



Release Notes for Cisco Video Assurance Management Solution 3.1

Revised: June 28, 2011, OL-24868-01

Contents

- [Introduction, page 1](#)
- [New Features with Release 3.1, page 4](#)
- [Solution Requirements, page 5](#)
- [Installation Notes, page 9](#)
- [Important Notes, page 10](#)
- [Open Caveats, page 11](#)
- [Related Documentation, page 12](#)



Note

Visit http://www.cisco.com/en/US/products/ps9518/prod_release_notes_list.html to view the latest version of these release notes.

Introduction

Cisco VAMS 3.1 provides service providers with a modular, end-to-end video assurance management architecture, including real-time, centralized monitoring of headends, hubs, core, distribution, regional, and aggregation networks for broadcast video services.

Cisco VAMS includes a service-aware dashboard that pinpoints and correlates alarms related to video service availability and quality from the headend or the transport network. Using Cisco VAMS, you can monitor and manage video services, such as linear broadcast and video on demand (VoD) based on MPEG-2 transmission streams (TS) and uncompressed flows.

See [Solution Requirements, page 5](#) for descriptions of the solution components and required software versions.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco VAMS 3.1 uses Cisco Multicast Manager (CMM CMM 3.1.2) with patch 3.1.23.1.2 for multicast monitoring and troubleshooting functions, such as monitoring of VidMon devices, and the Cisco ROSA Copernicus Network Management System (NMS) for monitoring of video headend events.

Additionally, the Cisco VAMS 3.1 system architecture includes an interface between Cisco Info Center and CMM. This interface is provided by:

- The Cisco Info Center Object Server (central DB)
- IBM Tivoli Business and Services Manager (TBSM), a service dashboard and visualization tool
- IBM Tivoli Impact, which supports the definition of service and network correlations

This accomplishes two key objectives for Cisco VAMS 3.1. It provides:

- Connectivity between Cisco ANA, CMM, the Cisco ROSA NMS, and Cisco Info Center.
- A “Single Pane of Glass” toolset¹ for Cisco VAMS 3.1.

Cisco Info Center contains rules files that specify the rules that define multicast alerts from various sources, such as probes, routers, Cisco 7600 series routers, Cisco ASR 9000 aggregation series routers, Digital Content Managers (DCMs), and other network management systems. The rules files contain code that extracts the multicast group and source information from these alerts and provides the operator with a Launch CMM Multicast Trace option and a Launch CMM Tree Change report option.

By integrating CMM and the Cisco ROSA NMS with Cisco Info Center, you can view all the alarm conditions and data for service level correlation and analysis. Additionally, for CMM events, you can launch troubleshooting and diagnostic analysis directly from Cisco Info Center.

Cisco VAMS 3.1 supports several third-party video probes. CMM supports video probes in two ways:

- CMM can receive SNMP traps directly from the following video probes or element managers:
 - IneoQuest iVMS
 - BridgeTech probes
 - Mixed Signals probes



Note Although CMM does not generate events or status from iVMS traps, CMM displays the traps.

- In addition, CMM can display flow trace status for probes for which it can be configured to poll directly:
 - IneoQuest probes
 - BridgeTech probes

