

Intrusion Detection System Compatibility Matrix

[TAC Notice: What's Changing on TAC Web](#)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[IPS Hardware/Software Compatibility](#)

[Management and Configurations Options](#)

[CiscoWorks Management Center for IPS Sensors \(IPS MC\)](#)

[CiscoWorks Monitoring Centre for Security \(SecMon\)](#)

[Cisco Security Monitoring, Analysis and Response System \(MARS\)](#)

[Cisco Threat Response \(CTR\)](#)

[IDS Event Viewer \(IEV\)](#)

[IDS Device Manager \(IDM\)](#)

[Cisco Secure Policy Manager \(CSPM\)](#)

[UNIX Director](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)



Introduction

This document provides a hardware/software compatibility matrix for the Cisco Intrusion Prevention System (IPS) Appliances (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255), Adaptive Security Appliance Security Services Module (SSM), Router Module and Catalyst 6000 Intrusion Detection System Modules (IDS-M-1, IDS-M-2). This document also provides an overview of the Management options. A brief overview of each application is provided, as well as a version compatibility matrix. Versions listed in each compatibility matrix are the only supported versions.

The Cisco Intrusion Prevention System was formerly known as Cisco Intrusion Detection System (IDS) or NetRanger. The Cisco Intrusion Prevention System Appliances are also known as Sensors. Refer to the relevant product documentation and release notes for more information.

Note: Be aware of the product status column in the tables within this document. This column denotes relevant End-of-Life (EoL)/End-of-Sale (EoS) notifications.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Intrusion Prevention System (IPS) Appliances (4210, 4215, 4220, 4230, 4235, 4240, 4250, 4255)
- Adaptive Security Appliance Security Services Module (SSM)
- Router Module
- Catalyst 6000 Intrusion Detection System Modules (IDSM-1, IDSM-2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

IPS Hardware/Software Compatibility

Table 1—Appliances

Appliance	Part #	Hardware	Optional Interfaces	Available Additional Hardware	Compatible Software Versions	Product Status
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	IDE hard drive with CDROM available for software upgrade and image recovery purposes.		IDS-4210-MEM-U= Additional 256 MB memory for SmartNet customers only to upgrade to version 4.1 and later. Customers can order the memory through the Product Upgrade Tool (registered customers only) .	3.1 to current *	End of Sale: December 8, 2003 Last Day of Support: December 8, 2008

IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	IDE hard drive and compact Flash. No CDROM drive is available for software upgrade and image recovery purposes.	IDS-4FE-INT=		4.1 to current *	Current
IDS-4220	IDS-4220-E	IDE hard drive with CDROM available for software upgrade and image recovery purposes.		IDS-4220-MEM-U= Additional 256 MB memory for SmartNet customers only to upgrade to version 4.1 and later. Customers can order the memory through the Product Upgrade Tool (registered customers only) .	3.1 to 4.1	End of Sale: July 31, 2002 Last Day of Support: July 31, 2007
IDS-4230	IDS-4230-FE	IDE hard drive with CDROM available for software upgrade and image recovery purposes.			3.1 to 4.1	End of Sale: July 31, 2002 Last Day of Support: July 31, 2007

IDS-4235	IDS-4235-K9	SCSI hard drive with CDROM available for software upgrade and image recovery purposes.	IDS-4FE-INT=	IDS-PWR= Spare power supply	3.1 to current *	End of Sale: May 31, 2005 Last Day of Support: May 31, 2010
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9 (DC powered, NEBS-Compliant only)	Compact Flash. No CDROM drive available for software upgrade and image recovery purposes.			4.1.4 to current *	Current
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	SCSI hard drive with CDROM available for software upgrade and image recovery purposes.	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	IDS-PWR= Spare power supply IDS-SCSI= Spare SCSI Hard drive	3.1 to current *	TX version only End of Sale: May 31, 2005 Last Day of Support for TX: May 31, 2010 The other two IDS 4250 platforms are not affected by this EoL announcement.
IPS-4255	IPS-4255-K9	Compact Flash. No CDROM drive available for software upgrade and image recovery purposes.			4.1.4 to current *	Current

