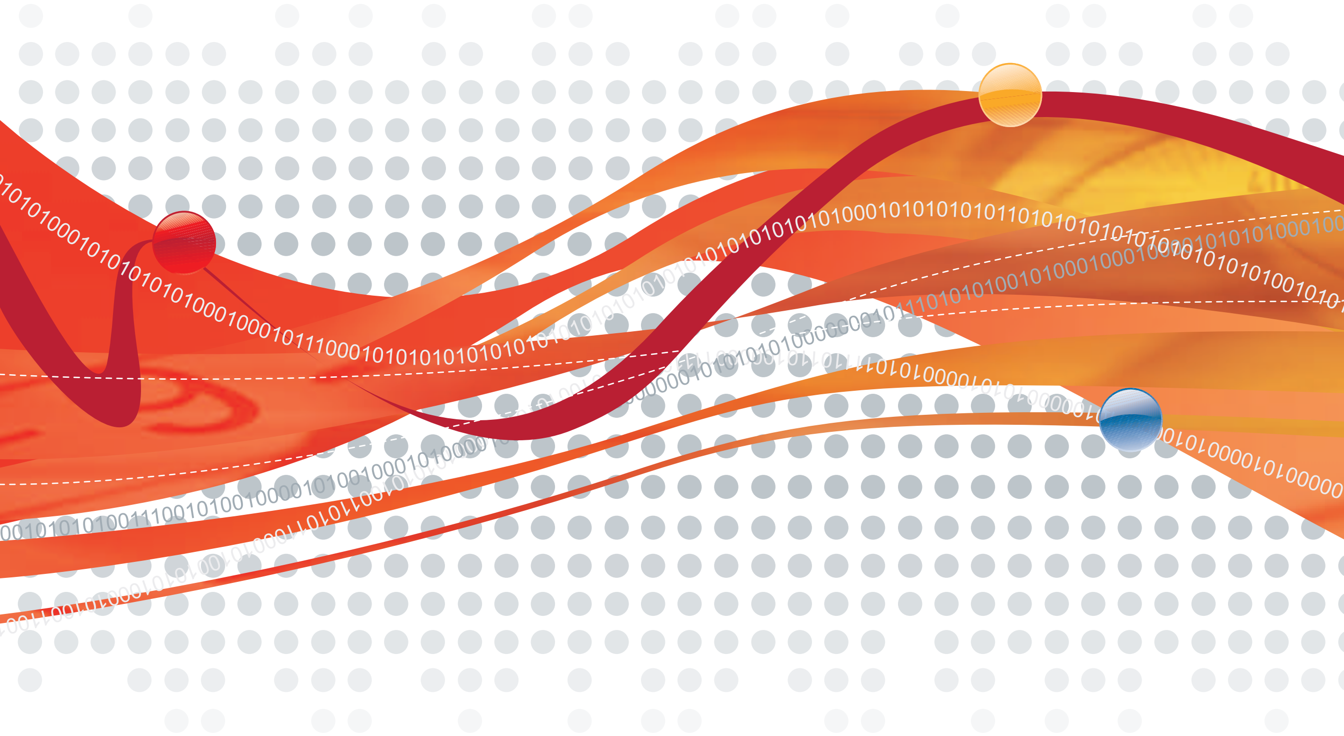
InterScan™ Messaging Security Suite 7

for Enterprise and Medium Business

for Crossbeam X-Series Platforms

Installation Guide



Messaging Security

General Copyright Information

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, expressed or implied, and users must take full responsibility for their application of any products specified in this document. Trend Micro Incorporated disclaims responsibility for errors that may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

For permission to reproduce or distribute please contact your Trend Micro Incorporated account executive.

Trend Micro Copyright Information

Trend Micro, Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document Part No. MSEM74077/90424

Release Date: May 2009

Patents Pending

Crossbeam Systems Copyright Information

Contents

Preface

Audience x
InterScan Messaging Security Suite Documentation x
Crossbeam Systems Related Documentation xi
Document Conventions xii

Chapter 1: Introducing InterScan Messaging Security Suite

About IMSS 1-2
Deployment Options 1-2

Chapter 2: Component Descriptions

Prerequisites for Using InterScan Messaging Security Suite 2-2
- Licensing Requirements 2-2
- Software Requirements 2-2
- Hardware Requirements 2-3
- General XOS Setup Information 2-4
- XOS Setup Requirements 2-4

XOS Setup Instructions 2-4
- Create and Configure a VAP Group for the Application 2-4
- Configure an NTP Server for the X-Series Platform 2-5
- Create and Configure a Management Circuit 2-6
- Creating Traffic Circuits 2-7

Chapter 3: Installing the Application

Loading the Application 3-2
Installing the Application 3-2
Verifying the Installation 3-7

