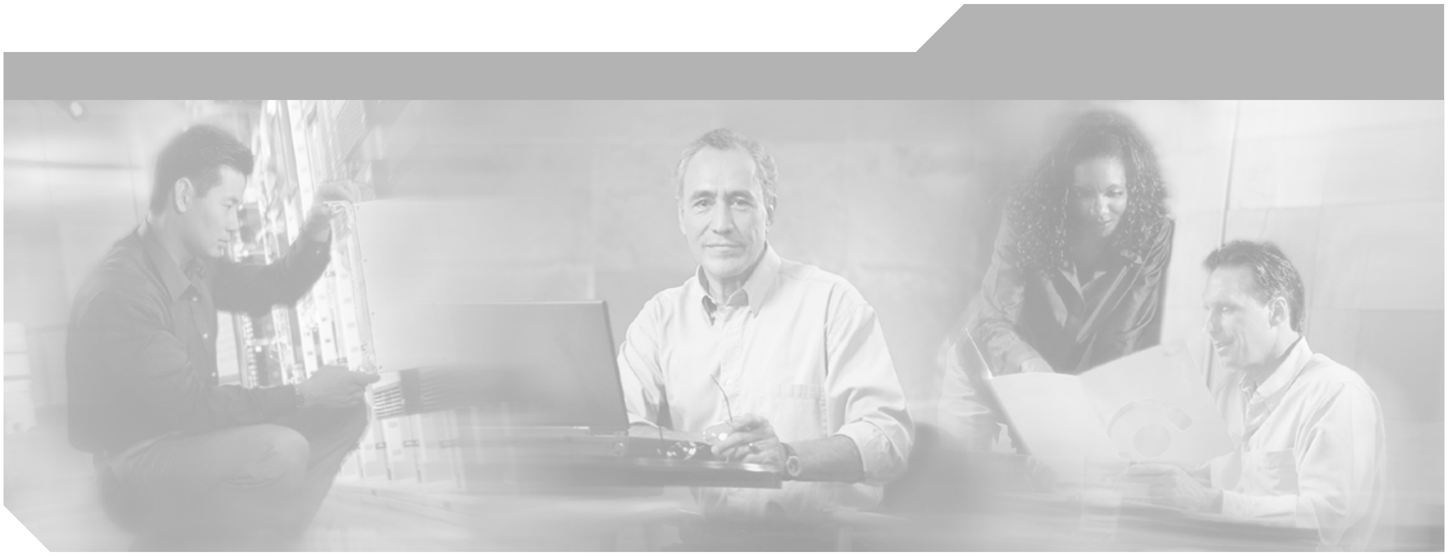


Cisco Incident Control Server 1.0 Administrator Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8059-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco Incident Control Server Administrator Guide

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, ìCUSTOMERî) TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

The following terms of this End User License Agreement (ìAgreementî) govern Customerís access and use of the Software, except to the extent (a) there is a separate signed agreement between Customer and Cisco governing Customerís use of the Software or (b) the Software includes a separate ìclick-acceptî license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the signed agreement, (2) the click-accept agreement, and (3) this End User License Agreement.

License. Conditioned upon compliance with the terms and conditions of this Agreement, Cisco Systems, Inc. or its subsidiary licensing the Software instead of Cisco Systems, Inc. (ìCiscoî), grants to Customer a nonexclusive and nontransferable license to use for Customerís internal business purposes the Software and the Documentation for which Customer has paid the required license fees. ìDocumentationî means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Cisco with the Software in any manner (including on CD-Rom, or on-line).

Customerís license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or that number of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s) or site(s), as set forth in the applicable Purchase Order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee.

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customerís internal business purposes. NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.Cisco Incident Control Server 1.0 Administrator Guide

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(v) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. For purposes of this Agreement, ìSoftwareî shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware, as provided to Customer by Cisco or an authorized Cisco reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, ìUpgradesî) or backup copies of the Software licensed or provided to Customer by Cisco or an authorized Cisco reseller. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. Customer may terminate this Agreement and the license at any time by destroying all copies of Software and any Documentation. Customerís rights under this Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled ìU.S. Government End User Purchasersî and ìGeneral Terms Applicable to the Limited Warranty Statement and End User Licenseî shall survive termination of this Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customerís books, records and accounts during Customerís normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation (ìFARî) (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User License Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are ìcommercial computer softwareî and ìcommercial computer software documentation,î and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the software warranty period (if any) set forth in the warranty card accompanying the product of which the Software is a part (the ìProductî) (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers and licensors under this limited warranty will be (i) replacement of defective media and/or (ii) at Ciscoís option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to Cisco or the party supplying the Software to Customer, if different than Cisco, within the warranty period. Cisco or the party supplying the Software to Customer may, at its option, require return of the Software as a condition to the remedy. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and End User License Agreement

Disclaimer of Liabilities. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' or licensorsí liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Cisco. Customer acknowledges and agrees that Cisco has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. Except as expressly provided herein, this Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. This Agreement has been written in the English language, and the parties agree that the English version will govern.

CONTENTS

Preface

This preface introduces the Cisco Incident Control Server Administrator Guide. It contains the following sections:

Document Objectives

The purpose of this guide is to help you install and configure the Cisco Incident Control Server (Cisco ICS) using the web console, a web-based GUI application. This guide does not cover every feature, but describes only the most common configuration scenarios.

Audience

The Cisco ICS documentation is for experienced network administrators who are responsible for configuring switches, routers, IPS appliances, and Cisco IOS IPS devices. In-depth knowledge of the following topics is required:

- Network communication protocols
- General switch, router, IPS appliance, and Cisco IOS IPS device configuration commands from a Telnet, console, and aux connection
- Virtual LANs (VLANs)
- Access Control Lists (ACLs) and ACL syntax

Documentation Organization

Table 1 describes the chapters and appendixes contained in this guide.

Table 1 Documentation Organization

Chapter/Appendix	Definition
Chapter 1, "Introducing Cisco Incident Control Server"	Provides a high-level overview of the product.
Chapter 2, "Installing and Uninstalling Cisco ICS"	Describes how to install and uninstall Cisco ICS.
Chapter 3, "Getting Started"	Describes how to get started using the Cisco ICS web console and provides an overview of outbreak prevention.
Chapter 4, "Managing Devices"	Describes how to add and configure devices.
Chapter 5, "Updating Components"	Describes how to download and deploy the components you need to implement your incident control strategy.
Chapter 6, "Managing Outbreaks"	Describes how to create outbreak management tasks to help protect against network virus outbreaks.
Chapter 7, "Using Watch Lists"	Describes how to use watch lists to monitor potentially infected hosts.
Chapter 8, "Using Reports"	Describes how to use reports that provide a summary of outbreak management tasks.
Chapter 9, "Configuring Global Settings"	Describes how to configure notifications, manage administrator accounts, import licenses, add syslog servers, set a schedule to check network connection to devices, and back up the database.
Chapter 10, "Using Logs"	Describes how to query and maintain logs.
Appendix A, "Damage Cleanup Services"	Describes how to use Damage Cleanup Services (DCS) to clean infected hosts.
Appendix B, "Preparing Cisco IOS Routers"	Provides procedures for configuring a Cisco IOS router
Appendix C, "Log Severity Levels"	Describes the severity levels associated with logs entries.
Appendix D, "Troubleshooting and FAQs"	Provides solutions to problems that you might encounter and answers to commonly asked questions.
Appendix E, "Acronyms"	Provides a list of acronyms used in this document.

Document Conventions

The Cisco ICS documentation uses the following conventions:

- Braces ({ }) indicate a required choice.
- Boldface font indicates a UI element you must interact with and commands you must enter.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Introducing Cisco Incident Control Server

This chapter introduces Cisco Incident Control Server (Cisco ICS). It contains the following sections:

- Cisco Incident Control Server Overview, page 1-1
- Cisco ICS Technology, page 1-1
- Minimum System Requirements, page 1-6
- Cisco ICS Services, Ports, and Protocols, page 1-8
- User Documentation, page 1-8

Cisco Incident Control Server Overview

Cisco Incident Control Server (Cisco ICS) is a server-based software application that helps you manage your incident control initiatives. Built on incident-control technology from Trend Micro, Cisco ICS gives you the means to protect your organization from newly discovered network-based threats.

- Use the Cisco ICS web console to manage the Cisco ICS server and perform the following tasks:
- Deploy policies to Cisco network devices to block the traffic and ports network-based threats use to propagate.
- Create reports about the tasks you create to address threats on your network.
- Use logs to analyze your protection.
- Configure notifications to alert you about threat-related events and Cisco ICS threat-protection updates.
- Clean up infected hosts to remove viruses and other threats.

Cisco ICS Technology

Cisco ICS helps protect your network by combining Cisco networking and security expertise with Trend Micro antivirus and incident-control technology.

This section describes the Cisco ICS and contains the following topics:

- Incident Control System, page 1-2
- About Cisco ICS Components, page 1-3

- Understanding Network-based Threats, page 1-5
- About Risk Ratings, page 1-6

Incident Control System

Cisco provides an incident control system—a means to control the outbreak of network-based threats on your network. The incident control system is managed by a central server, the Cisco ICS server, and uses threat-specific access control lists (ACLs) and signature files to help identify network threats and mitigate the effects of outbreaks. With these components, your Cisco network devices can become defense nodes against new outbreaks.

You can deploy Outbreak Prevention ACLs (OPACLs) and Outbreak Prevention Signatures (OPSigs) from the web console when you create items called outbreak management tasks or when you enable Cisco ICS to automate the creation of tasks. For an explanation of OPACLs and OPSigs, see About Cisco ICS Components, page 1-3. To understand how outbreak management tasks can help protect your network, see About Outbreak Management Tasks, page 6-1.

This section describes the elements of ICS and the ICS in action and contains the following topics:

- Elements of the Incident Control System, page 1-2
- The Incident Control System in Action, page 1-2

Elements of the Incident Control System

The following elements comprise the Cisco implementation of the incident control system:

- TrendLabs—The Trend Micro worldwide, real-time monitoring and signature-development infrastructure.
- Cisco Incident Control Server (Cisco ICS)—A product that delivers protection from viruses, worms, spyware, and other potential threats.
- Mitigation devices—Switches, routers, IPS appliances, and Cisco IOS IPS devices.

The Incident Control System in Action

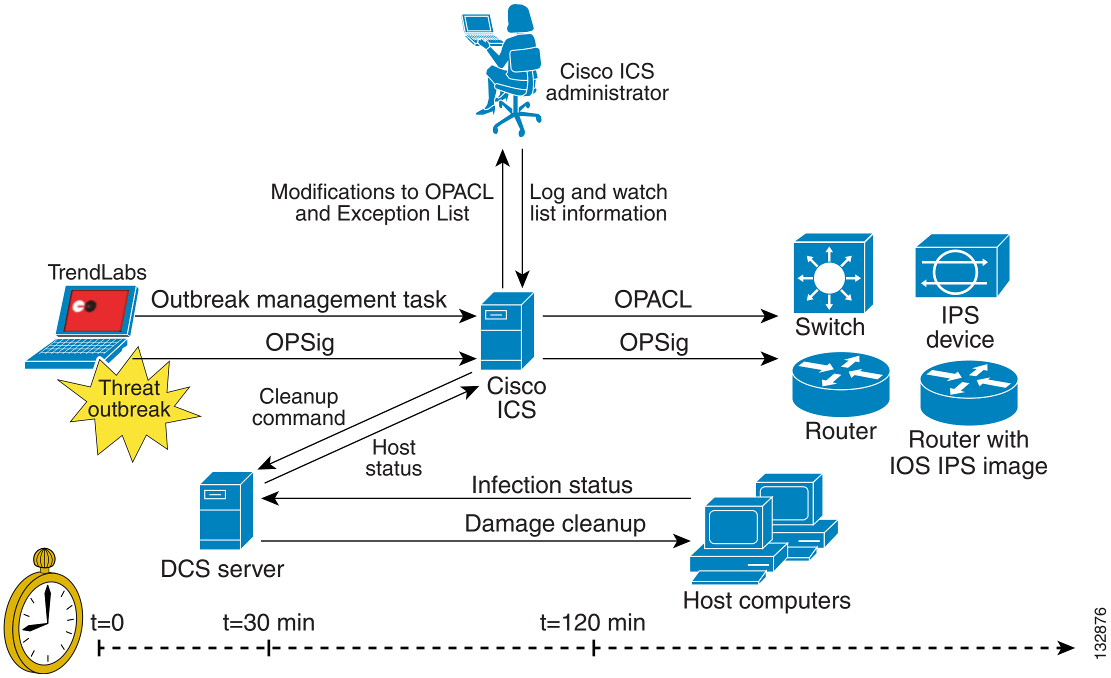
Soon after TrendLabs discovers a new threat, the following sequence of events takes place:

1. TrendLabs releases an outbreak management task file that contains an OPACL to address the new threat.
2. As the Cisco ICS server polls the update source for new components, it discovers that the new outbreak management task is available.
3. Cisco ICS downloads the new outbreak management task file.
4. If Cisco ICS is enabled to deploy outbreak management tasks automatically, it activates a new task and deploys the OPACL to network devices.
5. Your Cisco network devices block the ports and the types of traffic specified in the OPACL until the OPACL expires.
6. Approximately 2 hours after TrendLabs releases the OPACL, it releases an OPSig, which enables IPS devices to detect the new threat as well as other threats TrendLabs discovered.
7. Cisco ICS downloads and deploys the OPSig to IPS devices. The OPACL for the threat expires on all devices when Cisco ICS deploys the OPSig.

8. While they scan network traffic, IPS devices use the OPSig to identify any threats that might attack the network.
9. If an IPS device detects a threat in network traffic from a certain host, Cisco ICS considers the host to be potentially infected and puts it on a watch list. You can view the watch list to see which hosts on your network need attention.
10. If you installed Damage Cleanup Services, you can run a Damage Cleanup scan on the potentially infected host to attempt to remove the threat.

Figure 1-1 provides a graphical overview.

Figure 1-1 Incident Control System Overview



About Cisco ICS Components

Cisco ICS downloads the following components from Trend Micro and uses them to block network traffic, scan for network-based threats, and clean infected hosts:

- Outbreak-threat Components, page 1-4
- Damage Cleanup Components, page 1-4

Outbreak-threat Components

The outbreak-threat components consist of the following:

- Outbreak Prevention ACL (OPACL)—An ACL that network devices use to block the ports and the types of traffic that threats use to propagate. The OPACL is associated with a task you create to block a specific threat for a limited period of time. The devices use the OPACL to block traffic, not scan traffic. For more information, see About Outbreak Management Tasks, page 6-1.
- Outbreak Prevention Signature (OPSig)—A file that helps IPS devices identify unique patterns of bits and bytes that signal the presence of a network-based threat. IPS devices can continually scan traffic and, when using an OPSig, can block a threat that is attacking your network or any host on your network.

Damage Cleanup Components

The Damage cleanup components consist of the following:

- Damage Cleanup engine—The engine that Damage Cleanup Services (DCS) uses to scan for and remove Trojans and Trojan processes and cleanup hosts.
- Damage Cleanup template—The file that the Damage Cleanup engine uses to help identify Trojan files and processes to be eliminated.
- Spyware cleanup pattern—The file that the Damage Cleanup engine uses to eliminate spyware and other intrusive code, known as grayware.

This section describes the component download and deployment and contains the following topics:

- Component Download, page 1-4
- Component Deployment, page 1-5

Component Download

Cisco ICS offers two methods for downloading components from the update source to the Cisco ICS server:

- Scheduled—Download all components according to a configurable schedule to automate the task of keeping your threat protection up-to-date.
- Manual—Download selected components on demand when a new threat appears and you do not want to wait for the next scheduled download.

Note The Cisco ICS server polls the update source and downloads components only if new versions are available. If the Cisco ICS versions are up-to-date, no download occurs.

For more information, see Downloading Components, page 5-2.

Component Deployment

The Cisco ICS server deploys the following components to different network devices at different times:

- OPACLs—Cisco ICS deploys the OPACL to Cisco switches, routers, and IPS devices. Automatic deployment takes place after outbreak management task creation.
- OPSigs and DCS components—Cisco ICS deploys the OPSig to IPS devices and the Damage Cleanup components to Damage Cleanup servers. Automatic deployment takes place after an updated component is downloaded, a new device is added, or the status of any device changes to online.

You can manually download and deploy components on demand at any time if you want to update your threat protection immediately without waiting for the next automatic update.

For more information, see Downloading Components, page 5-2, and Deploying Components, page 5-7.

Understanding Network-based Threats

Tens of thousands of threats exist, with more being created each day. Although once most common in DOS or Windows, threats today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems, and websites.

Most threats fall into the following categories:

- ActiveX malicious code—Resides in web pages that run ActiveX controls.
- Boot sector viruses—Infect the boot sector of a partition or a disk.
- COM and EXE file infectors—Viruses within executable programs that typically have a .com or .exe extension.
- Joke programs—Virus-like programs that often manipulate the appearance of things on a computer monitor.
- Java malicious code—Operating system-independent virus code written or embedded in Java.
- Macro viruses—Viruses encoded as application macros and often included in a document.
- Trojans—Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter. Trojans often use ports to gain access to computers.
- VBScript, JavaScript or HTML viruses—Viruses that reside in web pages and are downloaded through a browser.
- Worms—A self-contained program (or set of programs) that can spread functional copies of itself or its segments to other computer systems, often via email.

Network-based Threats

A virus spreading throughout a network is not, strictly speaking, a network-based threat. Only some of the threats mentioned previously, such as worms, qualify as network-based threats. Specifically, network-based threats use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failures. Because network-based threats often remain in memory, they are often undetectable by conventional file I/O based scanning methods.

About Risk Ratings

Each threat is associated with a risk rating. TrendLabs, the global network of antivirus research and product support for Trend Micro, provides rapid response to any virus outbreak or urgent customer support issue. When it receives a case, TrendLabs immediately evaluates the threat and assigns a risk rating of low, medium, or high.

The TrendLabs Risk Rating Evaluation is also an early warning system backed by professional antivirus and security researchers. Information gathered from its various service centers and business units (BUs) is polled, analyzed, and redistributed with solutions to help network administrators and managers assess the vulnerability of their systems and advise them in securing their networks during an outbreak.

Overall Risk Rating Levels

TrendLabs determines risk rating levels using specific criteria and takes corresponding action. Table 1-1 provides an explanation of each risk rating.

Table 1-1 Risk Ratings

Risk Level	Criterion	Action
High	Several infection reports are received from each business unit (BU) about rapidly spreading malware. Gateways and email servers might need to be patched.	Trend Micro's Red Alert process is started: an official pattern release (OPR) is deployed with notification of its availability, any other relevant notices are sent, and fix tools and information regarding vulnerabilities are posted on the download pages.
Medium	Infection reports are received from several BUs as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download.	In case of an email-spreading malware, content filtering rules, called outbreak prevention policies (OPPs), are sent out to automatically block related attachments on servers equipped with the product functionality.
Low	Single infection reports are received, and daily virus definitions, called controlled pattern releases (CPRs), are made available for download.	In some instances where a proof-of-concept malware is handled, media attention, or numerous support inquiries are received, TrendLabs might raise the risk level from very low to low and send out a corresponding notice together with an official pattern release (OPR).

Minimum System Requirements

This section describes the minimum requirements for Cisco ICS. It contains the following topics:

- Cisco ICS Server, page 1-7
- Supported Cisco Devices, page 1-7
- Syslog Servers, page 1-8

Cisco ICS Server

The Cisco ICS server has the following minimum requirements:

- Operating system (one of the following)
  - Windows 2000 Server or Advanced Server with SP3
  - Windows 2003 Server Standard Edition or Enterprise Edition (English)
- Web server (one of the following)
  - IIS: Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0
  - Apache: 2.0
- Web browser (for web console access)
  - Internet Explorer version 5.5 SP2
- Hardware
  - 866 MHz Intel Pentium III processor or equivalent
  - 512 MB of RAM
  - 350 MB of disk space

Supported Cisco Devices

Table 1-2 lists the devices that Cisco ICS can manage. For more information, see About Device Types, page 4-1, and About Device Licenses, page 9-9.

Table 1-2 Supported Cisco Devices

Device Type	Model	Minimum Software Version	Required License
Cisco switches	Cisco 3550 Series switches	12.1(22)EA5	ACL ICS service or IPS ICS service
	Cisco Catalyst 6500 Series switches	12.2(18)SXD5	
	Cisco 7600 Series switches	12.2(17)SXB8	
Cisco routers	Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3800, 7200 and 7301 Series routers	12.4(4)T second release	ACL ICS service or IPS ICS service
Cisco Integrated Services Routers	3800, 7200	12.4(4)T second release	IPS ICS service
Cisco 4200 Series Intrusion Prevention System Sensors	IPS 4200	5.1	IPS ICS service

Table 1-2 Supported Cisco Devices (continued)

Device Type	Model	Minimum Software Version	Required License
Cisco Intrusion Detection System Service Module	IDSM2	5.1	IPS ICS service
Cisco ASA 5500 Series Adaptive Security Appliances with Advanced Inspection and Prevention Modules	ASA-5500-AIP	ASA 7.0 5.1 or greater on the AIP SSM	IPS ICS service

Syslog Servers

The following Syslog server is recommended:

- Cisco Monitoring, Analysis, and Response System (Cisco MARS)

Cisco ICS Services, Ports, and Protocols

The following ICS services, ports, and protocols are required:

- Services
  - Cisco ICS Flexlm License Manager
  - Cisco ICS Master Service
- Communication Ports and Protocols
  - Telnet (port 23) and SSH (port 22) to communicate with switches and routers
  - HTTP (port 80) and HTTPS (port 443) to communicate with the update source and IPS devices

User Documentation

Cisco ICS documentation set contains the following:

- *Cisco Incident Control Server Administrator Guide*—Helps you plan for and install the Cisco ICS server program and configure all features. The latest version of the administrator guide is available in electronic form at the following location:

  http://www.cisco.com
- *Online help*—Helps you configure all features and is accessible from the web console.
- *Readme*—Contains 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.

For information about what kind of technical knowledge you should have before reading the documentation, see Audience, page -xvii.

CHAPTER 2

Installing and Uninstalling Cisco ICS

This chapter explains how to install Cisco ICS. It contains the following sections:

Preparing for Installation

The setup program prompts you for the following information during installation:

- Web server details—The Cisco ICS server uses a web server for web console access. During installation, you can select an existing IIS or Apache web server installation. If you select Apache and an Apache 2.x web server is not already installed, the setup program can install one automatically. Decide the web port you want to use, whether you want to use SSL, and which type of website (default or virtual) to use if you are installing on an IIS web server.
- Proxy server details—If a proxy server handles Internet traffic on your network, configure proxy server information, including the proxy server username and password. This information is necessary if you need to download the latest components, including OPACLs and OPSigs, from the Trend Micro update source. You can enter proxy server information either during installation or at a later time through the web console.
- Root account username and password—To prevent unauthorized access to the web console and to uninstall the Cisco ICS server program, establish a root account. For more information, see Managing Administrator Accounts, page 9-5.
- Cisco ICS license—Obtain a license file from Cisco to install Cisco ICS. If you do not have a license file, you can register for one during installation or online at the following website: http://www.cisco.com/CICS/registration/regnow

Note For generating reports, Cisco ICS requires the Microsoft .NET Framework 1.1 and Microsoft Data Access Component 2.8. If these are not installed on the computer, the setup program can install them during server installation, or you can install them at a later time from the Cisco ICS CD-Rom. For more information, see About Outbreak Management Reports, page 8-1.

Installing Cisco ICS

Before you start, verify that the computer on which you will install Cisco ICS meets the system requirements. For more information, see Minimum System Requirements, page 1-6.

To install Cisco ICS, follow these steps:

Step 1 Double-click the **Setup.exe** file.

The setup program opens.

Step 2 Click **Next**.

The Software License Agreement window appears.

Step 3 Read the license carefully.

Step 4 Click **Yes** to accept the agreement.

The setup program begins collecting information about the computer. If the operating system on your computer is not Windows 2000 Server with Service Pack 3 or later or Windows 2003, a prompt appears notifying you that installation cannot continue.

Note When you run the setup program on your computer, the minimum acceptable screen resolution is 800 x 600.

Step 5 Click **OK**. One of the following appears.

- Web server window—The computer has the required software components to use the Cisco ICS reporting feature. Skip to Step 8.
- A prompt—The computer does not have the required software components to use the Cisco ICS reporting feature. If you do not install the components, Cisco ICS cannot generate reports and you cannot perform outbreak log queries for an outbreak management task. To install the components, click **Yes**. A confirmation message appears.

Step 6 If you want to install the Microsoft .NET Framework 1.1, do the following:

a. Click **Yes.**

A license agreement window appears.

b. Read the agreement carefully.

c. Click **I agree**.

d. Click **Install**.

The installer completes the .NET installation. A confirmation prompt appears.

e. Click **OK**.

The Web server window appears.

Step 7 If you want to install the Microsoft Data Access Components, do the following:

a. Click **OK**.

A license agreement window appears.

b. Read the agreement carefully.

c. Check the check box to accept the agreement.

d. Click **Next**.

The installer completes the Data Access component installation. A confirmation prompt appears.

e. Click **Finish**.

f. Click **Close**.

Step 8 Choose one of the following radio buttons to install Cisco ICS on a web server:

- **Install Cisco ICS on the IIS server**—This radio button is active only if a Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0 web server is already installed on the computer.
- **Install Cisco ICS on Apache web server 2.0**—Install on any existing Apache 2.0 web server. If an Apache server version 2.x is not installed, the setup program installs version 2.0.54 automatically.

