Quick Start Guide
Version 3.5
## Contents

### Preface
- Overview .................................................. 5
- How to use Proventia Network ADS Documentation .................. 6
- Conventions Used in this Guide ....................................... 7
- Getting Technical Support ............................................ 9

### Chapter 1: Introduction to Proventia Network ADS Appliances
- Overview .................................................. 11
- Deployment Scenarios .............................................. 12
- Analyzer Ports Diagram ........................................... 15
- Collector Ports Diagram ........................................... 17
- Recommended Firewall Port Configuration .......................... 19

### Chapter 2: Getting Started
- Overview .................................................. 21
- Appliance Package Contents ...................................... 22
- First-Time Appliance Setup ....................................... 23
- Analyzer Settings Checklist ....................................... 24
- Collector Settings Checklist ...................................... 26
- Connecting to the ADS Setup Wizard ............................... 28
- Configuring the Analyzer ....................................... 30
- Configuring Collectors .......................................... 34
- Accessing the ADS Web User Interface ............................ 38

### Chapter 3: Reinstalling the Appliance
- Overview .................................................. 41
- Reinstallation Requirements ....................................... 42
- Reinstalling an Appliance ....................................... 43

### Index .................................................. 45
Preface

Overview

Introduction  This guide contains information about deploying and installing your Proventia Network ADS Analyzer and Collector appliances for the first time.

Scope  This guide includes basic information and required procedures for connecting the appliances and configuring basic settings.

Audience  This guide is intended for network operators who use Proventia Network ADS to secure their network. Users should have a fundamental knowledge of their network security policies and network configuration.
How to use Proventia Network ADS Documentation

Using this guide

Please read this guide before you install or operate this product. An overview of the setup process and a checklist is provided to help you gather and record required information. ISS recommends that you review the network deployment diagrams, prerequisites, and considerations before you begin the setup process.

Related publications

For more information, see the following:

<table>
<thead>
<tr>
<th>Document</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proventia Network ADS User Guide</td>
<td>Includes instructions for and information about using your ADS appliances in the Web user interface.</td>
</tr>
<tr>
<td>Proventia Network ADS Advanced Configuration Guide</td>
<td>Includes instructions for and information about advanced configuration and integration options that you can set in the command line interface (CLI).</td>
</tr>
</tbody>
</table>

Table 1: Related documents

Additional documentation

Additional ISS documentation is available on the ISS Web site:

http://www.iss.net/support/documentation
Conventions Used in this Guide

Introduction

This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures

The typographic conventions used in procedures are shown in the following table:

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it Indicates</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>An element on the graphical user interface.</td>
<td>Type the computer’s address in the <strong>IP Address</strong> box. Select the <strong>Print</strong> check box. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>SMALL CAPS</strong></td>
<td>A key on the keyboard.</td>
<td>Press <strong>ENTER</strong>. Press the <strong>PLUS SIGN (+)</strong>.</td>
</tr>
<tr>
<td><strong>Constant width</strong></td>
<td>A file name, folder name, path name, or other information that you must type exactly as shown.</td>
<td>Save the <strong>User.txt</strong> file in the <strong>Addresses</strong> folder. Type <strong>IUSR__SMA</strong> in the <strong>Username</strong> box.</td>
</tr>
<tr>
<td><strong>Constant width italic</strong></td>
<td>A file name, folder name, path name, or other information that you must supply.</td>
<td>Type <strong>Version number</strong> in the <strong>Identification information</strong> box.</td>
</tr>
<tr>
<td>$\Rightarrow$</td>
<td>A sequence of commands from the taskbar or menu bar.</td>
<td>From the taskbar, select <strong>Start</strong>$\Rightarrow$<strong>Run</strong>. On the <strong>File</strong> menu, select <strong>Utilities</strong>$\Rightarrow$<strong>Compare Documents</strong>.</td>
</tr>
</tbody>
</table>

Table 2: Typographic conventions for procedures
### Command conventions

The typographic conventions used for command lines are shown in the following table:

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it Indicates</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Constant width bold</strong></td>
<td>Information to type in exactly as shown.</td>
<td><code>md ISS</code></td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Information that varies according to your circumstances.</td>
<td><code>md your_folder_name</code></td>
</tr>
<tr>
<td>[]</td>
<td>Optional information.</td>
<td><code>dir [drive:] [path]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>[filename] [/P] [/W]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>[D]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Two mutually exclusive choices.</td>
</tr>
<tr>
<td>{}</td>
<td>A set of choices from which you must choose one.</td>
<td><code>% chmod { u g o a }= [r] [w] [x] file</code></td>
</tr>
</tbody>
</table>

*Table 3: Typographic conventions for commands*
Getting Technical Support

Introduction

ISS provides technical support through its Web site and by email or telephone.