Chapter 4: Application Management

Basic Application Management Commands 4-2
Using the show application vap-group Command 4-3
Uninstalling the Application 4-6

Chapter 5: Troubleshooting and Support Information

IMSS Installation Issues 5-2
Support and Training 5-3
Customer Comments 5-3

Appendix A: Configuring Firewall Rules for Ports Used by the IMSS Gateway

Inbound Ports to IMSS Gateways A-2
Outbound Ports from IMSS Gateways A-2
Other Ports A-3

Index

Preface

Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Security Suite 7.0 for Crossbeam X-Series Platfroms Installation Guide*. This guide describes how to install and configure InterScan Messaging Security Suite on a Crossbeam Systems X-Series Platform.

Please refer to the *IMSS 7.0 Administrator's Guide* for information on how to configure IMSS settings and the Online Help in the Web management console for detailed information on each field on the user interface.

This preface discusses the following topics:

- Audience on page x
- InterScan Messaging Security Suite Documentation on page x
- Crossbeam Systems Related Documentation on page xi

Audience

The InterScan Messaging Security Suite documentation is written for IT administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks.

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

InterScan Messaging Security Suite Documentation

The InterScan Messaging Security Suite (IMSS) documentation consists of the following:

- **Installation Guide**—Contains introductions to IMSS features, system requirements, and provides instructions on how to deploy and upgrade IMSS in various network environments.
- **Administrator's Guide**—Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.
- **Online Help**—Provides detailed instructions on each field and how to configure all features through the user interface. To access the online help, open the Web management console, then click the help icon (?).
- **Readme Files**—Contain late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The *Installation Guide, Administrator's Guide* and *readme files* are available at:
`http://www.trendmicro.com/download`

Crossbeam Systems Related Documentation

The following Crossbeam Systems documentation may be helpful when configuring Crossbeam Systems products:

- X80 Platform Hardware Installation Guide
- X45 Platform Hardware Installation Guide
- XOS Command Reference Guide
- XOS Release Notes
- XOS Configuration Guide
- Install Server User Guide

Visit the Crossbeam Systems Customer Support Web site at http://www.crossbeam.com/services/online_support.php for the latest updates to Crossbeam technical documentation.

Document Conventions

To help you locate and interpret information easily, the IMSS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and other user interface items
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that must be avoided

Chapter 1

Introducing InterScan Messaging Security Suite

This chapter introduces InterScan Messaging Security Suite (IMSS) features, capabilities, and technology, and IMSS's operation on a Crossbeam Systems X-Series Platform.

Topics include:

- About IMSS on page 1-2
- Deployment Options on page 1-2

About IMSS

InterScan Messaging Security Suite (IMSS) 7.0 integrates antivirus, anti-spam, anti-phishing, and content filtering for complete email protection. This flexible software solution features award-winning anti-virus and zero-day protection to block known and unknown viruses.

Multi-layered anti-spam combines the first level of defense in Email Reputation Services with customizable traffic management through IP Profiler and the blended techniques of a powerful composite engine. Multi-lingual anti-spam provides additional support to global companies. Advanced content filtering helps to achieve regulatory compliance and corporate governance, and provides protection for confidential information. IMSS delivers protection on a single, highly scalable platform with centralized management for easy, comprehensive email security at the gateway.

Deployment Options

IMSS 7.0 only supports the distributed deployment option for X-Series Platforms. In this scenario, the Central Controller and the EUQ run on the high-performance, general-purpose hardware with redundant components (power supplies, cooling fans, hard drives, etc). The components participating in scanning and content filtering (MTA, Scanner, NRS, and IP Profiler) run on the X-Series APM blades.

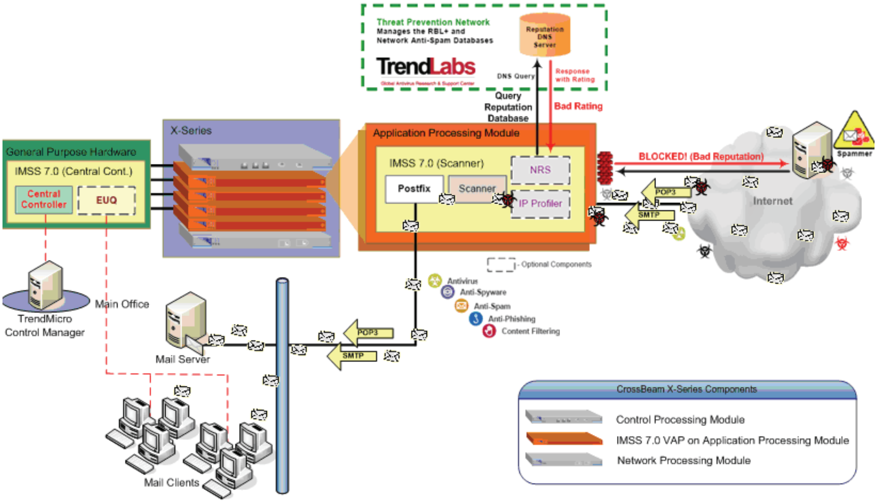


FIGURE 1-1. Distributed Deployment Option

Chapter 2

Component Descriptions

This chapter explains what requirements are necessary to manage IMSS and explains the various software components it needs to function.