Note See your Microsoft IIS and Apache web server documentation for information about server configuration, security issues, and so forth.

Step 9 Click **Next**.

The Server Information window appears.

Step 10 Configure the following information:

- Server information—Click one of the following:
  - **Domain Name**—Verify the target server domain name. You can also use the server fully qualified domain name (FQDN) if necessary. We recommend this option if Cisco ICS obtains a dynamically assigned IP address, such as from a DHCP server.
  - **IP Address**—Verify that the target server IP address is correct.

Tip If the server has multiple network interface cards (NICs), use a NIC IP address instead of the domain name or FQDN.

- IIS website—If you elected to install Cisco ICS on an IIS server, select one of the following in the IIS website section:
  - **IIS default website**—Install as an IIS default website (in the IIS default website folder).
  - **IIS virtual website**—Install as an IIS virtual website (in the IIS virtual website folder).
- Port Number—Enter a port to use as the server listening port. The Cisco ICS server address is the following:

  http://{server_name}:{port number}/CICS
- Secure Socket Layer—You also have the option of enabling Secured Socket Layer (SSL) security:

  a. Check the **Enable SSL** check box.

  b. Enter the number of years to keep the SSL certificate valid (the default is 3 years).

c. Enter an SSL port number. If you enable SSL, this port number is the server listening port. The Cisco ICS server address is then as follows:

https://{server_name}:{port number}/CICS

Tip Enable SSL to enhance security between the computer accessing the web console and the Cisco ICS server.

- Installation Directory—To change the target directory location, click **Browse** and select or create a new folder.

Step 11 Click **Next**.

A confirmation window appears displaying the Cisco ICS web console address.

Step 12 Verify that the port number is correct. Cisco ICS uses the same TCP port number that your HTTP server is using. Setup automatically retrieves this port number and displays it on this window.

Step 13 Click **OK**.

The Proxy Server window appears.

Step 14 If your organization uses a proxy server, enter the required information such as the proxy address, port, and your username and password for proxy server authentication.

Step 15 Verify that the information you provided on the window is correct. The Cisco ICS server uses this information to connect to the update source and download updated components, such as OPACLs and OPSigs.

Step 16 Click **Next**.

The Root Administrator Account Login Credentials window appears.

Step 17 Enter a username and password that serves as the root account. The root account manages all other accounts and is required for the first web console access and for uninstallation. The root account username cannot be changed hereafter; however, you can modify the password from the web console.

Step 18 Click **Next**.

The Product Activation window appears.

Step 19 If you do not have a Product Activation Key, click one of the following to register with Cisco:

- **Registered Users**—If you already registered with Cisco and obtained a CCO username and password.
- **Non-registered Users**—If you do not have a CCO account.

Step 20 Click **Import** to import the license file.

Step 21 Browse for the file on the computer and click **Open**.

Step 22 Click **Next**.

The Select Program Folder window appears.

Step 23 Verify that the program folder in which the setup program is installing Cisco ICS is correct. Modify it if necessary.

Step 24 Click **Next**. Installation begins.

The Setup Complete window appears.

Step 25 Check the check boxes to open the readme or web console.

Step 26 Click **Finish**.

Uninstalling Cisco ICS

To uninstall Cisco ICS, follow these steps:

Step 1 From the Windows Start menu, choose **Programs** > **Cisco Incident Control Server > Uninstall Cisco ICS**. A confirmation prompt appears.

Step 2 Click **Yes**. A prompt appears asking you to enter the Cisco ICS root account username and password.

Step 3 Enter the root account credentials.

Step 4 Click **OK**.

The uninstaller program begins removing Cisco ICS. When uninstallation is complete, a prompt appears.

Step 5 Click **OK**.

Uninstallation Notes

Note the following before you uninstall Cisco ICS:

- If the Cisco ICS setup program installed Apache 2.0.54 automatically, the uninstaller removes it. If an Apache or IIS installation existed on the machine before Cisco ICS installation, the uninstaller does not remove it.
- If a backup of the database exists in the default backup folder (Program Files\Cisco Systems\CICS\backup), it is preserved.
- OPACLs remain active on devices until their expiration date, even if you uninstall Cisco ICS without deactivating the OPACLs. To prevent OPACLs from continuing to block traffic, stop active tasks or active OPACLs through the web console before uninstallation. For more information, see Viewing a Summary of All Outbreak Management Tasks, page 6-10, and Stopping an Outbreak Management Task, page 6-13.

Getting Started

This chapter helps you get started using the Cisco ICS web console and provides an overview of incident control. It contains the following sections:

- Using the Cisco ICS Web Console, page 3-1
- Default Settings, page 3-5
- Protecting the Network, page 3-7
- Testing OPACL and OPSig Matching, page 3-8

Using the Cisco ICS Web Console

The web-based management console, or web console, is the central point for incident control.

This section explains how to start and navigate the web console and use the device list tree. It contains the following topics:

- Starting the Web Console, page 3-1
- Navigating the Web Console, page 3-2
- Using the Device List Tree, page 3-3

Starting the Web Console

You can start the web console from any computer on the network that meets the system requirements. For more information, see Minimum System Requirements, page 1-6.

The following are valid URLs for the Cisco ICS web console:

- Without SSL:

  http://{server}:{port number}/CICS

- With SSL:

  https://{server}:{port number}/CICS

In the Login window, enter an account username and password. The Outbreak Management Task Summary window is displayed by default.

Note The web console times out after 30 minutes of inactivity.

Navigating the Web Console

The web console consists of the header menu and the main menu.

This section describes the Header and Main menus. It contains the following topics:

- Header Menu, page 3-2
- Main Menu, page 3-2
- Allowing Pop-ups, ActiveX Controls, and Scripts, page 3-3

Header Menu

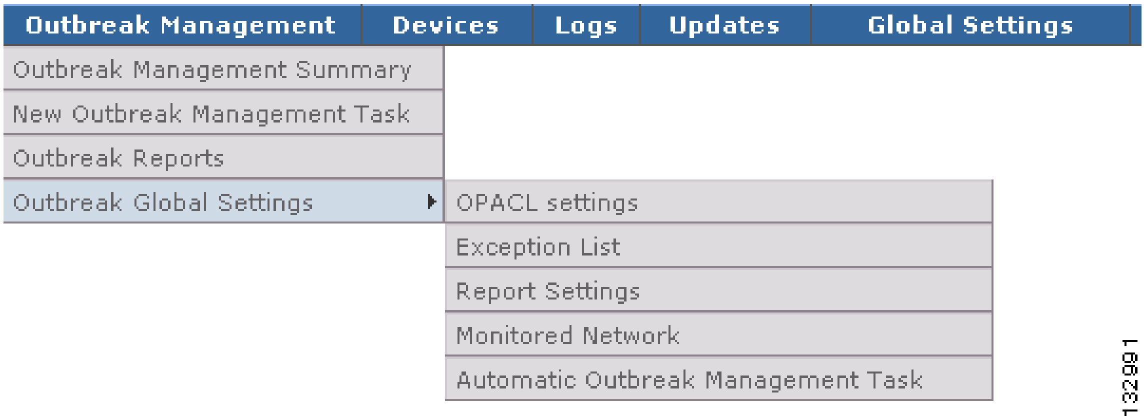
The header menu provides a link to log off the web console and a drop-down list of items that link to sources of important antivirus and security information.

- Log off—Click to log off the web console and return to the login window.
- Help list—Contains the following options:
  - Contents and Index—Opens the Cisco ICS online help.
  - Products and Services —Opens the Cisco Products and Services website, from which you can access several valuable resources, including product and service details, support information and documentation, learning materials, and items related to partners and resellers.
  - Technical Support and Documentation—Opens the Cisco support website, where you can find support contact information and download product documentation.
  - Networking Solutions—Opens the Cisco Networking Solutions website, an overview of solutions for various types of enterprises and organizations.
  - Ordering—Opens the Cisco website from which you can order products and services.
  - About—Displays information about Cisco ICS, including the version and build number.

Main Menu

The main menu is a series of drop-down lists that provide access to all Cisco ICS features. Figure 3-1 on page 3-3 provides a graphical overview of the main menu with the Outbreak Management > Outbreak Settings drop-down list expanded.

Figure 3-1 Main Menu



The main menu contains the following primary items:

- Outbreak Management—Lets you create and configure outbreak management tasks to monitor potential threats on the network.
- Devices—Lets you manage switches, routers, and IPS devices.
- Logs—Lets you query and display logs for incidents, events, and outbreaks.
- Updates—Lets you download and deploy OPACLs, OPSigs, and other components.
- Global Settings—Lets you configure notifications and Syslog server information, verify device connection, manage Cisco ICS accounts, view licensing information, and back up the database.

Allowing Pop-ups, ActiveX Controls, and Scripts

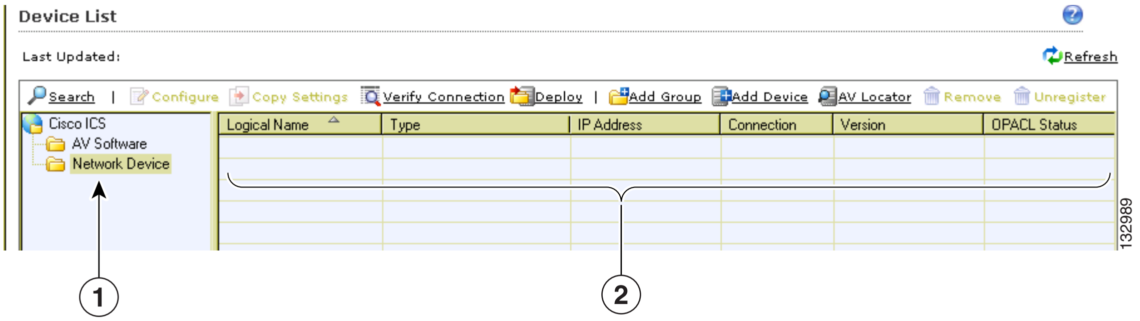
You can configure your web browser to allow pop-up windows to appear. Cisco ICS often uses pop-ups to prompt you to perform additional actions. See your Internet Explorer help for instructions on allowing pop-ups.

To allow the online help to display properly, verify that your browser is not blocking ActiveX and script components.

Using the Device List Tree

The device list tree is an ActiveX control that appears in the main frame of the Device List window. Figure 3-2 on page 3-4 provides a graphical overview of the device list tree. For specific instructions on using the links in the top menu, see Using the Device List Window, page 4-3.

Figure 3-2 Device List Tree



1	Directory pane	**2**	Device list pane

This section describes the device list tree components and how to navigate it. It contains the following topics:

- Device List Tree Components, page 3-4
- Navigating the Device List Tree, page 3-4

Device List Tree Components

The device list tree consists of the following sections:

- Top menu—Contains the following options:
  - Search—Searches for devices already registered with Cisco ICS.
  - Configure—Lets you configure device settings.
  - Copy Settings—Copies configuration settings from one device type to another.
  - Verify Connection—Verifies that the Cisco ICS server can successfully connect to a registered device.
  - Deploy—Deploys the components on the Cisco ICS server to the selected devices.
  - Add Group—Adds a group folder to the Directory pane.
  - Add Device—Registers a device with the Cisco ICS server.
  - AV Locator—Locates an existing Trend Micro OfficeScan server installation.
  - Remove—Removes a device.
  - Unregister—Removes a Trend Micro Damage Cleanup Services (DCS) server.
- Directory pane—Contains a hierarchical list of group folders.
- Device List pane—Contains a list of devices in the current group folder.

As in all windows, the Refresh link appears on the top right. You can click Refresh to update the status of devices in the device list pane.

Navigating the Device List Tree

When the Device List window opens, the root directory is selected by default and the contents of the root directory appear in the Device List pane.

You can perform the following actions:

- To move from one group folder to another, click the group name next to the group folder icon.
- To perform one of the actions in the top menu on a device or on several devices, click the device name. Use the Shift and/or Ctrl keys to select multiple devices. When you select multiple devices, the Configure and Copy Settings links in the top menu are disabled.
- To move devices from one group folder to another, click the device and drag it to the desired folder in the Directory pane.

Note Clicking the group folder does not select all devices in that group; it displays only the devices for the group in the device list. Click the devices in the device list to perform actions on them.

Default Settings

By default, critical incident control functions and features are enabled after installation. Verify the default selections after installation. Table 3-1 describes all default settings.

Table 3-1 Default Settings

Setting	Default Value	Description
Automatic outbreak management tasks	• Enabled for red alerts. • OPACLs deployed to all network devices. • Newly released OPACLs are deployed and overwrite older OPACLs. • OPACLs stop after OPSig deployment or after 4 hours.	Automatic outbreak management tasks address critical threats, automatically helping to prevent red alert outbreaks from spreading on your network. For more information, see Automating Outbreak Management, page 6-8.
OPACL mode	Blocking	Devices block the traffic specified in the OPACLs. For more information, see Automating Outbreak Management, page 6-8.
Exception list	• TCP port 4343 or 443 (access to the web console using the default web port number during installation). • TCP port 22 (SSH communication with switches and routers). • TCP port 23 (Telnet communication with routers and switches). • TCP port 25 (SMTP for notifications). • TCP port 80 (HTTP communication with IPS devices).	OPACLs do not block these ports, which are required for communication among the Cisco ICS server and the computer accessing the web console, the mail server, and network devices. For more information, see Configuring the Exception List, page 6-9.

Table 3-1 Default Settings (continued)

Setting	Default Value	Description
Scheduled download	• Outbreak management task polling schedule enabled, polling the update source every 5 minutes. • OPSig polling schedule enabled, polling the update source twice daily. **Note** After installation is complete, Cisco ICS immediately downloads the latest components from the default update source using HTTPS. This one-time post-installation download is enabled by default and cannot be disabled.	Cisco ICS polls the update source for the latest outbreak management tasks, which include OPACLS, OPSigs, and DCS components to keep up-to-date with the latest threats. OPSigs and DCS component download follow the OPSig polling schedule when no tasks are active. For more information, see Configuring Scheduled Download, page 5-3 and Scheduled Download Behavior, page 5-3.
Automatic deployment	Enabled.	Cisco ICS deploys all components under the following circumstances: • After an updated component is downloaded. • When a new device is added. • When the status of any device changes to online. For more information, see Enabling Automatic Deployment, page 5-8.
Report settings	Daily automatic report generation.	Cisco ICS generates reports for each active outbreak management task to provide an overview of incident control. For more information, see To Automatically Generate a Report, page 8-3.
Monitored network	The entire network.	Cisco ICS monitors all hosts on the network for watch list inclusion. For more information, see Setting the Monitored the Network, page 7-2.
Automatic device connection verification	Enabled and performed daily at 11:30 p.m.	Cisco ICS automatically verifies that it can communicate with the devices registered to it. For more information, see Setting a Verify Connection Schedule, page 9-5.

You may also want to configure the following features:

- Automatic outbreak management task deployment for yellow alerts.

  For more information, see Automating Outbreak Management, page 6-8.
- Notifications that Cisco ICS sends automatically when certain incidents and events occur.

  For more information, see Configuring Notifications, page 9-1.
- Syslog severs that collect all log information.

  For more information, see Managing Syslog Servers, page 9-4.
- Database backup that preserves Cisco ICS settings in the event of database corruption.

  For more information, see Backing Up the Database, page 9-12.

Protecting the Network

Your network is now protected. By default, Cisco ICS automatically downloads the latest components after installation and deploys them when you add devices to Cisco ICS.

Cisco ICS deploys the following components:

- The OPSig to IPS devices
- Damage cleanup components to Damage Cleanup servers

Caution We strongly recommend that you take the following minimum steps to verify that incident control is functioning properly.

To verify that incident control is functioning properly, follow these steps:

Step 1 Verify that the automatic download after installation was successful:

a. Choose **Logs** > **Event Log Query**.

b. Under Event, click **Server update event** and preserve the other default selections.

c. Click **Display Logs**.

The Event Log window appears.

d. If the update was successful, go to Step 2. If not, download it manually.

For more information, see Downloading Manually, page 5-4.

Step 2 Add devices to the device list tree and configure them.

For more information, see Adding a Device, page 4-4, and Configuring Devices, page 4-12.

Step 3 Verify that the devices received the components when they were added:

a. Choose **Logs** > **Event Log Query**.

b. Under Event, click **Deployment event** and preserve the other default selections.

c. Click **Display Logs**.

The Event Log window appears.

d. If the deployment was not successful, verify that the devices can communicate with Cisco ICS and manually deploy the components.

For more information, see Verifying Device Connectivity, page 4-9, and Deploying Manually, page 5-8.

Note By preserving the default settings and performing the previous steps, you can be confident that Cisco ICS is helping to protect your network from new threats. If a new red alert threat breaks out, Cisco ICS automatically deploys a new outbreak management task and corresponding OPACL and OPSig to stop the threat from spreading on your network.

Testing OPACL and OPSig Matching

You can verify that your devices are using OPACLs and OPSigs properly to identify threats.

The following components are required:

- A host on your network to serve as a victim of a threat attack.
- A host on your network to serve as an attacker.
- A device to detect the threat. To test an OPACL, you can use a switch, router, or IPS device. To test OPSig matching, use an IPS device.
- A network packet generating tool, such as Netcat. To test OPACL matching, run the tool on the computer that serves as the receiver of the virus.
- The Malware Tester utility, located on the Cisco ICS server at the following location:

  C:\Program Files\Cisco Systems\CICS\PCCSRV\Admin\Utility\malware_tester

This section describes how to test OPACL and OPSig matching. It contains the following topics:

- Testing OPACL Matching, page 3-8
- Testing OPSig Matching, page 3-9

Testing OPACL Matching

By default, Cisco ICS includes a threat named Malware. The threat's OPACL blocks Telnet traffic that uses port 52843. You can create a test outbreak management task using the Malware threat and its associated OPACL to test OPACL matching.

To test OPACL matching, follow these steps:

Step 1 Create a new manual outbreak management task (see Creating a New Manual Outbreak Management Task, page 6-6.) Configure the following settings for the task:

- Threat name—Select CICS_TEST_FILE, which is the last task in the list.
- Other settings—Leave the default settings. Do not modify them.

Step 2 On the host serving as the victim, use the network tool, such as Netcat, to open port 52843.

Step 3 On the host serving as the attacker, telnet to the victim host at port 52843. The device between the hosts should realize that the Telnet traffic matches the OPACL and create a log entry.

Step 4 Choose **Logs > Incident Log Query** in the main menu of the web console.

Step 5 Under Incident, select OPACL matching.

Step 6 Click **Display Logs**.

Step 7 Check for the log entry that indicates OPACL matching.

Step 8 To stop the network devices from using the OPACL that identifies the test virus, stop the task (see Stopping an Outbreak Management Task, page 6-13).

Testing OPSig Matching

You can use the Malware Tester tool on two hosts, one serving as the victim, the other serving as the attacker, to transmit a packet that any OPSig identifies as a virus.

To test OPSig matching, follow these steps:

Step 1 Copy the Malware Tester utility file Malware_Tester.exe to both hosts.

Step 2 Open a command prompt on the host serving as the victim.

Step 3 Instruct the Malware Tester tool to listen for the test virus packet:

```
Malware_Tester.exe -l
```

Step 4 Open a command prompt on the host serving as the attacker.

Step 5 Instruct the Malware Tester tool to send a test virus packet:

```
Malware_Tester.exe -s {IP address of victim}
```

The device between the hosts should identify the packet as a virus.

Step 6 Choose **Logs > Incident Log Query** in the main menu of the web console.

Step 7 Under Incident, select OPSig matching.

Step 8 Click **Display Logs**.

Step 9 Verify that there is a log entry that indicates OPSig matching.

Step 10 If the host serving as the victim was in the monitored network, it should appear as an infected host for the task you created. Verify that it appears on the watch list (see Viewing the Watch List Window, page 7-3).

For a list of messages you can see on the Malware Tester utility interface, see Malware Tester Utility Messages, page D-15.

CHAPTER 4

Managing Devices

This chapter explains how to manage network devices through the web console. It contains the following sections:

- About Device Types, page 4-1
- About the Device List Window, page 4-2
- Managing Antivirus Installations, page 4-15

About Device Types

Cisco ICS can manage switches, routers, IPS appliances and Cisco IOS IPS devices. For a more detailed list of supported device types and models, see Minimum System Requirements, page 1-6.

Table 4-1 contains important information about each type of device.

Table 4-1 Device Types

Device Type	Description	Account Credential	OPACL Deployment	OPSig Deployment	OPACL Mode
Switches	Standard Cisco switches	Level 15 or root view	To physical interfaces (inbound traffic only) To VLANs (inbound and outbound traffic)	No	Blocking
Routers	Standard Cisco routers	Level 15 or root view	To interfaces (inbound and outbound traffic)	No	Blocking

Table 4-1 Device Types (continued)

Device Type	Description	Account Credential	OPACL Deployment	OPSig Deployment	OPACL Mode
IPS devices	An IPS device is the combination of the following: • Cisco 4200 Series Intrusion Prevention System Sensors (IPS-4200) • Intrusion Detection System Service Modules (IDSM2) • Cisco ASA-5500 Series Adaptive Security Appliances with Advanced Inspection and Prevention modules (ASA-5500-AIP)	Admin	To interfaces (inbound and outbound traffic)	Yes	Blocking and Logging
Cisco IOS IPS devices	Any router with an Cisco IOS IPS image	Admin	To interfaces (inbound and outbound traffic)	Yes	Blocking and Logging

In addition to routers, switches, IPS appliances, and Cisco IOS IPS devices, you can also add a Damage Cleanup Services server and a Trend Micro OfficeScan server to Cisco ICS. For more information, see Registering a DCS Server to a Cisco ICS Server, page A-2, and Managing Antivirus Installations, page 4-15.

You can add a device and an interface to more than one Cisco ICS server, but we do not recommend doing so. Use only one Cisco ICS server to manage each device.

For instructions on preparing a Cisco IOS IPS router to be used with Cisco ICS, see Appendix B, "Preparing Cisco IOS Routers."

About the Device List Window

This section describes the Device List window and how to use it. It contains the following topics:

Using the Device List Window

Cisco ICS manages a variety switches, routers, and IPS devices to provide comprehensive virus outbreak protection. If a Damage Cleanup Services (DCS) server is installed on the network, Cisco ICS can also help clean up infected hosts if an outbreak has already occurred.

The Device List window displays the device list tree, a tool that provides centralized management of your network devices (see Using the Device List Tree, page 3-3). A menu, located at the top of the tree, lets you accomplish the following tasks:

- Add and remove devices

  Before you can manage devices, you must add them to the device list tree, which registers devices to the Cisco ICS server. For details, see Adding a Device, page 4-4, and Removing a Device or DCS Server, page 4-8.

- Verify device connectivity

  You can verify that the Cisco ICS server can successfully connect to and communicate with the devices registered to it. Cisco ICS generates an Event log entry every time you verify device connectivity. For more information, see Event Logs, page 10-5.

  Note You cannot add DCS servers from the Cisco ICS web console until after you register the Cisco ICS server with a DCS server from the DCS web console. See your DCS documentation for details.

- Add groups

  You can keep the device tree organized and arrange devices into groups. Group folders appear on the Directory pane.

- Move devices

  You can move devices from one group folder to another by clicking the device and dragging it to the desired folder in the Directory pane.

- Search for devices

  You can locate registered devices by searching according to device type, device name, IP address, connection status, or OPACL deployment status.

- Configure devices

  You can configure interface and VLAN settings and modify the device communications settings, such as the logical name and IP address.

- Copy settings

  If multiple devices require the same settings, you can configure one device and copy its settings to the others instead of configuring each device separately.

- Deploy components to IPS devices and DCS servers

  You can manually deploy OPSig files to IPS devices and Damage Cleanup engines and pattern files to DCS servers.

  Note By default, Cisco ICS deploys the components on the server immediately after download. To deploy the most up-to-date versions, download the latest components from the update source.

- Locate antivirus installations

  If Trend Micro OfficeScan servers are installed on the network, you can log in to an OfficeScan server web console from the Cisco ICS web console. To locate antivirus installations, click AV Locator in the device tree menu.

Adding a Device

To add a device, follow these steps:

Step 1 Do one of the following:

- Choose **Devices** > **Add Device**.
- Click **Device List** and then click **Add Device** in the top menu of the device tree.

  The Add Device window appears.

Step 2 Configure the following:

- Device Type—Select from the following:
  - Cisco IPS device/Cisco IOS IPS device

    For instructions on preparing a Cisco IOS IPS router to be used with Cisco ICS, see Appendix B, "Preparing Cisco IOS Routers."
  - Cisco router
  - Cisco switch
- License—Click **ACL License** or **IPS License**. You can add devices only if corresponding licenses are available. For more information, see About Device Licenses, page 9-9.
- Logical Name—Enter a name between 1 and 31 characters to identify the device. This name appears in the device tree. The following characters are not allowed: / \ [ ] " : ; | < > + = , ? ' * !
- IP Address—Enter the IP address of the device. Subnet mask information is not necessary.
- Communication—Select the protocol for Cisco ICS to use to communicate with the device: SSH or Telnet for switches and routers, HTTP or HTTPS for IPS devices.
- Port—Enter the port number through which to communicate with the device.
- Username, Password, and Password Confirmation—Enter the administrator account username and password and confirm the password to access the device. Spaces and the question mark character (?) are not allowed.