Table 2—Modules

Module	Part #	Hardware	Optional Interfaces	Available Additional Hardware	Compatible Software Versions	Product Status
SSM	ASA-SSM-AIP-10-K9 (ASA AIP Security Service Module-10) ASA-SSM-AIP-20-K9 (ASA AIP Security Service Module-20)	Compact Flash. No CDROM drive available for software upgrade and image recovery purposes.			5.0 to current *	Current
Router Module	NM-CIDS-K9 NM-CIDS-K9= (RMA Part # only)	Compact Flash. No CDROM drive available for software upgrade and image recovery purpose.			Cisco IOS® Software Release 12.2 (15)ZJ or later Cisco IOS Software Release 12.3 (4)T or later IDS 4.1 to current *	Current
IDSM-1	WS-X6381-IDS WS-X6381-IDS= (RMA Part # ONLY)	IDE hard drive. No CD ROM drive available for software upgrade or image recovery purposes.			2.5 to 3.0	End of Sale: April 20, 2003 Last Day of Support: April 20, 2008
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (RMA Part # only)	IDE hard drive and compact Flash. No CDROM drive available for software upgrade and image recovery purposes.			4.0 to current *	Current

Note: The latest version of software available at the time of the publication of this document is 5.1. If you need a software version that is later

than 5.1, check the documentation for that version of code to ensure compatibility.

Management and Configurations Options

You can manage and configure IPS Sensors via the command line interface, or via one of the configuration or management tools listed in these sections.

CiscoWorks Management Center for IPS Sensors (IPS MC)

CiscoWorks Management Center for IPS Sensors is a tool with a scalable architecture for the configuration of Cisco Systems Network Sensors, switch IPS Sensors, IPS network modules for routers, and inline intrusion prevention software in routers. CiscoWorks Management Center for IPS Sensors allows administrators to save time by configuring multiple Sensors concurrently using group profiles. Additionally, it provides a powerful signature management feature that increases the accuracy and specificity in the detection of possible network intrusions.

Refer to the [Supported Devices and Software Versions for Management Center for IPS Sensors](#) documentation for compatibility information.

CiscoWorks Monitoring Centre for Security (SecMon)

CiscoWorks Monitoring Center for Security is a tool to capture, store, view, correlate, and report on security events from:

- Cisco Network IPS
- Cisco Network IDS
- Cisco Switch IDS
- Cisco IOS routers with inline IPS functions
- Cisco IDS modules for routers
- Cisco PIX firewalls
- Cisco Catalyst 6500 Series Firewall Services Modules (FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- CiscoWorks Monitoring Center for Security servers

Refer to the [Supported Devices and Software Versions for Monitoring Center for Security](#) documentation for compatibility information.

Cisco Security Monitoring, Analysis and Response System (MARS)

The Cisco Security Monitoring Analysis and Response System (MARS) is a family of high-performance, scalable appliances for threat management, monitoring, and mitigation that helps customers to make more effective use of network and security devices. Cisco Security MARS combines traditional security event monitoring with network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. With the combination of these capabilities, Cisco Security MARS helps companies to accurately identify and eliminate network attacks while maintaining network compliance.

MARS Versions	Supported Appliance/Sensor Software
3.3.x	3.x and 4.x
3.4.x	3.x, 4.x, 5.x

Refer to the product [Release Notes](#) for more information.

Cisco Threat Response (CTR)

Cisco Threat Response (CTR) works with Cisco IPS Sensors to provide an efficient intrusion protection solution. Cisco Threat Response virtually eliminates false alarms, escalates real attacks, and aids in the remediation of costly intrusions.

Cisco Threat Response is compatible with Cisco IPS version 3.x or later. Refer to the product [Release Notes](#) for more information. Also, be aware of the [End-of-Life announcement](#) for Cisco Threat Response.

IDS Event Viewer (IEV)

IDS Event Viewer (IEV) is a Java-based application that enables you to view and manage alarms for up to five Sensors. With IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms and import and export event data for further analysis. IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

IEV is supported from IDS version 3.1 to version 4.x. Although no longer supported from version 5.x, it can be used to monitor version 5.x Sensors. However, the new 5.0 features are not reported by IEV. Refer to the product [Release Notes](#) and [Configuration Guides](#) for more information.

IDS Device Manager (IDM)

IDS Device Manager (IDM) is a web-based application that allows you to configure and manage your Sensor. The web server for IDS Device Manager resides on the Sensor. You can access it through Netscape or Internet Explorer web browsers.