The ISS Web site

The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase.

Support levels

ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24x7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

<table>
<thead>
<tr>
<th>Location</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>24 hours a day</td>
</tr>
<tr>
<td>All other locations</td>
<td>Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays</td>
</tr>
</tbody>
</table>

Note: If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: Hours for technical support
The following table provides electronic support information and telephone numbers for technical support requests:

<table>
<thead>
<tr>
<th>Regional Office</th>
<th>Electronic Support</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>Connect to the MYISS section of our Web site: <a href="http://www.iss.net">www.iss.net</a></td>
<td>Standard: (1) (888) 447-4861 (toll free) (1) (404) 236-2700 Select and Premium: Refer to your Welcome Kit or call your Primary Designated Contact for this information.</td>
</tr>
<tr>
<td>Latin America</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(1) (888) 447-4861 (toll free) (1) (404) 236-2700</td>
</tr>
<tr>
<td>Europe, Middle East, and Africa</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(44) (1753) 845105</td>
</tr>
<tr>
<td>Asia-Pacific, Australia, and the Philippines</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(1) (888) 447-4861 (toll free) (1) (404) 236-2700</td>
</tr>
<tr>
<td>Japan</td>
<td><a href="mailto:support@isskk.co.jp">support@isskk.co.jp</a></td>
<td>Domestic: (81) (3) 5740-4065</td>
</tr>
</tbody>
</table>

Table 5: Contact information for technical support
Chapter 1

Introduction to Proventia Network ADS Appliances

Overview

Introduction

This chapter contains introductory information about deploying your Proventia Network ADS Analyzer and Collector appliances.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Scenarios</td>
<td>12</td>
</tr>
<tr>
<td>Analyzer Ports Diagram</td>
<td>15</td>
</tr>
<tr>
<td>Collector Ports Diagram</td>
<td>17</td>
</tr>
<tr>
<td>Network Firewall Diagram</td>
<td>19</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction to Proventia Network ADS Appliances

Deployment Scenarios

Overview
This topic describes the two scenarios for deploying Proventia Network ADS: Standalone and Two-tier. The main difference between the scenarios is that Standalone mode does not require Collector appliances, whereas Two-tier mode does.

Appliance types
The two types of Proventia Network ADS appliances are as follows:

- The Analyzer is a 2U appliance that stores network traffic databases, generates alerts, and provides the primary Web user interface.
- The Collectors are 1U appliances that accept and process network traffic data and report summary information to the Proventia Network ADS Analyzer appliance.
**Standalone diagram**  Figure 1 shows an example of a standalone mode deployment:

![Standalone mode deployment diagram](image)

**Standalone mode**  Standalone mode is for smaller deployments in which an Analyzer collects network flow information without using a Collector. In this mode, the Analyzer collects data from up to three flow sources, and accepts raw packet data from network SPAN ports or TAPs.
Two-tier mode is for large deployments using both Analyzer and one or more Collector appliances. In this type of deployment, network flow information and raw packet data from SPAN ports or TAPs is directed to Collector appliances. The Collector appliances then forward consolidated traffic data to an Analyzer appliance.

The Collectors can collect information from a variety of flow sources, depending upon the Collector models and the number of Collectors deployed.
Analyzer Ports Diagram

Overview

This topic describes the Analyzer ports and includes a diagram of the back panel for reference.

Analyzer back panel diagram

The back panel of the Proventia Network ADS Analyzer appliance is shown in Figure 3:

![Analyzer Ports Diagram](image)

**Figure 3**: Proventia Network ADS Analyzer appliance back panel diagram

The back panel includes the following:

- Serial console port (RJ-45)
- Management/NetFlow Ethernet port
- Packet capture Ethernet port for Standalone mode
- two AC power connections
Within the Proventia Network ADS application, the Ethernet ports are referenced by their hardware identifiers. Table 6 shows the correct correlation between the hardware identifiers and the appliance labels.

<table>
<thead>
<tr>
<th>Hardware Identifier</th>
<th>Back Panel Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3/4/1</td>
<td>Management/NetFlow port</td>
</tr>
<tr>
<td>e3/4/0</td>
<td>Packet capture port for Standalone mode</td>
</tr>
</tbody>
</table>

Table 6: Port representations
Introduction

This topic describes the Collector ports and includes a diagram of the back panel for reference.