  For routers and switches, enter level 15 or root view account credentials. For IPS and Cisco IOS IPS devices, enter administrator access account credentials.
- ACL Settings—If you are adding a switch, click the location to which Cisco ICS deploys the OPACL: **Physical interface** or **VLAN**. For routers and IPS devices, OPACLs are applied to physical interfaces only.
- Public Key Deployment Settings—If you are adding an IOS IPS device, specify the settings Cisco ICS will use to deploy the Trend Micro public key to the device. Use the default selections (SSH for connection and 22 for port) or change the settings.

Note If you select Telnet, the port number will automatically change to 23. If your IOS IPS devices will use a different port to establish connection, or if several IOS IPS devices will share the same IP address in a Network Address Translation (NAT) environment, enter a different port number after selecting SSH or Telnet.

Step 3 Click **Save** to save the settings and return to the Device List window.

If you are adding a router or switch, click **Save & Configure** to add the device, import the device certificate, and configure additional settings.

If you are adding an IPS or IOS IPS device, click **Save & Verify** to add the device, import the device certificate, and test that the network connection between Cisco ICS and the device is working properly.

Step 4 Verify that the device appears in the device list tree.

Note By default, the device appears in the main folder under the root icon. To move devices from one group folder to another, click the device and drag it to the desired folder in the Directory pane.

Adding Multiple Devices

If you want to add many devices concurrently, you can use a command line tool that is automatically included in the Cisco ICS program package. The following components are required:

- BatchAddDev.ini—The configuration file that the tool uses to access the Cisco ICS server.
- BatchAddDev.exe—The executable file that runs the tool.
- Device information file—A comma-delimited text file you create to list the details for all devices. The following are requirements for the device information file:
  - An ASCII text-based file.
  - One or more comma-delimited fields for each device entry.
  - No spaces between fields.
  - A carriage return after each entry.
  - Comment lines that begin with a colon (:). For example,

    : comment line
  - The following format for each entry in the file:

```
<device_type>,<license_level>,<logical_name>,<IP_address>,<protocol>,<port>,
<username>,<password>,<importing_protocol>,<importing_port>,<acl_setting>,<interfa
ce_name_n>,<opacl_direction_n>,<pre_acl>
```

Table 4-2 describes each field.

Table 4-2 Device Information

Field	Description
<device_type>	• SWT—switch • RTR—router • IPS—IPS appliance or Cisco IOS IPS device
<license_level>	License type—1 for an ACL license or 2 for an IPS license. If the device type is IPS, Cisco ICS automatically sets the license level to 2.
<logical_name>	A name that identifies the device. This name appears in the device tree. The following characters are not allowed: / \ [ ] " : ; | < > + = , ? ' * !
<IP_address>	The IP address of the device. Subnet mask information is not necessary.
<protocol>	The protocol that Cisco ICS uses to communicate with the device: • SSH or TELNET—For switches and routers • HTTP or HTTPS—For IPS devices
<port>	The port number through which communication takes place.
<username>	The administrator account username required to access the device. If you are adding a switch or router, use the required username to access it through a virtual VTY connection. If the switch or router does not require a VTY password, leave this field blank.
<password>	The corresponding password for the username. If you are adding a switch or router, use the required password to access it through a VTY connection. If the switch or router does not require a VTY user name, leave this field blank.
<importing_protocol>	If the entry is an IOS IPS device, the protocol Cisco ICS uses to deploy the Trend Micro public key to the device: • SSH or TELNET If you do not specify a protocol, Cisco ICS uses SSH by default. Leave this field blank if the entry is not an IOS IPS device.
<importing_port>	If the entry is an IOS IPS device, the port number Cisco ICS uses to deploy the Trend Micro public key to the device. If you do not specify a port number, Cisco ICS will use port 22 by default. Leave this field blank if the entry is not an IOS IPS device.
<acl_setting>	• PHYS—Apply the OPACL to physical interfaces. Use this option for routers. • VLAN—Apply the OPACL to VLANs. Cisco ICS ignores this field if the device is an IPS appliance or a Cisco IOS IPS device.
<interface_name_n>	The same string output as in the **show interface** command. Add multiple interface names if necessary. Each interface name must be followed by the OPACL direction field (see the next command). Enter any number of field pairs, provided that they exist on the device.

Table 4-2 Device Information (continued)

Field	Description
<opacl_direction_n>	• IN—Apply OPACL rules to incoming traffic. • OUT—Apply OPACL rules to outgoing traffic. Each OPACL direction field follows an interface name (see the previous command). Enter any number of field pairs provided that they exist on the device.
<pre_acl>	An optional ACL that takes precedence over an OPACL and any other ACL that already exists on a device. This field must contain a valid Cisco IOS syntax command or series of commands separated by semicolons.

Table 4-2 shows sample entries for each device:

Table 4-3 Sample Entries

Device Type	Sample Entry
Router or Switch	`SWT,1,Switch_1,10.10.10.10,TELNET,23,UserName,Password,,,PHYS,Ethernet0,IN,PreACL`
IPS device	`IPS,2,IPS_1,10.10.10.11,HTTP,80,UserName,Password`

IOS IPS device	If the default import protocol and port are used:
	`IPS,2,IOSIPS_1,10.10.10.12,HTTP,80,UserName,Password`
	OR
	`IPS,2,IOSIPS_1,10.10.10.12,HTTP,80,UserName,Password,SSH,22`
	If the default import protocol and port are not used:
	`IPS,2,Device_C,200.1.1.2,HTTP,3002,UserName,Password,TELNET,3001`

Note If you add multiple switches and routers that have different virtual terminal (VTY) connection username and password requirements, the tool might not add some devices. You should add devices that require a username and password in one batch and devices that do not require a username and password in another batch. Mixing the two types of devices can cause a CGI timeout or connection failure error message to appear.

To add multiple devices, follow these steps:

Step 1 Create a device information text file with an entry for each device you want to add.

Step 2 Open a command prompt on the computer hosting the Cisco ICS server.

Step 3 Go to the following directory:

C:\Program Files\Cisco Systems\CICS\ PCCSRV\Admin\Utility\BatchAddDev

Step 4 Configure the BatchAddDev.ini file:

a. Open the file in a text editor.

b. Modify the address and port values to your Cisco ICS server IP address and the port you use to connect to the web console.

c. If you are using HTTP to connect to the web console, modify the SSL_Enable value to **0**. If you are using HTTPS, modify the value to **1**.

Step 5 Enter the following command: `BatchAddDev.exe {filename}`, where {filename} is name of the device information text file you created. Cisco ICS parses the file and shows a result for each entry.

Step 6 Verify that the devices appear in the device list.

If Cisco ICS is unable to parse an entry, modify the entry in the text file and run the tool again.

Note If Cisco ICS cannot add an interface, it skips that interface but continues to add the other specified interfaces.

For a list of the error messages that might appear when you are using the tool and for potential solutions., see Multiple Device Addition Messages, page D-10.

Importing Device Certificates

By default, all network devices that Cisco ICS supports generate a digital certificate. Cisco ICS obtains certificate information from the devices when you add them to the device list, but you must import the certificates through the web console. If you do not import a device's certificate, the device appears offline in the device list and you cannot manage it. You can import a certificate at the time you are adding the device, or later from the Device Certificates window. For more information, see Managing Certificates, page 9-6.

Removing a Device or DCS Server

To remove a device or DCS server, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 In the device list, select the items you want to remove. Use the Ctrl and Shift keys to make multiple selections.

Step 3 Click **Remove**.

Step 4 To remove a DCS server, click **Unregister**.

Note Removing a device or DCS server does not remove any Pre-ACLs, OPACLs, OPSigs, or DCS components already applied to devices. You can manually stop active tasks to remove applied OPACLs or leave OPACLs on the devices. They expire automatically at the configured OPACL end date (default is 2 hours for automatic tasks). You can also modify or remove OPACLs by connecting to the device directly.

Viewing Device Details

The Device List pane shows the following details about each device:

- Logical Name—The name of the entity (group name or device name).
- Type—The type of entity (folder or device type).
- Product Version—DCS server version number.

  This appears only if Cisco ICS is registered with a DCS server and you click the AV Software folder.
- IP Address—The IP address of the device as configured for the device communication settings.
- Connection—Online or Offline.
- Version—The Cisco IOS image on a switch or router or the IPS image on an IPS appliance.
- OPACL Status—If the OPACL on the Cisco ICS server was deployed, a green check mark appears. If not, the field is empty.
- OPSig—If the OPSig on the Cisco ICS server was deployed, the version number appears. If not, the field is empty.
- DCT—Damage Cleanup template version number.

  This appears only if Cisco ICS is registered with a DCS server and you click the AV Software folder.
- DCE—Damage Cleanup engine version number.

  This appears only if Cisco ICS is registered with a DCS server and you click the AV Software folder.
- Spyware pattern—Spyware pattern version number.

  This appears only if Cisco ICS is registered with a DCS server and you click the AV Software folder.

Verifying Device Connectivity

To test whether the Cisco ICS server can successfully communicate with registered devices, use the Device List window to verify the connection. Cisco ICS uses the device communications setting protocol you selected for the verification.

Cisco ICS generates an event log entry every time you verify device connectivity. For more information, see Event Logs, page 10-5.

You can also set a verify connection schedule. For more information, see Setting a Verify Connection Schedule, page 9-5.

To verify device connectivity, follow these steps:

Step 1 Click a device on the Device List window. To select multiple devices, click a group folder or click the root icon to select all devices registered to the server.

Step 2 Click **Verify Connection**.

A confirmation message appears.

Step 3 Click **Refresh**.

Step 4 Click **OK**.

Step 5 Under Connection in the Device List pane, verify that the status of the device is online. If the device is still offline after you verify the connection, for tips on resolving connection issues, see Device Configuration Troubleshooting Tips, page D-8.

Note The default verify connection timeout is 22 seconds. You cannot modify this value from the web console.

Managing Groups

To help keep the device tree organized, arrange devices into groups. Groups appear as folders in the device list tree. A maximum of three subgroup folders can exist in one hierarchy under a single group folder.

This section describes how to add and remove groups and contains the following topics:

- Adding a Group, page 4-10
- Removing a Group, page 4-11

Adding a Group

To add a group, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click the main folder under the Cisco ICS root in the Directory pane.

Step 3 Click **Add Group**.

The Add Group window appears.

Step 4 Enter a name for the group up to 31 characters. The following characters are not allowed:

/ \ [ ] " : ; | < > + = , ? ' * !

Step 5 Click **Save**.

The group appears in the device tree.

Removing a Group

To remove a group, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click the group folder in the Device List pane (not the Directory pane).

Step 3 Click **Remove**.

The group no longer appears in the device tree.

Searching for Devices

Cisco ICS provides the option of searching for the following devices and products in the device tree:

- Cisco IPS device
- Cisco router
- Cisco switch
- Trend Micro OfficeScan server
- Trend Micro Damage Cleanup Services server (if Cisco ICS registers with a DCS server)

To search for devices in the device tree, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click **Search** on the Device List window.

The Search window appears.

Step 3 Check the check boxes next to the criteria that define the search:

- Product type—Select the device or product from the list.
- Logical name—Enter the name of the device or product. The name is case-sensitive and must match exactly.
- IP—Click either **IP range** or **IP address** and enter the range or the specific IP address and the corresponding mask. Cisco ICS uses the exact value of the IP address bits that correspond to the 1 bits in the mask. For example, if you use the IP address 10.10.10.10 with the mask 255.255.0.0, Cisco ICS searches for IP addresses 10.10.0.0 to 10.10.255.255.
- Connection—Click **Online** or **Offline**.
- OPACL—Click **Deployed** or **Disabled**.

Step 4 Click **Search**. The results appear in the device tree.

Step 5 Click **Search Result** to see the items that match the criteria.

Configuring Devices

The following section explains how to configure switches, routers, and IPS devices already registered to Cisco ICS. It contains the following topics:

- Configuring Switches, page 4-12
- Configuring Routers, page 4-14

Configuring Switches

You configure physical interface or VLAN settings after you add a switch and configure communication settings. If changes occur to switch settings, such as the IP address or authentication credentials, modify the communications settings again.

This section describes how to configure interface and VLAN settings and contains the following topics:

- Configuring Interface Settings, page 4-12
- Configuring VLAN Settings, page 4-13

Configuring Interface Settings

If physical interfaces are configured on the switch, specify which interfaces Cisco ICS manages while outbreak management tasks are active.

Note OPACL rules are applied to both inbound and outbound traffic for VLANs and inbound traffic for physical interfaces.

To configure interface settings, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click a switch in the device list.

Step 3 Click **Configure**.

The Configure Cisco Switch window appears with the Communication Settings tab displayed by default.

Step 4 Click the **Interface Settings** tab or the **VLAN Settings** tab. The tabs available depend on your selection for ACL settings on the Add Device window.

The following information appears in the Interface Settings table:

- Interface Name—The name of the interface as configured for the switch. You cannot modify interface names from the Cisco ICS console.
- Direction—The traffic direction to which the ACL blocking settings are applied.
- ACL Settings—The names of ACLs applied to the interface.
  - Pre-ACL—ACL commands that appear first in the ACL. Click **Edit** to modify.
  - Current ACL—The combination of Pre-ACL, OPACL, and any preconfigured ACL currently applied to the interface. Click the link to view.

Step 5 Click **Add Interface**.

Step 6 Click the names of the switch interfaces to add.

Note Adding one interface could result in the automatic addition of other interfaces if they have the same ACL applied. Interfaces with the same ACL applied are grouped together.

Step 7 From the Direction list, choose the traffic direction to which the ACL blocking settings are applied:

- In
- Out
- In/Out

Step 8 Click **Save**.

A window appears, showing a summary of the interfaces you added. If you applied more than one interface to the same ACL, all the interfaces are added and grouped together.

Step 9 Click **Close**.

Verify that the interface was added to the summary table. If an outbreak management task is active, the Deploy to Network Devices link becomes active.

Step 10 Click **Deploy to Network Devices** to deploy the existing ACLs to the new interface.

Note If one or more outbreak management tasks are active and you add an interface, Cisco ICS does not apply the existing OPACL to the new interface. You must update the device manually by clicking Deploy to Network Devices.

Configuring VLAN Settings

If VLANs are configured on the switch, specify which VLANs Cisco ICS will manage while outbreak management tasks are active.

To configure VLAN settings, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click a switch in the device list.

Step 3 Click **Configure**.

The Configure Cisco Switch window appears, with the Communication Settings tab displayed by default.

Step 4 Click the **VLAN Settings** tab. The tabs available depend on the selection for ACL settings on the Add Device window.

The following information appears on the VLAN Settings tab:

- VLAN Name—The name of the VLAN as configured for the switch. You cannot modify VLAN names from the Cisco ICS console.
- VLAN Interfaces—The number of interfaces associated with the VLAN.
- VLAN Map
  - Pre-ACL—An ACL that applies to a VLAN map while an outbreak management task is active. The Pre-ACL is located first in the VLAN map.
  - VLAN Map Name.

Step 5 Click **Add VLAN**.

Step 6 Click the names of the switch VLANs to add.

Step 7 Click **Save**. If you applied more than one VLAN to the same VLAN map, all the VLANs are added and grouped together.

Step 8 Click **Close**. Verify that the VLAN was added to the summary table. If an outbreak management task is active, the Deploy to Network Devices link becomes active.

Step 9 Click **Deploy to Network Devices**.

Note If one or more outbreak management tasks are active and you add a VLAN, Cisco ICS does not apply the existing OPACL to the new VLAN. You must update the device manually by clicking **Deploy to Network Devices**.

Configuring Routers

After you add a router and configure initial communication settings, configure the interface settings. If changes occur to router settings, such as the IP address or authentication credentials, modify the communications settings again.

This section describes how to configure interface settings for routers. It contains the following topic:

- Configuring Interface Settings, page 4-14

Configuring Interface Settings

You can specify which interfaces Cisco ICS will manage while outbreak management tasks are active.

To configure interface settings, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click a router in the device list.

Step 3 Click **Configure**.

The Configure Cisco Router window appears, with the Communication Settings tab displayed by default.

Step 4 Click the **Interface Settings** tab. The following information appears:

- Interface Name—The name of the interface as configured for the router. You cannot modify interface names from the Cisco ICS console.
- Direction—The traffic direction to which the ACL blocking settings are applied.
- ACL Settings—The names of ACLs applied to the interface.
- Pre-ACL—ACL commands that appear first in the ACL. Click **Edit** to modify.
- Current ACL—The combination of Pre-ACL, OPACL, and any preconfigured ACL currently applied to the interface. Click the link to modify.

Step 5 Click **Add Interface**.

Step 6 Click the names of the router interfaces to add.

Step 7 From the Direction list, choose the traffic direction to which the ACL blocking settings are applied:

- In
- Out
- In/Out

Step 8 Click **Save**.

A window appears, showing a summary of the interfaces you added. If you applied more than one interface to the same ACL, all the interfaces are added and grouped together.

Step 9 Click **Close**. Verify that the interface was added to the summary table. If an outbreak management task is active, the Deploy to Network Devices link becomes active.

Step 10 Click **Deploy to Network Devices** to deploy the existing ACLs to the new interface.

Step 11 Click **Save**.

Note If one or more outbreak management tasks are active and you add an interface, Cisco ICS does not apply the existing OPACL to the new interface. You must update the device manually by clicking Deploy to Network Devices.

Copying Device Settings

If multiple devices require the same settings, you can configure one device and copy its settings to the others instead of configuring each device separately. Copying is possible between devices of the same type only.

To copy device settings, follow these steps:

Step 1 In the device list tree, click the device that has the settings you want to copy.

Step 2 Click **Copy Settings**.

The Copy Settings window appears.

Step 3 Select the devices to which you want to apply the settings. To select multiple devices, click a group folder or click the root icon to select all devices registered to the server.

Step 4 Click **Copy**.

A confirmation window appears.

Step 5 Click **Back** to return to the Device List window.

Managing Antivirus Installations

Cisco ICS is also a central point to access antivirus protection. If Trend Micro OfficeScan servers are installed on the network, you can log in to an OfficeScan server web console from the Cisco ICS web console. First, locate the OfficeScan servers on the network.

This section describes how to locate and access the OfficeScan servers on the network and contains the following topics:

- Locating OfficeScan Servers, page 4-16
- Accessing an OfficeScan Server, page 4-16

Locating OfficeScan Servers

To locate OfficeScan servers, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click **AV Locator** in the top menu.

The Antivirus Product Locator window appears.

Step 3 In the Port to scan field, enter the port to use to scan for OfficeScan servers. This is the HTTP web port number used to access the OfficeScan servers.

Step 4 In the IP range field, enter a range of IP addresses in which to search.

Step 5 Next to Console Protocol, choose the type of protocol you use to connect to the OfficeScan server (HTTP or HTTPS).

Step 6 In the Port field, enter the port you use to access the OfficeScan server web console.

Step 7 Click **Search**.

The OfficeScan server details appear in the results window.

Step 8 Do one of the following:

- Check the check boxes next to the OfficeScan servers to add.
- Check the check box at the top to select all servers in the list.

Note If the OfficeScan server is already in the device list, a check box does not appear next to the OfficeScan server name.

Step 9 Click **Snap-in**.

The OfficeScan servers appear in the Device List. You can snap-in one OfficeScan server to more than one Cisco ICS server.

Accessing an OfficeScan Server

To access an OfficeScan server, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click the **AV Software** group folder in the directory tree.

Step 3 Click the desired OfficeScan server in the device list.

Step 4 Click **Configure**.

The OfficeScan web console opens within the Cisco ICS web console. You can navigate to other Cisco ICS features by using the top menu.

CHAPTER 5

Updating Components

This chapter explains how to download and deploy the components you need to implement your incident-control strategy. It contains the following sections:

- About Updating, page 5-1
- Downloading Components, page 5-2
- Creating an Alternate Update Source, page 5-5
- Deploying Components, page 5-7

About Updating

You must periodically update Cisco ICS components to help protect the network from the latest threats. Updating refers to two actions:

- Downloading—The Cisco ICS server pulls components from the update source (by default, the Trend Micro ActiveUpdate server).
- Deploying—The Cisco ICS server pushes components to network devices and the DCS server.

For an outline of the components Cisco ICS uses, see About Cisco ICS Components, page 1-3.

This section describes updates and contains the following topics:

- Manual and Automatic Updates, page 5-1
- Update Verification, page 5-2
- Update Sources, page 5-2
- Proxy Server Connection, page 5-2

Manual and Automatic Updates

Trend Micro typically releases updated components at least once daily, and more often when a new threat is discovered. You can download and deploy components manually on demand through the Cisco ICS web console. However, we do not recommend this because it would require the Cisco ICS administrator to update the components at least once a day to keep antivirus protection current.

To relieve the Cisco ICS administrator of this task, configure a download schedule and enable automatic deployment. You can still update manually at any time.

Note After installation is complete, Cisco ICS immediately downloads the latest components from the default update source using HTTPS. This one-time, post-installation download is enabled by default and cannot be disabled.

Scheduled downloads for OPSigs and DCS components follow the outbreak management task download schedule when outbreak management tasks are active. For more information, see Scheduled Download Behavior, page 5-3.

Update Verification

Periodically verify component download and deployment by viewing the Outbreak Management Task Summary window or the event log. For more information, see Viewing a Summary of All Outbreak Management Tasks, page 6-10, and Event Logs, page 10-5.

Update Sources

By default, Cisco ICS downloads components from the Trend Micro ActiveUpdate server; however, you can select another update source. For more information, see Modifying the Download Source, page 5-4.

Proxy Server Connection

If the network has a proxy server, you must configure the server information on the Update Download Source window to successfully connect with the download source. For more information, see Modifying the Download Source, page 5-4.

Downloading Components

To automate the task of keeping the Cisco ICS server components current, configure scheduled download. By default, scheduled download is enabled and configured to poll the update source every 5 minutes for a new OPACL and every 12 hours for other components. If a new version of a component is available, Cisco ICS downloads the new version. Alternatively, to avoid waiting for the next scheduled download, you can download the components manually at any time.

This section describes how to configure scheduled downloads and contains the following topics:

- Configuring Scheduled Download, page 5-3
- Scheduled Download Behavior, page 5-3
- Downloading Manually, page 5-4
- Modifying the Download Source, page 5-4

Configuring Scheduled Download

Tip The default selections provide adequate protection without overburdening the network with excessive downloads.

To configure scheduled downloads, follow these steps:

Step 1 Choose **Updates > Scheduled Download**.

The Scheduled Download window appears, showing two schedules:

- Outbreak Management Task Polling Schedule—Downloads the outbreak management task file, which includes the latest OPACL configurations for all threats.
- OPSig Polling Schedule—Downloads OPSig files and the files that DCS uses.

Note Damage Cleanup and spyware components are available only when a DCS server registers to the Cisco ICS server. You cannot download DCS components separate from the OPSig.

Step 2 Ensure that the check boxes for the components you want to download are checked.

Step 3 For each schedule, click one of the following and choose the frequency for downloading:

- **Minute**—every { } minutes.
- **Hour**—every { } hours.
- **Day**—every { } days at the selected time of day.
- **Week, on**—once per week on the selected day and time.

Step 4 Click **Save**.

Download schedules differ when one or more outbreak management tasks are active. For more information, see Scheduled Download Behavior, page 5-3.

Scheduled Download Behavior

Scheduled download behavior for OPSigs and DCS components differs when outbreak management tasks are active and the required OPSig is not yet deployed.

- Normal download scheduling—Both outbreak management task downloads and OPSig/DCS component downloads take place according to their respective schedules under either of the following circumstances:
  - No outbreak management tasks are active.
  - One or more tasks are active and Cisco ICS has already successfully deployed the OPSigs required to address the associated threats.

- Outbreak management task download schedule usage—Cisco ICS ignores the time interval for OPSig/DCS component scheduled downloads when both of the following are true:
  - One or more tasks are active.
  - Cisco ICS has not yet successfully deployed the OPSigs required to address the associated threat.

  In this situation, Cisco ICS downloads both the outbreak management task, including the latest OPACL, and OPSig/DCS components according to the outbreak management task polling schedule.

  When Cisco ICS downloads the required OPSig for the outbreak management task, the OPSig/DCS component polling schedule interval resumes precedence for OPSigs and DCS components. Outbreak management task downloads, which include the latest OPACL file, continue to follow the OPACL download schedule.

Downloading Manually

To download an update manually, follow these steps:

Step 1 Choose **Updates** > **Manual Download**.

Step 2 Select the components to download. To select all components, check the **Components** check box.

Step 3 Click **Download**.

The Manual Download Progress window appears, showing the progress of the download and the result.

Step 4 Click **Back** to return to the Manual Download window.

Modifying the Download Source

By default, Cisco ICS downloads components from the Trend Micro ActiveUpdate server; however, other update sources are also allowed. To successfully connect with the download source when a proxy server is on the network, you must configure the proxy server information on the Update Download Source window.

Note By default, Cisco ICS uses Secure HTTP (HTTPS) when connecting to the download source for enhanced security.

To modify the download source, follow these steps:

Step 1 Choose **Updates > Download Source**.

Step 2 Under Download Source, click one of the following options:

- **Trend Micro ActiveUpdate Server**—Choose the connection protocol (HTTP or HTTPS).
- **Other update source**—Enter the full address of the source URL. For example:

  http://www.ciscoicsupdatesource.com/activeupdate
  https://www.ciscoicsupdatesource.com/activeupdate

Step 3 Click **Save**.