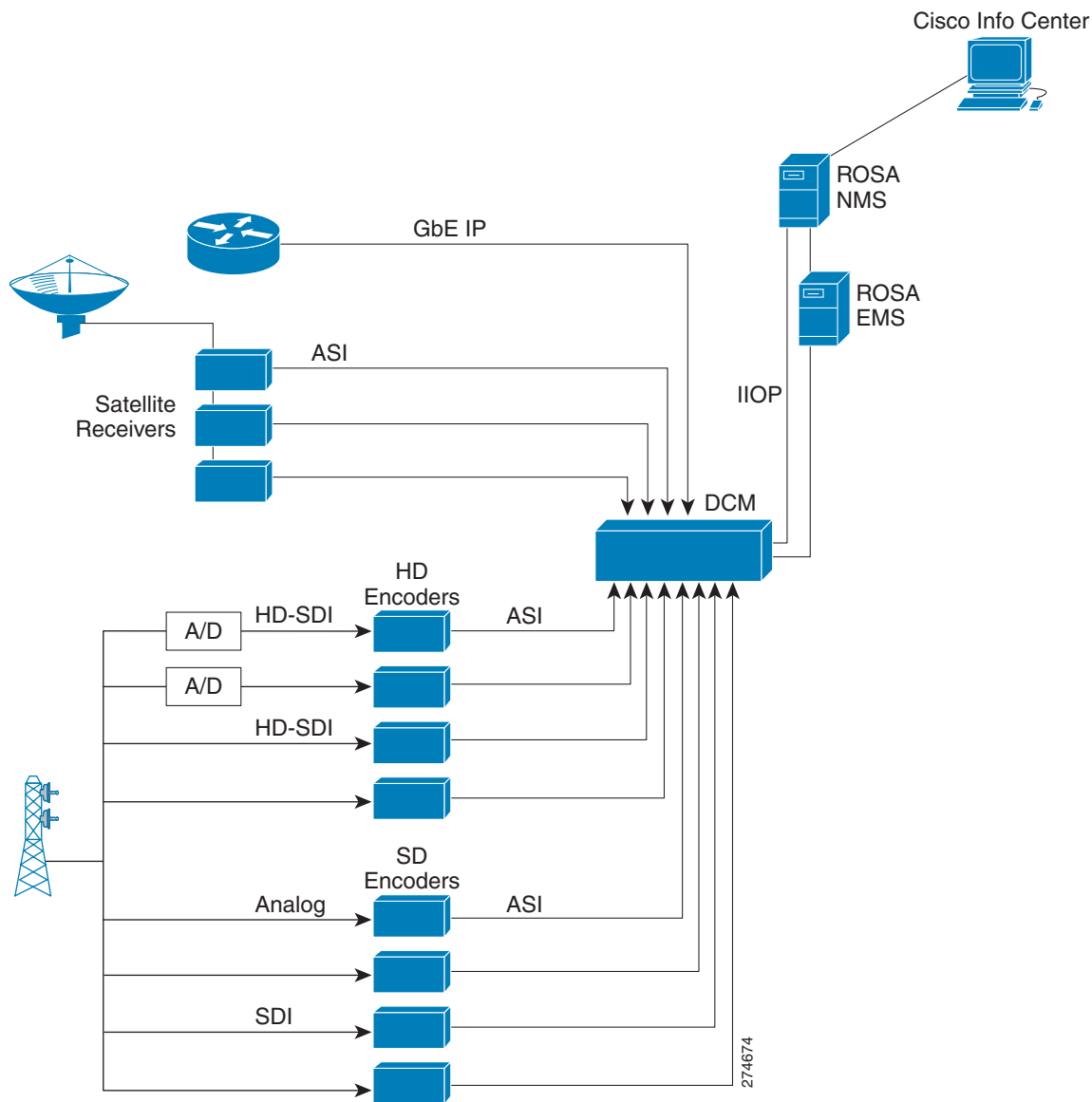
For a list of the video probes and element managers that you can use with CMM, and information on software and firmware versions, see [Table 1 on page 5](#).

Cisco VAMS 3.1 can be used with Cisco ANA 3.7 to build an abstracted network model through a set of virtual network elements (VNEs). Each VNE represents an element in the managed network.

See [Figure 1](#) and [Figure 2](#) for an overview of the Cisco VAMS components (the topologies shown in the figures are examples). [Figure 1](#) shows Cisco VAMS in the video headend network, and [Figure 2](#) shows Cisco VAMS in a video transport network.

