62
flows 
details table 106
exporting 107
searching 107
viewing 106

g
general settings 
configuring 86
generating 
ACLs 115
graph controls 
using 98
group objects
adding 51
configuring 49
creating 108
deleting 55
editing 51
exporting 53
importing 53
merging 53
naming 51
Group Objects Configuration page 
about 50
groups 
about contents 51
user 28

h
help

using 15
host 
details 133
host relationship

details table 104
host relationships
exporting 105
searching 104
viewing 104
host scan descriptions 82
hosts
searching 98

icons
alerting 22
importing 
group objects 53
port objects 82
SiteProtector groups 53
Info page 137
SiteProtector 138
information
sorting 14
initial setup
recommended 23
Internet Security Systems
technical support x
Web site x

i
Last
timeframe 99
link 
descriptions 100
log details
viewing 132

m
managing
policy rules 111
reports 148
maximums
alert 112
alerting 125
report 144
merging

group objects 53
<table>
<thead>
<tr>
<th>Port objects</th>
<th>82</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs</td>
<td>39</td>
</tr>
<tr>
<td>saving</td>
<td>38</td>
</tr>
<tr>
<td>viewing</td>
<td>38</td>
</tr>
<tr>
<td>Microsoft SQL</td>
<td>34</td>
</tr>
<tr>
<td>configuring</td>
<td>34</td>
</tr>
<tr>
<td>mode</td>
<td>5</td>
</tr>
<tr>
<td>standalone</td>
<td>5</td>
</tr>
<tr>
<td>two-tier</td>
<td>5</td>
</tr>
<tr>
<td>monitoring</td>
<td>123</td>
</tr>
<tr>
<td>network</td>
<td></td>
</tr>
<tr>
<td>activity summary</td>
<td>127</td>
</tr>
<tr>
<td>notification object</td>
<td>38</td>
</tr>
<tr>
<td>notification objects</td>
<td>41</td>
</tr>
<tr>
<td>rules</td>
<td>117</td>
</tr>
<tr>
<td>time objects</td>
<td>47</td>
</tr>
<tr>
<td>navigation</td>
<td></td>
</tr>
<tr>
<td>controls</td>
<td>14</td>
</tr>
<tr>
<td>network</td>
<td></td>
</tr>
</tbody>
</table>

| Choosing       | 29 |
| PFCAP Expressions |    |
| Searching with | 151|
| PFCAP expressions |    |
| searching      | 98 |
| using          | 151|
| Policy page    |    |
| about          | 58 |
| policy settings|    |
| configuring    | 57 |
| pop-up menus   |    |
| reports        | 146|
| Port objects   |    |
| table          | 60 |
| port objects   |    |
| adding         | 81 |
| deleting       | 84 |
| editing        | 81 |
| exporting      | 82 |
| importing      | 82 |
| merging        | 82 |
| port scan descriptions | 82 |

| Rates         |    |
| Alerting      |    |
| configuring   | 69 |
| Rates         |    |
| over          | 69 |
| under         | 69 |
| Rebooting     |    |
| system        | 87 |
| recent changes|    |
| viewing       | 59 |
| recommended   |    |
| initial setup | 23 |
| recreating    |    |
| reports       | 147|
| refreshing    |    |
| pages         | 14 |
| report        |    |
| canceling     | 145|
| deleting      | 145|
| maximums      | 144|
| pop-up menus  | 146|
| templates     | 140|
| Report aggregate |    |
| using         | 51 |
| Report icons  |    |
| using         | 146|
| Reports       |    |
| creating      | 142|
emailing 147
exporting 147
managing 148
recreating 147
types 141
viewing 144, 146
restoring
  system configuration 87
rule
  status 113
rules
  creating 117
  editing 117, 119
  managing 111
  naming 117