Configuring Proxy Settings for Downloads

If the network has a proxy server, you must configure the server information on the Update Download Source window to successfully connect with the download source.

Step 1 Choose **Updates > Download Source**.

Step 2 Under Proxy Settings, check the **Use a proxy server** check box.

Step 3 Configure the following:

- Proxy type—The protocol the proxy server uses (HTTP Proxy or SOCKS version 4/5).
- Server name or IP address—The domain name or the IP address of the proxy server.
- Port—The port the Cisco ICS server uses to connect to the proxy server.
- User name and Password—The login credentials.

Step 4 Click **Save**.

Creating an Alternate Update Source

By default, Cisco ICS downloads components from the Trend Micro ActiveUpdate server, which is the only source for new OPACLs, OPSigs, and DCS components. However, you might want to allow Cisco ICS servers to download components from an alternate update source located on your network in certain situations, such as the following:

- Your Cisco ICS server is not connected to the Internet.
- The connection between your Cisco ICS server and the Internet is not reliable.
- The bandwidth between your Cisco ICS server and the Internet is restricted.

You can set up and maintain an alternate update source server anywhere on your network that you can access from your Cisco ICS server. However, to keep the Cisco ICS components up-to-date, you must regularly download a configuration file and all the Cisco ICS components from the Trend Micro ActiveUpdate server to the alternate update source sever.

If scheduled download is enabled on Cisco ICS, the Cisco ICS server automatically discovers and downloads the new components from the alternate update source. You can also manually download the components.

This section describes how to create an alternate update source and contains the following topics:

- Minimum System Requirements for an Alternate Update Source Server, page 5-6
- Downloading the server.ini File, page 5-6
- Setting up the Alternate Update Source Server, page 5-6
- Updating the Alternate Update Source Server, page 5-7

Minimum System Requirements for an Alternate Update Source Server

The following versions or later are required for any computer you want to serve as an alternate update source server.

- Operating system (one of the following)
  - Windows 2000
  - Redhat Linux 6.2
- Web server (one of the following)
  - IIS: Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0
  - Apache: 2.0
- Network Protocol
  - TCP/IP
- Hardware
  - 586 Intel Pentium processor or equivalent
  - 256 MB of RAM
  - 4 GB of disk space

Downloading the server.ini File

All information related to Cisco ICS components is contained in a configuration file named server.ini. Trend Micro updates this file every time a new component is ready. When you are setting up and updating your alternate update source server, download server.ini from the Trend Micro website at the following location: http://cics-p.activeupdate.trendmicro.com/activeupdate.

Setting up the Alternate Update Source Server

This section explains how to set up an alternate update source server on a computer that meets the minimum system requirements.

To set up the alternate update source server, follow these steps:

Step 1 Create a shared directory with two subdirectories named *PATTERN* and *ENGINE*. The PATTERN directory holds the OPACL, OPSig, Damage Cleanup template, and Spyware pattern files. The ENGINE directory holds the Damage Cleanup engine.

Step 2 Map the shared directory to your web server's virtual directory. See your web server documentation for details.

Step 3 Download the server.ini file:

http://cics-p.activeupdate.trendmicro.com/activeupdate

And then save the file in the shared directory that you created.

Step 4 Open the server.ini file in a text editor.

Step 5 Obtain the filenames of the components to download. The component filenames immediately follow a string which identifies each component:

- OPACL—Search for the string **P.10000040=pattern/**.
- OPSig—Search for the string **P.10000004=pattern/**.
- Damage Cleanup pattern—Search for the string **P.800=pattern/**. The filename after this string is a zip file that contains a single pattern file. Download this file.

  The pattern file is divided into several subfiles. You also need to search for each of the subfiles starting with the string **P.800.Merge.1/** and ending with **P.800.Merge.x/**, where x is the last entry in the list. Download all of these subfiles in addition to the zip file.
- Spyware pattern—Search for the string **P.1000000=pattern/**. The filename after this string is a zip file that contains a single pattern file. Download this file.

  The pattern file is divided into several subfiles. You also need to search for each of the subfiles starting with the string **P.1000000.Merge.1/** and ending with **P.1000000.Merge.x/**, where x is the last entry in the list. Download all of these subfiles in addition to the zip file.
- Damage Cleanup engine—Search for the string **E.1000000=TSC,engine/**.

  For example, the filename of the OPACL in a server.ini file with the entry P.10000040=pattern/opacl0.3.zip,204,23039, is opacl0.3.zip.

Step 6 Download each component file:

a. Enter the name of a component file at the end of the URL you used to access the server.ini file. For example, if the filename of the OPACL that you want to download is opacl0.3.zip, enter the following URL in your web browser:
http://cics-p.activeupdate.trendmicro.com/pattern/activeupdate/opacl.0.3.zip

A prompt appears.

b. Click **Save** to save the file to the correct subdirectory in the shared directory you created. Save the Damage Cleanup engine in the ENGINE subfolder and the other components in the PATTERN subfolder.

Step 7 On the Cisco ICS server which will use the new alternate update source, modify the download source.

Updating the Alternate Update Source Server

To keep your threat-protection current, update the alternate update source every 2 to 3 days. A daily update is the most optimal. The update process is identical to the process that you performed to set up the alternate update source server.

To verify that new components are available before you perform the update, download the server.ini file and open it in a text editor. Compare the filenames of the components to see which files Trend Micro changed. Download any component file with an updated filename.

Deploying Components

You can automate the task of updating network devices and DCS servers by enabling automatic deployment. Alternatively, to avoid waiting for the next automatic deployment, you can manually deploy the OPSig, Damage Cleanup engine and template, and the spyware pattern files on the Cisco ICS server at any time.

Note Damage Cleanup and spyware components are available only when a DCS server registers with the Cisco ICS server.

This section describes how to deploy components and contains the following topics:

- Enabling Automatic Deployment, page 5-8
- Deploying Manually, page 5-8

Enabling Automatic Deployment

Cisco ICS can automatically deploy the OPSig, Damage Cleanup engine and template, and the spyware cleanup pattern in the following situations:

- After you download an updated component.
- After you add a new device.
- If the status of any device changes to online.

Note Automatic deployment is enabled by default.

To enable automatic deployment, follow these steps:

Step 1 Choose **Updates > Deployment Settings**.

Step 2 Click the **Automatically deploy components under these circumstances** radio button.

Step 3 Click **Save**.

Deploying Manually

To deploy a device manually, follow these steps:

Step 1 Choose **Devices** > **Device List**.

The Device List window appears.

Step 2 Choose the devices to update.

Note When you added IPS devices, the username must have administrator or root view account access for deployment to succeed.

Step 3 Click **Deploy**.

A confirmation message appears.

Step 4 Click **OK**.

Note If a device is offline when you deploy manually, it cannot receive the updated components. If you enable automatic deployment, the Cisco ICS server automatically deploys the components immediately after the device comes back online. This option is enabled by default.

CHAPTER 6

Managing Outbreaks

This chapter explains how to create outbreak management tasks to help protect against network virus outbreaks. It contains the following sections:

About Outbreak Management Tasks

An outbreak management task is a file that contains an OPACL. Cisco ICS uses outbreak management tasks to help protect the network from various threats. Each task is associated with a single threat. You can manually create and activate tasks or allow Cisco ICS to do so automatically. A maximum of 32 tasks can be active concurrently.

This section describes outbreak management tasks and contains the following topics:

Terms and Concepts

Become familiar with the following information before you create and configure tasks:

- Known threats—Viruses, Trojans, and other malicious code that Trend Micro already detected. Only one threat can be associated with an outbreak management task. For more information, see Understanding Network-based Threats, page 1-5, and About Risk Ratings, page 1-6.
- Outbreak Prevention ACL (OPACL)—A file that Cisco ICS deploys to specified devices to log or block certain types of network traffic. On all devices, the OPACL is disabled when the end date is reached or when Cisco ICS deploys the OPSig. For more information, see About Outbreak Policy ACLs and Pre-ACLs, page 6-4.
- Outbreak Prevention Signature (OPSig)—A file that Cisco ICS deploys to IPS devices only to detect and block the a threat from spreading. If automatic deployment is enabled, Cisco ICS deploys the OPSig immediately after downloading it. If automatic deployment is not enabled, you must deploy the OPSig manually. For more information, see About Outbreak Prevention Signatures, page 6-6, Enabling Automatic Deployment, page 5-8, and Deploying Manually, page 5-8.
- OPACL mode—A setting that determines tasks for network devices when they receive an OPACL from the Cisco ICS server. Two modes are available:
  - Blocking mode—Instructs devices to block certain types of traffic and ports and create log entries if blocking occurs.
  - Logging mode—Instructs IPS devices to create log entries if network packets match the OPACL policy. Note that the devices do not block any traffic

Note Logging mode applies to IPS devices only.

Types of Tasks

Two types of tasks are available:

- Automatic—Tasks that automatically deploy the latest OPACLs to specified devices for newly discovered red and yellow alerts. Cisco ICS periodically checks the update source server and triggers an automatic task when the solution for a new threat is ready. The OPACL for the new task defines the start and end times for the task. However, you can continue to configure basic OPACL settings, such as the task end date; whether to stop the task when Cisco ICS deploys an OPSig; and whether to overwrite an existing OPACL with a newly updated one.
- Manual—Administrator-created tasks with configurable options, such as the end date for the task, and the type of traffic and ports to block or log. Automatic tasks address only the threats discovered after you enable automatic task deployment. However, manual tasks can address existing threats.

Task Lifetime

Table 6-1 explains when tasks are activated and terminated.

Table 6-1 Outbreak Management Task Lifetime

Task Type	Activation	Termination
Automatic	Cisco ICS downloads a new task from the update source.	• Click **Stop Running Tasks** or **Remove OPACL** on the Outbreak Management Task Summary window. • Cisco ICS deploys an OPSig after you CHOOSE the option to stop the OPACL on the Automatic Outbreak Management Task window.
Manual	Immediately after creation.	Click **Stop Running Tasks** or **Remove OPACL** on the Outbreak Management Summary window.

Note Do not confuse outbreak management task lifetime with OPACL lifetime. For more information, see About Outbreak Policy ACLs and Pre-ACLs, page 6-4.

Task Creation

Table 6-2 explains when and how you can create automatic and manual tasks.

Table 6-2 Outbreak Management Task Creation

Type	Recommendation
Automatic	We recommend that you enable Cisco ICS to automatically create tasks and keep this option enabled. Cisco ICS can deploy outbreak management tasks for newly discovered red and yellow alerts after it downloads the tasks from Trend Micro. The advantage of enabling automatic tasks is that it relieves you of creating tasks manually. You must enable scheduled download for Cisco ICS to periodically poll the update source for new tasks. For more information, see Configuring Scheduled Download, page 5-3. However, automatic tasks address only the threats discovered after you enable Cisco ICS to create automatic tasks. To guard against the threats that were discovered before you enabled automatic tasks, which might still be propagating through the Internet, you must create a manual task.
Manual	We recommend that you create tasks manually if you are concerned that an existing threat poses a risk to your network. Cisco ICS offers protection from a variety of known threats detected by Trend Micro TrendLabs. The advantage of creating a task manually is that you can guard against a threat that is already in circulation before you enabled automatic tasks. If you enabled automatic tasks immediately after installing Cisco ICS and you are confident that no threats exist on your network, you do not need to create a manual task.

About Outbreak Policy ACLs and Pre-ACLs

When outbreak management tasks become active, Cisco ICS can deploy OPACLs and Pre-ACLs.

This section describes OPACLs and ACLs and contains the following topics:

- OPACLs, page 6-4
- About Pre-ACLs, page 6-5

OPACLs

This section describes OPACLs and contains the following topics:

- About OPACLs, page 6-4
- OPACL Mode, page 6-4
- Modifying the OPACL, page 6-4
- OPACL Expiration, page 6-5
- Verifying OPACL Deployment, page 6-5

About OPACLs

An OPACL is an ACL that contains instructions for addressing a variety of threats. Cisco devices use OPACLs to block the types of network traffic and the ports that threats use to launch attacks and infect hosts. When Trend Micro discovers a new threat or new information on an existing threat, the OPACL on the ActiveUpdate server is updated. You must download the new OPACL either manually or by schedule to obtain the most up-to-date virus protection.

Each OPACL is associated with a single outbreak management task (both manual and automatic).

OPACL Mode

If one or more tasks are active, the associated OPACLs are in blocking mode or logging mode.

- Blocking mode—Instructs devices to block certain types of traffic and ports and create log entries if blocking occurs.
- Logging mode—Instructs IPS devices to create log entries if network packets match the OPACL policy. Note that the devices do not block any traffic.

Note Logging mode applies to IPS devices only. You cannot change the OPACL mode if one or more outbreak management tasks are active.

Modifying the OPACL

Each OPACL has default settings that block the type of traffic and the ports that the threat uses to attack hosts. However, you can modify the contents of the OPACL during task creation and after task deployment.

OPACL Expiration

The OPACL stops blocking or logging traffic under the following circumstances:

- The OPACL end date is reached.
  - For manual tasks, configure the end date on the Specify Outbreak Management Task window.
  - For automatic tasks, configure the end date on the Automatic Outbreak Management Task window. The default is 4 hours.
- You click Remove OPACL on the Outbreak Management Task Summary window, which ends the task and the associated OPACL.
- You click Stop next to OPACL Mode on the summary window for an active outbreak management task. Stopping the OPACL does not stop the task.
- Cisco ICS deploys the OPSig for the threat. Although Cisco ICS deploys OPSigs to IPS devices only, the OPACLs for the same threat on switches and routers also stop when Cisco ICS deploys the OPSig.

Verifying OPACL Deployment

If at least one outbreak management task is active and the registered devices received the required OPACL, a green check mark appears in the OPACL Status column on the Device List window.

Pre-ACLs

This section describes Pre-ACLs and contains the following topics:

- About Pre-ACLs, page 6-5
- Access Control List Precedence, page 6-5

About Pre-ACLs

A Pre-ACL is an optional ACL that takes precedence over an OPACL and any other ACL that already exists on a device. You can deploy a Pre-ACL for each router interface and each switch interface or VLAN to instruct the devices to block or allow traffic not already addressed in an OPACL or existing ACL.

The status of outbreak management tasks and associated OPACLs does not prevent Pre-ACL deployment.

Access Control List Precedence

ACLs on devices that Cisco ICS manages have the following order of priority:

1. Pre-ACL
2. OPACL
3. Other ACL

About Outbreak Prevention Signatures

An OPSig is a file that helps IPS devices identify unique patterns of bits and bytes that signal the presence of a network virus or other threat.

Once deployed, OPSigs continue to help IPS devices scan traffic for network-based threats. Unlike the OPACL, the OPSig never expires. However, an OPSig becomes out-of-date when Trend Micro releases a newer version that addresses new threats and existing threats with improved accuracy.

Tip Trend Micro typically updates OPSigs daily and more frequently during virus outbreaks. To keep your antivirus protection current, set schedules for automated OPSig download and deployment.

This section describes how to download and deploy OPSigs and how to verify the deployment. It contains the following topics:

- Downloading and Deploying OPSigs, page 6-6
- Verifying OPSig Deployment, page 6-6

Downloading and Deploying OPSigs

Download OPSigs manually or by schedule. By default, the OPSig download schedule is enabled and polls the update source every 12 hours. However, if one or more outbreak management tasks are active and Cisco ICS has not yet deployed the required OPSig, downloads follow the OPACL download schedule. For more information, see Scheduled Download Behavior, page 5-3.

Deploy OPSigs manually from the Device List window or use Automatic Download, which is enabled by default and downloads OPSigs under the following circumstances:

- An updated component is downloaded.
- A new device is added.
- The status of any device changes to online.

Verifying OPSig Deployment

After registered IPS devices receive the required OPSig, the version number of the file appears in the OPSig Status column on the Device List window.

Creating a New Manual Outbreak Management Task

To immediately protect your network from an existing threat, you should create a new manual outbreak management task.

To create a manual outbreak management task, follow these steps:

Step 1 Start the Cisco ICS web console.

The Outbreak Management Summary window appears.

Step 2 Choose **Outbreak Management > Outbreak Settings > OPACL Settings**.

Step 3 Under OPACL Mode, choose one of the following:

- Blocking mode—Instructs devices to block certain types of traffic and ports and create log entries if blocking occurs.
- Logging mode—Instructs IPS devices to create log entries if network packets match the OPACL policy. Note that the devices do not block any traffic.

Note Logging mode applies to IPS devices only. You cannot change the OPACL mode if one or more outbreak management tasks are active.

Step 4 Click **Save**.

Step 5 Choose **Outbreak Management > New Outbreak Management Task**.

Step 6 Select a known threat to start monitoring on the network. Only one threat for each task is allowed.

Step 7 Click **Next**.

The Edit Outbreak Management Task window appears.

Step 8 Configure the following:

- Task name—By default, the task name is the name of the threat and the word Task, for example, WORM_BAGLE.AT Task. You cannot modify the name when the task is active.
- OPACL end date—The date and time that the OPACL settings should cease to be in effect.
- OPACL Configuration—The type of network traffic and ports to block. Select the default policy, or customize the policy by configuring the settings of your choice. To block or log multiple ports, include a dash or semicolon. For example, enter **21;81-65535** to block port 21 and all ports between 81 and 65535, inclusive.

  If a port is on the exception list, you cannot add it to the OPACL for a new manual outbreak management task. You must first remove it from the exception list. For more information, see Configuring the Exception List, page 6-9.

Caution The default OPACL settings adequately address the associated threat. If customization is necessary, make the OPACL blocking settings stricter. If you make them less strict, you could expose your network to network-based threats.

Step 9 Click **View ACL Configuration** to see the rules defined in the OPACL as they appear in Cisco ACL format.

Step 10 Verify that the OPACL configuration is correct. If it is incorrect, do the following:

a. On the Edit Outbreak Management Task window under OPACL configuration, click **Custom policy**.

b. Modify the OPACL configuration.

c. Click **View ACL Configuration** again to verify that the OPACL rules are correct. If they are incorrect, modify them under OPACL configuration.

Step 11 Click **Next**.

Step 12 Select the devices to which to apply the OPACL.

Step 13 Click **Finish**.

Cisco ICS puts the new outbreak management task into effect immediately.

Step 14 Click **Back** to go to the summary window for the new task.

Automating Outbreak Management

To relieve administrators of creating new outbreak management tasks, you can automate the creation of tasks. Cisco ICS deploys automatic tasks when a new OPACL becomes available on the update source.

To automate outbreak management, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Settings > OPACL Settings**.

Step 2 Under OPACL Mode, choose one of the following:

- Blocking mode—Instructs devices to block certain types of traffic and ports and create log entries if blocking occurs.
- Logging mode—Instructs IPS devices to create log entries if network packets match the OPACL policy. Note that the devices do not block any traffic.

Note Logging mode applies to IPS devices only. You cannot change the OPACL mode if one or more outbreak management tasks are active.

Step 3 Click **Save**.

Step 4 Choose **Outbreak Management > Outbreak Management Task Summary**.

Step 5 Do one of the following:

- Click one of the following under Automatic Outbreak Management Task (both links go to the same window):
  - **Automatic Red Alert Outbreak Management Tasks**
  - **Automatic Yellow Alert Outbreak Management Tasks**
- Click **Outbreak Management** > **Automatic Outbreak Management Task**.

  The Automatic Outbreak Management Task window appears.

Step 6 Choose one or both of the following options:

- **Automatically stop the OPACL when Cisco ICS deploys the OPSig to online IPS devices**
- **Automatically overwrite the OPACL after Cisco ICS downloads a new OPACL**

Step 7 Configure OPACL settings:

a. Click the **OPACL Settings** tab (shown by default).

b. Choose one or both of the following:
   - **Enable automatic Red Alert Outbreak Management Task**
   - **Enable automatic Yellow Alert Outbreak Management Task**

c. Next to End OPACL after: { } days, choose the number of days, hours, and minutes after which the OPACL expires.

Note The **Automatically stop the OPACL when Cisco ICS deploys the OPSig to IPS devices** selection overrides the number of days you choose from the list.

Step 8 Select the mitigation devices to which Cisco ICS applies the OPACL:

a. Click the **OPACL Mitigation Devices** tab.

b. From the Specify Mitigation Devices for OPACL table, click one of the following:

- **All devices**—Click to apply the OPACL to all devices registered to Cisco ICS.
- **Specific devices**—Click to apply the OPACL to only certain devices registered to Cisco ICS. Check the check boxes next to the devices.

Step 9 Click **Save**.

Note The automatic task becomes active when Cisco ICS receives a new OPACL. You must enable Scheduled Download to ensure that Cisco ICS regularly receives updated OPACLs.

Configuring the Exception List

Configure the OPACL exception list to exclude specified ports from OPACL blocking settings. The exception list applies to all OPACLs used in active outbreak management tasks, regardless of the OPACL mode (Blocking or Logging).

If a port is on the exception list, you cannot add it to the OPACL for a new manual outbreak management task. You must first remove it from the exception list. For more information, see Creating a New Manual Outbreak Management Task, page 6-6.

To configure the exception list, follow these steps:

Step 1 Choose **Outbreak Settings > Exception List**.

Step 2 Configure one or more of the following options:

- Under Commonly Used Ports, select the ports to exclude from OPACL blocking. Check the check box at the top to select all commonly used ports.
- Under Specified Port Range, select **TCP**, **UDP**, or both and enter the port numbers in the corresponding text boxes. For multiple ports, include a dash or semicolon. For example, enter **21;81-65535** to block port 21 and all ports between 81 and 65535, inclusive.
- Select **Internet Control Messaging Protocol** to allow all ICMP traffic.

Step 3 Click **Save**.

Viewing the Network Viruses in a Policy

Each OPACL contains pattern files to detect a large number of threats. If you want to know whether or not the OPACL on the Cisco ICS server is addressing a certain threat that you have in mind, you can view a list of all threats in the Network Viruses in Policy window.

To view the network viruses in a policy, follow these steps:

Step 1 Do one of the following:

- Start the Cisco ICS web console. The Outbreak Management Summary window appears.
- Choose **Outbreak Management** > **Outbreak Management Summary**.

Step 2 In the OPACL table, click **Network viruses in policy**. The Network Viruses in Policy window appears, showing the following information:

- Threat Name—The official name of the threat. Click the threat name to open the Trend Micro Virus Encyclopedia, which contains detailed information about the threat.
- Last Updated—The date the threat information was last updated.
- Alert Type—An indication of the prevalence of the threat.
- Red Alert—An indication that the threat is widespread.
- Yellow Alert—An indication that the threat was detected but is not widespread.
- Risk—An indication of the amount of damage the threat can create. For more information, see About Risk Ratings, page 1-6.
- Req'd OPACL—The version number of the OPACL required to protect the network from the threat.
- Req'd OPSig—The version number of the OPSig required for IPS devices to detect and block the threat.
- Policy—A link to a summary of what the OPACL is doing to address a given threat. For example, a summary that reports TCP Port =8181 means the OPACL instructs devices to block TCP port 8181.

Note The table shows only ten threats per page. To view additional pages, click the advance arrow.

Step 3 Click **Back** to return to the Outbreak Management Summary window.

Viewing a Summary of All Outbreak Management Tasks

Use the Outbreak Management Summary window to view summaries of all active outbreak management tasks, create a new outbreak management task, set up new automatic outbreak management tasks for red and yellow alerts, and view details of the latest OPACL and OPSig files on the server.

To access the Outbreak Management Summary window, start the Cisco ICS web console. The Outbreak Management Summary window opens by default. If you are not in this window, choose **Outbreak Management > Outbreak Management Summary**.

The following appears in the Running Outbreak Management Tasks table:

- Task name—An icon indicating whether the task is a yellow alert or red alert and the name of the task.
- Hosts in watch list—The number of hosts on your network that are on the watch list because they are at risk from the threat associated with the task. Click the number to go to the Watch List window.
- Initiated Date/Time—The date and time of day the outbreak management task became active.
- OPACL End Date/Time—The date and time of day the OPACL associated with the task ends.
- Action—One of the following appears:
  - Stop Running Task—Appears if the OPACL is not active. Click to stop the task.
  - Remove OPACL—Appears if the OPACL is active. Click to stop the task and remove the associated OPACL and Pre-ACL.

The following appear in the OPACL and OPSig tables:

- Current version—The version numbers of the OPACL and OPSig files on the Cisco ICS server.
- Last updated—The date of the last OPACL or OPSig update.
- Network viruses in policy—The number of network viruses the current OPACL addresses. Click the number to view a list of the viruses on the Network Viruses in Policy window.
- Number of devices—The number of registered IPS devices. Click the number to view the devices in the device tree.
- Outdated devices—The number of IPS devices with an out-of-date OPSig. Click the number to view the devices in the device tree.

Viewing an Active OPACL

To verify that the OPACL is correct, you can view any OPACL associated with both an active outbreak management task and a specific router or switch to which the OPACL was applied.

To view an active OPACL, follow these steps:

Step 1 Choose **Devices > Device List**.

The device list tree appears.

Step 2 Click the device on which the OPACL resides.

Step 3 Verify that a green check mark appears in the OPACL Status column, signifying that the device has the required OPACL.

Step 4 Click **Configure**.

The configuration window for the device appears, with the **Communication Settings** tab displayed by default.

Step 5 Click the **Interface Settings** tab.

Step 6 In the interface settings table, click a link under Current ACL.

The OPACL appears in a read-only window.

Note You cannot modify an active OPACL from this window. For more information, see Modifying the OPACL, page 6-4.