Topics include:

- Prerequisites for Using InterScan Messaging Security Suite on page 2-2
- XOS Setup Instructions on page 2-4

Prerequisites for Using InterScan Messaging Security Suite

Licensing Requirements

InterScan Messaging Security Suite requires the following licenses:

- InterScan Messaging Security Suite Anti-Virus and Content Filter
- InterScan Messaging Security Suite Spam Prevention Solution and IP Filtering Service

Note: To obtain access to all IMSS features, you must install both of the above licenses on each VAP on the X-Series Platform.

Software Requirements

InterScan Messaging Security Suite requires Postfix 2.1 or above. The following additional components may also be required depending on your installation:

- Directory Servers:
  - Microsoft Active Directory 2000 and 2003
  - IBM Lotus Domino 6.0 or above
  - Sun Java System Directory Server
- Trend Micro Control Manager Version 3.5

Note: For proper IMSS operation, firewall rules must be configured to allow the IMSS Gateway to use specific ports for incoming and outgoing traffic. See Configuring Firewall Rules for Ports Used by the IMSS Gateway on page A-1, for a list of ports over which firewalls must allow traffic to and from the IMSS Gateway.

The Crossbeam Systems X-Series Platform on which you are installing InterScan Messaging Security Suite must meet the following OS version requirements:

- The X-Series Platform must be running XOS version 8.5.x.
- The VAP group on which the application is to be installed must be configured to run the xslinux_v3 VAP OS.

Hardware Requirements

To ensure optimal performance, each APM on which the application is to be installed should have more memory than the minimum required. Additionally, heavy traffic or a large number of sustained network connections require more APM memory. The following table lists the hardware requirements for this application.

TABLE 2-1. X-Series Hardware Requirements

X-Series Chassis Models Supported	X80, X45
APM Modules Supported	APM-8600, APM-8650
Minimum APM Memory	4GB RAM
Supported CPM Modules	CPM-8600
Supported NPM Modules	NPM-8600, NPM-8620, NPM-8650
APM Local Disk Requirements	On each APM: • One APM Local Disk is required. **Tip:** Crossbeam recommends using two Local Disks configured for RAID-1. • 10GB disk space for mail storage. • 4GB disk space for the working quarantine folder.

Trend Micro recommends the following for the general-purpose hardware on which the Central Controller and EUQ are installed :

- 50GB disk space for the Admin Database.
- 20GB disk space for the EUQ Database

Note: The recommendation is based on 500,000 email messages per day, 50% quarantine rate, and logs preserved for a month.

General XOS Setup Information

Consider the following general setup recommendations for this application on an X-Series Platform:

- Trend Micro recommends that you run only one application per VAP group.
- If you uninstall the application, do not reuse the VAP group; delete the group and create a new VAP group.

XOS Setup Requirements

The following XOS-related setup requirements are discussed in the next section in this chapter:

- Create and Configure a VAP Group for the Application on page 2-4
- Configure an NTP Server for the X-Series Platform on page 2-5
- Create and Configure a Management Circuit on page 2-6
- Creating Traffic Circuits on page 2-7

XOS Setup Instructions

Before installing IMSS, you must perform the following steps to configure XOS to support the IMSS application.

Note: Refer to the Crossbeam Systems *XOS Configuration Guide* and *XOS Command Reference Guide* to modify the XOS setup commands for your installation requirements.

Create and Configure a VAP Group for the Application

To create and configure a VAP group for the application:

```
CBS# configure vap-group <vAP group name> xslinux_v3

    vap-count <number of vAPs>

    ap-list <list of ap>

    max-load-count <number of vAPs set to run>
```

```
   ip-flow-rule <flow rule name>
      action load-balance
      activate
      end
```

For example:

```
CBS# configure vap-group imss xslinux_v3
   vap-count 2
   ap-list ap1 ap2
   max-load-count 2
   ip-flow-rule imss_fr
      action load-balance
      activate
      end
```

WARNING! **Quarantined messages reside on the local disk and are accessed through the IMSS scanner that quarantined them. In order for users to gain access to the quarantined messages, the VAP** *MUST* **always use the same APM blade. Therefore, VAP failover** *SHOULD NOT* **be performed. This risk is reduced by specifying the ap-list in the example above.**
Make sure that the max-load-count is set to the same number as the vap-count before continuing the installation.