IDM is supported from IDS version 3.1. Refer to the product [Release Notes](#) and [Configuration Guides](#) for more information.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) provides policy-based security management for Cisco IDS Sensors, PIX firewalls and IPsec VPN routers.

Note: CSPM has reached its EoL. Refer to the [EoS/EoL Announcement for Cisco Secure Policy Manager 2.x & 3.x](#).

Model	CSPM 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i
IDS 4210 IDS 4220 IDS 4230	2.2.0.x	2.2.0.x 2.2.1.x	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0 2.5(1)S2 3.0(1)S3 3.0(1)S4	2.2.0.x 2.2.1.x 2.5.(0)S0 2.5(1)S0 2.5(1)S2 3.0(1)S3 3.0(1)S4	2.2.0.x 2.2.1.0 2.2.1.1 2.2.1.2 2.2.1.3 2.2.1.4 2.2.1.5 2.2.1.6 2.5(0)S0 2.5(1)S0 2.5(1)S1 2.5(1)S2 2.5(1)S3 2.5(1)S4 3.0(1)S3 3.0(1)S4 3.0(1)S5 3.0(1)S6 3.0(1)S7 3.0(1)S8
Catalyst 6000 Intrusion Detection System Module (IDSM-1)	2.5 IDSM	2.5 IDSM	2.5 IDSM 3.0 IDSM	2.5 IDSM 3.0 IDSM	2.5(0)S0 IDSM 2.5(1)S0 IDSM IDSM 2.5(1)S1 IDSM IDSM 2.5(1)S2 IDSM 3.0(1)S4 3.0(1)S6

UNIX Director

The UNIX Director provides a centralized graphical interface for the management of security across a distributed network. It can also perform other important functions such as data management through third-party tools, access to the NSDB, remote monitoring and management of

Sensors and IDSMs, and send pages or e-mail to security personnel when security events occur. The Director interface runs on top of HP OpenView.

Note: Software release 2.2.x for the Cisco IDS Appliance Sensor has reached its EoL. Refer to the [End of Life for Cisco IDS 2.2.x Sensor Software](#) documentation.

Director Versions	Supported Appliance/Sensor Software
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 and 2.5
2.2.3*	2.2.3, 3.0, 3.1

* 2.2.3 is the last available version of IDS Director Software and supports Sensor Software 3.1 and earlier.

While the 2.2.x Director may be backwards compatible with 2.2.x Sensor versions, if you do not have at least the same version of software on both Directors and Sensors, newer Sensor functionality may not be available in the Director. This forces a manual command line configuration. Refer to [Release Notes](#) and [Product Documentation](#) for more details.

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Security
Security: Intrusion Detection [Systems]
ASA-SSM-20 and tacacs+ - Oct 3, 2008
Reg. upgrading Cisco IDS 4.0 Version to 5.0 - Oct 3, 2008
IOS IDS vs. ASA Module vs. ISR module vs. Blade vs. Appliance - Oct 3, 2008
What is EPA in terms for security? - Oct 3, 2008
CSC not connect - Oct 2, 2008
Security: AAA
4.1 to 4.2 upgrade aborts on backup error - Oct 3, 2008
AAA configuration on switches 2960 - Oct 3, 2008
AD with ACS 4.2 issues - Oct 3, 2008
 - Oct 2, 2008
Machine authentication and MAR not working. - Oct 2, 2008
Security: General
isakmp keepalive - Oct 3, 2008
NAC Appliance: how to clear configuration ? - Oct 3, 2008
CSA MC Events Log and Agent Panel Events Corrolation - Oct 3, 2008
CSM VPN discovery - Oct 3, 2008
ASA5510-AIP10-K9 and Security Plus License - Oct 3, 2008
Security: Firewalling
Access - Oct 3, 2008
Cant ping the inside address of the ASA - Oct 3, 2008
Two public networks on ASA outside interface - Oct 3, 2008
Active/active, or active/standby? - Oct 3, 2008
www problem while upgrading in asa - Oct 3, 2008

Related Information

- [Cisco Intrusion Prevention System](#)
- [Security Product Field Notices \(including CiscoSecure Intrusion Detection\)](#)
- [Technical Support & Documentation - Cisco Systems](#)



Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)