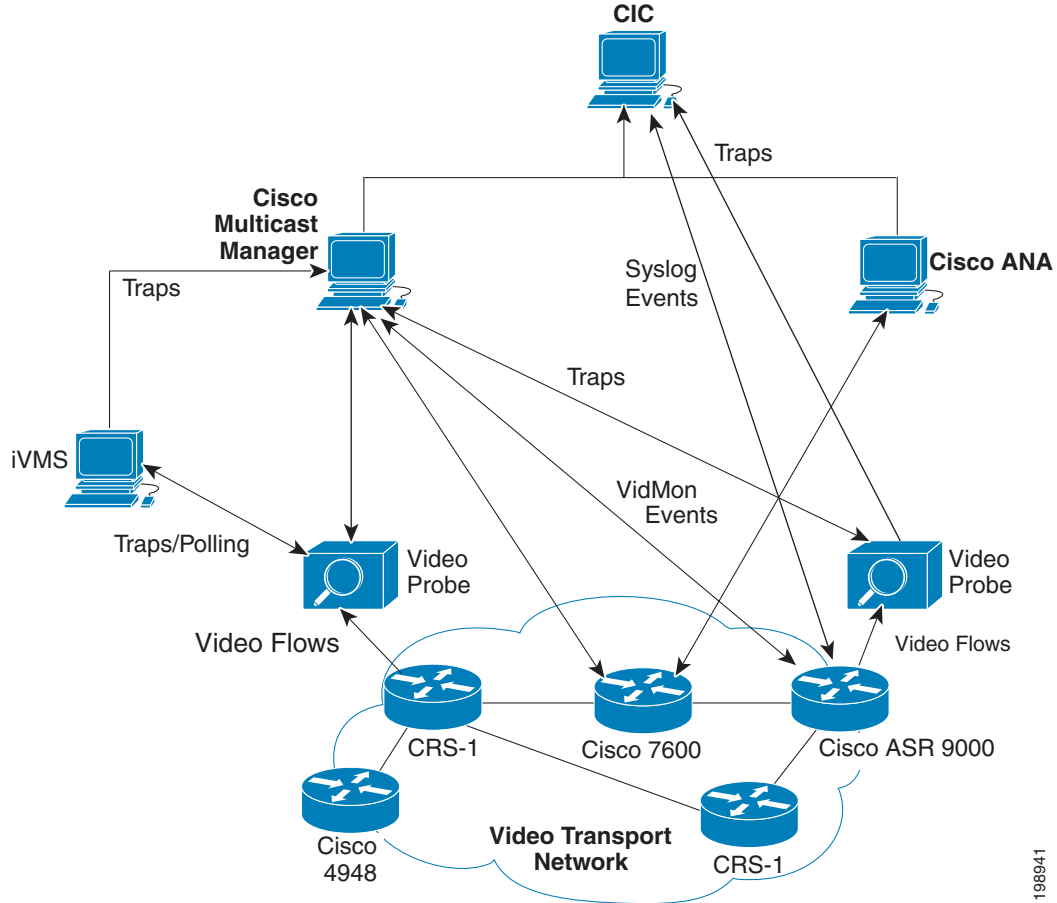
1. Single Pane of Glass—The ability to utilize multiple interconnected tools to monitor, diagnose, and troubleshoot network and video impairments from a single console.

Figure 1 Cisco Video Assurance Management Solution 3.1 Components for Video Headend Monitoring



The ROSA Copernicus NMS receives events either directly from the DCM, or, if the ROSA EMS is deployed in the headend network, from the ROSA EMS.

Figure 2 Cisco Video Assurance Management Solution 3.1 Components



198941

New Features with Release 3.1

Cisco VAMS 3.1 provides the following new features and functionality:

- Cross launching of the DCM GUI directly from TBSM events—When a DCM event is reported in Cisco Info Center (CIC), you can cross launch the DCM contextually by right-clicking the event.
- Channel-based service lineup—In VAMS 3.0, Cisco Info Center concatenated all channel names used in a give MuxID and displayed them as a single service. VAMS 3.1 introduces channel-based service lineup. In VAMS 3.1, Cisco Info Center creates a service for each channel that is defined in the channels.csv configuration file and makes each multicast flow carrying the channel a child of the channel service as shown in the TBSM Service Tree. Sometimes, multicast flow may not exist; existence of multicast flow is not required to create a service. This makes it easy for operators to identify the service events and MPTS streams affecting the channel service.
- Filtering alarms generated by NMS—CIC filters alarms generated by ROSA NMS before storing in the database. This prevents too many alarms being stored and reducing the performance of CIC. The probe filter rules can be customized to suit your requirement.
- Creating and editing channel line-up automatically—This feature allows you use a script that will edit CSV files and input them into the appropriate CIC components.

Solution Requirements

Table 1 lists the software and firmware requirements for the Cisco VAMS components.