Configure an NTP Server for the X-Series Platform

Configure the X-Series Platform to use the same Network Time Protocol (NTP) server that the Central Controller and EUQ use, so that you can achieve proper time synchronization between all components of the solution.

To configure an NTP server for the X-Series Platform, enter the following XOS CLI command:

```
CBS# configure ntp server <NTP_server_IP_address>
```

Create and Configure a Management Circuit

To create and configure a circuit to manage the application:

1. Create a management circuit.

```
CBS# configure circuit <name of management circuit>

  device-name <name of the device>

  vap-group <vAP group name>

    ip <starting ip-address>/<netmask> <broadcast-address>
    increment-per-vap <high range ip-addr>

    end
```

For example:

```
CBS# configure circuit management

  device-name mgmt

  vap-group imss

    ip 192.168.10.124/24 192.165.10.255 increment-per-vap
    192.168.10.125

    end
```

Note: You must specify the increment-per-vap parameter even if the VAP group contains only one VAP.

2. Assign the circuit to a physical interface (chassis slot #/port #).

```
CBS# configure interface <interface type> <slot
number>/<port number>

  logical <name of logical>

    circuit <name of management circuit>

    end
```

For example:

```
CBS# configure interface gigabitethernet 1/1

  logical lgcl11
```

```
    circuit mgmt

    end
```

3. Configure a default route.

   ```
   CBS# configure ip route 0.0.0.0/0 <default_gateway_ip>
   vap-group <vap_group_name>
   ```

   For example:

   ```
   CBS# configure ip route 0.0.0.0/0 192.168.10.1 vap-group
   imss
   ```

4. Setup a DNS server for the VAP group.

   ```
   CBS# configure dns server <dns_server_ip> vap-group
   <vap_group_name>
   ```

   For example:

   ```
   CBS# configure dns server 192.168.15.25 vap-group imss
   ```

Creating Traffic Circuits

Since the flow originates from the APM, you must specify a unique IP address for the external network side of the VAP so that return packets will be correctly load-balanced. To accomplish this, you must configure increment-per-vap on the external circuit. Please refer to the *XOS Configuration Guide* and the *XOS Commands Reference Guide* for configurations involving advanced circuit and interface options.

To create a multiple interface configuration:

1. Create one circuit for the internal traffic interface.

   ```
   CBS# configure circuit <name of internal traffic circuit>

     device-name <name of the device>

     vap-group <vAP group name>

       ip <ip-address>/<netmask> <broadcast-address>

       end
   ```

   For example:

   ```
   CBS# configure circuit inttraffic
   ```

```
  device-name trf1
  vap-group imss
    ip 10.201.162.3/23 10.201.163.255
    end
```

2. Create one circuit for the external traffic interface.

```
CBS# configure circuit <name of external traffic circuit>
  device-name <name of the device>
  vap-group <VAP group name>
    ip <starting ip-address>/<netmask> <broadcast-address>
     increment-per-vap <high range ip-addr> alias <shared-ip>
    end
```

For example:

```
CBS# configure circuit exttraffic
  device-name trf2
  vap-group imss
    ip 10.201.164.3/23 10.201.165.255 increment-per-vap
     10.201.164.6 alias 10.201.164.7/23
    end
```

3. Assign each circuit to a physical interface (chassis slot#/port #).

```
CBS# configure interface <interface type> <slot
number>/<port number>
  logical <name of logical>
    circuit <name of internal traffic circuit>
    end


CBS# configure interface <interface type> <slot
number>/<port number>
  logical <name of logical>
```

```
    circuit <name of external traffic circuit>

    end
```

For example:

```
CBS# configure interface gigabitethernet 1/4

  logical lgcl14

    circuit inttraffic

    end


CBS# configure interface gigabitethernet 1/5

  logical lgcl15

    circuit exttraffic

    end
```

To create a single interface configuration:

1. Create one circuit for the internal and external side traffic interface. The alias is used to connect from the internal side while the increment-per-vap addresses are used for the external side.

```
CBS# configure circuit <name of traffic circuit>

  device-name <name of the device>

  vap-group <vAP group name>

    ip <starting external ip-address>/<netmask>
    <broadcast-address> increment-per-vap
    <high range external ip-address> alias
    <shared internal ip-address>

    end
```

For example:

```
CBS# configure circuit traffic

   device-name trf1

   vap-group imss
```

```
      ip 10.201.162.3/23 10.201.163.255 increment-per-vap
      10.201.162.6 alias 10.201.162.7/23

       end
```

2. Assign the circuit to a physical interface (chassis slot#/port #).

```
CBS# configure interface <interface type> <slot
number>/<port number>

  logical <name of logical>

    circuit <name of traffic circuit>

    end
```

For example:

```
CBS# configure interface gigabitethernet 1/4

  logical trflgcl14

    circuit traffic

    end
```

Chapter 3

Installing the Application

This chapter provides instructions for loading and installing the application and for verifying the installation.