Modifying Outbreak Management Task Options

The first step in modifying an existing outbreak management task is specifying task details and modifying OPACL settings. Details about the selected threat appear at the top of the window.

To modify an existing outbreak management task, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 Click the name of the task you want to modify.

The summary window for that task appears.

Step 3 Click **View/Edit Outbreak Policy**.

The Edit Outbreak Management Task window appears.

Step 4 The Specify Outbreak Management Task table contains the details of the task. Modify any of the following:

- Task name—By default, the task name is the name of the threat and the word "Task," for example, WORM_BAGLE.AT Task. You cannot modify the name when the task is active.
- OPACL end date—The date the OPACL settings should cease to be in effect. If necessary, modify the date by clicking the calendar icon and choose a start time in hours and minutes from the hh and mm lists.
- OPACL Configuration—The traffic and ports the OPACL can block. Choose one of the following:
  - **Default policy**—Click to use the settings associated with the default OPACL for this threat.
  - **Custom policy**—Click to customize the OPACL settings. Check the check boxes to block any of the following types of traffic:

    ICMP

    TCP Port—Enter the TCP ports to block or log.

    UDP Port—Enter the UDP ports to block or log.

  Note To block or log multiple ports, include a dash or semicolon. For example, enter 21; 81-65535 to block port 21 and all ports between 81 and 65535, inclusive.

  If a port is on the exception list, you cannot add it to the OPACL for a new manual outbreak management task. You must first remove it from the exception list. For more information, see Configuring the Exception List, page 6-9.

- View ACL Configuration—Click to verify that the OPACL settings are correct. If they are incorrect, modify the OPACL settings on this window. You can modify the OPACL mode on the OPACL Settings window.

Step 5 Click **Next** to continue or click **Cancel** to stop and return to the Outbreak Management Summary window. The Specify Outbreak Management Task table contains the device tree. The following information appears in the table:

- **All devices**—Click to apply the OPACL to all devices registered to Cisco ICS.
- **Specific devices**—Click to apply the OPACL to only certain devices registered to Cisco ICS. Check the check boxes next to the devices.

Step 6 Click **Finish** to finish modifying the task. Cisco ICS updates the outbreak management task immediately.

Alternatively, click **Cancel** to stop creating a new task and return to the Outbreak Management Summary window.

Modifying the OPACL Mode

Be default, devices block the traffic and ports specified in OPACLs. The other option is logging mode, which instructs IPS devices to allow the traffic to pass. Cisco ICS then creates Incident log entries when IPS devices detect traffic matching deployed OPACLs in active outbreak management tasks.

Note The OPACL mode applies to all outbreak management tasks. You can change between modes only when no outbreak management tasks are active.

To modify the OPACL mode, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Global Settings > OPACL Settings**.

Step 2 Choose one of the following:

- **Blocking mode**—Instructs devices to block certain types of traffic and ports and create log entries if blocking occurs.
- **Logging mode**—Instructs IPS devices to create log entries if network packets match the OPACL policy. Note that the devices do not block any traffic.

Step 3 Click **Save**.

Stopping an Outbreak Management Task

If the threat that a task is addressing no longer poses a risk to the network, you can stop the task, which also stops the associated OPACL and Pre-ACL. The advantage of stopping the task before its expiration is that the network can regain use of the traffic and ports the OPACL is blocking.

Note Do not confuse stopping an outbreak management task with stopping an OPACL. For more information, see Stopping an OPACL, page 6-14.

To stop an outbreak management task, follow these steps:

Step 1 Do one of the following:

- Start the Cisco ICS web console.

  The Outbreak Management Summary window appears.
- Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 Do one of the following:

- In the Running Outbreak Management Tasks table, find the task to end and click **Stop**. A confirmation message appears.
- In the Running Outbreak Management Tasks table, do the following:
  a. Click the name of the task. The summary window for that task appears.
  b. Click one of the following:
  - **Stop Running Task**—This appears if the OPACL is not active. Click to stop the task.
  - **Remove OPACL**—This appears if the OPACL is active. Click to stop the task and remove the associated OPACL and Pre-ACL.

  A confirmation message appears.

Step 3 Click **OK**. Cisco ICS notifies you that it ended the task.

Step 4 Click **Back** to return to the Outbreak Management Summary window.

Step 5 Verify that the task no longer appears in the Running Outbreak Management Tasks table.

Stopping an OPACL

If the threat that a task addresses no longer poses a risk to the network, you can stop the OPACL associated with a task without stopping the task itself. Stopping the OPACL also stops the Pre-ACL. The advantage of stopping the OPACL before it expires without stopping the task is that the network can regain use of the traffic and ports that the OPACL is blocking but Cisco ICS can still monitor hosts on the watch list for the task.

If you did not check the Automatically stop the OPACL when Cisco ICS deploys the OPSig to online IPS devices check box for automatic tasks, Cisco ICS does not stop the OPACL. The OPACL continues blocking or logging until it reaches the end time, which is 4 hours by default.

Note Do not confuse stopping an outbreak management task with stopping an OPACL. For more information, see Stopping an Outbreak Management Task, page 6-13.

To stop an OPACL, follow these steps:

Step 1 Do one of the following:

- Start the Cisco ICS web console. The Outbreak Management Summary window appears.
- Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 In the Running Outbreak Management Tasks table, click the name of a task which is using the OPACL that you want to stop. The summary window for the task appears.

Step 3 Next to OPACL mode, click **Stop** A confirmation message appears.

Step 4 Click **OK**. Cisco ICS notifies you that it stopped the task.

Step 5 Click **Back** to return to the summary window for the task.

Step 6 Verify that Stopped appears next to OPACL mode.

Modifying Switch and Router Pre-ACLs

While outbreak management tasks are active, you can modify the Pre-ACL directly if necessary. For more information, see About Outbreak Policy ACLs and Pre-ACLs, page 6-4.

To modify switch and router pre-ACLs, follow these steps:

Step 1 Choose **Devices > Device List**.

Step 2 Click a switch or router in the device list.

Step 3 Click **Configure**.

The configuration window for the device appears, with the **Communications Settings** tab displayed by default.

Step 4 Click the **Interface Settings** tab or the **VLAN Settings** tab for a switch with configured VLANs.

Step 5 Click the link in the Pre-ACL for an interface.

The editing window for that ACL appears. If the Pre-ACL was already configured, the configuration settings appear in the text field.

Step 6 Modify the Pre-ACL as needed. The Pre-ACL must contain a valid Cisco IOS syntax command or series of commands.

Step 7 Click **Save**.

Step 8 Click **Close**.

Step 9 Click **Deploy to Network Devices** to redeploy the Pre-ACL.

Step 10 To view the current ACL that apply ACLs to interfaces, click the link under Current ACL. If outbreak management tasks are active, the current ACL includes the Pre-ACL, the OPACL, and any other ACL already on the device.

Note To modify the VLAN map name for a switch, connect directly to the switch through a console or Telnet connection. You cannot modify the VLAN map name through the web console.

CHAPTER 7

Using Watch Lists

This chapter explains how to use watch lists to monitor potentially infected hosts. It contains the following sections:

- About Watch Lists, page 7-1
- Setting the Monitored the Network, page 7-2
- Viewing the Watch List Window, page 7-3
- Manually Removing Hosts from the Watch List, page 7-4
- Exporting the Watch List, page 7-4

About Watch Lists

A watch list is an at-a-glance summary of potentially infected hosts on the network. Each outbreak management task has an associated watch list for its threat. When an IPS device detects network traffic containing the threat, Cisco ICS automatically puts the host from which the traffic originated on the watch list. Use the watch list to view summary information for these hosts, access host logs, and clean damage on host machines.

This section describes the watch list and contains the following topics:

- Monitoring the Network, page 7-1
- About the Risk Index, page 7-2
- Clearing the Watch List, page 7-2

Monitoring the Network

Before Cisco ICS can add hosts to a watch list, you must specify a portion of the network for Cisco ICS to monitor. Only hosts on the monitored network can be included on the watch list. For more information, see Setting the Monitored the Network, page 7-2.

About the Risk Index

The watch list section of a specific task shows the number of hosts that the threat infected and a risk index, which indicates how many infected hosts are currently on the network. The risk index calculation is as follows:

Risk Index = Infected Hosts - Cleaned Hosts

Clearing the Watch List

Cisco ICS removes hosts from the watch list only after DCS successfully cleans the host and you selected automatic removal on the monitored network window (Damage Cleanup Settings tab). Alternatively, you can manually remove hosts from the Watch List window.

Setting the Monitored the Network

Cisco ICS can automatically add infected hosts to the watch list associated with a specific outbreak management task. However, you must manually add a specific host or range of hosts to the monitored network first. Only hosts on the monitored network can appear on a task-specific watch list.

When you modify the monitored network, the watch lists for active tasks do not reflect the change. Only watch lists for later tasks use the new monitored network settings.

This section describes the monitored network and contains the following topics:

- Including the Entire Network, page 7-2
- Specifying the Monitored Network, page 7-2

Including the Entire Network

By default, the entire network is included on the monitored network. However, after you add a host IP address or range of addresses, Cisco ICS no longer monitors other hosts for inclusion on the watch list. If you clear the monitored network again, Cisco ICS monitors the entire network.

Tip For the most comprehensive watch list inclusion, do not add any hosts to the monitored network. Then Cisco ICS monitors the entire network.

Specifying the Monitored Network

To specify the monitored network, follow these steps:

Step 1 Choose **Outbreak Management** > **Outbreak Settings** > **Monitored Network**.

The Monitored Network window appears, showing the Watch List tab.

Step 2 Click **Add**.

The Add Hosts window appears.

Step 3 Click one of the following:

- **IP address**—Enter a single host IP address and the corresponding mask. The mask determines which IP address bits to include. Cisco ICS uses the exact value of the IP address bits that correspond to the 1 bits in the mask. For example, if you use the IP address 10.10.10.10 with the mask 255.255.0.0, Cisco ICS adds IP addresses 10.10.0.0 to 10.10.255.255.
- **IP range**—Enter a range of IP addresses to add multiple hosts or an entire segment of the network.

Step 4 Click **Save**.

Viewing the Watch List Window

To view the Watch List window, follow these steps:

Step 1 Choose **Outbreak Management** > **Outbreak Management Summary**.

Step 2 Click an active task name.

The summary window for that task appears.

Step 3 Under Watch List, click the link for the number of infected hosts or the number of cleaned hosts. The Watch List window appears, displaying the following:

- Risk Index—The number of hosts still infected or under attack from the associated threat. The risk index calculation is as follows:

  Risk Index = Infected Hosts - Cleaned Hosts.
- Host IP address.
- Hostname.
- Host MAC address.
- Network Device—The device that detected the infected host.
- Interface—The interface that leads to the network where the host is located.
- VLAN—The VLAN of which the host is a member, if any. The word default is displayed if the host is not a member of a VLAN group.
- Cleaned—The status of the hosts. (This item appears only when a DCS server is registered to Cisco ICS.)

Step 4 If too many hosts appear on the watch list, filter the list to display the infected hosts or the cleaned hosts or filter by the network device that detected the infected host.

- Next to Display, select **All hosts**, **Infected hosts,** or **Cleaned hosts** in the first drop-down list.
- From the second list, select **All devices** or any single device name.
- From the third list, select the number of hosts per page.
- Click a heading in the list to sort by that item.

Manually Removing Hosts from the Watch List

After DCS successfully cleans a host, you might not need to keep it on the watch list.

To manually remove hosts from the watch list, follow these steps:

Step 1 Choose **Outbreak Management** > **Outbreak Management Summary**.

Step 2 Click an active task name.

The summary window for that task appears.

Step 3 Under Watch List, click the link that shows the number of infected hosts or cleaned hosts.

The Watch List window appears.

Step 4 Check the check boxes next to the hosts to remove or check the check box at the top to select all hosts.

Step 5 Click **Remove**.

A confirmation message appears.

Step 6 Click **OK**.

Exporting the Watch List

You can export and save the watch list as a .csv file to view in a spreadsheet application.

To export and save the watch list, follow these steps:

Step 1 Choose **Outbreak Management** > **Outbreak Management Summary**.

Step 2 Click an active task name.

The summary window for that task appears.

Step 3 Under Watch List, click the link that shows the number of infected hosts or cleaned hosts.

The Watch List window appears.

Step 4 Click **Export**.

Step 5 Click **Save**.

Step 6 Select a location to save the watch list.

Step 7 Click **Save**.

Using Reports

This chapter explains how to use reports that provide a summary of outbreak management tasks. It contains the following sections:

- About Outbreak Management Reports, page 8-1
- Generating Reports, page 8-2
- Viewing and Deleting Reports, page 8-3

Outbreak Management Reports

This section describes outbreak management reports and contains the following topics:

- About Outbreak Management Reports, page 8-1
- Required Components, page 8-2

About Outbreak Management Reports

You can view reports to review overall outbreak management task settings and performance. A report contains the following information:

- Initiated date/time—The time the task became active.
- OPACL end date/time—The time the OPACL expired. OPACL expiration does not mean that the task is no longer active. For more information, see About Outbreak Management Tasks, page 6-1.
- OPACL mode—Blocking, logging, or stopped. To stop the network device from performing the action specified in the OPACL, click Stop.
- Threat name—The official name of the threat as it appears in the Trend Micro Virus Encyclopedia.
- Alert type—Yellow or red.
- Threat information—A description of the threat and how it attacks computers and networks.
- Risk Index Graph—The risk index, which changes from day to day for the length of the threat.
- Hosts on Watch List Status—The number of infected hosts for each day during the threat.
- OPSig Matching Status—The number of virus incidents for each day during the threat.
- OPACL Matching Status—The number of times a network device detected traffic that matched OPACL settings.

- Accumulated Logged Incidents—The number of times IPS devices detected the threat and the number of times network traffic matched the associated OPACL.
- OPACL Status—The number of active devices (received the OPACL), inactive devices (did not receive the OPACL), and the total number of devices for the associated task.
- Service Component Status—Components, the version deployed, and the version required to address the threat. It also includes the number of components deployed, undeployed, and total number.

Note The reports are in .pdf format. To open the reports, you must have Adobe Acrobat or Acrobat Reader. (See the Adobe Systems website for details on obtaining the appropriate software.)

Required Components

To generate reports, Cisco ICS requires the following:

- Microsoft .NET Framework 1.1
- Microsoft Data Access Component 2.8

If these are not installed on your computer, you can install them from the Cisco ICS CD.

Generating Reports

You must generate reports before you can access them. You can generate reports manually or enable Cisco ICS to generate them automatically, which it does by default every day for active outbreak management tasks.

This section describes how to manually and automatically generate reports. It contains the following topics:

- Manually Generating a Report, page 8-2
- To Automatically Generate a Report, page 8-3

Manually Generating a Report

To manually generate a report, follow these steps:

Step 1 Do one of the following:

- Start the Cisco ICS web console.

  The Outbreak Management Summary window appears.
- Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 In the Active Outbreak Management Tasks table, click the name of the task report to view.

A summary window for that task appears.

Step 3 Click **Generate Report**.

A confirmation window appears.

Step 4 Click **Back** to return to the task summary window.

To Automatically Generate a Report

You can automate the generation of outbreak management task reports so that you can keep up-to-date with outbreak management task performance.

To automatically generate a report, follow these steps:

Step 1 Choose **Outbreak Management > Report Settings** in the Cisco ICS web console.

Step 2 Check the **Automatically generate reports for all outbreak management tasks** check box.

Step 3 From the list, select the frequency in days to generate the report.

Step 4 Click **Save**.

Viewing and Deleting Reports

You can access reports in two ways:

- From the summary window for an individual task—View the latest generated report for the active task.
- From the Outbreak Reports window—View any report generated since Cisco ICS installation. These reports are for both active and inactive tasks.

This section describes how to view and delete reports and contains the following topics:

- Accessing the Latest Report for a Specific Task, page 8-3
- Accessing a Report from the Outbreak Reports Window, page 8-4
- Deleting Reports, page 8-4

Accessing the Latest Report for a Specific Task

To access the report for a specific task, follow these steps:

Step 1 Do one of the following:

- Start the Cisco ICS web console.

  The Outbreak Management Summary window appears.
- Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 In the Active Outbreak Management Tasks table, click the name of the report to view.

A summary window for that task appears.

Step 3 Click **View Latest Report**.

The report opens in another window.

Accessing a Report from the Outbreak Reports Window

To access a report from the Outbreak Reports window, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Reports**.

The Outbreak Reports window contains the following information:

- Task Name—The name of the outbreak management task.
- Status—Active or inactive.
- Task Duration—The period of time during which the task was active.

Step 2 Click the name of the task.

The report opens in another window.

Deleting Reports

To delete reports, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Reports**.

The Outbreak Reports window appears, showing all the reports that Cisco ICS generated.

Step 2 Check the check boxes next to the reports to delete.

Note You can delete a report only when the corresponding task is inactive.

Step 3 Click **Remove**.

A confirmation window appears.

Step 4 Click **OK**.

Configuring Global Settings

This chapter explains how to configure a variety of global settings. It contains the following sections:

- Configuring Notifications, page 9-1
- Managing Syslog Servers, page 9-4
- Setting a Verify Connection Schedule, page 9-5
- Managing Administrator Accounts, page 9-5
- Managing Certificates, page 9-6
- Managing Licenses, page 9-8
- Backing Up the Database, page 9-12

Configuring Notifications

Certain incidents, errors, or events on the network, such as OPACL matching or license expiration, require immediate action. To monitor the incidents and events related to your outbreak protection strategy, configure Cisco ICS notifications. Send messages to the Cisco ICS administrator via email, write entries in the Windows Event log, or do both when certain incidents, errors, or events occur.

This section describes notifications and how to configure them. It contains the following topics:

- Incident and Event Types for Notifications, page 9-1
- Selecting Notifications and Modifying Messages, page 9-2
- Using Token Variables, page 9-3
- Notification Message Example, page 9-4
- Configuring SMTP Settings, page 9-4

Incident and Event Types for Notifications

Check any of the following check boxes to enable notifications for the following:

- Incidents:
  - **OPSig Matches**—An IPS device detected a virus.
  - **OPACL Matches**—A switch, router, or IPS device detects network traffic that matches the configuration settings in its OPACL.

- Errors:
  - **Event Log Errors**—An error severity type for events, such as device communication or authentication errors, the Cisco ICS service stopping for an unknown reason, and database backup attempt unsuccessful. For more information about different types of errors, see About Incidents, Events, and Severity Levels, page 10-2. For more information about resolving errors, see Device Configuration Troubleshooting Tips, page D-8.
- Events:
  - **OPSig Downloaded**
  - **Outbreak Management Task Downloaded**
  - **Outbreak Management Task Started**
  - **Outbreak Management Task Stopped**
  - **Report Generated**
  - **License Expired**—Cisco ICS sends a notification message on the following number of days after expiration: 30, 15, 7, and 1.

Selecting Notifications and Modifying Messages

By default, no notifications are selected. Select the notifications to send and either use the default messages or modify them. For information on displaying details in messages, such as the names of viruses, see Using Token Variables, page 9-3.

Note Cisco ICS saves notifications even if you do not enable them.

To choose notifications and to modify message, follow these steps:

Step 1 Choose **Global Settings** > **Notifications**.

The Events tab appears by default.

Step 2 Check the check boxes next to the incidents or events for which Cisco ICS should send notices.

If you checked **OPSig matches** or **OPACL matches**, specify the following parameters:

- The number of incidents
- The number of minutes during which the incidents occur

If you checked **Event logs**, specify the number of minutes after which Cisco ICS sends a notice after receiving the first error event. Cisco ICS does not continue to send a notice at every interval you specified unless it continues to receive error events from devices.

For example, if you enter 10 minutes, and Cisco ICS receives error events at 1:00 p.m., 1:02 p.m., 1:12 p.m., and 1:30 p.m., Cisco ICS sends a notification at the following times:

- 1:10 p.m.—10 minutes after the first error event, consolidating two errors.
- 1:22 p.m.—10 minutes after the next event that occurs after the last notification.
- 1:40 p.m.—10 minutes after the next event that occurs after the last notification.

Step 3 Click the name of the incident or event to configure the following notification items:

- Mail Notification:
  - **Send email notifications to the following recipients**—Check the check box to enable the notification.
  - To, Subject, Message—Enter the destination email address. If necessary, modify the default subject line and message.
- Windows Event log:
  - **Write to Windows Event Log**—Check the check box to write to the Windows Event log.

Note View Windows Events Log Notifications on the Windows Event Viewer. To access the viewer, choose **Control Panel** > **Administrative Tools** > **Event Viewer** > **Application Log**. See your Windows documentation for details on the Event Viewer.

Step 4 Click **Save**.

Using Token Variables

Notifications for OPACL and OPSig matches can include the following token variables to display important details:

- OPSig matches
  - %VC: number of OPSig matches.
  - %VS: number of computers that Cisco ICS detects as the source of a network virus outbreak when OPSig matching occurs. If an IPS device detects a host as the source of a specific network virus outbreak more than once, Cisco ICS counts the host only once.
  - %VD: number of OPSig matches. If a network traffic from a specific virus matches the OPSig more than once, Cisco ICS counts the match only once.
  - %VI: number of device interfaces detecting the OPSig matches. If an interface detects OPSig matches from a specific virus more than once, Cisco ICS counts the match only once.
- OPACL matches
  - %OC: number of OPACL matches.
  - %OS: number of computers whose source traffic matched OPACL rules. If a computer generates traffic that matches an OPACL more than once, Cisco ICS counts the OPACL match only once.
  - %OD: number of OPACL matches. If a device detects OPACL matches from a specific virus more than once, Cisco ICS counts the match only once.
  - %DC: number of devices detecting traffic that matched OPACL rules. If a device detects OPACL matches from a specific virus more than once, Cisco ICS
  - counts the match only once.
- Event log errors
  - %EC Number of event errors

- Other variables
  - \n: line break
  - \\: a single backslash

Notification Message Example

The following is the default notification message for OPSig matches:

OPSig matched.\n% VC viruses were found in %VI interfaces.\n There were %VS sources of infection and %VD infections.

Configuring SMTP Settings

You can configure SMTP server settings to enable Cisco ICS to send email notices.

To configure SMTP settings, follow these steps:

Step 1 Choose **Global Settings** > **Notifications**.

The Events tab displays by default.

Step 2 Click the **SMTP Server** tab.

Step 3 Enter the SMTP server domain name and the port it uses

The default is port 25.

Step 4 Click **Save**.

Managing Syslog Servers

The Cisco ICS server can send its logs to any Syslog servers on the network. A maximum of eight Syslog servers is allowed.

Note If a Syslog server is installed on the same computer as Cisco ICS, it can have the same IP address as the Cisco ICS server, but it must have a different port number than 514, the default.

To add a Syslog server, follow these steps:

Step 1 Choose **Global Settings** > **Syslog Servers**.

Step 2 Click **Add**.

The Add Syslog Server window appears.

Step 3 Enter the Syslog server IP address and UDP port number

The default is port 514.

Step 4 Click **Save**.

A confirmation message appears.

Step 5 Click **Back** to return to the Syslog Server window.

Step 6 Make sure the Syslog Server Service is active to start receiving log information.

Setting a Verify Connection Schedule

You can set a verification schedule to automate the task of verifying that the Cisco ICS server can communicate with the devices registered to it.

Note You should verify the connection daily, which is the default selection.

To verify the connection schedule, follow these steps:

Step 1 Choose **Global Settings** > **Verify Connection Settings**.

Step 2 Check the **Enable verify connection schedule** check box.

Step 3 Under Verify Connection Schedule, choose one of the following frequency settings:

- **Once**—Verifies connection only after you click **Save**. This is the same as verifying the connection from the Device List window. Select a start time.
- **Every Minute**—Selects a time to verify the connection every { } minutes.
- **Hourly**—Selects a start time in minutes after the hour. For example, if the current time is 5:53 and you select 54, the verify connection begins in 1 minute. If the current time is 5:53 and you select 52, the verify connection begins at 6:52.
- **Daily**—Selects a start time.
- **Weekly, every { }**—Selects a day and start time from the lists.

Step 4 Click **Save**.

Managing Administrator Accounts

This section describes how to create and manage Administrator accounts. It contains the following topics:

- About Administrator Accounts, page 9-6
- Creating a User Account, page 9-6

About Administrator Accounts

You can create administrator accounts to log in to the Cisco ICS web console. Two types of accounts are available:

- Root account—Cisco ICS allows a single root account to manage all other accounts. The root account is created during Cisco ICS installation. You cannot modify or delete the username; however, you can change the password.
- User accounts—Cisco ICS allows a maximum of seven user accounts. Users who log in with a user account can modify the credentials for that account only.

Note The only difference between the root account and the user accounts is the ability to add, delete, or modify user accounts. Owners of user accounts can modify only their own credentials. Both accounts allow full access to Cisco ICS features.

The Administrator Account window displays the following information:

- Username—The name of the root or user account.
- Last Logon Date/Time—The last time this account was used to log into the web console.

Creating a User Account

To create a user account, follow these steps:

Step 1 Start the Cisco ICS web console and log in to it with the root account.

Step 2 Choose **Global Settings** > **Administrator Accounts**.

Step 3 Click **Add**.

The Add Account window appears.

Step 4 Enter the new username and password.

The username must be 1 to 32 alphanumeric characters long, and passwords must be 4 to 32 alphanumeric characters long. The username is not case sensitive. The following characters are not allowed: / \ [ ] " : ; | < > + = , ? ' * !