Collector back panel diagram

The back panel of the Proventia Network ADS Collector appliance is shown in Figure 4:

- Serial console port (RJ-45)
- Management/NetFlow Ethernet port
- optional NetFlow Ethernet port
- four packet capture Ethernet ports
- AC power connection
Chapter 1: Introduction to Proventia Network ADS Appliances

Interfaces and ports

Within the Proventia Network ADS application, the Ethernet ports are referenced by their hardware identifiers. Table 7 shows the correct correlation between the hardware identifiers and the appliance labels:

<table>
<thead>
<tr>
<th>Hardware Identifier</th>
<th>Back Panel Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3/4/1</td>
<td>Management/NetFlow port</td>
</tr>
<tr>
<td>e3/4/0</td>
<td>Optional NetFlow port</td>
</tr>
<tr>
<td>e2/3/1</td>
<td>Packet capture port A</td>
</tr>
<tr>
<td>e2/3/0</td>
<td>Packet capture port B</td>
</tr>
<tr>
<td>e3/7/0</td>
<td>Packet capture port C</td>
</tr>
<tr>
<td>e3/7/1</td>
<td>Packet capture port D</td>
</tr>
</tbody>
</table>

Table 7: Port representations on the Collector appliances

Flow source limits

The number of flow sources you can have depends upon the Collector model you have purchased. Table 8 shows the maximum number of flow sources per Collector model:

<table>
<thead>
<tr>
<th>Model</th>
<th>Description and Maximum Number of Flow Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD3000</td>
<td>Packet Collector appliance (0 flow sources)</td>
</tr>
<tr>
<td>AD3007</td>
<td>Flow/Packet Collector (7 flow sources)</td>
</tr>
<tr>
<td>AD3014</td>
<td>Flow/Packet Collector (14 flow sources)</td>
</tr>
<tr>
<td>AD3020</td>
<td>Flow/Packet Collector (20 flow sources)</td>
</tr>
</tbody>
</table>

Table 8: Collector models
Recommended Firewall Port Configuration

Introduction

This topic provides information about the ports that various components of Proventia Network ADS use.

Firewall ports diagram

If you have firewalls in between the appliances, you must open the ports on the firewall to ensure that your deployment of ADS is successful. Figure 5 shows an example of a typical Proventia Network ADS deployment and the traffic that flows between the devices. Use this diagram as a guide to configure access rules in any firewalls you may have in your network:

Figure 5: Typical Proventia Network ADS port usage
Proventia Network ADS might use additional ports in certain situations. See the *Proventia Network ADS Advanced Configuration Guide* for more details.
Chapter 2

Getting Started

Overview

Introduction

This chapter contains information about the appliance package contents, and instructions for setting up and configuring the appliances for the first time.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Package Contents</td>
<td>22</td>
</tr>
<tr>
<td>First-time Appliance Setup</td>
<td>23</td>
</tr>
<tr>
<td>Analyzer Settings Checklist</td>
<td>24</td>
</tr>
<tr>
<td>Collector Settings Checklist</td>
<td>26</td>
</tr>
<tr>
<td>Connecting to the ADS Setup Wizard</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the Analyzer</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Collectors</td>
<td>34</td>
</tr>
<tr>
<td>Accessing the Web User Interface</td>
<td>38</td>
</tr>
</tbody>
</table>
Appliance Package Contents

Overview

This topic lists the contents of your appliance packages and the information about the tools and tasks required to connect them.

Verifying the contents

Verify the appliance package includes the following:

<table>
<thead>
<tr>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer or Collector appliance</td>
</tr>
<tr>
<td>one AC power cord (two in Analyzer packages)</td>
</tr>
<tr>
<td>recovery CD pack</td>
</tr>
<tr>
<td>one Proventia Network ADS Quick Start Guide</td>
</tr>
<tr>
<td>one crossover Ethernet cable</td>
</tr>
<tr>
<td>one bezel faceplate per package</td>
</tr>
<tr>
<td>rack mount kit</td>
</tr>
<tr>
<td>warranty statement</td>
</tr>
</tbody>
</table>

Figure 6: Appliance box contents

Rack mount kit contents and instructions

Rack mounting procedures are included in the rack mount kit for your appliance box as follows:

- slide rail kit and cable management arm for Analyzers
- mid-mount kit (two- and four-post systems) for Collectors
First-Time Appliance Setup

Introduction
This topic describes the connection options and the tasks required to set up your appliances for the first time.

