Preface

Published: August 3, 2013, OL-29166-01

Revised: February 18, 2014

Contents

This document describes how to install, configure, and use the Intrusion Prevention System Device Manager (IDM) for IPS 7.2. It includes a glossary that contains expanded acronyms and pertinent IPS terms. It is part of the documentation set for the Cisco Intrusion Prevention System 7.2. Use this guide with the documents listed in Related Documentation, page xxviii.

This document contains the following topics:

Audience

This guide is for administrators who need to do the following:

- Install and configure the IDM.
- Secure their networks with IPS sensors.
- Prevent intrusion on their networks and monitor subsequent alerts.

Organization

This guide includes the following sections:

Section	Title	Description
1	"Getting Started"	Describes how to get started using Cisco IPS and sensors.
2	"Configuring Dashboards"	Describes how to add and configure dashboards in the IDM.
3	"Using the Startup Wizard"	Describes how to use the Startup wizard to set up your sensor using the IDM.
4	"Setting Up the Sensor"	Describes how to configure the basic settings of your sensor using the IDM.
5	"Configuring Interfaces"	Describes how to configure interfaces on your sensor using the IDM.
6	"Configuring Policies"	Describes how to configure polices on your sensor using the IDM.
7	"Defining Signatures"	Describes how to configure IPS signatures on your sensor using the IDM.
8	"Using the Signature Wizard"	Describes how to use the Signature wizard to configure signatures using the IDM.
9	"Configuring Event Action Rules"	Describes how to configure event action rules policies on your sensor using the IDM.
10	"Configuring Anomaly Detections"	Describes how to configure anomaly detection policies on your sensor using the IDM.
11	"Configuring Global Correlation"	Describes how to configure global correlation on your sensor using the IDM.
12	"Configuring SSH and Certificates"	Describes how to configure SSH and TLS on your sensor using the IDM.
13	"Configuring Attack Response Controller for Blocking and Rate Limiting"	Describes how to set up blocking on your sensor using the IDM.
14	"Managing Time-Based Actions"	Describes how to manage time-based actions on your sensor using the IDM.
15	"Configuring SNMP"	Describes how to configure SNMP on your sensor using the IDM.
16	"Configuring External Product Interfaces"	Describes how to set up an external product interface to CSA MC using the IDM.
17	"Managing the Sensor"	Describes how to manage your sensor using the IDM.
18	"Monitoring the Sensor"	Describes how to configure monitoring on your sensor using the IDM.
19	"Initializing the Sensor"	Describes how to initialize your sensor.
20	"Logging In to the Sensor"	Describes how to log in to the appliances and modules.

Section	Title	Description
21	"Obtaining Software"	Describes how to locate and install the latest Cisco IPS software found on Cisco.com.
22	"Upgrading, Downgrading, and Installing System Images"	Describes how to upgrade, downgrade, and install new system images on your sensor.
A	"System Architecture"	Describes the underlying software architecture of IPS 7.2.
B	"Signature Engines"	Lists the IPS signature engines with their options.
C	"Troubleshooting"	Lists troubleshooting procedures and advice.
	"Glossary"	Lists the IPS terms and acronyms.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

For a complete list of Cisco IPS 7.2 documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/ips/7.1/roadmap/roadmap7_2.html

For a complete list of the Cisco ASA 5500 series documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.