Table 1 Requirements for VAMS Solution Components

Solution Component	Version Information	Notes
Cisco VAMS	3.1	Installation script
Active Network Abstraction (ANA)	3.7.2	ANA Gateway—Sun Fire V490, Solaris 10 ¹ ANA Unit—Sun Fire V480, Solaris 10 ¹ ANA Client—IBM or PC compatible work station, Windows 2000 or Windows XP ¹
Cisco Multicast Manager	3.1.2	Sun—Solaris 8, 9, or 10 Linux—Linux 4 or 5
ROSA Copernicus Element Management System	4.2	The ROSA EMS is supported on the following operating systems: <ul style="list-style-type: none"> • Microsoft Windows 2000 • Microsoft Windows Server 2003 • Windows XP, Service Pack 2 • Microsoft Windows Vista
ROSA Copernicus NMS	4.2	—
Digital Content Manager	DCM software V8.7	Model D9900 and D9901 with GbE interface card.
Cisco 7600 Series router	RLS8	Supervisor card: 7600-SUP720-3BXL with redundant SUP720-3BXL. Line cards include the following Ethernet Services Plus (ES+) line cards: 76-ES+T-4TG, 76-ES+T-40G, 7600-ES+4TG3C, 7600-ES+20G3C, and several other versions. Cisco 7600 Series Route Switch Processors (RSPs) 720 with 10 Gigabit Ethernet uplinks include the RSP720-3C-GE and the RSP720-3CXL-10GE.
Cisco ASR9000 series routers	IOS XR 4.0.1	Apply IOS-XR Software Maintenance Upgrade (SMU) <i>asr9k-mcast-3.9.1.CSCtf69443-1.0.0</i> to all ASR 9000 routers.
Cisco uBR10K	12.2(33)SCB4	
Cisco Catalyst 6500 switch	12.2(33)SXI	—
Cisco Carrier Routing System-1 (CRS-1)	IOS-XR 4.0.1	Line cards include CRS-MS-C, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE
Cisco Catalyst 4948 switch (CAT 4948-10GE)	12.2(46)SG	—

Table 1 Requirements for VAMS Solution Components (continued)

Solution Component	Version Information	Notes
Cisco Info Center	—	VAMS release 3.1 includes the following Cisco Info Center IBM Tivoli Netcool components: <ul style="list-style-type: none"> • ObjectServer - 7.3 • TBSM - 4.2.1 • Impact - 5.1.1
IneoQuest iVMS (IneoQuest NMS for IQ probes)	Version 4.02.001.02.29	
IneoQuest video probes	<ul style="list-style-type: none"> • Singulus G1-T Media Analyzer, Geminus G1-T • Geminus G10 • Geminus G2x • IQ Media Monitor • Cricket - ASI version • Cricket - MS version • Cricket - IP version • Cricket - QAM and 8VSB versions • Cricket - QAM Plus versions 	<ul style="list-style-type: none"> • Firmware Version: TB6x-3.10a-120109.iqz Software Version: 3.10a • Firmware Version: Denali-2.1-4a-120109.iqz Software Version 2.14a • Firmware Version: MAG2x-1/23a-120109.iqz Software Version 1.23a • Firmware Version: MA6x-3.10a-120109.iqz Software Version: 3.10a • Firmware version: Cricket-MS6x-2.11a-120109.iqz Software Version: 2.11aa • Firmware Version: Cricket-6x-2.10a-120109.iqz Software Version: 2.10a • Firmware version: Cricket-6x-2.10a-120109.iqz Software Version: 2.10a • Firmware Version: Cricket-Q6x-2.10a-120109.iqz Software Version: 2.10a • Cricket-DQ-1.4a-120109.iqz Software Version: 1.4a

Table 1 **Requirements for VAMS Solution Components (continued)**

Solution Component	Version Information	Notes
Mixed Signals video probe	Sentry 136 Digital Content Monitor ²	Sentry Engine Version: PDM (build 1460.84) Sentry Database Version: 3.1.31 Sentry Configuration: TRANSPORT
Bridge Technologies video probes	VB Series	Version: 3.1.0-26, including the VB260 QAM probe. <ul style="list-style-type: none"> • VB220—Version 4.2.0-15 • VB250—Version 4.2.0-15 • VB260—Version 4.2.0-15 • VB270—Version 4.2.0-15 • VB280—Version 4.2.0-15

1. See the *User Guide for Cisco Video Assurance Management Solution 2.0* at http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/user/guide/vams_20_user.html for detailed specifications.
2. Cisco VAMS 3.1 does not support carousel-related traps for the Mixed Signals Sentry 136.