S
saving
  MIBs 39
  searching
    aggregated data 102
    flows 107
    host relationships 104
    hosts 98
    PFCAP expressions 98
    services 98
    traffic 95, 98
    using timeframes 99
See 28
service
  details 133
services
  adding 91
  configuring 89
  deleting 91
  exporting 91
  searching 98
  table 90
  uploading 91
Services page
  about 90
severity
  alert types 60
  how ADS determines 60
  values 129
severity settings
  about 60
SiteProtector
  configuring communication with 35
  Info page 138
  notifications 40
SiteProtector groups
  importing 53
SNMP
  about agent community 88
  notifications 40
SNMP notifications
  adding 41
sorting
  information 14
SQL settings
  configuring 34
standalone
  mode 5
Status
  table 128
status
  ADS 129
  appliance 126
  monitoring network 123
  rule 113
  status sheet 144
summary
  network activity 127
Summary page
  alerts 125
  navigation links 124
  viewing 124
syslog
  notifications 40
  syslog notifications
  adding 42
system
  exporting configuration 87
  rebooting 87
  restoring configuration 87
  System events 63
table
  Accounts 28
  Activity 112
  alerting 54, 114
  Alerts 125
  Details 133
  flow details 106
  host relationship details 104
  notification object 38
  Port objects 80
  Report templates 148
  Services 90
graph controls 98
help 15
PFCAP expressions 151
report aggregate 51
report icons 146

V
values
severity 129
viewing
ACLs 122
ADS status 128
alert details 135
entity information 137
event details 114
flows 108
host relationships 104
log details 132
MIBs 38
recent changes 59
reports 144, 148
Summary page 124

W
Web site, Internet Security Systems x
worm descriptions 62
worms
enforcing 121

U
under
rate alerts 69
uploading
service files 91
user
groups 28
user accounts
adding 29
editing 29
User Accounts page
navigating
User Accounts page 28
user-defined rules
configuring alerting 67
users
deleting 31
using
breadcrumb trail 14
**Internet Security Systems, Inc. Software License Agreement**

**THIS SOFTWARE PRODUCT IS LICENSED IN OBJECT CODE AND IS LICENSED, NOT SOLD. BY INSTALLING, ACTIVATING, COPYING OR USING THIS SOFTWARE PRODUCT YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT ("LICENSE"), EXCEPT AS MAY BE MODIFIED BY AN APPLICABLE ISS LICENSE NOTIFICATION OR ISS SOFTWARE LICENSES, AS PROVIDED IN THE USER DOCUMENTATION ACCOMPANYING THE SOFTWARE PRODUCT, OR AS FURTHER SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPY AND/OR PRODUCT IDENTIFICATION COPY, AS SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPY AND/OR PRODUCT IDENTIFICATION COPY, AS SET FORTH BELOW."**

1. **License** - Upon your payment of the applicable fees and ISS delivery to you of the applicable license notification, Internet Security Systems, Inc. ("ISS") grants to you, for the term indicated in the above license notification, the right to install, use, copy, and distribute the software product specified in the above license notification, only on the specific network configuration for which a license was purchased, and only for the number of users and/or the number and type of devices upon which it may be installed, used, copied, downloaded, or otherwise used by you, provided that you only use the software product for its intended purpose and in accordance with this license agreement. You may not exceed the number or type of devices authorized for use under the license notification. The use of a network address or other unique identifier for the purpose of limiting the number of devices on which the software product may be used is prohibited.

2. **Migration Utilities** - For Software ISS marks or data and migration utilities ("Migration Utilities") that shall be provided with the Software Product, ISS grants to you the right to use such Migration Utilities only for the express purpose of migrating such Software from one network configuration to another, provided that you only use the Migration Utilities for the purpose of migrating the Software from one network configuration to another and not for any other purpose.

3. **Support Services** - ISS reserves the right to provide support services, but you are subject solely to the manufacturer's terms and conditions that will be provided with support services. Support services are provided at ISS’s option and may be terminated by ISS at any time for any reason.