Step 5 Click **Save**.

A confirmation message appears.

Step 6 Click **Back** to return to the Administrator Accounts window.

Managing Certificates

Digital certificates add security to your network environment. By using device-generated certificates, the Cisco ICS server validates whether it is communicating with the correct network devices to stop the spread of threats. Without certificates, Cisco ICS could not guarantee it is deploying threat-protection components to the correct devices, which increases the chances that you network is being exposed to risks.

This section describes how to use and manage certificates. It contains the following topics:

- Importing Certificates, page 9-7
- Importing Untrusted Device Certificates, page 9-7
- Adding Multiple Devices and Certificates, page 9-7
- Viewing Certificate Details, page 9-8
- Updating Certificates, page 9-8

Importing Certificates

By default, all network devices that Cisco ICS supports generate a digital certificate. Cisco ICS obtains certificate information from the devices when you add them to the device list, but you must import the certificates through the web console. If you do not import a device's certificate, the device appears offline in the device list and you cannot manage it. You can import a certificate at the time you are adding the device, or later from the Device Certificates window.

Importing Untrusted Device Certificates

Untrusted certificates are device certificates that you did not import when you added a device. You cannot manage devices with untrusted certificates. The Untrusted Certificates window allows you to import or delete untrusted certificates and view untrusted certificate details. The following information appears on this screen:

- Fingerprint—The hash value of the encoded certificate.
- Device IP Address—The IP address of the device to which the certificate belongs.
- Device Port—The port on the device to which the certificate belongs.

If you did not import a device's certificate when you added it, Cisco ICS considers the certificate untrusted and the device appears offline in the device list tree. You can import the untrusted certificate at any time to bring the device online.

To import untrusted device certificates, follow these steps:

Step 1 Choose **Global Settings** > **Device Certificates**.

Step 2 Check the check box next to the certificates you want to import.

Step 3 Click **Import**.

Adding Multiple Devices and Certificates

If you are using the tool for adding multiple devices, follow these steps:

Step 1 Run the tool so that Cisco ICS can receive the certificate information.

Step 2 Import the certificates from the Device Certificates window.

Step 3 Run the tool again to finally add the devices to the device list.

For the procedure, see Adding Multiple Devices, page 4-5.

Viewing Certificate Details

You can view the details of each certificate on the Cisco ICS server and verify that they match the certificate details on the devices. When you add a device through the web console, a window displays the device's certificate details. You can establish a telnet, console, or aux connection to the device and use the appropriate command to verify that the certificate on the device is the same as the certificate you are importing.

Updating Certificates

You must update the device certificates on the Cisco ICS server if the certificates on the device change, if you reimage the device's operating system, or if you generate a new certificate on the device. See the documentation for your Cisco devices for more information on certificates.

Managing Licenses

You can view existing licensing information and import a new license through the web console.

This section describes licenses and how to manage them. It contains the following topics:

- About Cisco ICS Server Trial and Full Versions, page 9-8
- About Device Licenses, page 9-9
- Device License Expiration, page 9-10
- Device License Renewal, page 9-10
- Registering for a License File, page 9-11
- Importing a License File, page 9-11
- Viewing License Information, page 9-11

About Cisco ICS Server Trial and Full Versions

The trial version of Cisco ICS allows full product functionality for a limited amount of time. You can upgrade to a full version by obtaining a full version Product Activation Key from Cisco and importing it through the web console. Contact your sales representative for details. Note the following:

- When the trial version expires, Cisco ICS can no longer download components, including OPACLs and OPSigs.
- You cannot upgrade from one trial license to another trial license.
- Full versions never expire.

Note Do not confuse device licenses with the Cisco ICS license. The full version of the Cisco ICS license, which you import during installation, never expires. However, device licenses expire. For more information, see About Device Licenses, page 9-9.

If you installed Cisco ICS with a trial version license and want to upgrade to the full version, you must import the full version license before importing the device licenses.

About Device Licenses

The following types of device licenses are available:

- ACL license—Allows router and switch management, including the ability to create, download, and deploy outbreak management tasks and their associated OPACLs.
- IPS Low-end License—Allows router, switch, and low-end IPS device management, including the ability to create, download, and deploy outbreak management tasks, their associated OPACLs, and OPSigs.
- IPS High-end License—Allows router, switch, and high-end IPS device management, including the ability to create, download, and deploy outbreak management tasks, their associated OPACLs, and OPSigs.

The license file you imported during Cisco ICS server installation give you the right to manage a certain number of network devices. You cannot add more devices to the device list tree than you have licenses for.

Table 9-1 contains important information about each type of device and its required license.

Table 9-1 Device Licenses

Incident Control System Type	Device	License
ACL Incident Control System service (OPACL)	• Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3800, 7200 and 7301 Series routers • Cisco 3550 Series switches • Cisco Catalyst 6500 Series switches • Cisco 7600 Series switches	ACL license (ICS-LIC-ACL-25)

Table 9-1 Device Licenses (continued)

Incident Control System Type	Device	License
IPS Incident Control System service (OPACL + OPSig)	• Cisco 3800 Series integrated services routers • Cisco 7200 Series routers • Cisco IPS 4235 Sensors • Cisco IPS 4240 Sensors • Cisco IPS 4250 Sensors • Cisco IPS 4250 XL Sensors • Cisco IPS 4255 Sensors • Cisco IDSM2 Catalyst Modules • Cisco ASA 5500 adaptive security appliances with AIP-SSM 20	IPS high-end license (ICS-LIC-IPS-HE-1)
	• Cisco IPS-4215 Appliances • Cisco ASA 5500 adaptive security appliances with AIP-SSM 10 • Cisco 800 Series routers, Cisco 1800 Series integrated services routers, Cisco 1700 Series modular access routers, Cisco 2600XM and 3700 Series multiservice access routers • All other Cisco routers	IPS low-end license (ICS-LIC-IPS-LE-5)

Device License Expiration

When a device license expires, you cannot manage the devices that previously used the license. Cisco ICS moves existing devices on the device list to the Expired Device folder and disables the OPACL on those devices. The devices can no longer receive OPACLs or OPSigs.

Note Do not confuse device licenses with the Cisco ICS license. The full version of the Cisco ICS license, which you import during installation, never expires.

Device License Renewal

Contact your Cisco sales representative for information about how to renew device licenses. After renewal, move the devices from the Expired Device folder to other locations in the device directory.

Registering for a License File

When you obtain a new license file from Cisco, save it on the computer on which Cisco ICS is installed and then import it from the Licenses window. If you did not register with Cisco to obtain a license file, you can do so now.

To register for a license file, follow these steps:

Step 1 Choose **Global Settings** > **Licenses**.

Step 2 Click **Import License File**.

Step 3 Click **Registered Users** to register with Cisco if you already have a Cisco.com account, or click **Non-registered Users** if you do not have a Cisco.com account.

Another window opens directing you to the Cisco website.

Step 4 Follow the instructions on the Cisco website to obtain the license file.

Importing a License File

To import a license file, follow these steps:

Step 1 Choose **Global Settings** > **Licenses**.

Step 2 Click **Import License File**.

Step 3 Click **Browse**.

Step 4 Select the license file.

Step 5 Click **Import**.

Viewing License Information

The Licenses window displays summary information for all Cisco ICS licenses, including expired licenses.

To view license information, follow these steps:

Step 1 Choose **Global Settings** > **Licenses**.

The License Summary table displays aggregate information for all active licenses:

- Available ACL Licenses—The number of routers and switches allowed to register with Cisco ICS.
- Available IPS Low-end Licenses—The number of routers, switches, and low-end IPS devices allowed to register with Cisco ICS.
- Available IPS High-end Licenses—The number of routers, switches, and high-end IPS devices allowed to register with Cisco ICS.
- Host ID—The MAC address of the Cisco ICS server.

Note You will receive an email when your license enters its grace period. You can enable Cisco ICS to send a notification message the following number of days after expiration: 30, 15, 7, and 1. For more information, see Configuring Notifications, page 9-1.

Step 2 Choose one of the following from the Display list:

- **All licenses**
- **Active licenses**
- **Expired licenses**

The following information appears in the table:

- License Type—Cisco Incident Control Server, ACL Outbreak Management License, and IPS Outbreak Management License
- Mitigation Devices—The number of licenses available for each license
- Expiration Date
- Version Type—Trial or full version

Backing Up the Database

The Cisco ICS database contains configuration information about managed devices and contains all logs. If the database becomes corrupt, you can restore configuration settings from a backup. For more information, see Restoring Program Settings, page D-1.

You can back up the database manually at any time or configure a schedule for automatic backup. When backing up the database, Cisco ICS helps defragment the database and repairs index file corruption, if any. Cisco ICS preserves seven backups and deletes additional backups starting with the oldest.

Caution Do not back up the database with any other tool or software.

This section describes the database and how to back it up. It contains the following topics:

- Viewing the Last Backup, page 9-12
- Specifying a Backup Location, page 9-13
- Setting a Backup Schedule, page 9-13
- Backing Up Manually, page 9-14

Viewing the Last Backup

Choose **Global Settings > Database Backup**. The Database Backup window shows the following details on the Database tab:

- Start Time—The time the last backup began.
- Finish Time—The time the last backup was completed.

- Path—The location of the backup.
- Result—Whether the backup was successful.

Specifying a Backup Location

You must first decide the location in which to save the backup.

To specify a backup location, follow these steps:

Step 1 Choose **Global Settings** > **Database Backup**.

Step 2 Click the **Settings** tab.

Step 3 Next to Backup Path, modify the default backup path (Program Files\Cisco Systems\CICS\backup) by entering the new path in one of the following formats:

- Windows full path—C:\Cisco_ICS_backup
- Universal Naming Convention (UNC)—\\servername\sharedname\

Step 4 If the backup location is on a remote computer, enter an appropriate account name and corresponding password for write access.

Step 5 Check the **Create the folder if not already present** check box to have Cisco ICS automatically create the folder.

Step 6 Click **Save**.

A confirmation message appears.

Step 7 Click **Back** to return to the Database Backup window.

Setting a Backup Schedule

Tip Configure a schedule for automatic backup. Schedule the backup for nonpeak hours when demand on the server is low.

To set a backup schedule, follow these steps:

Step 1 Choose **Global Settings** > **Database Backup**.

Step 2 Click the **Settings** tab.

Step 3 Check the **Enable scheduled database backup** check box.

Step 4 Click one of the following:

- **Daily**—Back up daily.
- **Weekly, every { }**—Back up weekly. Select a day from the list.
- **Monthly, on day { }**—Back up monthly. Select a day of the month from the list.

Step 5 Regardless of the frequency, select a start time from the lists.

Step 6 Click **Save**.

A confirmation message appears.

Step 7 Click **Back** to return to the Database Backup window.

Backing Up Manually

To back the database manually, follow these steps:

Step 1 Choose **Global Settings** > **Database Backup**.

Step 2 Click the **Settings** tab.

Step 3 Make sure the location in the Backup path is correct.

Step 4 If you made changes, click **Save**.

Step 5 Click **Back**.

Step 6 Click **Back Up**.

Using Logs

This chapter explains how to query and view various Cisco ICS logs. It contains the following sections:

About Cisco ICS Logs

Use the logs to evaluate overall Cisco ICS security strategy. The following events generate log entries:

- System event—Cisco ICS services starts or stops; accounts are added, modified, or deleted; devices or tasks expire; and devices, a DCS server, and OfficeScan servers are added or removed.
- Outbreak event—Outbreak management tasks are created, modified, or stopped; OPACLs are stopped; or reports are generated.
- Server update event—Outbreak management tasks, OPSigs, or DCS components are downloaded either manually or by schedule.
- Deployment event—OPACLs, OPSigs, or DCS components are deployed. This includes redeployment for all components.
- Connection status event—Cisco ICS verifies connection with devices and DCS servers and when a DCS server reports its status.
- Host event—A host cleanup notification is sent or hosts are removed from the watch list.
- OPSig matching—IPS devices detect a virus or other threat.
- OPACL matching—Traffic matches the settings specified in an OPACL.
- Damage cleanup—Hosts are cleaned.

Note To allow Cisco IPS and Cisco IOS IPS devices to send logs to Cisco ICS, you must enable Security Device Event Exchange (SDEE) on the IPS and Cisco IOS IPS devices.

Layer 2 switches do not generate logs. See your switch documentation for information on logs.

Cisco ICS provides a severity level entry to represent how potentially damaging an event or incident was to your network.

About Incidents, Events, and Severity Levels

To organize logs, Cisco ICS classifies everything it detects and all actions it performs as either incidents or events. It also includes a severity level to represent how potentially damaging an incident or event was to your network.

The severity levels are as follows:

- Alert—Very important, might require immediate action.
- Info—Information message only, no action required.
- Error—An error occurred.

  For possible solutions to the errors, see Device Configuration Troubleshooting Tips, page D-8.
- Notice—A normal event that might not require action.

Cisco ICS assigns more than one security level to certain incidents and events. For a classification of events and incidents by severity level, see Appendix C, “Log Severity Levels.”

Incident Logs

You can query incident logs to view details about IPS devices that detect infected hosts and devices that detect network traffic matching an OPACL.

This section describes how to query and view incident logs. It contains the following topics:

- Querying Incident Logs, page 10-2
- Viewing OPSig Matching Incident Logs, page 10-3
- Viewing OPACL Matching Incident Logs, page 10-4
- Viewing Damage Cleanup Incident Logs, page 10-4

Querying Incident Logs

To query incident logs, follow these steps:

Step 1 Choose **Logs** > **Incident Log Query**.

Step 2 Click one of the following types of incidents:

- **OPSig matching**—Generated when IPS devices detect a virus or other threat.
- **OPACL matching**—Generated when traffic matches the settings specified in an OPACL.

- **Damage cleanup**—Generated when DCS cleans a host (visible only if a DCS server is registered to Cisco ICS).

Step 3 Under Time Period, click one of the following:

- Time period list—Select **All dates**, **Last 24 hours**, **Today**, **Last 7 days**, **Last 14 days**, or **Last 30 days**.
- Time range—Click the calendar icon, select a date, and select the time of day in hours and minutes from the lists.

Step 4 Click **Display Logs**.

The OPSig Matching, OPACL Matching, or Damage Cleanup window appears.

Viewing OPSig Matching Incident Logs

After you submit an incident log query for OPSig matching, the results appear in tabular form. The following information appears in the table:

- Results from—The time period you selected for the query.
- Date/Time—The date (dd/mm/yyyy) and time (hh:mm:ss) the event occurred.

Note If you previously restored Cisco ICS program settings from a database backup, the date and time might indicate the date and time of the backup, not the time that the event occurred. The most accurate time period occurs in the title of the table next to **Results from**.

- Severity—An indication of the level of severity. All OPSig matching events are classified as alerts. For more information, see About Incidents, Events, and Severity Levels, page 10-2.
- Event Type—OPSig Matching.
- IPS Log Generation Time—The time that the original log was generated.
- IPS Name—The logical name of the IPS device that detected the threat.
- IPS IP—The IP address of the IPS device that detected the threat.
- Virus Name—The official name of the threat.
- Action—The action the IPS device took against the threat.
- Infection Source—The IP address of the first-infected computer.
- Suspect Host—The IP address of the computer that might be infected and the port number through which the traffic entered the host computer.

To change the log display, do any of the following:

- Use the navigation arrows to scroll through the pages of hosts or enter a page number. Select the number of hosts per page from the list.
- Click one of the headings in the table to sort by that item.

Viewing OPACL Matching Incident Logs

After you submit an incident log query for OPACL matching, the results appear in tabular form. The following information appears in the table:

- Results from—The time period you selected for the query.
- Date/Time—The date (dd/mm/yyyy) and time (hh:mm:ss) the event occurred.

Note If you previously restored Cisco ICS program settings from a database backup, the date and time might indicate the date and time of the backup, not the time that the event occurred. The most accurate time period occurs in the title of the table next to Results from.

- Severity—An indication of the level of severity: Alert, Info, Error, Notice. For more information, see About Incidents, Events, and Severity Levels, page 10-2.
- Event Type—OPACL matching.
- Device Log Generation Time—The time that the original log was generated.
- Device Name—The logical name of the device.
- Device IP—The IP address of the device.
- Action—OPACL mode (blocking or logging).
- Protocol—The protocol of the packet that matched the OPACL (TCP, UDP, or ICMP).
- Source IP—The IP address of the computer from which the traffic originated.
- Destination IP—The IP address of the computer to which the traffic was destined.
- Destination Port—The port number on the computer to which the traffic was destined.
- Packet Number—The total number of packets matching the OPACL.
- ACL/IPS Interface Name—The interface that detected the matching packet.

To change the display, do any of the following:

- Use the navigation arrows to scroll through the pages of hosts or enter a page number. Select the number of hosts per page from the list.
- Click one of the headings in the table to sort by that item.

Viewing Damage Cleanup Incident Logs

After you submit an incident log query for Damage Cleanup, the results appear in tabular form. The following information appears in the table:

- Results from—The time period you selected for the query.
- Date/Time—The date (dd/mm/yyyy) and time (hh:mm:ss) the event occurred.

Note If you previously restored Cisco ICS program settings from a database backup, the date and time might indicate the date and time of the backup, not the time that the event occurred. The most accurate time period occurs in the title of the table next to Results from.

- Severity—An indication of the level of severity: Alert, Info, Error, Notice. For more information, see About Incidents, Events, and Severity Levels, page 10-2.

- Event Type—Damage Cleanup.
- DCS Log Generation Time—The time that the original log was generated.
- DCS Name—The logical name of the DCS server.
- DCS IP—The IP address of the DCS server.
- Virus Name—The name of the threat that was cleaned.
- Infected Host—The hostname of the computer that DCS cleaned.
- Result—The result of the cleaning; one of the following:
  - Virus detected but passed (not cleaned).
  - Virus detected and cleaned.
  - Virus detected but unable to clean.

To change the log display, do any of the following:

- Use the navigation arrows to scroll through the pages of hosts or enter a page number. Select the number of hosts per page from the list.
- Click one of the headings in the table to sort by that item.

Event Logs

Query event logs to view details about the following:

- All events.
- System events, such as the start or stop of the Cisco ICS service.
- Outbreak events, such as the creation of a new outbreak management task.
- Server update events, such as outbreak management task download.
- Deployment events, such as OPACL deployment.
- Connection status events, such as verifying connection.
- Host events, such as removing a host from the watch list.

This section describes how to query and view event logs. It contains the following topics:

- Querying Event Logs, page 10-5
- Viewing Event Logs, page 10-6

Querying Event Logs

To query event logs, follow these steps:

Step 1 Choose **Logs** > **Event Log Query**.

Step 2 Click a type of event.

Step 3 Under Severity, select the level that represents how potentially damaging the event was:

- **All.**
- **Alert**—Very important, might require immediate action.

- **Info**—Information message only, no action required.
- **Error**—An error occurred.

  For possible solutions to the errors, see Device Configuration Troubleshooting Tips, page D-8.
- **Notice**—A normal event that might not require action.

Step 4 Under Time Period, click one of the following:

- Time period list—**All dates**, **Last 24 hours**, **Today**, **Last 7 days**, **Last 14 days**, or **Last 30 days**.
- **Time range**—Click the calendar icon, select a date, and select the time of day in hours and minutes from the lists.

Step 5 Click **Display Logs**.

The Event Log window appears for the selected type of event.

Note If Cisco ICS deploys or removes an OPACL, the following event detail appears: Deployed OPACL update to an individual device for a new or modified task.

Viewing Event Logs

After you query an event log, the results appear in tabular for. The following information appears in the table:

- Results from—The time period you selected for the query.
- Date/Time—The date (dd/mm/yyyy) and time (hh:mm:ss) the event occurred.

Note If you previously restored Cisco ICS program settings from a database backup, the date and time might indicate the date and time of the backup, not the time that the event occurred. The most accurate time period occurs in the title of the table next to Results from.

- Severity—An indication of the level of severity: Alert, Info, Error, Notice.

  For more information, see About Incidents, Events, and Severity Levels, page 10-2.
- Event Type.
- Task Name—The specific name of the task that Cisco ICS performed.
- Event Details—A description of the event.
- Account—The initiator of the event. For an event that Cisco ICS initiates, System-initiated appears. For user-initiated events, the user account name appears.
- Device Logical Name—The logical name of the device that performed the event.
- Device IP—The IP address of the device that performed the event.
- Result—The result of the event. If an error occurred, click the link to go to the Device Configuration Troubleshooting Tips help file.

Note If Cisco ICS deploys or removes an OPACL, the following event detail appears: Deployed OPACL update to an individual device for a new or modified task.

Outbreak Logs

This section describes how to query and view outbreak logs. It contains the following topics:

- Querying Outbreak Logs, page 10-7
- Viewing Outbreak Logs, page 10-7

Querying Outbreak Logs

You can query outbreak logs to view details about a specific outbreak management task.

To query outbreak logs, follow these steps:

Step 1 Choose **Logs** > **Outbreak Log Query**.

The Outbreak Log Query appears showing all outbreak management tasks created.

Step 2 Click a task (only one is allowed).

Step 3 Under View Logs, click one of the following:

- **OPSig matching**—Generated when IPS devices detect a virus or other threat.
- **OPACL matching**—Generated when traffic matches the settings specified in an OPACL.
- **Damage cleanup**—Generated when DCS cleans a host (visible only if a DCS server is registered to Cisco ICS).
- **Task tracking event**—All server update, outbreak, deployment, and host events.

Step 4 Click **Display Logs**.

The Outbreak Log window appears for the selected type of log.

Viewing Outbreak Logs

After you query an outbreak log, the results appear in tabular form. The information for OPSig matching, OPACL matching, and Damage Cleanup outbreak logs is the same as the information for incident logs. For more information, see the following:

- Viewing OPSig Matching Incident Logs, page 10-3.
- Viewing OPACL Matching Incident Logs, page 10-4.
- Viewing Damage Cleanup Incident Logs, page 10-4.

The information for task tracking outbreak events is the same as the information for all event logs. For more information, see Viewing Event Logs, page 10-6.

Viewing Host Logs

Host logs show the following information about hosts in the watch list:

- Results from—The time period you selected for the query
- Date/Time—The date (dd/mm/yyyy) and time (hh:mm:ss) the event occurred

- Severity—An indication of the level of severity: Alert, Info, Error, Notice

  For more information, see About Incidents, Events, and Severity Levels, page 10-2.
- Event Type
- Log Generation Time—The original log generation time
- IPS/DCS Name—The logical name of the IPS device that detected the threat or the DCS server that cleaned the host
- IPS/DCS IP—The IP address of the IPS device that detected the threat or the DCS server that cleaned the host
- Virus Name—The official name of the threat
- Infection Source—The computer first infected
- Suspect Host—The computers the threat infected
- Result

To view host logs, follow these steps:

Step 1 From the menu, choose one of the following:

- **Outbreak Management > Outbreak Management Summary > {Task Name} > Watch List Infected**
- **Outbreak Management > Outbreak Management Summary > {Task Name} > Cleaned Hosts**

Step 2 Click **View Host Logs**.

Exporting Logs

You can export logs to CSV files, which you can open in a spreadsheet program.

To export logs, follow these steps:

Step 1 From any view log window, click **Export to CSV**.

Step 2 Click **Save**.

Step 3 Select a location to save the log.

Step 4 Click **Save**.

Maintaining Logs

Use Log Maintenance to manually delete logs, configure auto deletion, and delete log entries created by specific outbreak management tasks. All tabs on the Log Maintenance window display the following information:

- Log Type
- First Log Entry—The date (dd/mm/yyyy) and time (hh:mm:ss) Cisco ICS made the first log entry

- Most Recent Log Entry—The date (dd/mm/yyyy) and time (hh:mm:ss) Cisco ICS made the most recent log entry

This section describes how to maintain logs and contains the following topics:

- Deleting Logs Manually, page 10-9
- Configuring Auto Deletion, page 10-9
- Deleting Log Entries Created by Specific Outbreak Management Tasks, page 10-10

Deleting Logs Manually

To delete logs manually, follow these steps:

Step 1 Choose **Logs > Log Maintenance**.

The Manual Deletion tab appears by default.

Step 2 Under Delete Logs Older Than, enter the number of days.

Step 3 Click **Delete**.

A confirmation message appears.

Step 4 Click **OK**.

Configuring Auto Deletion

To configure auto deletion, follow these steps:

Step 1 Choose **Logs > Log Maintenance**.

The Manual Deletion tab appears by default.

Step 2 Click the **Auto Deletion** tab.

Step 3 Check the check boxes next to the types of logs to delete or check the check box at the top to select all logs.

Step 4 Under Delete logs Older Than, enter the number of days.

Step 5 Click **Save**.

A confirmation window appears.

Step 6 Click **Back** to return to the Log Maintenance window.

Cisco ICS deletes the selected logs at 2:00 a.m. daily.

Deleting Log Entries Created by Specific Outbreak Management Tasks

To delete log entries created by specific outbreak management tasks, follow these steps:

Step 1 Choose **Logs** > **Log Maintenance**.

The Manual Deletion tab appears by default.

Step 2 Click the **Outbreak Deletion** tab.

Step 3 Find the task whose logs require deletion.

Step 4 Click **Delete**.

A confirmation message appears.

Step 5 Click **OK**.

