Dragon[™] Intrusion Defense System

7.0 Tutorial



Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc. 50 Minuteman Road Andover, MA 01810

© 2005 Enterasys Networks, Inc. All rights reserved.

Part Number: 9034126 January 2005

ENTERASYS, ENTERASYS NETWORKS, DRAGON, NETSIGHT, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc. in the United States and other countries.

Adobe, Acrobat, and Acrobat Reader are registered trademarks of Adobe Systems Incorporated.

Celeron, Intel, and Pentium II are trademarks or registered trademarks of Intel Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

FireWall-1, OPSEC and Check Point are trademarks or registered trademarks of Check Point Software Technologies Ltd.

IPX/SPX, Novell and NetWare are trademarks or registered trademarks of Novell, Inc.

Linux is a trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat, Inc.

Solaris is a trademark of Sun MicroSystems, Inc.

SPARC is a registered trademark of SPARC International, Inc.

Sun and Java are trademarks or registered trademarks of Sun Microsystems, Inc.

UNIX is a registered trademark of The Open Group.

Dragon Intrusion Detection System includes software whose copyright is licensed from MySQL AB.

Support Site URL: https://dragon.enterasys.com

ii

Dragon 7.0 Tutorial

Dragon is an intrusion defense solution consisting of an Intrusion Detection System (IDS), active response, and intrusion prevention. This guide provides a basic tutorial that describes how to get Dragon 7.0 up and running in a standalone installation. It is recommended that you read the *Dragon Intrusion Defense System Installation Guide* and the *Dragon Intrusion Defense System Configuration Guide* in addition to this guide.

This tutorial provides instructions to install the Dragon Server, Network Sensor, and Host Sensor on a single Linux machine (not a Dragon appliance) and the Dragon Management Client GUI on a Windows machine. Sample criteria is provided. To use this as a working model, you must provide criteria that matches your network configuration. Follow these instructions in the order that they are presented.

EMS Server Installation

The Dragon Enterprise Management Server (EMS) server portion is installed on a Linux machine. It is assumed that the machine is up and running.

To start the installer:

1. Locate the Dragon Server Installation bundle for your platform either on your CD or in the location to which it was downloaded (for upgrades) and untar the bundle.



Note: If you are using a GUI facility to untar the bundle, make sure the "recreate folder" structure option is enabled.

2. Execute the installation file, **Dragon.bin**, from the location to which it was untarred. The Installer wizard opens.

The Dragon Enterprise Standalone selection installs all possible server components.

3. Click **Next** to accept all defaults through accepting the default installation directory screen. Make sure you accept the license agreement.



4. Select **Dragon Enterprise Standalone** from the pulldown menu.

- 5. Click Next.
- 6. Enter the following criteria:

Enterprise Management Server Bind Address: 10.100.100.55

Configuration Channel Server Bind Address: 10.100.100.55

Configuration Channel port: 9111

	Dragon
	EMS Settings
 Introduction License Agreement Choose Install Folder Choose Install Set System Configuration Pre-Installation Summary Install Complete 	Enterprise Management Server Management Server & Config Channel Settings Management Server Bind Address: 10.100.100.55 Configuration Channel Server Bind Address: 10.100.100.55 Configuration Channel Port: 9111
InstallAnywhere by Zero G	Previous Next

- 7. Click Next.
- Enter the following criteria: Sensor, Agents & reporting Node IP Address: 10.100.100.55 Enterprise Management Server IP Address: 10.100.100.55 Configuration Channel port: 9111

	Dragon
	Node Configuration Channel Settings
 Introduction License Agreement Choose Install Folder Choose Install Set System Configuration Pre-Installation Summary Installing. Install Complete 	Sensors, Agents & Reporting Configuration Channel Communication Settings Sensor, Agent & Reporting Node IP Address: 10.100.100.55 Enterprise Management Server IP Address: 10.100.100.55 Configuration Channel Port: 9111 Configuration Channel Connection Type: OUTBOUND
InstallAnywhere by Zero G Cancel	Previous

Configuration Channel Connection Type: Outbound

- 9. Click Next.
- 10. Enter the encryption type **AES** and the shared secret **dragon**.