4. **Beta Software** - ISS provides beta software products ("Beta Software") for evaluation purposes only. ISS grants to you the right to install, use, store, copy, and distribute Beta Software only for evaluation purposes, but you may not exceed the number or type of devices authorized for use under the license notification. You may not resell, sublicense, modify, or incorporate Beta Software into another product without the express written consent of ISS. Beta Software is not subject to any warranty or support services.

5. **Evaluation License** - ISS is providing Licensee with the Software subject to the terms of this Evaluation License Agreement. Licensee agrees to use the Software only for the purposes set forth in the License Agreement. Licensee further agrees to return all copies of the Software to ISS upon expiration of the Evaluation License or upon request from ISS. Licensee acknowledges that the Beta Software may contain defects, produce erroneous and unintended results and outcomes, or otherwise fail to perform in accordance with the Evaluation License Agreement. Licensee agrees to provide ISS with all feedback, results, and data as requested by ISS.

This agreement is subject to change at any time without notice. You may terminate this agreement at any time by returning the Software to ISS. ISS may terminate this agreement at any time for any reason. You agree to indemnify ISS for any damages or losses arising out of your use of the Software. This agreement is governed by the laws of the jurisdictions in which ISS has a presence. This agreement shall be governed by the laws of the jurisdiction in which you are located. You agree to submit to the jurisdiction of the courts in such jurisdiction for the resolution of any disputes arising out of this agreement.

**IN THE EVENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS LICENSE AGREEMENT AND ANY ISS DOCUMENTATION, THE TERMS OF THIS LICENSE AGREEMENT WILL PREVAIL.**

**ISS LICENSE AGREEMENTS, SOFTWARE LICENSES, AND ISS SOFTWARE LICENSE NOTIFICATIONS ARE AVAILABLE AT HTTP://WWW.ISS.COM/PRODUCTS/SOFTWARE/LICENSES. FOR ADDITIONAL INFORMATION, CONTACT ISS AT 1-800-877-4445 OR HTTP://WWW.ISS.COM.**

**ISS LICENSE AGREEMENTS, SOFTWARE LICENSES, AND ISS SOFTWARE LICENSE NOTIFICATIONS ARE AVAILABLE AT HTTP://WWW.ISS.COM/PRODUCTS/SOFTWARE/LICENSES. FOR ADDITIONAL INFORMATION, CONTACT ISS AT 1-800-877-4445 OR HTTP://WWW.ISS.COM.**

**ISS LICENSE AGREEMENTS, SOFTWARE LICENSES, AND ISS SOFTWARE LICENSE NOTIFICATIONS ARE AVAILABLE AT HTTP://WWW.ISS.COM/PRODUCTS/SOFTWARE/LICENSES. FOR ADDITIONAL INFORMATION, CONTACT ISS AT 1-800-877-4445 OR HTTP://WWW.ISS.COM.**
NATURE AND EXPENSES INCURRED BY LICENSEE. LICENSEE SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE EVALUATION LICENSE BY WRITTEN NOTICE TO ISS.

6. Covenants - ISS reserves all intellectual property rights in the Software, software content and Beta Products. Licensee agrees: (i) the Software, security content or Beta Products it is licensed by ISS or its licensors, is a valuable trade secret of ISS, and IS protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software, software content or Beta Product from unauthorized access, decompilation, disassembly, reverse engineering, or other proprietary system or code that is intended to discover the source code of the Software, security content or Beta Product, if any, in written or electronic form; (iii) if not to use the Software, software content or Beta Product; (iv) to report all of ISS trademarks, and protect all of ISS and its licensors copyright notices on any copies of the Software, software content or Beta Product or make it available for time-sharing, service bureau, managed services offering, or on-line use.

7. Support and Maintenance - Depending upon what maintenance programs Licensee has purchased, ISS will provide maintenance, during the period for which Licensee has paid the applicable maintenance fees, in accordance with its prevailing Maintenance and Support Policy that is available at http://docs.iss.com/maintenancer_policy.pdf. Any supplemental Software code or materials that ISS provides to Licensee with the Software, and any other maintenance, updates or bug fixes that ISS provides to Licensee shall be at Licensee's expense.