Setup wizard
When your appliance is new, you configure basic settings using a Web-based wizard that you access from a computer directly connected to the appliance using a crossover Ethernet cable. After completing the setup steps, deploy the appliance into your network.

Setup process tasks
To setup your appliance, you must complete the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect cables and start the appliance.</td>
<td>See “Connecting to the ADS Setup Wizard” on page 28.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the appliance.</td>
<td>See “Configuring the Analyzer” on page 30.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Collectors” on page 34.</td>
</tr>
<tr>
<td>3</td>
<td>Connect to the network.</td>
<td>See “Connecting the Analyzer to the network” on page 33.</td>
</tr>
<tr>
<td>4</td>
<td>Continue setup in the Web user interface.</td>
<td>See “Initial Configuration” in the Proventia Network ADS User Guide.</td>
</tr>
</tbody>
</table>

Table 9: Setup tasks
## Analyzer Settings Checklist

Use the following worksheet to gather and document the information for your Analyzer appliance:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer mode</td>
<td>Two-tier for use with Collectors or Standalone for Analyzer-only deployments.</td>
</tr>
<tr>
<td>Appliance hostname</td>
<td>The unique computer name for your appliance used for external alerting and for identification. This can be either a fully qualified domain name (ISSAnalyzer.iss.net) or just the appliance name (ISSAnalyzer).</td>
</tr>
<tr>
<td>Appliance domain name server</td>
<td>The IP address of the server you are using to perform domain name lookups. <strong>Important:</strong> You must configure a DNS server for the Active Threat Feed (ATF) to work.</td>
</tr>
<tr>
<td>Management IP address and Subnet Mask</td>
<td>The unique IP address and the appropriate network mask. <strong>Note:</strong> If you do not set the correct IP address, you will be unable to access the Web user interface.</td>
</tr>
<tr>
<td>NetFlow sources (for Standalone mode)</td>
<td>Up to three source router IP addresses that will send NetFlow to the Analyzer.</td>
</tr>
</tbody>
</table>

*Table 10: Worksheet for Analyzer configuration information*
## Analyzer Settings Checklist

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default route (or gateway)</td>
<td>The first router hop that sends outbound network traffic, typically the subnet switch or router.</td>
</tr>
<tr>
<td>NTP server (optional)</td>
<td>The IP address for the server that sets network time.</td>
</tr>
<tr>
<td>Administrative password</td>
<td>The password for administrative access to the appliance.</td>
</tr>
<tr>
<td>SMTP server</td>
<td>The SMTP relay address that sends outgoing mail.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>The zone secret is a word or phrase that the system uses to encrypt traffic between the Analyzer and Collectors. You must set the same secret on the Collectors.</td>
</tr>
<tr>
<td>Location of certificate package</td>
<td>The location where you have stored the certificate package. You must upload the certificate on each appliance from the computer you will use to configure your appliances.</td>
</tr>
</tbody>
</table>

Table 10: *Worksheet for Analyzer configuration information* (Continued)
Collector Settings Checklist

Use the following worksheet to gather and document the information for your Collector appliances:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer address</td>
<td>The Management IP address of the Analyzer to which this Collector reports traffic data.</td>
</tr>
<tr>
<td>Appliance hostname</td>
<td>The unique computer name for your appliance. This can be either a fully qualified domain name (ISSCollector1.iss.net) or just the appliance name (ISSCollector1).</td>
</tr>
<tr>
<td>Management IP address and Subnet Mask</td>
<td>The unique IP address and the appropriate network mask.</td>
</tr>
<tr>
<td>NetFlow IP address and Subnet Mask</td>
<td>If configured, the IP address to which NetFlows are sent. If not configured, NetFlows should be sent to the Management IP address.</td>
</tr>
<tr>
<td>NetFlow sources</td>
<td>The router source IP addresses that will send NetFlow to the Collector. Note: The number of sources allowed depends upon the Collector model you are configuring.</td>
</tr>
<tr>
<td>Default route (or gateway)</td>
<td>The first hop that sends outbound network traffic, typically the subnet switch or router.</td>
</tr>
</tbody>
</table>

Table 11: Worksheet for Collector configuration information
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server (optional)</td>
<td>The IP address for the server that sets network time.</td>
</tr>
<tr>
<td>Administrative password</td>
<td>The password for administrative access to the appliance.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>The zone secret is a word or phrase that the system uses to encrypt traffic between the Analyzer and Collectors. You must use the same secret that you set on the Analyzer.</td>
</tr>
<tr>
<td>Location of certificate package</td>
<td>The location where you have stored the certificate package. You must upload the certificate on each appliance from the computer you will use to configure your appliances.</td>
</tr>
</tbody>
</table>

Table 11: Worksheet for Collector configuration information (Continued)
Connecting to the ADS Setup Wizard

**Introduction**

This topic provides the instructions for connecting cables and starting the Analyzer and Collector appliances for the first time.

