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.

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Trend Micro Incorporated), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Trend Micro Incorporated.

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

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.
Crossbeam Systems Copyright Information

CROSSBEAM, CROSSBEAM SYSTEMS, X40, X45, X80, C2, C6, C10, C12, C25, C30, C30i, SecureShore, and any logos associated therewith are trademarks or registered trademarks of Crossbeam Systems, Inc. in the U.S. Patent and Trademark Office, and several international jurisdictions.
## Contents

### Preface

 Related Documentation ................................................................. viii
  InterScan Messaging Security Suite Related Documentation .......... viii
  Crossbeam Systems Related Documentation ................................ viii
 Audience ......................................................................................... viii
 Document Conventions ................................................................. ix

### Chapter 1: Introducing InterScan Messaging Security Suite

 About InterScan Messaging Security Suite ....................................... 1-2
 Deployment Options ................................................................. 1-2

### Chapter 2: Before You Begin

 Prerequisites for Using InterScan Messaging Security Suite .......... 2-2
  Licensing Requirements ................................................................. 2-2
  Other Requirements ................................................................. 2-2
 XOS-Specific Requirements ............................................................. 2-2
  X-Series Platform Hardware Requirements ................................ 2-2
  General XOS Setup Information .............................................. 2-3
  XOS Setup Requirements ............................................................... 2-4
 XOS Setup Instructions ................................................................. 2-4
  Create and Configure a VAP Group for the Application ................ 2-4
  Create and Configure a Management Circuit ............................. 2-5
  Create Traffic Circuits ............................................................... 2-7

### Chapter 3: Installing the Application

 Loading the Application ................................................................. 3-2
 Installing the Application ............................................................. 3-2
 Verifying the Installation ................................................................. 3-5
Chapter 4: Application Management

XOS Basic Application Management Commands ........................................ 4-2
  Show Application Command .................................................................. 4-2
Uninstalling the Application ..................................................................... 4-3

Appendix A: Troubleshooting

IMSS Installation Issues ........................................................................ A-2
Support and Training ............................................................................. A-3
Customer Comments ............................................................................. A-3
Preface

Welcome to the Trend Micro™ InterScan™ Messaging Security Suite for Crossbeam X-Series Installation Guide. This guide describes how to install and configure InterScan Messaging Security Suite on a Crossbeam Systems X-Series (XOS) security switch.

This preface discusses the following topics:

• Related Documentation on page 1-viii
• Audience on page 1-viii
• Document Conventions on page 1-ix
Related Documentation

InterScan Messaging Security Suite Related Documentation

The following Trend Micro documentation may be helpful:

- InterScan Messaging Security Suite for Linux v7.0 Readme
- InterScan Messaging Security Suite for Linux v7.0 Getting Started Guide

To obtain this documentation, visit http://www.trendmicro.com/download.

Crossbeam Systems Related Documentation

The following Crossbeam Systems documentation may be helpful when configuring our product:

- X40 and X80 Security Services Switch Hardware Installation Guide
- XOS Commands Reference Guide
- XOS Release Notes
- XOS Configuration Guide
- Install Server Users Guide


Audience

The IMSS documentation is written for IT managers and email administrators. 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.
Document Conventions

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

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td>Bold</td>
<td>Menus and menu commands, command buttons, tabs, options, and other tasks</td>
</tr>
<tr>
<td>Italics</td>
<td>References to other documentation</td>
</tr>
<tr>
<td>Monospace</td>
<td>Examples, sample command lines, program code, Web URL, file name, and program output</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Reminders on actions or configurations that should be avoided</td>
</tr>
</tbody>
</table>
Introducing InterScan Messaging Security Suite

This chapter provides a brief introduction to InterScan Messaging Security Suite and its operation on a Crossbeam Systems XOS platform.

Topics include:

• *About InterScan Messaging Security Suite* on page 1-2
• *Deployment Options* on page 1-2
About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 7.0 is a gateway email security software solution that integrates multi-tiered anti-spam and anti-phishing with award-winning antivirus and anti-spyware capabilities. Innovative techniques such as customer-specific reputation services and patent-pending image spam detection keep customers safe as threats evolve while predictive techniques such as zero-day protection, advanced heuristics, and behavior analysis block targeted attacks.

This comprehensive email protection solution also provides flexible content filtering to enforce compliance and to prevent data leakage. With a highly scalable platform and centralized management for easy administration, the solution is optimized to block the full range of standalone, blended-threat, and customer-specific attacks at the POP3 and SMTP 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   Deployment Options
Before You Begin

This chapter presents product-specific prerequisites and pre-installation setup required for installing this application on a Crossbeam Systems X-Series platform.

Topics include:

• Prerequisites for Using InterScan Messaging Security Suite on page 2-2
• XOS-Specific Requirements on page 2-2.
• XOS Setup Instructions on page 2-4
Prerequisites for Using InterScan Messaging Security Suite

Licensing Requirements

InterScan Messaging Security Suite has the following licensing requirements:

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

Other Requirements

InterScan Messaging Security Suite requires Postfix 2.1 or above. It may require these other components:

- 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

XOS-Specific Requirements

X-Series Platform Hardware Requirements

The following table lists the hardware requirements for this application. In addition, heavy traffic or a large sustained number of network connections require more memory.