WARNING! **Ensure to complete the pre-configuration requirements in the previous chapter before continuing.**

Topics include:

- Loading the Application on page 3-2
- Installing the Application on page 3-2
- Verifying the Installation on page 3-7

Loading the Application

Complete the following steps to load the application on your Crossbeam Systems X-Series Platform.

To load the application:

1. Log on to the X-Series Platform as **root**.

   ```
   CBS# unix su

   Password:

   [root@xxxx admin]#
   ```

2. Copy the CBI package to /crossbeam/apps/archive/.

   ```
   [root@xxxxx admin]# cp imss-7.0-14-xos.cbi
   /crossbeam/apps/archive/
   ```

3. Use the following command to return to the CBS# prompt.

   ```
   [root@xxxxx admin]# exit
   ```

4. Save the running configuration.

   ```
   CBS# wr
   ```

5. Check that the application is present.

   ```
   CBS# show application
   App ID           : imss
   Name             : InterScan Messaging Security Suite
   Version          : 7.0
   Release          : 14-xos
   CBI Version      : 1.0.0.0
   ```

Installing the Application

Complete the following steps to install the application on your Crossbeam Systems X-Series Platform.

To install the application:

1. Execute the following XOS CLI command.

   ```
   CBS# application imss version 7.0 vap-group <VAP_group_name>
   install
   ```

2. When the license agreement is displayed, accept the license agreement.
3. Type the Admin database information of the existing Central Controller.

   ```
   All instances of the Scanner Service need to be registered to
   an existing Central Controller.

   Please provide database info of existing IMSS server:

   IMSS database server IP []: <ip of the Central Controller>

   IMSS database name [imss]: <name of the database on the
   Central Controller>

   IMSS database user name [sa]:<username>

   IMSS database user password

   Password: <password>

   Confirm Password: <password>
   ```

   For example:

   ```
   Please provide database info of existing IMSS server:

   IMSS database server IP []: 192.168.13.50

   IMSS database name [imss]: imss

   IMSS database user name [sa]: sa

   IMSS database user password

   Password: ******

   Confirm Password: *******
   ```

4. Type the local IP address the IMSS instances will use to connect to the existing Central Controller. This would be the increment-per-vap IP address assigned to each VAP.

```
(imss_1) Please enter the IP address this IMSS instance will
use to connect to the existing IMSS server []: <ip address of
the management interface on the first vap>
```

```
(imss_2) Please enter the IP address this IMSS instance will
use to connect to the existing IMSS server []:<ip address of
the management interface on the second vap>
```

For example:

```
(imss_1) Please enter the IP address this IMSS instance will
use to connect to the existing IMSS server []:
192.168.10.124
```

```
(imss_2) Please enter the IP address this IMSS instance will
use to connect to the existing IMSS server []:
192.168.10.125
```

5. Type the domain name that you want to specify in the mydomain parameter of the Postfix configuration file.

   ```
   Enter your domain name []: <domain name>
   ```

   For example:

   ```
   Enter your domain name []: yourcompany.com
   ```

6. Confirm/deny installation of the Network Reputation Services (NRS).

   ```
   Do you want to install Network Reputation Services? [y]: y
   ```

7. If you choose to install the NRS, the installer prompts for the NRS Activation Code:

   ```
   Please enter your NRS Activation Code []:
   <XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX>
   ```

8. Confirm/deny installation of the IP Profiler.

   ```
   Do you want to install IP Profiler? [y]: y
   ```

WARNING! **IP Profiler uses port 25 by default. Postfix listens to the same port by default. If IP Profiler is installed, change the Postfix listening port to 2500 in the IMSS Web console before installing IMSS on the X-Series Platform.**

9. When prompted to indicate whether changes need to be made, type n and press **Enter**.

```
Are any changes needed? [n]: n

At this stage, the IMSS installer is extracted and installed
on every member of the VAP group.

** A reboot is required for the change(s) to take affect. **

Extracting Bundle: [####################] 100% [ok]

Installing IMSS on VAP imss_2: [####################] 100%
[ok]

Installing IMSS on VAP imss_1: [####################] 100%
[ok]
```

WARNING! When IMSS is installed, Postfix 2.0 is removed from the VAP and Postfix 2.1 is installed. The bind-libs and bind-utils RPMs are also installed. IMSS is installed with Service Pack 1 and Hot Fix 31670 (Build 3167). Please note that both should be installed on the Central Controller in distributed architecture. Service Pack 1 can be obtained from the Trend Micro Web site. The hot fix may be obtained from Trend Micro Technical Support.