**Connecting the cables for Web-based setup**

To connect the cables for using the Web-based Proventia ADS Wizard:

1. Plug one end of the provided crossover cable into the Management Interface port on the back panel of the appliance.
   
   See Figure 3 on page 15 for Analyzers.
   
   See Figure 4 on page 17 for Collectors.

2. Plug the other end of the crossover cable into the Ethernet port on the computer you will use to configure the appliance.

3. Plug the AC Power connector into the back of the appliance where indicated in Figure 3 on page 15, and then plug the other end into a standard AC receptacle.

4. Turn the appliance on, and then start your computer.

5. Follow the procedure “Network adapter TCP/IP settings,” below.

**Network adapter TCP/IP settings**

You must change your network adapter TCP/IP settings on your computer in order to use the Web-based Proventia Network ADS Setup Wizard with the crossover connection. Make a note of your existing settings.

**Note:** Access may be different depending on your operating system version. These are general guidelines, based on Microsoft XP.

**Procedure**

To change your TCP/IP adapter settings:

1. Access your Local Area Connection properties on your PC in one of the following ways:
   - right-click My Network Places, and then choose Properties.
   - go to your control panel, and then choose Network Connections.

2. Right-click Ethernet Connections, and then choose Properties.

3. Select Internet Protocol TCP/IP.
4. Click **Properties**.

5. Configure your computer with the following settings:
   
   IP address: **192.168.123.10**
   
   Netmask: **255.255.255.0**
   
   Default gateway: **192.168.123.123**
   
   **Note:** If your operating system is not Microsoft Windows, refer to your computer documentation for instructions on how to change your network adaptor IP address. You must reset your network adaptor IP to your original settings before you can access the Proventia Network ADS Web user interface.

6. Proceed to one of the following:
   
   ■ “Configuring the Analyzer” on page 30.
   
   ■ “Configuring Collectors” on page 34.
Configuring the Analyzer

Overview

This topic provides the instructions for configuring your Analyzer using the Web-based Proventia Network ADS Setup Wizard.

Mode settings

There are two different modes you can configure, depending upon your deployment. Before you begin the setup process, you should decide which mode to use:

- Standalone mode
- Two-tier mode

Reference: See “Overview” on page 12 for a description of these modes.

Configuring the Analyzer

To configure the Analyzer appliance using the crossover connection and the Web-based wizard:

1. Connect the cables as instructed in “Connecting the cables for Web-based setup” on page 28.
2. Reset your TCP/IP settings as instructed in “Network adapter TCP/IP settings” on page 28.
3. Open a browser window, and then enter http://192.168.123.123.
   The Proventia Network ADS Setup Wizard Welcome screen appears.
4. Click NEXT.
5. Read the ISS Software License Agreement, select the check box to accept the license, and then click ACCEPT.
6. Read the GPL License Agreement, select the check box to accept the license, and then click ACCEPT.
   The Certificate Package screen appears.
7. To install the certificate package provided by ISS, click Browse, and then select the location where you stored the certificate package.
8. Click NEXT to install the certificate package.
   The Analyzer Mode screen appears.
9. Do one of the following to select the Analyzer mode:
Select the Two-tier Mode option, and then enter the shared secret to enable communication between the Analyzer and Collector(s) in the Collector Communication Shared Secret box.

The shared secret can be any word or phrase, but you must configure the same secret on the Analyzer and Collectors.

Select the Standalone Mode option for standalone Analyzer deployments.

See “Overview” on page 12 for descriptions of the modes.

10. Click NEXT.

The Network Interfaces screen appears.

11. Type the management interface address in the IP address box.

12. Type in the Subnet Mask.

13. For Standalone mode Analyzers, you can optionally type up to three NetFlow sources in the Source IP address boxes.

   The Source IP refers to the IP address of the router or device that will be sending NetFlow data to the appliance.

14. Click NEXT.

   The Default Route screen appears.