<table>
<thead>
<tr>
<th>TABLE 2-1. XOS Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Series Chassis Models Supported</td>
</tr>
<tr>
<td>APM Modules Supported</td>
</tr>
</tbody>
</table>
Ensure that the Crossbeam Systems X-Series platform on which you are installing InterScan Messaging Security Suite meets the following requirements:

- A supported X-Series system, running XOS version 7.3.x
- VAP Group OS Requirements: xslinux_v3

### General XOS Setup Information

Consider the following general setup recommendations for this application on an XOS system:

- 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.
In most cases, when using an increment-per-vap circuit, you should enable the `ip-flow-rule-no-failover` parameter.

### 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
- Create and Configure a Management Circuit on page 2-5
- Create Traffic Circuits on page 2-7

### XOS Setup Instructions

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

---

**Note:** Refer to the *Crossbeam Systems XOS Configuration Guide* and *CLI 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:

```bash
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 avoided 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.

---

### 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-flow-rule-no-failover
       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-flow-rule-no-failover
        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. Associate the management circuit with the VAP group.

CBS# configure management-circuit vap-group <vAP group name> circuit <name of management circuit>

For example:

CBS# configure management-circuit vap-group imss circuit mgmt

3. 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
4. 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

5. 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

Create 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-flow-rule-no-failover
   ip <ip-address>/<netmask> <broadcast-address>
   end
For example:

CBS# configure circuit intrtraffic
  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-flow-rule-no-failover
    ip <starting ip-address>/<netmask> <broadcast-address>
    increment-per-vap <high range ip-addr> alias <shared-ip>
  end

For example:

CBS# configure circuit extrtraffic
  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 external traffic circuit>
    device-name <name of the device>
    vap-group <vAP group name>
    ip-flow-rule-no-failover
    ip <starting ip-address>/<netmask> <broadcast-address>
    increment-per-vap <high range ip-addr> alias <shared-ip>
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 external traffic circuit>
    end

For example:

CBS# configure interface fastethernet 1/4
    logical trflgcl14
    circuit traffic
    end
Chapter 3

Installing the Application

This chapter provides instructions for loading, installing, and 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 3-5
Loading the Application

Complete the following steps to load the application on your Crossbeam Systems XOS.

To load the application:
1. Log on to your XOS system as root.
   
   CBS# unix su
   
   Password:
   
   [root@xxxxADMIN]

2. Copy the CBI package to /crossbeam/apps/archive/.
   
   [root@xxxx ADMIN]# cp imss-7.0-x.cbi /crossbeam/apps/archive/

3. Save the running configuration.
   
   CBS# wr

4. Check that the application is present.
   
   CBS# show application
   
   App ID:imss
   
   Name: Interscan Messaging Security Suite
   
   Version: 7.0
   
   Release: 6-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. Install the CBI <insert proper name>.
   
   CBS# application imss version 7.0 vap-group imss 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
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 for proper operation.

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. 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 'aplocaldisk1' or 'aplocaldisk2' 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

11. Save the running configuration again.

    CBS# wr

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 : 6-xos
Start on Boot : yes

imss_1 : running
imss_2 : running
This chapter provides information about basic application management controls. For additional information refer to the XOS Command Reference Guide.

Topics include:

- **XOS Basic Application Management Commands** on page 4-2
- **Uninstalling the Application** on page 4-3
XOS Basic Application Management Commands

Use the following commands at the XOS system prompt to perform basic application management:

**Note:** The VAP must be listed as “UP” for the following Start, Stop, and Restart commands to take effect.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>application imss vap-group &lt;vap-group-name&gt; start</td>
<td>Start an application</td>
</tr>
<tr>
<td>application imss vap-group &lt;vap-group-name&gt; stop</td>
<td>Stop an application</td>
</tr>
<tr>
<td>application imss vap-group &lt;vap-group-name&gt; restart</td>
<td>Restart an application</td>
</tr>
<tr>
<td>application-update vap-group &lt;vap-group-name&gt;</td>
<td>Update VAPs. This command is used when the VAP count of the VAP group is incremented after the application configuration. The update command installs the application on the newly created VAPs.</td>
</tr>
<tr>
<td>show application [vap-group &lt;vap-group-name&gt;]</td>
<td>Display (show) all applications installed on all VAP groups or a specified VAP group.</td>
</tr>
</tbody>
</table>

Show Application Command

The following example shows the state of the application on a VAP group named imss:

VAP Group : imss
App ID : imss
Name : InterScan Messaging Security Suite
Version : 7.0
**Uninstalling the Application**

**To uninstall the application:**

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

```bash
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. Reload VAP group
   CBS# reload vap-group imss

3. (Optional) Remove the application files.
   CBS# application-remove imss
Troubleshooting

This chapter provides troubleshooting options if InterScan Messaging Security Suite does not install.

Topics include:

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

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

- /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:

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:

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 VAP 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

Support calls related to your Crossbeam Systems platform should be directed to:

• Crossbeam Systems Customer Service at 1-800-331-1338 (within the U.S. only) or +1-978-318-7595 for international customers.

• For additional information, please contact your account representative or refer to www.crossbeamsystems.com for product training offerings and schedules.

Customer Comments

To submit comments regarding the products or their documentation send an email to alliance_support@trendmicro.com.