ROSA NMS Requirements

Table 2 indicates the requirements for the computer used to run the ROSA NMS client.

Engineers, please verify the numbers below.

Table 2 ROSA NMS Client Requirements

Item	Minimum Requirements	Recommended
Processor	600 Mhz Pentium III compatible or higher	1 Ghz Pentium III compatible or higher
Memory	Minimum 192 MB	512 MB
Free disk space	1 GB	10 GB
Operating System	Windows 2000, Windows Server 2003, Windows XP, Windows Vista	
Web browser	Microsoft Internet Explorer v. 5 or higher	
Serial Ports	One or more serial ports (RS-232 and/or RS-285 if needed)	
Ethernet Adapter	Required	

TBSM Requirements

Hardware Requirements

TBSM requires:

- A 4-CPU system with 2.0 GhZ or greater CPUs
- 8 GB of RAM

Software Requirements

The IBM Tivoli Service Manager (TBSM) console supports the IBM 1.5 Java Runtime Environment (JRE). TBSM 4.2.1 also supports Sun Microsystems JRE version 1.6.

TBSM 4.2.1 requires one of the following browsers:

- Internet Explorer 6.0 or 7.0
- Mozilla Firefox 2.0

JRE level 1.6 or later is recommended.

Installation Notes

Installation of Cisco VAMS involves installation of its key components:

Hardware Installation

- The core network elements of the video transport network:
 - Cisco 7600 Series router
 - Cisco ASR 9000
 - Cisco Catalyst 6500 Series switch
 - Cisco uBR 10000
 - Cisco CRS-1
 - Cisco Catalyst 4948 Series switch
- Management servers for Cisco Multicast Manager (CMM) 3.1.2
- Management servers for Cisco Active Network Abstraction (ANA) 3.7 (includes gateway, unit, and client installation)
- ROSA Copernicus NMS 4.0.4.8
- Digital Content Manager and related video headend equipment
- Third-party video probes:
 - Bridge Technologies VB Series, including the VB260 QAM probe
 - IneoQuest probes
 - Mixed Signals Sentry Digital Content Monitor
- Management servers for Cisco Info Center Tivoli Integrated Portal (TIP) and TBSM

Software Installation

- The IPTV-enabled IOS software versions:
 - 12.2(33)ZI on the Cisco 7600 Series
 - 12.2(33)SCB4 on the uBR10K
 - IOS XR 3.9 on the Cisco ASR 9000 and Cisco CRS-1
 - 12.2(46)SG on the Cisco Catalyst 4948 Series switch
- Cisco ANA 3.7.2 (includes gateway, unit, and client installation)
- Cisco Multicast Manager (CMM) 3.1.2 software on dedicated server

- VAMS release 3.1 includes the following Cisco Info Center IBM Tivoli Netcool components:
 - Object Server 7.3
 - Impact 5.1.1
 - TBSM 4.2.1



Note

Cisco Advanced Services will assist you in any modifications that might be required for the Impact component or other Cisco Info Center components.

For complete details of the VAMS 3.1 installation workflow, including procedures and references to installation documents, see the *User Guide for Cisco Video Assurance Management Solution, 3.1*, available online at:

http://www.cisco.com/en/US/products/ps9518/products_user_guide_list.html .

For details on the VAMS 3.1 installation workflow, consult with your Cisco Advanced Services representative.

Uninstall

You uninstall Cisco VAMS 3.1 by deleting the Cisco Info Center components The uninstallation procedure is described in the *User Guide for Cisco Video Assurance Management Solution 3.1*.

Important Notes

This section contains the following note:

- [Increasing the Heap Size Used by Netcool Impact to Handle High Event Loads, page 10](#)

Increasing the Heap Size Used by Netcool Impact to Handle High Event Loads

By default, the allocated heap size for IBM Tivoli Netcool Impact is 1204 MB. If your VAMS installation has high event loads, you might receive alerts regarding Impact’s heap size. For example, the following alert might appear:

```
Alert: Impact's Heap size is very close to Max Heap Size! Impact's Heap using 1707M out of 1200M, Free System Memory Available: 5499M, Impact requires at least: 1350M of memory
```

To prevent this issue, we recommend that you increase Impact's maximum heap size to 3072 MB to handle the high event loads.