	Dragon
	DEC Encryption Configuration
 Introduction License Agreement Choose Install Folder Choose Install Set System Configuration Pre-Installetion Softmanov Installing Install Completes 	Sensors, Agents & Reporting Configuration Channel Encryption Settings Encryption Type: AES Shared Secret: dragon
InstallAnywhere by Zero G —— Cancel	Previous Next

- 11. Click Next.
- 12. Review the components to be installed and click Install.
- 13. Click **Done** when the installation is complete.

Dragon License Key Installation

This section assumes that you have already downloaded your license key as described in the *Dragon Intrusion Defense System Installation Guide* and have it available on diskette.

To copy the file from a floppy diskette:

1. Type mount /dev/fd0 /mnt

- 2. Type cp /mnt/keyfilename /usr/dragon/dragon.key
- 3. Type cp /mnt/keyfilename /usr/dragon/policymgr/keys/dragon.key
- 4. Ensure that the dragon.key file has the correct file permissions (Owner=dragon, Group=dragon) by entering the following commands:

cd /usr/dragon for your EMS server or usr/dragon/policy/keys for other devices.

./install/fixperms.pl



Note: Ignore missing file messages.

- 5. Type **umount /mnt**
- 6. Type **reboot** at the command prompt to reboot the system.

Starting the Server

After the server is installed, it must be started.

To start the server:

- 1. At the command prompt, enter cd /usr/dragon
- 2. At the command prompt, enter **./dragon-mgr-start.sh** The server is started. This may take some time. You can monitor progress in logs/jbsos.log.

EMS GUI Client Installation

The EMS Management GUI is installed on a Windows machine. It is assumed that this machine is up and running.

To start the installer:

1. Locate the Dragon Client Installation bundle either on your CD or in the location to which it was downloaded (for upgrades) and unzip the bundle.



Note: If you are using a GUI facility to unzip the bundle, make sure the "recreate folder" structure option is enabled.

- 2. Execute the installation file EMSClient.exe from the location to which it was unzipped.
- 3. Follow the instructions in the wizard to complete your installation by accepting all defaults. Click **Finish** when the installation screens are complete.

Opening the EMS Client Application

Open the EMS Client on your Windows machine.

To open the EMS:

 Open the Desktop folder entitled Enterasys and select DragonEMSClient>EMSClientWindow.

EMSClientWindow is the executable. A login window appears.

2. Enter your username and password.

The default user ID is **dragon** and there is no password. If you have already changed the default password, use your own credentials.

- 3. Enter the IP address of your Linux server machine (10.100.100.55).
- 4. Click OK.

A status screen appears indicating connection status. Once the connection is established, the Main window is displayed.

Add Your Linux Server to the Tree

Your Linux machine acts as server, Network Sensor, and Host Sensor. The server is a top-level node in the tree.

To add your Linux server:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- Right-click the top-level Enterprise node and select Add New Device Node. The Device Node Configuration window appears.
- 3. Enter the following criteria:

Name: fedora55

Shared Secret: dragon

Encryption Type: AES

Operating System: Linux

Node IP: 10.100.100.55

Note that the hostname is case sensitive and must match the hostname in your key file.

All other default settings are accepted for this device. Note that in the Connection Type field, the connection is set to inbound. This is correct because your server was set to outbound.

🐴 Create Device N	lode	×
Device Node		
Device Name:	Fedora55	
Operating System:	Linux	•
Encryption Type:	AES	•
Node IP:	10.100.100.55	
Port:	9111	
Shared Secret:	dragon	
Connection Type:	inbound	•
Retry Timeout 1:	5	
Retry Timeout 2:	5	
Retry Timeout 3:	5	
Retries:		
Unlimited Retries		
		OK Cancel

4. Click OK.

The display area is populated and the device is added to the tree under the selected node.