15. Type the IP address for the default route (or gateway) for the Analyzer in the Default Route box.

16. Click NEXT.

17. The Appliance Hostname screen appears.

18. Type the Analyzer name you want to appear in alert notifications and on Collectors in the Hostname box.

   Enter either a fully qualified domain name (ISSAnalyzer.iss.net) or just the appliance name (ISSAnalyzer).

19. Click NEXT.

   The Network Services screen appears.
20. Select the check boxes for the types of network services you want to allow.

   **Important:** ISS recommends that you enable SSH because it provides access to a command line interface (CLI) that updates appliance software and allows troubleshooting.

   **Note:** You must explicitly allow a service. Otherwise, network access is denied.

21. Click **NEXT**.

   The Domain Name Service screen appears.

22. Type the IP address of your **DNS Server**.

23. Click **NEXT**.

   The Outgoing Mail Server screen appears.

24. Type the IP address of the outgoing mail server in the **SMTP Relay** box.

25. Click **NEXT**.

   The Administrator Password screen appears.

26. Type the password for the “admin” primary administrator account in the **Password** box.

27. Re-type the password in the **Confirm Password** box, and then click **NEXT**.

   The System Time screen appears.

28. Select the timezone for the Analyzer location from the **Timezone** list.

29. Do one of the following to set the system time:

   ■ Type the IP address for the server that synchronizes network time protocol in the **NTP Server** box.

   ■ Type the **Month, Day, Year**, hours (**HH**) and minutes (**MM**).

30. Click **NEXT**.

   The Review screen appears.

31. Review the settings, and then do one of the following:

   ■ Click **APPLY CHANGES AND SHUTDOWN** to apply the settings.
32. Wait one minute, and then turn off the appliance.

33. Disconnect the Ethernet cable between your computer and the appliance, and then follow the steps in the procedure Connecting the Analyzer to the network.

To connect to the network to access the Web user interface:

1. Connect an Ethernet cable between the Analyzer’s management port on the back panel to the network you will use to manage it.
   
   In Standalone mode, you can also connect an Ethernet cable between the Packet Capture port and a SPAN port or network tap. The Packet Capture port needs no configuration and automatically captures any traffic it observes.
   
   Reference: See “Analyzer back panel diagram” on page 15.

2. Turn on the appliance.
   
   The appliance runs as configured.

3. See “Accessing the ADS Web User Interface” on page 38 for instructions about starting to use Proventia Network ADS.
Chapter 2: Getting Started

### Configuring Collectors

#### Overview
This topic provides the instructions for configuring your Collectors using the GUI-based Proventia Network ADS Setup Wizard.

#### Management and NetFlow interface settings
You can configure your Collectors in two different ways, depending upon your deployment. Before beginning the setup process, you should decide which configuration setup to use:

- management and NetFlow collection on one interface (typical)
- management and NetFlow collection on separate interfaces

You might want to use this option to manage the appliance from a different network than where the flows are received.

#### Procedure
To configure the Collector appliances using the crossover connection and the GUI-based wizard:

1. Connect the cables, and then reset your TCP/IP settings as instructed in “Network adapter TCP/IP settings” on page 28.
3. Click **NEXT**.
4. Read the ISS Software License Agreement, select the check box to accept the license, and then click **ACCEPT**.
5. Read the GPL License Agreement, select the check box to accept the license, and then click **ACCEPT**.
   The Certificate Package screen appears.
6. To install the certificate package you received from ISS, click **Browse**, and then select the location where you stored the certificate package.
7. Click **NEXT** to install the certificate package.
   The Analyzer Address screen appears.
8. Type the IP address for the Analyzer in the **Analyzer Address** box.
9. Type the secret that allows the Collector to communicate with the Analyzer in the Encrypt Secret box.
   **Note:** You must enter the same shared secret you set in Step 9 of “Configuring the Analyzer” on page 30.

10. Click **NEXT**.
    The Network Interfaces screen appears.

11. Select one of the following options:
    - Management and NetFlow Collection on one interface
    - Management and NetFlow Collection on separate interfaces

12. Type the **IP Address** of the Management (and NetFlow) Collection Interface.

13. Type the **Subnet Mask** of the Management (and NetFlow) Collection interface.

14. Type the IP addresses for the NetFlow sources in the **Source IP** boxes.
    The Source IP refers to the IP address of the router or device that will be sending NetFlow data to the appliance.
    The number of boxes presented corresponds to the Collector model and ranges from 0-20.