To increase the maximum heap size for Impact:

Step 1 On the VAMS host device, change directory to the */bin* directory for Impact:

```
bash-3.00# cd $NCHOME/eWAS/profiles/ImpactProfile/bin
```

Step 2 Enter the commands shown in [Figure 3](#) to start the *wsadmin* utility and increase Impact’s heap size.

Figure 3 Increasing Maximum Heap Size Used by Impact

```

vams-ed-server-102 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
bash-3.00# cd #NCHOME/eWAS/profiles/ImpactProfile/bin
bash-3.00# ./wsadmin.sh -lang jython -username wasadmin -password netcool
WASK7209I: Connected to process "server1" on node ImpactNode using SOAP connector; The type of process is: UnManagedProcess
WASK7031I: For help, enter: "print Help,help()"
wsadmin>jvm = AdminConfig.list("JavaVirtualMachine").split("\r\n") [0]
wsadmin>AdminConfig.modify(jvm, "[[maximumHeapSize 3072]]")
wsadmin>AdminConfig.save()
wsadmin>exit
bash-3.00#

```

Ready ssh2: AES-128 12, 12 26 Rows, 94 Cols VT100

Open Caveats

Table 3 indicates the open caveats for Cisco VAMS 3.1.

Table 3 *Open Defects in Cisco VAMS 3.1*

Defect ID	Description
CSCtq35139	<p>Incorrect node and channel names for ASSR Events.</p> <p>Conditions The channel and node names of ASSR events are incorrectly displayed in the AEL. For example, the following output is generated for an ASSR Service Loss event:</p> <ul style="list-style-type: none"> Actual channel name—EURONEWS; Actual node name—RHE-1-DCM-1. Output channel name—CNBC; Output node name—EURONEWS@RHE-1-DCM-1. <p>Workaround None</p>
CSCtq46248	<p>Some cross-launches, such as CMM, CMM_FlowChange, CMM_TreeChange, are applied to non-related events.</p>
CSCtq54496	<p>Removing a service in the .csv file may not reflect in the Dashboard.</p> <p>Conditions Sometimes, after deleting a service and replacing it with another, the changes are not reflected on the Dashboard.</p> <p>Workaround Remove the service via the GUI manually. From Administration > Event Management Tools > Service Administration, from the Service Navigation view, select Services. Remove the service that you wish to delete.</p>
CSCtq54601	<p>Service Tree not updated when adding new MPTS alias.</p> <p>Conditions When a new service is added against an existing multicast alias, the addition is not reflected in the service tree. The Service Tree continues to display the older service.</p>
CSCtq57153	<p>Event List displays entire list of events against a given multicast alias instead of displaying the events of just the channel selected.</p> <p>Conditions When a channel from the Service Tree on the Service Dashboard is selected, the Event List displays the events of all channels associated with the multicast group. AEL events of the just channel selected is not displayed.</p>

Related Documentation

See the following sections for information on related documentation:

- [Cisco VAMS 3.1 Documentation, page 12](#)
- [Documentation for VAMS Components, page 13](#)

Cisco VAMS 3.1 Documentation

In addition to the *User Guide for Cisco Video Management Solution, 3.1*, the Cisco VAMS documentation set comprises:

- *User Guide for Cisco Video Management Solution, 3.1*

Provides an overview of the solution features and architecture, installation and configuration instructions, and information on using the TBSM and Webtop interfaces to view events and troubleshoot events in the video network. This document is viewable online at:

http://www.cisco.com/en/US/products/ps9518/products_user_guide_list.html

- *Documentation Guide for Cisco Video Management Solution, 3.1*

Provides links to the documentation for the Cisco VAMS 3.1 component products and for related products. This document is available online at:

http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Documentation for VAMS Components

For links to the documentation for the VAMS product components, see the *Documentation Guide for Cisco Video Management Solution, 3.1*, viewable online at:

http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)