8. Limited Warranty - The commencement date of the limited warranty is the date on which ISS provides Licensee with the Software. ISS warrants that the Software or security content will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless: (i) the Software or security content is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, fixes, versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software or security content, (ii) modification of the Software or security content, (iii) failure by Licensee to use compatible computer and networking hardware and software, or (iv) interactions with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, ISS may, at its option, either repair or replace the Software or security content that ISS determines that repair or replacement is impractical. ISS may terminate the applicable licenses and refund the applicable software or security content fee if ISS determines that repair or replacement is impractical. ISS may terminate the applicable licenses and refund the applicable software or security content fee. ISS does not warrant that the Software or security content will meet Licensee's requirements, that the operation of the Software or security content will be uninterrupted or error-free, or that all SOFTWARE SECURITY CONTENT ERRORS WILL BE CORRECTED. ISS DISCLAIMS ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. ISS EXPRESSLY DISCLAIMS ANY REPRESENTATION OR WARRANTY MADE REGARDING THE SOFTWARE OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.

Proprietary Rights - ISS represents and warrants that it has the rights to the Software and security content to the Software and security content contained herein. ISS shall not be liable, however, for damages either to Licensee for any actual, potential, or alleged trade secret, patent, or copyright or any other type of proprietary right that Licensee may have in the Software and security content, as a result of the use of the Software or security content to the Software and security content contained herein. ISS shall not be liable for any claims, actions, suits, or causes of action whether arising out of contract, tort, or otherwise, whether brought by Licensee or any third party, for infringement or misappropriation of any right, trade secret, patent or copyright as a result of the use of the Software or security content to the Software and security content, or any other copyrighted work which Licensee may incorporate into the Software or security content. If Licensee incorporates any copyrighted work into the Software or security content, Licensee shall indemnify and hold ISS harmless from and against any and all claims, actions, suits, or causes of action alleged to arise out of such incorporation, including but not limited to claims, actions, suits, or causes of action alleging that such copyrighted work infringes or misappropriates any right, trade secret, patent or copyright as a result of the use of the Software or security content, or any other copyrighted work which Licensee may incorporate into the Software or security content. If Licensee incorporates any copyrighted work into the Software or security content, Licensee shall indemnify and hold ISS harmless from and against any and all claims, actions, suits, or causes of action alleged to arise out of such incorporation, including but not limited to claims, actions, suits, or causes of action alleging that such copyrighted work infringes or misappropriates any right, trade secret, patent or copyright as a result of the use of the Software or security content, or any other copyrighted work which Licensee may incorporate into the Software or security content.

11. Limitation of Liability - ISS’ ENTIRE LIABILITY FOR MONETARY DAMAGES ARISING OUT OF OR FROM TRANSACTIONS UNDER THIS THREE-YEAR LICENSE SHALL BE LIMITED TO THE AMOUNT OF THE LICENSE FEES ACTUALLY PAID BY LICENSEE OR THE LICENSEE RECEIVED, AS APPLICABLE, IN NO EVENT SHALL ISS BE LIABLE TO LICENSEE UNDER ANY THEORY INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY OF THE FOLLOWING: LOSS OR DAMAGE TO DATA, LOSS OF OR DAMAGE TO LICENSEE’S BUSINESS, LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF PROFITS, LOSS OF DATA, LOSS OF USE, OR LOSS OF COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS IS ADVISED OR SHOULD HAVE BEEN AWARE OF THE BALANCE OF THE LICENSE, THE LIMITATION OF LIABILITY OF ISS AS SET FORTH IN THIS SECTION IS NOT THE COMPLETE EXCLUSION OF LIABILITY FOR SUCH DAMAGES.

12. Termination - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License shall terminate immediately, without prior written notice from ISS, at the end of the term of the License, if not permitted. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of a license for Software or security content, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software or security content that are in Licensee's possession or control. Licensee's failure to cease use of the Software or security content that are in Licensee's possession or control shall constitute a breach of this License and may result in an action by ISS for monetary damages and/or injunctive relief. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not affect any rights or obligations accruing prior to such termination.