Damage Cleanup Services

This appendix explains how to use Damage Cleanup Services (DCS) to clean infected hosts. It contains the following sections:

- About Damage Cleanup Services, page A-1
- Registering a DCS Server to a Cisco ICS Server, page A-2
- Specifying DCS Servers and Modifying DCS Settings, page A-2
- Cleaning Infected Hosts, page A-3
- Accessing a DCS Server, page A-4
- Removing a DCS Server, page A-4

About Damage Cleanup Services

Cisco ICS uses Damage Cleanup Services (DCS) to help protect computers against Trojans and to rid hosts of potentially unwanted spyware and other types of grayware.

This section describes Trojans, spyware, grayware, and how DCS deals with them. It contains the following topics:

- Trojans, page A-1
- Grayware and Spyware, page A-2
- The Damage Cleanup Services Solution, page A-2

Trojans

A Trojan is a malicious program that masquerades as a harmless application. Unlike viruses, Trojans do not replicate, but they can be just as destructive. An application that claims to rid computer of viruses when it actually introduces viruses onto a computer is an example of a Trojan. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those that are already running on the system.

Grayware and Spyware

Grayware refers to several types of files and applications that can be covertly installed on computers to track user web-surfing habits, display advertisements, log key strokes, change Internet settings, cause abnormal computer behavior, and even compromise system security. Spyware, the most commonly found type of grayware, monitors user behavior, logs key strokes, and sends the data it collects to another source.

The Damage Cleanup Services Solution

To address the threats and nuisances posed by Trojans and grayware, DCS does the following:

- Detects and removes live Trojans and active grayware applications.
- Kills processes that Trojans and grayware applications create.
- Repairs system files that Trojans and grayware modify.
- Deletes files and applications that Trojans and grayware drop.

To accomplish these tasks, DCS uses these components:

- Damage Cleanup engine—The engine that DCS uses to scan for and remove Trojans and Trojan processes.
- Damage Cleanup template—The file that the Damage Cleanup engine uses to help identify Trojan files and processes to be eliminated.
- Spyware pattern—The file that the Damage Cleanup engine uses to eliminate spyware and other grayware.

Registering a DCS Server to a Cisco ICS Server

The Cisco ICS server to DCS server relationship is a one-to-many relationship. A single Cisco ICS server can register many DCS servers to it, but a single DCS server can be registered to only one Cisco ICS server.

You cannot add DCS servers from the Cisco ICS web console. Before you can use DCS, you must register the Cisco ICS server with a DCS server from the DCS web console. See your DCS documentation for details.

A registered DCS server appears in the AV Software folder in the Directory pane of the device list tree. For more information, see Using the Device List Tree, page 3-3. After successful registration, Cisco ICS creates an event log entry. For more information, see Event Logs, page 10-5.

Specifying DCS Servers and Modifying DCS Settings

If more than one DCS server is registered to Cisco ICS, you can specify hosts to associate with certain DCS servers.

To specify DCS servers and modify the DCS settings, follow these steps:

Step 1 Choose **Outbreak Management** > **Outbreak Settings** > **Monitored Network**.

The Monitored Network window appears showing the Watch List tab.

Step 2 Click the **Damage Cleanup Settings** tab.

Step 3 Click **Add**.

The Add Hosts window appears.

Step 4 Click one of the following:

- **IP address**—Enter a single host IP address and the corresponding mask. The mask determines which IP address bits to include. Cisco ICS uses the exact value of the IP address bits that correspond to the 1 bits in the mask. For example, if you use the IP address 10.10.10.10 with the mask 255.255.0.0, Cisco ICS adds IP addresses 10.10.0.0 to 10.10.255.255.
- **IP range**—Enter a range of IP addresses to add multiple hosts or an entire segment of the network.

Step 5 Click **Save**.

Step 6 From the Associated Damage Cleanup Server list, select the DCS server that will clean the host.

Step 7 To modify DCS settings, check one or both of the following:

- **Automatically clean hosts after Cisco ICS adds them to a watch list**
- **Automatically remove hosts from a watch list after DCS cleans them**

Step 8 Click **Save**.

Cleaning Infected Hosts

On the Watch List window, you can use Damage Cleanup Services (DCS) on infected hosts.

To clean infected hosts, follow these steps:

Step 1 Choose **Outbreak Management > Outbreak Management Summary**.

Step 2 Click the name of an active task.

The summary window for that task appears.

Step 3 Click the link that represents the number of infected or cleaned hosts.

The Watch List window appears.

Step 4 If you are already on the Watch List window and need to confirm that you are viewing infected hosts, choose **Infected hosts** next to Display and click **Go**.

Step 5 Check the check boxes next to the hosts to clean or check the check box at the top to select all hosts.

Step 6 Click **Cleanup**.

Step 7 Verify that DCS successfully cleaned the hosts by confirming that the check mark icon appears under the Cleaned column.

Accessing a DCS Server

If a Damage Cleanup Services server is registered to Cisco ICS, you can access the DCS web console from the Cisco ICS web console. You cannot add DCS servers from the Cisco ICS web console. Before you can use DCS, you must register the Cisco ICS server with a DCS server from the DCS web console. See your DCS documentation for details.

To access a DCS server, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click the **AV Software** folder in the Directory Tree pane.

Step 3 Click the DCS server in the Device List pane.

Step 4 Click **Configure**.

The DCS web console opens.

Removing a DCS Server

You can remove a DCS server from the Cisco ICS web console or unregister the Cisco ICS server from the DCS Management console. See your DCS documentation for instructions. After a successful unregistration, Cisco ICS creates an event log entry. For more information, see Event Logs, page 10-5.

To remove a DCS server, follow these steps:

Step 1 Choose **Devices** > **Device List**.

Step 2 Click the **AV Software** folder in the Directory Tree pane.

Step 3 Click the DCS server in the Device List pane.

Step 4 Click **Delete**.

A confirmation window appears.

Step 5 Click **OK**.

APPENDIX B

Preparing Cisco IOS Routers

This appendix provides procedures for configuring a Cisco IOS router. It contains the following sections:

Preparing Cisco IOS Routers for Use With Cisco ICS as IPS Coverage Devices

The Cisco ICS uses Hypertext Transfer Protocol (HTTP) or HTTPS to communicate with Cisco IOS routers that are set up for Cisco IOS IPS (Intrusion Prevention System) coverage. Set up HTTP or HTTPS on the router with the proper authentication so that Cisco ICS can add the router into its database and deploy an Outbreak Management Task (OMT). An OMT is a Cisco IOS ICS object that ICS uses to track active outbreaks. An OMT will result in an OPACL being deployed to mitigation devices, and it may further be associated with its follow-on OPSig being deployed if and when one becomes available.

Note Cisco ICS manages Cisco IOS IPS coverage devices differently from Cisco IOS Access Control List (ACL) coverage devices. Cisco ICS utilizes HTTP or HTTPS for deploying OPACLs and OPSigs to IPS coverage devices, whereas ACL utilizes Telnet or SSH to deploy OPACLs to ACL coverage devices.

To prepare Cisco IOS routers as IPS coverage devices for use with Cisco ICS, follow these steps:

Note Steps 1 and 2 enable build-in signatures.

Step 1 Define an IPS rule.

```
yourHost(config)# ip ips name myOPS
```

Step 2 Specify the Cisco IOS Signature Definition File (SDF) location with **autosave** enabled to save the OPSig in a file. The file can be on a disk or in flash memory, depending on your router's hardware configuration.

```
yourHost(config)# ip ips sdf location flash:mysig.sdf [autosave]
```

If you specify **autosave**, the router saves new signatures to the specified location so that signatures are not lost after the router is rebooted. It is recommended that you specify **autosave** so that Cisco ICS will not redeploy any OPSigs that were previously running.

The *location* of the SDF can be either of the following:

- sig.sdf
- sig.xml

Note The SDF files can have any names, but they must be in proper xml format.

Step 3 Enable Security Device Event Exchange (SDEE) for event logging. SDEE is the notification protocol that Cisco ICS uses to query Cisco IPS for logging and notification messages.

```
yourHost(config)# ip ips notify SDEE
```

Step 4 To prevent event losses, increase to 1000 the maximum number of SDEE alerts that can be stored.

```
yourHost(config)# ip sdee alerts 1000
```

Step 5 Initialize Cisco IOS IPS by applying an IPS rule to an interface. Cisco IOS compiles the Signature Micro Engines (SMEs) that are the core of the Cisco IOS IPS subsystem; that is, it uses the signatures to build appropriate regular expression tables that are necessary for packet scans. The signature micro engine build times may vary, depending on the platform.

When configuring Cisco IOS IPS with Cisco ICS for the first time, no signatures will exist within flash:mysigs.sdf. Therefore, Cisco IOS IPS reverts to built-in signatures. After Cisco ICS deploys an OPACL and/or an OPSig to the device, the **autosave** parameter causes the flash file to be reinitialized and written to flash memory with the merged content of the built-in signatures and OPACL/OPSigs.

```
yourHost(config)# interface FastEthernet0/1
yourHost(config)# ip ips myOPS in
```

Step 6 Enable the Cisco IOS HTTPS or HTTP server, depending on the communication method configured for those devices on the Cisco ICS server. It is required that you enter **only one** of the following two commands or there may be a security problem.

Note HTTPS and HTTP do not support Authentication, Authorization, and Accounting (AAA). Local users must have a privilege of 15 so that the Cisco ICS server can access the Cisco IOS IPS router.

```
yourHost(config)# ip http server
yourHost(config)# ip http authentication local
yourHost(config)# username yourName privilege 15 password yourPassword
```

Verifying the Cisco IOS IPS Configuration for Use With Cisco ICS

To verify the Cisco IOS IPS configuration, follow these steps:

Step 1 **show ip ips all**

Make sure IPS and SDEE are enabled, and that the IPS rule is applied to interfaces:

```
yourHost(config)# show ip ips all

Configured SDF Locations:
 flash://mysig.sdf autosave
Builtin signatures are enabled but not loaded
Last successful SDF load time: 21:03:07 UTC Jun 20 2005
IPS fail closed is disabled
Fastpath IPS is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 82
Total Inactive Signatures: 0
IPS Rule Configuration
 IPS name myOPS
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is myOPS
  Outgoing IPS rule is not set
```

Step 2 **show ip ips signature | include** *number*

Verify that Outbreak Prevention ACLs (OPACLs), the 50000:0-2 signatures, are visible and ready for use.

In this example, Cisco ICS has not yet deployed an OPACL to Cisco IOS IPS. The OPACLs are visible, however, although Cisco ICS has not enabled or configured them. Cisco IOS IPS includes these signatures as part of Cisco IOS IPS "built-in" signatures.

```
yourHost(config)# show ip ips signature | include 5000

50000:0    N    A   HIGH     0     0     0     0    0   FA   N    OPACL
50000:1    N    A   HIGH     0     0     0     0    0   FA   N    OPACL
50000:2    N    A   HIGH     0     0     0     0    0   FA   N    OPACL
```

After an OPSig has been deployed, you can also use the following command to verify OPSigs.

```
yourHost(config)# show ip ips signature | section MULTI-STRING

SigID:SubID   On   Action   Sev   Trait   MH   AI   CT   TI   AT FA  WF Version
-----------   --   ------   ---   -----   --   --   --   --   -----  ----------
50002:0       Y    ADR      INFO  0       0    0     0    0   FA  N  V1.0
50010:0       Y    ADR      INFO  0       0    0     0    0   FA  N  V1.0
50010:1       Y    ADR      INFO  0       0    0     0    0   FA  N  V1.0
50010:2       Y    ADR      INFO  0       0    0     0    0   FA  N  V1.0
50010:3       Y    ADR      INFO  0       0    0     0    0   FA  N  V1.0
```

Step 3 **show crypto key pubkey-chain rsa**

Verify that Trend Micro's public key has been installed:

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually configured, C - Extracted from certificate
```

```
Code  Usage   IP-Address/VRF   Keyring   Name
M     Signing default realm-trend.pub
```

Step 4 **show ip http server status**

Verify that the HTTP or HTTPS server is enabled:

```
Router# show ip http server status

HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: local
HTTP server access class: 0
HTTP server base path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 86400 seconds
Maximum number of requests allowed on a connection: 10000
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

Preparing Cisco IOS Routers for Use With Cisco ICS as ACL Coverage Devices

Cisco ICS uses SSH or Telnet to communicate with Cisco IOS routers that are set up for ACL coverage. Set up SSH or Telnet on the router with the proper authentication so that Cisco ICS can add the router into its database and deploy to it.

The following SSH steps are required:

- Set up Cisco IOS for SSH access by setting up the host and domain names on Cisco IOS and creating an RSA key for SSH.
- Determine the authentication scheme.
- Verify the Cisco ICS "online" status from the Cisco ICS server.

For detailed information about SSH2, refer to *Cisco IOS Security Configuration Guide*, Release 12.4.

To prepare Cisco IOS routers for use with Cisco ICS as ACL coverage devices, follow these steps:

Step 1 Configure the hostname.

```
Router(config)# hostname yourHost
```

Step 2 Enter the following command:

```
yourHost(config)# ip domain-name yourDomain
```

Step 3 Configure a privilege level 15 user.

```
yourHost(config)# username yourName privilege 15 password yourPassword
```

Step 4 Generate the Rivest, Shamir, and Adelman (RSA) key with a length of 1024 so that the routers support Secure Shell (SSH).

```
yourHost(config)# crypto key generate rsa usage-keys

The name for the keys will be: yourHost.yourDomain
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys ...[OK]
% Generating 1024 bit RSA keys ...[OK]
```

Step 5 Configure VTY to allow Telnet and SSH.

```
yourHost(config)# line vty 0 4
yourHost(config)# login local
yourHost(config)# privilege level 15
yourHost(config)# transport input telnet ssh
```

Verifying the ACL Configuration

To verify the ACL configuration, follow these steps:

Step 1 **show crypto key mypubkey rsa**

Verify that the RSA key was generated:

```
Router# show crypto key mypubkey rsa

% Key pair was generated at: 22:42:55 UTC Jun 16 2005
Key name: yourHost.yourDomain
 Usage: Signature Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A1DECE D6307298
  A92ACD5E B55A1AAF CC5697CA 298A867C 1E6CE7BD F26ED862 0C665DE1 69E30D11
  A25B323C 78E0EBA3 341F7BEF 487B6030 BE5D1EC4 2265BCE8 15020301 0001
% Key pair was generated at: 22:42:55 UTC Jun 16 2005
Key name: yourHost.yourDomain
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00955C87 1A5C7556
  B9F24757 CAE115A8 0C887487 787C4EF1 2EC4AAD7 580E7F02 17A95593 9C68F105
  1C308AE6 5AA4CB78 4A54F1E7 4CD84F0F 74517EA4 894513C1 6D020301 0001
```

Step 2 `show ip access-list`

Verify that Cisco ICS has deployed an OPACL to the router.

The following example shows Cisco IOS output of a deployed OPACL. Cisco ICS is configured to deploy ACLs to the router's FastEthernet1 inbound and outbound. This example does not show an OPACL merged with an existing ACL for the interface because no ACL was previously configured on the interface.

```
yourHost(config)# show ip access-list

ip access-list extended CICS_FastEthernet1_0
 deny tcp any any eq 28435 log time-range CICS-9481d42a
 permit ip any any
ip access-list extended CICS_FastEthernet1_1
 deny tcp any any eq 28435 log time-range CICS-9481d42a
 permit ip any any
!
time-range CICS-b790571a
 absolute end 16:35 07 October 2005
```

ip ips sdf location

To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf location** command in global configuration mode. To remove an SDF location from the configuration, use the **no** form of this command.

ip ips sdf location *url* [**autosave**]

no ip ips sdf location *url* [**autosave**]

Syntax Description

url	Location of the SDF. Available URL options: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml
autosave	(Optional) Specifies that the router will save a new SDF to the specified location.

Defaults

If an SDF location is not specified, the router will load the default built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(4)T	The **autosave** keyword was added.

Usage Guidelines

When you specify the **ip ips sdf location** command, the signatures are not loaded until the router is rebooted or until the Intrusion Prevention System (IPS) is applied to an interface (via the **ip ips** command). If IPS is already applied to an interface, the signatures are not loaded. If IPS cannot load the SDF, an error message is issued and the router uses the built-in IPS signatures.

You can also specify the **copy ips-sdf** command to load an SDF from a specified location. Unlike the **ip ips sdf location** command, the signatures are loaded immediately after the **copy ips-sdf** command is entered.

When you specify the **autosave** keyword, the router saves a new SDF to the specified location when signatures are loaded using either the **copy** command or an external management platform such as Security Device Manager (SDM), IPS Management Center (IPSMC) or Cisco Incident Control Server (Cisco ICS). You can specify multiple autosave locations. The router will attempt to save to all autosave locations. The url must have proper write access permissions.

APPENDIX C

Log Severity Levels

Cisco ICS assigns more than one severity level to certain incidents and events. This appendix classifies the following events and incidents by severity level:

- System Event Severity Levels—Table C-1
- Outbreak Event Severity Levels—Table C-2
- Server Update Severity Levels—Table C-3
- Deployment Event Severity Levels—Table C-4
- Connection Status Event Severity Levels—Table C-5
- Host Event Severity Levels—Table C-6
- Incident Severity Levels—Table C-7

Table C-1 System Event Severity Levels

System Events	Alert	Info	Error	Notice
The Cisco ICS service started.		Info		
The Cisco ICS service stopped.		Info		
The Cisco ICS service stopped for an unknown reason.			Error	
The Cisco ICS administrator added, modified, or deleted an account.				Notice
The Cisco ICS administrator tried to but could not add or modify an account.			Error	
A user added or removed a device.				Notice
The device license expired and all tasks applied to it stopped.				Notice
A DCS server registered to Cisco ICS.				Notice
A DCS server reregistered to Cisco ICS.				Notice
A DCS server was removed.				Notice
A DCS server was manually unregistered from Cisco ICS.				Notice
An OfficeScan server was added.				Notice
An OfficeScan server was removed.				Notice
Manual database backup was completed.				Notice
Manual database backup attempt was unsuccessful.			Error	
Scheduled database backup was completed.				Notice

Table C-1 System Event Severity Levels (continued)

System Events	Alert	Info	Error	Notice
Scheduled database backup attempt was unsuccessful.			Error	
Manual Log Deletion				Notice
Scheduled Log Deletion				Notice

Table C-2 Outbreak Event Severity Levels

Outbreak Events	Alert	Info	Error	Notice
A user created or modified a new outbreak management task.				Notice
A user tried to create or modify a new outbreak management task but could not for an unknown reason, or because the maximum number of tasks (32) was exceeded.			Error	
An outbreak management task stopped.				Notice
An OPACL was stopped manually.				Notice
An OPACL was stopped automatically.				Notice
A user generated a report.				Notice
A user tried to generate a report but could not.			Error	

Table C-3 Server Update Severity Levels

Server Update Events	Alert	Info	Error	Notice
Cisco ICS downloaded a component. For more information, see About Cisco ICS Components, page 1-3.				Notice
Cisco ICS tried to download a component but could not because the component was up-to-date. For more information, see About Cisco ICS Components, page 1-3.				Notice
Cisco ICS tried to download a component but could not because of an error, such as a network connection problem, invalid file type, or HTTP timeout. For more information, see About Cisco ICS Components, page 1-3.			Error	

Table C-4 Deployment Event Severity Levels

Deployment Events	Alert	Info	Error	Notice
Cisco ICS deployed a component. For more information, see About Cisco ICS Components, page 1-3.		Info		

Table C-4 Deployment Event Severity Levels (continued)

Deployment Events	Alert	Info	Error	Notice
Cisco ICS tried to deploy a component but could not because the device was offline. For more information, see About Cisco ICS Components, page 1-3.				Notice
Cisco ICS tried to deploy a component but could not because of an error; for example, the device not was not online, or interfaces or VLANs were not selected. For more information, see About Cisco ICS Components, page 1-3.			Error	

Table C-5 Connection Status Event Severity Levels

Connection Status Events	Alert	Info	Error	Notice
Cisco ICS started or completed a manual or scheduled connection verification to a device.		Info		
Cisco ICS was unable to connect to the device.			Error	
Cisco ICS received a notification that a DCS server started.		Info		
Cisco ICS received a notification that a DCS server stopped.				Notice

Table C-6 Host Event Severity Levels

Host Event	Alert	Info	Error	Notice
Cisco ICS received a host cleanup notification from a DCS server (The cleanup might or might not have been successful.)		Info		
A DCS server cleaned a host and the host was not automatically removed from the watch list.		Info		
A user removed a host from a watch list.		Info		
Cisco ICS removed a host from a watch list automatically after the host was cleaned.		Info		

Table C-7 Incident Severity Levels

Incidents	Alert	Info	Error	Notice
An IPS device detects traffic matching an OPSig.	Alert			
A device detects traffic matching an OPACL.				Notice
The DCS server ran cleanup on a host that was already clean.		Info		
An IPS device detected a virus and the DCS server cleaned the infected host.		Info		
An IPS device detected a virus but the DCS server could not clean the infected host.	Alert			
The DCS server could not access an infected host.			Error	
An IPS device detected a virus but the DCS server took no action.				Notice

APPENDIX D

Troubleshooting and FAQs

This appendix provides solutions to problems you might encounter when using Cisco ICS and answers frequently asked questions. It contains the following sections:

- General Troubleshooting, page D-1
- Device Configuration Troubleshooting Tips, page D-8
- Multiple Device Addition Messages, page D-10
- Malware Tester Utility Messages, page D-15
- Frequently Asked Questions, page D-15

General Troubleshooting

This section provides solutions to general problems you might encounter. For specific problems related to configuring devices, see Device Configuration Troubleshooting Tips, page D-8.

This section contains the following topics:

- Restoring Program Settings, page D-1
- Device Connection Problems, page D-3
- Problems with OPACLs, page D-4
- Problems with OPSigs, page D-5
- Problems with the Web Console, page D-6
- Problems with the Cisco ICS Master Service, page D-7
- Problems with Adding Devices, page D-7
- Problems with Viewing Reports, page D-8

Restoring Program Settings

If you are experiencing problems with your Cisco ICS installation and want to reinstall or if you want to revert to a previous configuration, you can save a copy of the Cisco ICS database and important configuration files to roll back your Cisco ICS program.

To restore program settings, follow these steps:

Step 1 From the web console, back up the Cisco ICS server database to a location outside the Cisco ICS program directory. For more information, see Backing Up the Database, page 9-12.

Caution Do not back up the database with any other tool or software.

Table D-1 shows the files and folders you must manually back up.

Table D-1 Program Files and Folders to Back Up

File or Folder Name	Path	Description
ofcscan.ini	Program Files\Cisco Systems\CICS\PCCSRV	Global configuration settings
CSV folder	Program Files\Cisco Systems\CICS\PCCSRV\Log	Outbreak logs for viewing details related to a specific outbreak management task and the verify connection log
verconn.log	Program Files\Cisco Systems\CICS\PCCSRV\Web\TmOpp	Outbreak management task settings
ActiveAlertPolicy.xml		
CiscoAgent.ini	Program Files\Cisco Systems\CICS\PCCSRV\Private	Global configuration settings
DCS.ini		
Ofcserver.ini		
Backup Database	Copy all files in the backup DB folder to the following: Program Files\Cisco Systems\CICS\PCCSRV\HTTPDB	The Cisco ICS database

Step 2 Uninstall Cisco ICS.

For the precedure, see Uninstalling Cisco ICS, page 2-5.

Step 3 Perform a fresh install.

For the precedure, see Installing Cisco ICS, page 2-2.

Step 4 After installation is complete, stop the Cisco ICS service on the target computer:

a. In the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.

b. Stop **Cisco ICS Master Service**.

Step 5 With the backups you created previously, overwrite the Cisco ICS database and the relevant files and folders in the PCCSRV folder.

Step 6 Restart **Cisco ICS Master Service**.

Device Connection Problems

Table D-2 provides solutions to potential network connection problems between Cisco ICS and devices.

Table D-2 Device Connection Problems

Problem	Potential Solution
Verify Connection from the Device List window is unsuccessful.	Verify the following on the Cisco ICS server: • The device communication settings are correct. • The Cisco ICS server can access the network. • The device certificate is imported and is not untrusted. For the procedure, see Importing Untrusted Device Certificates, page 9-7. Verify the following on the device: • The device is online and operational. • No ACL is preventing communications. Verify the following on the network: • A firewall is not preventing communications between the Cisco ICS server and the device. The default verify connection timeout is 22 seconds. You cannot modify this value from the web console. Cisco ICS verifies connection using the protocol you selected for communication settings (switches and routers use HTTP or HTTPS; IPS devices use Telnet or SSH).

Problems with OPACLs

Table D-3 provides solutions to problems with OPACLs.

Table D-3 Problems with OPACLs

Problem	Potential Solution
Cisco ICS is unable to deploy an OPACL.	Verify the following: • The OPACL is not empty. To view the OPACL, choose **Outbreak Management > Outbreak Management Summary | View/Edit Outbreak Policy** from the menu. For more information, see Modifying Outbreak Management Task Options, page 6-12. If it is empty, connect to the device through a Telnet, console, or aux connection and enter at least one valid ACL command in the OPACL. • No undefined ACL is already applied to the interface or VLAN to which you are trying to apply the OPACL. Connect to the device through a Telnet, console, or aux connection and view the existing ACLs. • The certificate for the device to which you are deploying the OPACL is imported. For more information, see Importing Untrusted Device Certificates, page 9-7.
The OPACL Status column in the device list does not have a green check mark even though the latest OPACL is deployed.	Verify the following: • The deployment event was logged in the Event log. If the result was unsuccessful, the log displays the reason. • All required interfaces were already added through the web console. For the procedures, see Configuring Switches, page 4-12, and Configuring Routers, page 4-14. • The OPACL is not empty. To view the OPACL choose **Outbreak Management > Outbreak Management Summary | View/Edit Outbreak Policy** from the menu. For more information, see Modifying Outbreak Management Task Options, page 6-12. If it is empty, connect to the device through a Telnet, console, or aux connection and enter at least one valid ACL command in the OPACL.