10. When prompted, save the running configuration:

```
In order to successfully complete the application install,
the XOS configuration must be saved.


Any unsaved configuration will be lost.

Do you want to save it to startup-config? <Y or N>[Y]: y


Saving configuration ... Please be patient...

.

CBS#
```

11. Start the IMSS Filtering Service on each IMSS server (VAP), as follows:

   a. Use a Web browser to access the IMSS Web Management Console for the IMSS Central Controller used by the IMSS VAP group:

   ```
   https://<IMSS_Central_Controller_IP_address>:8445
   ```

   b. Enter your user name and password.

   c. Choose **Summary** from the main menu.

   d. In the Managed Server Settings section, click the **Start** buttons to start the Scanner Service and the Policy Service for each host (VAP).

12. Reload the VAP group.

```
CBS# reload vap-group imss
```

During reboot, when a local disk is present, the following folders are redirected to the local disk (local disk names may be in the format of 'aplocaldisk' or 'aplocaldisk_2' depending on your APM type and configuration):

- `/opt/trend/imss/temp -> /mnt/aplocaldisk/imss/temp`
- `/opt/trend/imss/queue -> /mnt/aplocaldisk/imss/queue`
- `/opt/trend/imss/log -> /mnt/aplocaldisk/imss/log`
- `/var/spool/postfix -> /mnt/aplocaldisk/imss/postfix`
- `/tmp -> /mnt/aplocaldisk/imss/tmp`

13. Save the running configuration again.

```
CBS# wr
```

14. **On the Central Controller**, perform the following steps to enable the IMSS servers to send syslogs to the Central Controller:

   a. If NRS is installed on the X-Series Platform, make sure IP Filtering is installed on the Central Controller.

   b. Add all the IMSS scanners to the /etc/hosts file.

   c. Stop the syslog daemon using either of the following commands:

   - service syslog stop
   - /etc/init.d/syslog stop

   d. Edit the /etc/sysconfig/syslog file to configure the syslog daemon to start with the "-r" flag:

   Edit this line:

```
SYSLOGD_OPTIONS="-m 0"
```

To add the "-r" flag:

```
SYSLOGD_OPTIONS="-m 0 -r"
```

The "-r" flag enables the syslog daemon's remote reception feature, which allows the Central Controller to receive incoming logs from the IMSS servers installed on X-Series Platforms.

e. Restart the syslog daemon using either of the following commands:

- service syslog start
- /etc/init.d/syslog start

Verifying the Installation

Execute the following command to verify the operational state of the application:

```
CBS# show application vap-group [<vap-group-name>]
```

The following example displays the operational state of the application on a VAP group named `imss`:

```
CBS# show application vap-group imss

VAP Group               : imss
App ID                  : imss
Name                    : InterScan Messaging Security Suite
Version                 : 7.0
Release                 : 14-xos
Start on Boot           : yes
App Monitor             : on
App State (imss_1)      : Up
App State (imss_2)      : Up
```

Chapter 4

Application Management

This chapter provides information about XOS CLI commands used to perform basic application management tasks. For additional information, refer to the *XOS Command Reference Guide*.

Topics include:

- Basic Application Management Commands on page 4-2
- Uninstalling the Application on page 4-6

Basic Application Management Commands

Table 4-1 lists the XOS CLI commands that you can use to perform basic application management tasks.

Note: All VAPs in the IMSS VAP group must be “UP” for the following start, stop, and restart commands to take effect.

TABLE 4-1. XOS CLI Commands

COMMAND	FUNCTION
application imss vap-group <vap-group-name> start	Start the application.
application imss vap-group <vap-group-name> stop	Stop the application.
application imss vap-group <vap-group-name> restart	Restart the application.
application-update vap-group <vap-group-name>	Update VAPs. Use this command when you increment the VAP group's VAP count after the initial application installation. The command installs the IMSS application on the newly created VAPs.
show application	Display (show) information about the applications that are currently loaded on the CPM on the X-Series Platform.
show application vap-group [<VAP_group_name>]	Display (show) information about the applications installed on all VAP groups configured on the X-Series Platform, or display information about the application installed on the specified VAP group.

TABLE 4-1. XOS CLI Commands

COMMAND	FUNCTION
configure vap-group <VAP_group_name> [no] application-monitor	Enable or disable (using no) application monitoring for the specified VAP group. By default, application monitoring is enabled for all VAP groups. When application monitoring is enabled for a VAP group, the XOS health system monitors that VAP group and reports the current state of the application to the CLI once every 5 seconds. If the application is not running on a VAP, the health system notifies the NPM to stop sending new flows to that VAP.