15. Click **NEXT**.
    The Default Route screen appears.

16. Type the IP address for the default route (or gateway) for the Collector in the **Default Route** box.

17. Click **NEXT**.
    The Appliance Hostname screen appears.

18. Type the Collector name you want to appear in alert notifications and in the Web user interface in the **Hostname** box.
    The hostname does not need to be a fully-qualified domain name.

19. Click **NEXT**.
    The Network Services screen appears.
20. Select the check boxes for the types of network services you want to allow.

   **Important:** ISS recommends that you enable SSH because it provides access to a command line interface (CLI) that updates appliance software and allows troubleshooting.

   **Note:** You must explicitly allow a service. Otherwise, network access is denied.

21. Click **NEXT**.
   
   The Administrator Password screen appears.

22. Type the password for the “admin” primary administrator account in the **Password** box.

23. Re-type the password in the **Confirm Password** box, and then click **NEXT**.
   
   The System Time screen appears.

24. Select the timezone for the Collector location from the **Timezone** list.

25. Do one of the following to set the system time:
   
   ■ Type the IP address for the server that synchronizes network time protocol in the **NTP Server** box.
   
   ■ Type in the **Month**, **Day**, **Year**, hours (**HH**) and minutes (**MM**).

26. Click **NEXT**.
   
   The Review screen appears.

27. Review the settings, and then do one of the following:
   
   ■ Click **APPLY CHANGES AND SHUTDOWN** to apply the settings.
   
   ■ Click **PREVIOUS** to return to prior screens to update the settings, and then click **APPLY CHANGES AND SHUTDOWN** to apply them.
   
   After you apply the configuration settings, the system displays a shutdown confirmation message.

28. Wait one minute, and then turn the appliance off.

29. Disconnect the Ethernet cable between your computer and the appliance, and then follow the steps in the procedure “Connecting a Collector to the network” on page 37.
Connecting a Collector to the network

To connect a Collector to the network:

1. Connect an Ethernet cable between the Collector management port on the back panel to the network you will use to manage it.

   You can also connect Ethernet cables between the Packet Capture ports and SPAN ports or network tap. The Packet Capture ports need no configuration and automatically capture any traffic they observe.

   Reference: “Collector back panel diagram” on page 17.

2. Turn on the appliance.

   The Collector runs as configured and will be displayed in the ADS Status section of the Summary page in the Web user interface.

3. See “Accessing the ADS Web User Interface” on page 38 for instructions about starting to use Proventia Network ADS.
Accessing the ADS Web User Interface

**Overview**

This topic describes how to log on to the ADS Web user interface to start using Proventia Network ADS to protect your network.

**Prerequisites**

After you connect and configure the appliance, you must do the following to access the Web user interface and use ADS:

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Details</th>
</tr>
</thead>
</table>
| ![ ] | Verify that you have one of the following items installed:  
  - Internet Explorer Version 6 or later  
  - FireFox Version 1.0 or later |
| ![ ] | Connect a computer or laptop to the internal network. |
| ![ ] | Verify that your TCP/IP settings are properly configured for your network. |

Table 12: Prerequisites for accessing the ADS Web user interface

**Logging on to Proventia Network ADS**

To log on to the Proventia Network ADS interface:

1. Start your browser.
2. Type `https://` followed by the IP address of your Analyzer appliance’s management interface you configured during initial configuration.
   
   See “Analyzer Settings Checklist” on page 24.
3. Log in using the user name “admin” and the Analyzer password you configured in “Configuring the Analyzer” on page 30.
   
   The Summary page appears.

**Connection problems**

If you entered the Management IP address incorrectly during initial appliance setup, you will be unable to access the Web user interface. If this happens, you must correct the address in one of the following ways:
Accessing the ADS Web User Interface

- Reinstall the appliances using the Recovery CD.
  
  **Reference:** See “Reinstalling an Appliance” on page 43.

- Connect to the command line interface to manually update the incorrect IP address.
  
  **Reference:** See the *Proventia Network Advanced Configuration Guide* for instructions about using the CLI.

If your appliance is not operational, contact ISS Customer Support at support@iss.net
Chapter 3
Reinstalling the Appliance

Overview

Introduction
This chapter describes the process and procedures for reinstalling the Proventia Network ADS Analyzer and Collector appliances.

Important: Reinstalling the appliance software clears the appliance’s current configuration settings and all data stored on the appliance. You must reconfigure all settings through the Proventia Network ADS Setup Wizard.