Adding a Network Sensor

Your Linux machine acts as server, Network Sensor, and Host Sensor. The network sensor is added as a node under the server.

To add a Network Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- 2. Right-click Fedora55 and select Add New Network Sensor.

The display area is populated with high-level sensor settings and the sensor is added to the tree under the selected node.

3. Click the desired **Network Sensor** in the tree.

The Device and Interfaces window is shown in the display area with the last tab selected open.

4. All default settings are accepted for this sensor.

You may need to specify which device the Network Sensor uses to gather packets. If you need to make these changes, execute the following steps:

- a. Click the **Basic** tab and enter the desired settings in the Interface Settings pane.
- b. Highlight DRAGON-DEFAULT.
- c. Click Edit to invoke the settings window.
- d. Enter the desired values and add an interface.
- e. Click Add.
- f. Click **OK**.
- g. Click **Commit** to apply the change.

Value No		
No No		
Value No		
no		
no		
no		
Description	 Time Stamp 	User
		>
	Description	Description Time Stamp

h. The values are displayed in the table for reference.

Adding a Virtual Network Sensor

Each physical network sensor must contain at least one virtual network sensor.

To add a Network Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- Right-click the Network Sensor and select Add Virtual Sensor. The Virtual Sensor Configuration window appears.

	M			
🖞 Enterprise View 🖄 🚺 🔫	Basic Settings Advanced Settings			
nterprise View	Available Devices	1.22		
Enterprise Sedora55 Sedora55 Setwork Sensor	Property Device Name: DRAGON-DEFA	Value		
	A Virtual Sensor Configurat	ion		
	Enter the name of the new Virtual S	iensor		
	Fedora55-VirtualSensor1			
		OK	Cancel	
	Add Edit Delete	OK	Cancel	
	Add Edit Delete	OK OK	Cancel	
	Add Edit Delete	OK OK	Cancel	User
	Add Edit Delete Commit Reset	OK OK	Cancel	User
	Add Edit Delete Commit Reset	OK OK	Cancel	User 3

3. Enter the name **Fedora55-VirtualSensor1**.

4. Click OK.

The display area is populated with Virtual Sensor settings and the device is added to the tree under the selected node.

- Click Fedora55-VirtualSensor1 in the tree.
 The display area is populated with Virtual Sensor settings. The last tab selected is on top.
- 6. Click the **Basic Settings** tab.
- 7. Enter the following criteria:

Check to enable Default Sensor

Network Sensor Device: Dragon Default

8. Click Apply.

EMS Client - Connected to 10.1	00.100.55 as dragon	
<u>Eile I</u> ools <u>H</u> elp		
Enterprise View Enterprise View Senterprise Senterpris	Basic Settings Network Settings Protocol Settings Port Settings VLAN Settings Protected Networks Sensor Name: Fedora55-VirtualSens ✓ Enable Default Sensor Device Settings Network Sensor Devices: DRAGON-DEFAULT ✓ Virtual Sensor Devices ✓ Virtual Sensor Devices ✓ Commit Reset	
	Operation Result Description Time Stamp User	
		>
	View	
<	Operations	
Current User:dragon		

- 9. Click the **Protected Network** tab.
- 10. Change the IP address to a subnet address for which you want to generate events, such as **10.100.100.0/24**.

11. Click **Add**.

EMS Client - Connected to 10.1	00.100.55 as dragon	
<u>File T</u> ools <u>H</u> elp		
🔼 Enterprise View 🛛 🔕 📕 😋	Basic Settings Network Settings Protocol Settings Port Settings VLAN Settings Protected Networks	
Enterprise View	Internal same as from	
Enterprise	Protected Networks	
SPedora55 SNetwork Sensor	IP Mask	
Fedora55-VirtualSenso	10.100.100.0 24	
	Network Settings	
	IP Address: 10 · 100 · 100 · 0 / 24	
	Add Delete	
	County Doort	
	Commit Reset	
	Operation Result Description Time Stamp	User
	C	>
	View Clear	
< >	Operations	
Current User:dragon		

12. Click Commit.

All other default settings are accepted for this sensor.