13. Governing Law - ISS agrees to the identification of the Software and security content, pricing and payment terms stated in the applicable ISS Software License Agreement for the Software or security content, and the corresponding License and Service Order, (if applicable) as accepted by ISS, constitute the entire agreement between Licensee and ISS and are in addition to any written or oral agreements contained in any purchase order or similar document that are hereby expressly rejected and shall have no force or effect. ISS acknowledges that it has not relocated, under control of or a national or resident of any such country or any such entity. ISS may not relocate, under control of or a resident of any such country or any such entity. ISS and the customer shall not be bound by the equable laws of the United States, including the application of its conflicts of law rules. This License will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the applicable law to the Licensee, which is expressly excluded. If any part of this License is in conflict with the terms and conditions, or (iii) a breach of this License under any applicable laws, including the United States Federal Acquisition Regulations at 48 C.F.R. Subpart 12.2 and DAF Subpart 277.202-2 and Clause 252.227-7015 or applicable subsequent regulations. Contracts; manufacturing and supply of defense products. ISS represents and warrants that it is not an excluded, unpunished or undesirable entity as defined in the United States Export Administration Regulations. ISS represents and warrants that it is not an excluded, unpunished or undesirable entity as defined in the United States Export Administration Regulations.

14. Export and Import Controls - Use Restrictions - Licensee will not transfer, export, or reimport the Software, security content, Beta Products, any related technologies, or any direct product of either except in full compliance with the export controls administered by the United States Government or its agencies in the United States, or its agents or their subsidiaries, or their respective affiliates, or its agents or their subsidiaries, or their respective affiliates, or its agents or their subsidiaries, or their respective affiliates, or its agents or their subsidiaries, or their respective affiliates, or its agents or their respective affiliates, or its agents or their respective affiliates. Licensee agrees that it will not export or reexport such items to anyone on the United States Treasury Department's list of specially designated nationals or the U.S. Commerce Department's Denied Persons List or Entity List or such additional lists as may be issued by the U.S. Government from time to time, or to any country to which the United States has embargoed the exportation of goods or for use with chemical or biological weapons, sensitive nuclear material, nuclear material, or military material.

15. Export and Import Controls - Use Restrictions - Licensee agrees to the following requirements for the Software and security content.
injury or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.

18. Confidentiality - "Confidential Information" means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party ("Receiving Party") which receives Confidential Information of the other party ("Disclosing Party") with respect to any particular portion of the Disclosing Party's Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public prior to the time of disclosure to the Receiving Party; (ii) it was publicly disclosed by the Receiving Party by its own decisions, which were not in violation of this Agreement; (iii) it was independently developed by the Receiving Party; (iv) it was already known to the Receiving Party, as evidenced by documents or other evidence accepted by the Disclosing Party; (v) it was lawfully obtained by the Receiving Party from a source other than the Disclosing Party free from any obligations of confidentiality to the Disclosing Party. Each party acknowledges that the use or disclosure of Confidential Information of the Disclosing Party in violation of this Agreement could severely damage the economic interests of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this Agreement.

19. Compliance - From time to time, ISS may request Licensee to provide a certification that the Software and security content is being used in accordance with the terms of this License. If requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensee's compliance or non-compliance, including the extent of any non-compliance. ISS may, at its own expense, appoint a nationally recognized software audit company to conduct such audit. Licensee shall provide ISS with all necessary access to the Software and security content in accordance with the terms of this License. ISS shall use commercially reasonable efforts to conduct such audit in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that the Software or security content has been used beyond the scope of use and/or the number of authorized devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list price for use of the Software or security content in violation of the terms of this License.

20. Data Protection - The data required to process this transaction will be stored by ISS and may be forwarded to companies affiliated with ISS and possibly to Licensee vendor within the framework of processing Licensees order. All personal data will be treated confidentially.

Revised October 7, 2005.