Using the *show application vap-group* Command

You can use the following CLI command to display the state of the IMSS application on each VAP in the VAP group on which the application is installed:

```
CBS# show application vap-group <VAP_group_name>
```

For example, the following command displays the state of the IMSS application on each VAP in the VAP group named `imss`:

```
CBS# show application vap-group imss

VAP Group             : imss
App ID                : imss
Name                  : InterScan Messaging Security Suite
Version               : 7.0
Release               : 14-xos
Start on Boot         : yes
App Monitor           : on
App State (imss_1)    : Up
App State (imss_2)    : Up
```

The following fields display status information for the IMSS application:

TABLE 4-1. Status Information

FIELD	DESCRIPTION

`Start on Boot`	Indicates whether the application automatically starts running when you boot up the VAP group:
	• `on` — Application automatically starts up when you boot up the VAP group.
	• `off` — You must manually start up the application each time you boot up the VAP group.
	`Start on Boot` is enabled (`on`) at install time and when a user issues the following command:
	`application imss vap group <VAP_group_name> start`
	`Start on Boot` is disabled (`off`) when a user issues the following command:
	`application imss vap-group <VAP_group_name> stop`

TABLE 4-1. Status Information

FIELD	DESCRIPTION
App Monitor	Indicates whether application monitoring is enabled (on) or disabled (off) on the VAP group on which the application is installed. By default, application monitoring is enabled (on). If application monitoring is enabled (on), the XOS health system monitors the VAP group and reports the current state of the application to the CLI once every 5 seconds. If the application is not running on a VAP, the health system notifies the NPM to stop sending new flows to that VAP. **Note:** Application monitoring cannot detect process hangs. If a process is not functioning, but the application is still running, the XOS health system continues to report the application as running.
App State	Indicates the current state of the IMSS application on each VAP in the VAP group. Possible application states are: • Up — Application is running on the VAP. • Down — Application is not running on the VAP, but the APM on which the VAP is loaded is functional. • Initializing — Application is initializing. • Not Monitored — Application monitoring is disabled on the VAP group on which the application is installed. Therefore, XOS is unable to determine the current state of the application on any VAP.

Uninstalling the Application

To uninstall the application:

1. At the XOS CLI prompt, type the following command to uninstall the application:

```
CBS# application imss version 7.0 vap-group <vap-group-name>
uninstall


Trend Micro, InterScan Messaging Security Suite  7.0
release 1

Stopping imss on VAP imss_2: [####################] 100% [
ok ]

Stopping imss on VAP imss_1: [####################] 100% [
ok ]

Uninstalling imss on VAP imss_2: [#################] 100% [
ok ]

Uninstalling imss on VAP imss_1: [#################] 100% [
ok ]

** A reboot is required for the change(s) to take affect. **
```

Note: If the application is installed on multiple VAP groups, repeat the previous step for each VAP group.

WARNING! When IMSS 7.0 is uninstalled, all IMSS files and directories are deleted. This includes any archived or quarantined mails. Postfix 2.1 is also removed and Postfix 2.0 restored. All Postfix settings are reset to default. The `/mnt/aplocaldisk/imss` folder is renamed to `/mnt/aplocaldisk/imss_old` and deleted the next time an uninstall is performed.

2. When prompted, save the running configuration:

```
In order to successfully complete the application uninstall,
the XOS configuration must be saved.
```

```
Any unsaved configuration will be lost.
Do you want to save it to startup-config? <Y or N>[Y]: y

Saving configuration ... Please be patient...
.
CBS#
```

3. Reload VAP group

```
CBS# reload vap-group <VAP_group_name>
```

4. (Optional) Remove the application files.

```
CBS# application-remove imss
```

Chapter 5

Troubleshooting and Support Information

This chapter provides troubleshooting options if InterScan Messaging Security Suite does not install and provides information on obtaining Customer Support for Trend Micro and Crossbeam Systems products.

Topics include:

- IMSS Installation Issues on page 5-2
- Support and Training on page 5-3
- Customer Comments on page 5-3

IMSS Installation Issues

If the IMSS installation does not succeed, examine the following files on each IMSS VAP:

- /tmp/imss_install.out
- /tmp/nrs_install.out
- /tmp/ip_install.out
- /tmp/sp1_install.out
- /tmp/hf3167_install.out

These files contain a record of the recent IMSS installation and any errors that were encountered during installation.

If you see the following error in `/var/log/messages` on a specific VAP:

```
IMSSXPlugin: The specified database cannot be accessed. Verify the
IP address, user name, and password
```

The installer cannot reach the existing Central Controller from the VAP on which you are installing IMSS. Verify that the VAP can ping the Central Controller IP address, and that the PostgreSQL database on the existing IMSS server is started.