Create a New Network Policy

You can use the existing Network Sensor policy as a basis for a new Network Sensor policy. To copy a policy:

- 1. Click the Network Policy View icon.
- 2. Click the expansion symbol to expand Master Policies.
- 3. Right-click Default_NetworkPolicy and highlight Copy.
- 4. Right-click Custom Policies and highlight Paste.A window appears asking you to provide a name for the policy.

5. Enter the name **Fedora-55-NIDS** for the policy.

EMS Client - Connected to 10.1	100.100.55 as d	ragon			
File Tools Help					
Network Policy View 🔼 🚺 😿 🏹 Network Policies Signature Libraries					
Constant Series Constant Series					
	A Network Pol	icy			
	Enter the name of	the new Network	Policy		
	Fedora-55-NIDS				
			OK	Cancel	
	Operation	Result	Description	🔺 Time Stamp	User
	<				>
	View,,, Clear				
Current User:dragon					

6. Click OK.

The policy is added to the tree. All default settings are accepted for this policy. Detailed instructions on configuring policies are described in *Dragon Intrusion Defense System Configuration Guide*.

Binding Policies

Now that you have created the Virtual Sensor and the sensor policy, you must bind them.

To bind your new policy to the Virtual Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- Right-click Fedora55-VirtualSensor1 and select Associate Network Policy. The Network Sensor Policy window appears.

3. Select Fedora-55-NIDS.

Network Policy Choose a Network Policy to associate to the Virtual Senso	or and
Fedora-SS-NIDS	
	OK Cancel

4. Click OK.

The policy is displayed below the Virtual Sensor in the tree.

Binding Signatures

You must also bind signatures to the Virtual Sensor.

To bind signatures to the Virtual Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- 2. Right-click **Fedora55-VirtualSensor1** and select **Apply/Remove Signature Library**. The Signature Library window appears.

3. Select each signature library and, using the arrows button, move it to Current Configuration.

Signature Library Choose a signature library to add or remove		
Available Configuration Objects	\$ \$	Current Configuration Objects APPS ATTACKS COMPROMISE DYNAMIC FAILURES AMISUSE
		OK Cancel

4. Click OK.

The signatures are displayed below the Virtual Sensor in the tree.

Adding a Host Sensor

For the purpose of this tutorial, your Linux machine acts as server, Network Sensor, and Host Sensor. The Host Sensor is added as a node under the server.

To add a Network Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- Right-click Fedora55 and select Add Host Sensor.
 The display area is populated and the sensor is added to the tree under the selected node.
- 3. All default settings are accepted for this sensor. No configuration is needed.

Create a New Host Policy

You can use the existing Host Sensor policy as a basis for a new Host Sensor policy.

To copy a policy:

- 1. Click the Host Policy View icon.
- 2. Click the expansion symbol to expand Master Policies.
- Right-click HOSTSENSOR_LINUX_Fedora_Core3 and highlight Copy.
 You should select a policy that matches your OS to ensure the best configuration basis.
- 4. Right-click Custom Policies and highlight Paste.A window appears asking you to provide a name for the policy.

5. Enter the name **Fedora-55-HIDS**.



6. Click OK.

The policy is added to the tree. All other default settings are accepted for this sensor.

Binding Host Sensor Policies

Now that you have created the Host Sensor and the sensor policy, you must bind them.

To bind your new policy to the Host Sensor:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- 2. Right-click the Host Sensor and select **Associate Host Policy**. The Host Sensor Policy window appears.

3. Select Fedora-55-HIDS.

Host Policy Choose a Host Policy to associate to the Host Sensor
Available Host Policies Image: Host Policies
OK Cancel

4. Click OK.

The policy is displayed below the Host sensor in the tree.