What you need
To reinstall an ADS appliance, you need the following:

- a computer to use as your configuration interface
- a Proventia Network ADS Appliance Recovery CD

In this chapter
This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinstallation Requirements</td>
<td>42</td>
</tr>
<tr>
<td>Reinstalling an Appliance</td>
<td>43</td>
</tr>
</tbody>
</table>
Reinstallation Requirements

Introduction

You can use a Proventia Network ADS Appliance Recovery CD to reinstall an appliance (Analyzer or Collector).

⚠️ Caution: Reinstalling the appliance means erasing all data from the system and returning it to its factory state. This should only be done in an emergency situation under the direction of ISS technical support.

Reinstallation process task overview

To reinstall the software, you must complete the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reinstall the appliance.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the appliance settings using the setup wizard.</td>
</tr>
<tr>
<td>3</td>
<td>Apply your settings and reboot the appliance.</td>
</tr>
</tbody>
</table>

Table 13: Reinstallation process

Before you begin

Before you reinstall the appliance, verify you have all of the information you need.

Reference: See “Analyzer Settings Checklist” on page 24 and “Collector Settings Checklist” on page 26 for the complete list of the information you need.
Reinstalling an Appliance

Introduction

Use the following procedure to reinstall the Proventia Network ADS Analyzer or Collector appliance software.

Procedure

To reinstall the appliance:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Place the Proventia Network ADS Recovery CD in the CD-ROM.
3. Choose one of the following methods to connect the appliance to initiate recovery:
   - Connect a VGA monitor and keyboard to the appropriate ports on the back of the appliance.
   - Connect using a serial cable.
   Reference: For instructions about using the serial console and the CLI, see the Proventia Network ADS Advanced Configuration Guide.
4. Restart the appliance.
   You can manually turn the power off and on if the appliance is not responding.
5. Watch for the message that says “Press any key to continue.”
6. When you see this message, press any key to start the boot menu.
7. At the boot menu, select one of the following options:
   - (re) install (VGA) if you are using a monitor and keyboard.
   - (re)install (serial console) if you are using the serial method.
8. After the installation process is complete, remove the CD-ROM, and then restart the appliance.
9. Configure your settings by following the procedure for your appliance:
   - See “Configuring the Analyzer” on page 30.
   - See “Configuring Collectors” on page 34.
10. After you reinstall the appliance, log on to the interface to use your appliance.
Index

a
accessing
  Web user interface 43
Analyzer
  back panel diagram 15
  hardware identifiers 16
  ports 15
  settings checklist 24
Analyzers
  defined 12
Analyzer configuring 30
appliance
  package contents 22
  setup 23
  types 12
appliances
  reinstalling 42

C
cables
  connecting 28
Collector
  back panel diagram 17
  flow source limits 18
  hardware identifiers 18
  models 18
  ports 17
  settings checklist 26
Collectors
  configuring 34
  defined 12

configuring
  Analyzer 30
  Collectors 34
  SiteProtector management settings 39
connecting
  cables 28
  to the network 33
connecting to
  Web user interface 28
connection
  problems 38
connection options 23
conventions, typographical
  in commands 8
  in procedures 7
  in this manual 7
deployment
  options 13
  scenarios 12
diagram
  Analyzer back panel 15
  Collector back panel 17
  firewall ports 19
  standalone mode deployment 13
  two-tier mode deployment 14

f
firewall
  ports 19
flow source
  Collector models 18
Index

h
hardware identifiers
 Analyzer 16
 Collector 18

i
interface settings
 management 34
 NetFlow 34
 Internet Security Systems
 technical support 9
 Web site 9

m
management
 interface settings 34
 mode
 standalone 13
 two-tier 14

n
NetFlow
 interface settings 34
 network
 connecting to 33

p
ports
 Analyzer 15
 Collector 17
 table 20
 problems
 connection 38

 publications
 related 6

r
rack mount
 kit instructions 22
 reinstallation
 requirements 42
 reinstalling
 appliances 42
 related
 publications 6
 requirements
 reinstallation 42

s
settings checklist
 Analyzer 24
 Collector 26
 setup
 appliance 23
 SiteProtector
 configuring 39
 standalone
 diagram 13
 mode 13

table
 ports used by ADS 20
 technical support, Internet Security Systems 9
 two-tier
 diagram 14
 mode 14
 types of appliances 12
 typographical conventions 7–8
W

Web site, Internet Security Systems  9
Web user interface
  accessing  43
  connecting to  28