Problems with OPSigs

Table D-4 provides solutions to problems with OPSigs.

Table D-4 Problems with OPSigs

Problem	Potential Solution
OPSig deployment is not successful.	Verify the following on your IPS devices: • The IPS account is not locked. • The IPS service is running. • The certificate for the IPS device to which you are deploying the OPSig is imported. For the procedure, see Importing Untrusted Device Certificates, page 9-7.
Registered Cisco IOS IPS devices cannot receive OPSig files.	IOS IPS devices use the Trend Micro public key to verify the OPSig. Trend Micro may have issued a new public key and this public key has not been deployed to registered IOS IPS devices. Cisco ICS automatically deploys the latest public key to IOS IPS devices. If deployment is not successful, manually deploy the public key. To manually deploy the public key: 1. Get the public key from the Cisco folder on your computer or from the Cisco website. • Open the PublicKey.txt file located in C:\Program Files\Cisco Systems\CICS\PCCSRV\Private\OPSig. OR • Go to http://www.cisco.com/cgi-bin/tablebuild.pl/ics. Type the user name and password you specified when you registered your product. 2. Connect to the Cisco IOS IPS device through a Telnet, console, or aux connection. 3. Enter the following commands and text: **configure terminal** **crypto key pubkey-chain rsa** **named-key realm-trend.pub** **key-string** *(paste the public key here)* **quit** **end**

Problems with the Web Console

Table D-5 provides solutions to problems with the web console.

Table D-5 Problems with the Web Console

Problem	Potential Solution
The root account password is lost or forgotten.	Cisco ICS provides a password recovery utility. To run the password recovery utility, do the following: 1. Open a command prompt on the Cisco ICS server and go to the following folder: Program Files\Cisco Systems\CICS\PCCSRV\Admin\Utility\PasswordRecovery\. 2. Enter **PasswordRecovery.exe** to start the utility. A confirmation message appears. 3. Enter **Y** or **y** to continue. The utility resets the web console password to the following: Cisco123 4. Log in to the web console using the root account username and the reset password. 5. Change the root account password using Cisco123 as the old password For the procedure, see Managing Administrator Accounts, page 9-5.
ActiveX warnings or errors keep appearing when you access the web console.	If you are accessing the web console from a computer running Windows 2003 Server, the default setting blocks ActiveX components. Modify the settings to allow ActiveX components and cookies.
The login window appears with only the Password field. The Username field is missing. The web console does not display any windows.	The web server service or Cisco ICS Master Service is not running. From the Windows Start menu, choose Settings > Control Panel > Administrative Tools > Services. Restart the web server service (IIS or Apache) and Cisco ICS Master Service.
The web console does not load the next page after I click certain buttons or links, such as Save or Delete.	Verify that your web browser allows pop-up messages to appear. Cisco ICS often uses pop-ups to prompt you to perform additional actions. See your Internet Explorer help for instructions on allowing pop-ups.
The web console cannot be accessed.	If a Cisco ICS administrator is logged in to the web console and the computer on which the web server is located loses power, the IIS virtual or default website might not restart automatically. To restart the virtual or default website, do the following: 1. Open a command prompt and enter **mmc**. The Microsoft Management Console opens. 2. Restart **OfficeScan**, which is the name of the website. 3. Verify that Cisco ICS Master Service is running.

Problems with the Cisco ICS Master Service

Table D-6 provides solutions to problems with the Cisco ICS master service.

Table D-6 Problems with the Cisco ICS Master Service

Problem	Potential Solution
Cisco ICS Master Service unexpectedly stopped.	The Cisco ICS service could unexpectedly stop for any of the following reasons: • Web server shutdown—Access the services running on the Cisco ICS server and verify that the web server (Apache or IIS) service is running. • Database corruption—If you have a recent backup of the necessary Cisco ICS folders and files, you can restore your program settings. For the procedures, see Backing Up the Database, page 9-12, and Restoring Program Settings, page D-1.

Problems with Adding Devices

Table D-7 provides solutions to problems with adding devices.

Table D-7 Problems with Adding Devices

Problem	Potential Solution
Devices appear offline in the device list.	A communication or authentication error might have occurred. For more information, see Device Configuration Troubleshooting Tips, page D-8.
Not all devices appear on the device list.	Click Refresh to update the device list. If you are using the tool for adding multiple devices, verify that the device information file is correct. For the procedure, see Adding Multiple Devices, page 4-5.

Problems with Viewing Reports

Table D-8 provides solutions to problems with viewing reports.

Table D-8 Problems with Viewing Reports

Problem	Potential Solution
Reports do not open properly.	Verify that Adobe Acrobat or Acrobat Reader is installed and functioning properly. If the HTTP error **404 file not found** appears in your browser when you open a report, do the following: 1. From the Internet Explorer main menu, choose **Tools** > **Internet Options**. 2. Click the **Advanced** tab. 3. Under Security, uncheck **Do not save encrypted pages to disk**.

Device Configuration Troubleshooting Tips

Table D-9 shows the errors that generate entries in the event log.

Table D-9 Device Configuration Troubleshooting Tips

Cause	Troubleshooting Tip
Communication Errors	
The incorrect IP address was entered when the device was added.	1. Choose **Devices** > **Device List**. 2. Click the device. 3. Click **Configure**. 4. Modify the IP address.
The device is unreachable because of a network connectivity problem.	Make sure Cisco ICS can communicate with the device.
The device certificate has not been imported into Cisco ICS.	If you selected SSH as the communication protocol for a switch or router or HTTPS for an IPS device, you must import the device's certificate. When you add a device, a certificate import window will appear after you click Save & Configure for a router or switch or Save & Verify for an IPS device. If you did not import the certificate when you added the device, choose Global Settings > Device Certificates and import the certificate. You must also reimport a device certificate if you generate a new certificate on the device or reimage the device operating system. For the procedure, see Importing Untrusted Device Certificates, page 9-7.

Table D-9 Device Configuration Troubleshooting Tips (continued)

Cause	Troubleshooting Tip
One of the following: • The selected communication type is not enabled on the device. • SSH (switches and routers only) is configured with an empty username. • The port number is incorrect.	Enable and completely configure the communication type on the device (SSH and/or Telnet for switches and routers and HTTP and/or HTTPS for IPS and Cisco IOS IPS devices). Also verify or modify the device communications port. Save the config file. To verify or modify the selected method of communication saved on the Cisco ICS server, do the following: 1. Choose **Devices** > **Device List**. 2. Click the device. 3. Click **Configure**. 4. Verify or change the selection in the Communication list and the Port list.

Table D-9 Device Configuration Troubleshooting Tips (continued)

Cause	Troubleshooting Tip
Authentication Errors	
The username or password is incorrect.	Verify that the login credentials in the device configuration file are correct. Also verify that the username has level 15 or root view privilege (for switches and routers) or administrator access (for IPS and Cisco IOS/IPS devices). To verify or modify the login credentials saved on the Cisco ICS server, access the web console, do the following: 1. Choose **Devices** > **Device List**. 2. Click the device. 3. Click **Configure**. 4. Verify or change the username or password.
Cisco ICS cannot add the device.	If you are adding a standard Cisco router without a Cisco IOS IPS image, you must select the Cisco router device type. Verify that you selected the correct device type. If you are adding an IPS device, verify that the account is not locked and that the IPS service is running.

Multiple Device Addition Messages

The tool for adding multiple devices displays a series of messages on the command line interface. Any of the messages in Table D-10 can appear. If the message states a problem, try to implement the recommended solution before calling support. For the procedure, see Adding Multiple Devices, page 4-5.

Table D-10 Multiple Device Addition Messages

Message	Description or Recommended Solution
Reading configuration file [{$file_name}]...	The ICS tool is obtaining information from the configuration file BatchAddDev.ini, which contains the Cisco ICS server IP address, and the port number and type of protocol (HTTP or HTTPS) used to access the web console.
Reading device information file [{$file_name}]...	The tool is obtaining information from the device information file you created.
Unable to connect to Cisco ICS. The configuration file parameters are incorrect.	Verify that the IP address, port number, and SSL value in the BatchAddDev.ini are correct. Modify the file if necessary.
Loading device information...	The tool is reading information about the devices.
Loading license information...	The tool is reading information about the available licenses.
{$device_numbers} devices are already registered with Cisco ICS.	The number of devices currently on the device list. To verify that this number is correct, see Using the Device List Window, page 4-3.

Table D-10 Multiple Device Addition Messages (continued)

Message	Description or Recommended Solution
{$license_numbers} ACL licenses and {$license_numbers} IPS licenses are available.	The available licenses. To verify the number of available licenses, see Viewing License Information, page 9-11.
No licenses available.	You do not have enough licenses available to add the devices in the device information file. Verify the number of licenses you have on the License Summary window by choosing Global Settings > Licenses.
Added device [{$Device_name}].	Cisco ICS added the specified device.
Tried to add device [{$Device_name}]. Response: [{$Response}].	The following are the possible responses: • Successful. • Unable to connect to the Cisco ICS database. • Not enough licenses are available to add this device. • The device information is incorrect. • Communication error. • Authentication error. • The IPS device does not authorize addition to Cisco ICS. • The IPS device is not available or not configured. • Cisco ICS is unable to add the device. The device you selected might be incorrect. If adding a standard Cisco router without an IOS IPS image, you must select the Cisco route device type. • Cisco ICS is unable to add the device. Check if the device is a real Cisco IPS device/Cisco IOS IPS. • Unsuccessful. If Cisco ICS cannot add the device, verify the following: • Enough valid device licenses are available. • The devices are online and working properly. • The Cisco ICS server can connect to the devices you are trying to add. • The username and password credentials for each device are correct and belong to an account with administrative privileges. For more information, see Device Configuration Troubleshooting Tips, page D-8.

Table D-10 Multiple Device Addition Messages (continued)

Message	Description or Recommended Solution
Unable to add device [{$Device_name}]. Reason: [{$Reason}].	Any of the following information for the device is invalid: • Protocol type • License number • Logical name • IP address format • Port • Username • PasswordACL setting • Product type • OPACL direction • Protocol type for importing public key • Port range for importing public key Modify the appropriate field in the device information file. For the valid information to specify, see Table D-11 on page D-14.
Skipping the interface [{$Device_name}].	Verify that the interface name is correct using the **show interface** command.
Tried to add interface [{$Interface_name}:{$Interface_Direction}]. Response: [{$Response}]. or Tried to add VLAN [{$VLAN_ID}]. Response: [{Response}].	The following are the possible responses: • Successful. • Unable to use Pre-ACL. • Unable to find this interface or VLAN. • Unable to get interface or VLAN information. • Unable to set the interface or VLAN. • The Pre-ACL commands are invalid. Modify the Pre-ACL information. • Unable to get interface direction. • Invalid interface direction. • An unknown error occurred. If Cisco ICS cannot add the interface or VLAN or use the Pre-ACL, verify the following: • The device, interface, and VLAN details are correct. • The devices are online and working properly. • The Cisco ICS server can connect to the devices you are trying to add. • The Pre-ACL commands are valid. For more information, see Device Configuration Troubleshooting Tips, page D-8.

Table D-10 Multiple Device Addition Messages (continued)

Message	Description or Recommended Solution
Unable to add interface [{$Interface_name}:{$Interface_Direction}]. Reason: [{$Reason}].	Any of the following information for the interface is invalid: • Protocol type • License number • Logical name • IP address format • Port • Username • PasswordACL setting • Product type • OPACL direction • Protocol type for importing public key • Port range for importing public key Modify the appropriate field in the device information file. for the valid information to specify, see Table D-11 on page D-14.
Processing complete.	The tool finished trying to add the devices.
The certificate for this device has not been imported into the Cisco ICS trusted root. You must import the certificate on the Global Settings Device Certificates window and run the add multiple device tool again.	If you are adding a router or switch and you selected SSL for the communication protocol, or if you are adding an IPS device and you selected HTTPS, you must import the device certificate. For more information, see Managing Certificates, page 9-6.
HTTP error, status code: [{$HTTP_error_code}] or HTTP error, status: [{$HTTP_error_description}]	An HTTP error of the specified type occurred. The error code or error description is automatically generated.
Level [{$value}] licenses are insufficient.	You do not have enough licenses available to add the devices in the device information file. Verify that you have the correct number of licenses on the License Summary window by choosing Global Settings > Licenses from the menu.
Unable to open configuration file [{$file_name}].	Verify that BatchAddDev.ini is a valid file and is not locked by another process.
Unable to open device information file [{$file_name}].	Verify that the device information file you created is a valid file and is not locked by another process.
Cisco ICS is not able to add this device. Another device with the same information already exists.	Modify the device information so that it is not the same as an existing device.

A device or interface cannot be added for the following reasons:

Table D-11 Reasons a device or interface cannot be added

Reason	Information to Specify
Invalid protocol type [{$Invalid_parameter_value}].	SSH or TELNET for switches and routers HTTP or HTTPS for IPS devices
Invalid license number.	1 for an ACL license 2 for an IPS license
Invalid logical name [{$Invalid_parameter_value}]. Enter a logical name from 1 to 31 characters. It cannot contain / \ [ ] " : ; | < > + = , ? ' * !	Between 1 and 31 characters for the logical name The following characters are not allowed: / \ [ ] " : ; | < > + = , ? ' * !
Invalid IP address format [{$Invalid_parameter_value}].	A valid IP address
Invalid port [{$Invalid_parameter_value}].	A port number between 1 and 65535
Invalid username [{$Invalid_parameter_value}].	A valid username
Invalid password [{$Invalid_parameter_value}].	The correct password for the username
Invalid ACL setting: [{$Invalid_parameter_value}].	PHYS to apply the OPACL to physical interfaces. Routers must use this option. VLAN to apply the OPACL to VLANs Cisco ICS ignores this field if the device is an IPS appliance or an IOS IPS device.
Invalid product type: [{$Invalid_parameter_value}].	SWT for Switch RTR for Router IPS for IPS appliance or Cisco IOS IPS device
Invalid OPACL direction: [{$Invalid_parameter_value}].	IN or OUT
Invalid protocol type for importing public key [{$Invalid_parameter_value}].	SSH or TELNET
Invalid port range for importing public key [{$Invalid_parameter_value}].	A port number between 1 and 65535

Note If you add multiple switches and routers that have different virtual terminal (VTY) connection username and password requirements, the tool might not add some or all devices. You should add devices that require a username and password in one batch and devices that do not require a username and password in another batch. Mixing the two types of devices can cause a CGI timeout or connection failure error message to appear.

Malware Tester Utility Messages

Table D-12 shows the messages the Malware Tester utility might display on the command line console For more information, see Testing OPACL and OPSig Matching, page 3-8.The messages are Windows Sockets Error Codes. Check the MSDN network for details.

Table D-12 Malware Tester Utility Messages

Message	Description or Recommended Solution
On host serving as the victim: Unable to receive attack packet. err = {variable}	A Windows error code that means that the host serving as the victim did not receive the virus packet from the Malware Tester utility. Try to run the Malware Tester utility again. If the problem persists, make sure that no network problems exist between the two hosts.
On host serving as the victim: Received attack packet.	The host serving as the victim received the virus packet from the host serving as the attacker.
On host serving as the attacker: Unable to send attack packet. err = {variable}	A Windows error code that means that the host serving as the attacker did not send the virus packet from the Malware Tester utility. Try to run the Malware Tester utility again. If the problem persists, make sure that no network problems exist between the two hosts.
On host serving as the attacker: Sent attack packet.	The host serving as the attacker sent the virus packet to the host serving as the victim.

Frequently Asked Questions

This section lists answers to frequently asked questions you might have about Cisco ICS. It contains the following topics:

- Outbreak Management Tasks, page D-16
- Downloading and Deploying, page D-16
- Logs, page D-17
- Reports, page D-17
- Database, page D-17
- Damage Cleanup Services, page D-18

Outbreak Management Tasks

Q. When should I create a manual task?

A. We recommend that you create tasks manually if you are concerned that an existing threat poses a risk to your network. Cisco ICS offers protection from a variety of known threats detected by Trend Micro TrendLabs. The advantage of creating a task manually is that you can guard against a threat that is already in circulation before the time when you enabled automatic tasks.

If you enabled automatic tasks immediately after installing Cisco ICS and you are confident that no threats exist on your network, you do not need to create a manual task.

We recommend that you enable Cisco ICS to automatically create tasks and keep this option enabled. Cisco ICS can deploy outbreak management tasks for newly discovered red and yellow alerts after it downloads the tasks from Trend Micro. The advantage of enabling automatic tasks is that it relieves you of creating tasks manually. You must enable scheduled download for Cisco ICS to periodically poll the update source for new tasks.

Q. When I download an automatic outbreak management task, what am I downloading?

A. The outbreak management task is an XML file that contains OPACLs that address all known threats. When Cisco ICS creates an automatic task for yellow or red alerts or when you manually create a task, Cisco ICS uses this file to create the OPACL necessary to prevent a specific threat from spreading.

Q. What's the difference between stopping a task and stopping the OPACL associated with the task?

A. When you stop a task, the associated OPACL and Pre-ACL also stop automatically and the task disappears from the list of tasks on the web console. If you stop a task, you cannot access the task watch list that Cisco ICS created for that task to monitor potentially infected hosts.

When you stop an OPACL, the task that uses the OPACL keeps running. Only the OPACL and Pre-ACL stop. If you stop the OPACL, you can continue to monitor hosts on the watch list as long as the task is active.

The advantage of stopping a task or its OPACL is that the network can regain use of the traffic and ports the OPACL is blocking. You should stop tasks and OPACLs only when you are sure that the threat that a task and the OPACL are addressing no longer poses a risk to the network.

Downloading and Deploying

Q. Do the default scheduled download and automatic deployment settings provide adequate protection?

A. Yes. The default settings keeps your outbreak prevention up-to-date. By default, Cisco ICS polls the update source every 5 minutes for outbreak management tasks and twice daily for OPSig files and DCS components. Cisco ICS deploys all components under these circumstances:

- After you download an updated component.
- After you add a new device.
- If the status of any device changes to online.

Q. When should I download and deploy components manually?

A. If you are concerned that a threat might put your network at risk, you can download and deploy all components manually instead of waiting for the next scheduled download or the next event to trigger an automatic deployment. You can also create a manual outbreak management task to deploy an OPACL.

We recommend, however, that you always keep scheduled download and automatic deployment enabled to allow Cisco ICS to do the job for you.

Logs

Q. Where does Cisco ICS save the debug log for report generation? When would I need this file?

A. The debug log is at the following location:

\Program Files\Cisco Systems\CICS\PCCSRV\Report\TMreportEx.log

If Cisco ICS is unable to generate logs, Cisco Technical Support might ask you to access this file.

Q. Can I still view Damage Cleanup logs even if I unregistered the DCS servers from the Cisco ICS console?

A. No. You will not be able to query Damage Cleanup logs from the web console if no DCS servers are registered with Cisco ICS.

Reports

Q. Where does Cisco ICS save reports?

A. Reports are at the following location:

\Program Files\Cisco Systems\CICS\PCCSRV\Download\Reports\<ReportID>\

Q. How do I know if a report is generated or still in progress?

A. Open Windows Task Manager and verify that TMreportEX.exe is still running.

Database

Q. What information is in the Cisco ICS database?

A. The database contains configuration information about managed devices and contains all logs.

Q. Why should I back up the Cisco ICS database?

A. If you have a backup of the database, you can restore Cisco ICS settings if required. If you want to reinstall Cisco ICS, or if you need to reinstall because of database corruption, you will be able to use the backup so that you won't lose any settings.

Damage Cleanup Services

Q. Some Damage Cleanup Services features, such as Damage Cleanup logs, are not appearing on the web console. Where are they?

A. You must register Cisco ICS to at least one DCS server for DCS features to appear on the web console.

APPENDIX E

Acronyms

Table E-1 defines the acronyms in this publication.

Table E-1 List of Acronyms

Acronym	Definition
BU	business unit
Cisco ICS	Cisco Incident Control Server
Cisco IOS IPS	Cisco IOS Intrusion Prevention System
CGI	Common Gateway Interface
CPR	controlled pattern release
DCS	Damage Cleanup Services
FTP	File Transfer Protocol
HTML	HypterText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IIS	Internet Information Server
OPACL	Outbreak Prevention access control list
OPP	outbreak prevention policy
OPSig	Outbreak Prevention Signature
SDEE	Security Device Event Exchange
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XML	Extensible Markup Language

GLOSSARY

A

ACL License

Enables router and switch management, including the ability to create, download, and deploy outbreak management tasks and their associated OPACLs.

AV locator

A Cisco ICS feature that enables you to access Trend Micro OfficeScan servers through the Cisco ICS web console.

D

Damage Cleanup engine

The engine that Damage Cleanup Services (DCS) uses to scan for and remove Trojans and Trojan processes and perform cleanup.

Damage Cleanup template

The file that the Damage Cleanup engine uses to help identify Trojan files and processes to be eliminated.

Damage Cleanup Services

A server-based antivirus software application that helps protect computers against Trojans and rid hosts of potentially unwanted spyware and other types of grayware.

I

incident control system (ICS)

The use of attack-specific ACLs and signatures files to help identify network threats and mitigate the effects of outbreaks. With these components, multiple device types and families can become defense nodes against new outbreaks.

Three elements comprise the Cisco implementation of ICS: TrendLabs worldwide real-time monitoring and signature development infrastructure; Cisco Incident Control Server—a product that delivers protection from viruses, worms, spyware, and other potential threats; mitigation network devices—switches, routers, IPS appliances, and IOS IPS devices.

IPS device

A type of device you can add to Cisco ICS through the web console. Cisco ICS classifies an IPS device as an IPS appliance or a router with an IOS IPS image. IPS devices can use OPSig files to scan for and identify network-based threats.

IPS High-end Licenses

Enables router, switch, and high-end IPS device management with the same functionality as a low-end IPS license.

IPS Low-end Licenses

Enables router, switch, and low-end IPS device management, including the ability to create, download, and deploy outbreak management tasks, their associated OPACLs, and OPSigs.

M

Microsoft .Net Framework 1.1 and Data Access Components 2.8
The components Cisco ICS requires to generate outbreak management reports. You can install the components during Cisco ICS installation or at a later time from the product CD.

N

network-based threats
Threats that use network protocols, such as TCP, FTP, UDP, HTTP, and e-mail protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failures.

O

OPACL
Outbreak Prevention Access Control List—An ACL that addresses a variety of threats. An OPACL is associated with an outbreak management task and is included in the outbreak management task file. Cisco ICS deploys the OPACL to switches, routers, and IPS devices. Automatic deployment takes place after outbreak management task creation.

OPSig
Outbreak Prevention Signature—A file that helps IPS devices identify unique patterns of bits and bytes that signal the presence of a network-based threat. Cisco ICS deploys the OPSig to IPS devices.

outbreak management report
An outbreak management task-specific report you can use to review overall outbreak management task settings and performance. Items in the report include the name of the threat that the task is addressing, the OPACL end time, the number of hosts on the watch list, and the number of times network traffic matched the rules specified in the OPACL and OPSig.

outbreak management task
A file that contains an OPACL. Cisco ICS uses outbreak management tasks to help protect the network from various threats. Each task is associated with a single threat.

R

red alert
A TrendLabs designation for a virus, worm, Trojan, or other threat that is widespread and poses a serious risk to computer networks.

risk index
The watch list section of a specific task shows the number of hosts that the threat infected and a Risk Index, which is an indicator of how many infected hosts are on the network. The calculation of the Risk Index is as follows: Risk Index = Infected Hosts - Cleaned Hosts

S

spyware A classification for several types of files and applications that can be covertly installed on computers to track user web surfing habits, display advertisements, log key strokes, change Internet settings, cause abnormal computer behavior, and even compromise system security.

Spyware pattern The file that the Damage Cleanup engine uses to eliminate spyware and other grayware.

T

threats Malicious code that can infect computers, negatively affect the performance of a computer network, and cause other nuisances. Threats include, but are not limited to, ActiveX malicious code, COM and EXE file infectors, spyware, Trojans, and worms.

TrendLabs The global network of antivirus research and product support centers for Trend Micro. TrendLabs monitors worldwide networks for threat outbreaks, analyzes threats, and releases outbreak prevention files that help devices and scan engines detect, block, and eliminate threats.

Trojan Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter. Trojans often use ports to gain access to computers.

V

virus A general term for malicious code that can infect computers and propagate across networks. Currently, viruses can be classified into a number of categories, including network-based threats, Trojans, and worms.

W

watch list An at-a-glance summary of potentially infected hosts on the network. Each outbreak management task has an associated watch list for its threat.

web console A web-based management console which serves as the central point for outbreak management. You can access the Cisco ICS web console at the following address: http(s)://{server}:{port number}/CICS. You must use Internet Explorer to access the Cisco ICS web console.

worm A self-contained program (or set of programs) that can spread functional copies of itself or its segments to other computer systems, often through e-mail.

Y

yellow alert A TrendLabs designation for a virus, worm, Trojan, or other threat that has been detected but is not widespread and poses a moderate risk to computer networks.

INDEX