Adding Agents to a Node

You can add agents to your Linux server node.

To add an agent:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- 2. Right-click **Fedora55** and select **Add/Remove Agents**. The Agent Creation/Deletion window appears.

3. Select all the agents using Ctrl-click and, using the right-arrow, move them to Current Configurations.

Agent Creation/Deletion			Ε
Choose agents to add or remove Available Configuration Objects		Current Configuration Objects	
		MD5 Sum RealTime Console	
	<-		
		OK	Cancel

4. Click OK.

The agents are added to the tree under the selected node.

5. The only agent for which we do not want to accept all defaults is the Alarmtool Agent. There is no need to configure the other agents.

Creating an Alarmtool Policy

You can use an existing policy to create a new policy.

To create a new policy:

1. Click the Alarmtool View icon.

A list of master and custom policies is displayed.

- 2. Click the expansion symbol to expand Master Policies.
- 3. Right-click Alarm Tool: Default and select Copy.
- 4. Right-click **Custom Policies** and highlight **Paste**.

A window appears asking you to provide a name for the policy.

5. Enter the policy name Email and click OK.

EMS Client - Connected to 10.1	00.100.55 as drago	n			
File Tools Help					
🖰 AlarmTool Policy View 🛛 🚺 🔫	U				1
Alarmitori Policy view Alarmitori Policies Alarmitori Policies Custom Policies	Alarm Tool Name: email	pol Policy Name	OK Cancel	×]]	
	Operation	Result	Description	▲ Time Stamp	User
	<				2
	View.,, Clear				
Current Liser:dragon	Operations				

- 6. The policy is added under Custom Policies.
- 7. Expand the tree to reveal the newly added policy and click it.

The display area is populated with the last tab selected on top.

8. All default settings are accepted for this sensor. No configuration is needed. It is important that you verify that the Sendmail location in the in the Global Option/Main tabs matches your Sendmail install location. Also, if you make any changes to Event Groups, the changes must be carried through each of the Alarmtool configuration tabs. See the *Dragon Intrusion Defense System Configuration Guide* for detailed configuration information.

Binding Policies

Now that you have created the policy, you must bind it to the agent.

To bind your new policy:

- 1. Click the Enterprise View icon and the Enterprise View tab.
- 2. Right-click the Alarmtool Agent and select **Associate Alarmtool Policy**. The Associate Alarmtool Policy window appears.

3. Select Alarm Tool: Email.

📀 Associate Alarm Tool Policy		
Alarm Tool: email		
	OK	Cancel

4. Click OK.

Deploying the Node

After you have set up your server node with its Network Sensor and Host Sensor as well as configured your agents, you must deploy the node.

To deploy the node:

1. Click the Enterprise View icon and the Enterprise View tab.

terprise View					
		Operating System:	Linux		
>Enterprise	-55	Node IP:	10.100.100.55	8	
- 🔁 >A	📀 Add/Remove Agents		9111		
>D >F	Event Channel Agent.	·· Iion Type:	AES		
₹ >М	Cache Manager Agent	Secret:	dragon		
- 🎦 >R	🛆 Add New Device Node	tion Type:	inhound •		
T 🖣 🔫	🖳 Add Host Sensor	limonut 1	5		
⊡ • 🍋 >N	💼 Add Network Sensor	imeout 1;	5		
))) Deploy	imeout 2:			
	Chave	imeout 3:	12		
	Start				
	Bectart	mited Retrie	s		
	S. Restart				
	💢 Delete				
		Commit Reset			
		Operation	Result Description	▲ Time Stamp	User

2. Right-click Fedora55 and select Deploy from the context menu.

The new configuration settings are deployed to your Linux machine. The operations tab displays deployment status. The main status window, visible at the enterprise node, displays all node status. This completes the Dragon 7.0 Tutorial.

Deploying the Node