If you see the following error in `/var/log/messages` on a specific VAP:

```
IMSSXPlugin: NRS AC validation failed. NRS AC invalid or host
utility not installed. Please note an Internet connection is needed
to validate the NRS AC
```

The installer cannot validate the NRS activation code. This problem may be caused by one or more of the following problems:

- The X-Series Platform has no route to the Internet. To perform validation of the activation code, the installer needs to connect to Trend Micro's RBL database.
- The host utility is not present on the VAP. By default, the IMSS CBI installs the bind-libs and bind-utils RPMs to provide this utility. To verify that the RPMs were installed properly, run the host utility on the VAP.
- The activation code is invalid.

Support and Training

Refer to the following Web site regarding support for this application:

http://esupport.trendmicro.com

To report issues and request technical assistance for Crossbeam X-Series Platform hardware and software, contact Crossbeam Systems Customer Support:

- **United States:** +1 800-331-1338 or +1 978-318-7595
- **EMEA:** + 33 4 8986 0400 (during normal working hours)

  +1 978-318-7595 (outside office hours and on public holidays, if applicable)
- **Asia Pacific:** +1 978-318-7595
- **Email Customer Support:** support@crossbeam.com

In addition, you can access online resources, submit new technical support requests, and view all of your open requests by logging into the Crossbeam Online Support Web site, located at:

http://www.crossbeam.com/services/online_support.php

Crossbeam Systems also offers extensive customer training on all of its products. For current course offerings and schedules, please refer to the Crossbeam Training and Education Web site located at:

http://www.crossbeam.com/services/training_education.php

Customer Comments

To submit comments regarding the products or their documentation send an email to

alliance_support@trendmicro.com.

Appendix A

Configuring Firewall Rules for Ports Used by the IMSS Gateway

For proper IMSS operation, firewall rules must be configured to allow the IMSS Gateway to use specific ports. This chaper provides information on which ports must be configured.

Topics include:

- Inbound Ports to IMSS Gateways on page A-2
- Outbound Ports from IMSS Gateways on page A-2
- Other Ports on page A-3

Inbound Ports to IMSS Gateways

TABLE A-1. Inbound Ports to IMSS Gateways

PORT	PROTOCOL	DESCRIPTION
25	TCP	IP Profiler/Postfix listening port on VAP
110	TCP	IMSS Scanner listening port on VAP – POP3 **Note:** 110 is the default setting, however the port number may vary.
5060	TCP	IMSS Policy Server listening port on VAP
15505	TCP	IMSS Manager listening port on VAP

Outbound Ports from IMSS Gateways

TABLE A-2. Outbound Ports from IMSS Gateways

PORT	PROTOCOL	DESCRIPTION
25	TCP	Outbound SMTP connection to SMTP server
53	TCP & UDP	Email Reputation Services
80	TCP	Outbound Control Manager agent connection to Control Manager server
443		
110	TCP	Outbound POP3 connection to POP3 server
163	TCP & UDP	Outbound SNMP notification
514	UDP	Outbound syslog connections to Central Controller
5432	TCP	PostgreSQL database port on Central Controller

Other Ports

Other ports used by IMSS that may or may not be opened (connections made locally on each VAP):

TABLE A-3. Other Ports

PORT	PROTOCOL	DESCRIPTION
2500	TCP	Postfix listening port if IP Profiler is installed
10025	TCP	IMSS Scanner listening port
10026	TCP	Postfix listening port – second instance

Index

A

about IMSS 1-2
application
    install 3-2
    load 3-2
    management commands 4-2
    uninstall 4-6
audienceX

C

configure
    Management Circuit 2-6
    NTP Server 2-5
    VAP group 2-4
create
    Management Circuit 2-6
    Traffic Circuits 2-7
    VAP group 2-4

D

deployment options 1-2
documentation
    Crossbeam System relatedxi
    IMSS relatedX

H

hardware requirements 2-3

I

IMSS 1-2
inbound ports A-2
install
    application 3-2
installation issues 5-2

L

licensing requirements 2-2
load
    application 3-2

M

Management Circuit
    create and configure 2-6
management commands
    application 4-2
    application monitoring 4-3
    restart the application 4-2
    show applications 4-2
    show applications on VAP groups 4-2
    start the application 4-2
    stop the application 4-2
    update applications 4-2

N

NTP server
    configure 2-5

O

Online HelpX
other ports A-3
outbound ports A-2

P

ports
    inbound A-2
    other A-3
    outbound A-2

R

Readme FileX
requirements
    hardware 2-3
    licensing 2-2
    setup 2-4
    software 2-2

S

setup
    requirements 2-4
software requirements 2-2
support 5-3

T

Traffic Circuits
    create 2-7
training 5-3

U

unistall
    application 4-6

V

VAP group
    create and configure 2-4
verify installation 3-7