



---

CyberCop Server

# Installation and Configuration Guide

Version 1.0

## COPYRIGHT

Copyright © 1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

## LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), WHICH SETS FORTH GENERAL LICENSE TERMS FOR NETWORK ASSOCIATES SOFTWARE. FOR THE SPECIFIC TERMS OF YOUR LICENSE, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees and subject to the terms and conditions of this Agreement, Network Associates hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the “Documentation”). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, “smart phone” or other electronic device for which the Software was designed (each, a “Client Device”). If the Software is licensed as a suite or is bundled with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.
    - a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is “in use” on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all proprietary notices.
    - b. **Server Use.** To the extent that the applicable product invoicing or packaging sets forth, you may install and use the Software on a Client Device or as a server (“Server”) within a multi-user or networked environment (“Server Use”) for either (i) connecting, directly or indirectly, to not more than the maximum number of specified Client Devices or “seats”; or (ii) deploying not more than the maximum number of agents (pollers) specified for deployment. If the applicable product invoicing or packaging does not specify a maximum number of Client Devices or pollers, this license gives you a single product use license subject to the provisions of subsection (a) above. A separate license is required for each Client Device or seat that can connect to the Software at any time, regardless of whether such licensed Client Devices or seats are connected to the Software concurrently, or are actually using the Software at any particular time.
-

Your use of software or hardware that reduces the number of Client Devices or seats that connect to and use the Software simultaneously (e.g., using “multiplexing” or “pooling” hardware or software) does not reduce the number of licenses you must have in total. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end.” If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses that you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits set forth in the product invoicing or packaging. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the proprietary notices for the Documentation.

- c. **Volume Use.** If the Software is licensed with volume use terms specified in the applicable product invoicing or packaging, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume use terms specify. This license authorizes you to make or download one copy of the Documentation for each such copy of the Software you may make according to the volume use terms, provided that each such copy contains all of the proprietary notices for the Documentation. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software is installed does not exceed the number of licenses you have obtained.
2. **Term.** This license is effective for the period of time specified in the product invoicing or packaging, or in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of the Agreement set forth here conflict with the provisions of the product invoicing or packaging, the README.1ST document, the LICENSE.TXT document, the product invoice, package, or the other text document will constitute the terms of your license grant to use the Software. Either you or Network Associates may terminate your license earlier than the period specified in the appropriate document in accordance with the terms set forth therein. This Agreement and your license will terminate automatically if you fail to comply with any of the limitations or other requirements described. When this agreement terminates, you must destroy all copies of the Software and Documentation. You may terminate this Agreement at any point by destroying the Software and Documentation together with all copies of the Software and Documentation.
3. **Updates.** During the term of your license, you may download revisions, upgrades, or updates to the Software when Network Associates publishes them via its electronic bulletin board system, website or through other online services.
4. **Ownership Rights.** The Software and the Documentation are protected by United States copyright laws and international treaty provisions. Network Associates owns and retains all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software, or permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not copy the Documentation accompanying the Software. You may not reverse engineer, decompile, or disassemble the Software, except to the extent that the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon the Software in whole or in part. You may not copy the Software except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Network Associates. Network Associates reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

## 6. **Warranty and Disclaimer**

- a. **Limited Warranty.** Network Associates warrants that for thirty (30) days from the date of original purchase or distribution the media (for example, the diskettes) on which the Software is contained will be free from defects in materials and workmanship.
- b. **Customer Remedies.** Network Associates' and its suppliers' entire liability, and your exclusive remedy, shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media on which the Software is contained with a copy on non-defective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent that Network Associates is subject to restrictions under United States export control laws and regulations.

**Warranty Disclaimer.** To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MIGHT NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Your purchase of or payment for the Software may entitle you to additional warranty rights, which Network Associates will specify in the product invoicing or packaging you received with your purchase, or in the README.1ST, LICENSE.TXT or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the product invoice or packaging, the README.1ST, the LICENSE.TXT, or similar documents, the invoice, packaging, or text file will set forth the terms of your warranty rights for the Software.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL NETWORK ASSOCIATES OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL NETWORK ASSOCIATES BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE NETWORK ASSOCIATES CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF NETWORK ASSOCIATES SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.
8. **United States Government.** The Software and accompanying Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.
9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department’s list of Specially Designated Nations or the United States Commerce Department’s Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing provisions and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

IN ADDITION, YOU SHOULD BE AWARE THAT EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SU

RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR ON THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY BUSINESS OR PERSONAL USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST, THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION OF ENCRYPTION TECHNOLOGY TO, OR IMPORTATION FROM: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE THAT IT IS YOUR RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS, AND THAT NETWORK ASSOCIATES HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, “High Risk Activities”). Network Associates expressly disclaims any express or implied warranty of fitness for High Risk Activities.
11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.
12. **Network Associates Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact Network Associates for any other reason, please call (408) 988-3832, fax (408) 970-9727, write Network Associates, Inc. at 3965 Freedom Circle, Santa Clara, California 95054, or visit the Network Associates website at <http://www.nai.com>.

# Table of Contents

|   |           |
|---|-----------|
| <b>Preface</b> .....  | <b>xi</b> |
| About this Manual .....                                     | xi        |
| Related Documentation .....                                 | xi        |
| Navigational Aids Used in This Manual .....                 | xii       |
| Conventions Used in This Manual .....                       | xii       |
| Operating System Information .....                          | xiii      |
| How to Contact Network Associates, Inc. ....                | xiv       |
| Customer Service .....                                      | xiv       |
| Technical Support .....                                     | xiv       |
| Training .....  | xv        |
| <br><b>Chapter 1. Introduction to CyberCop Server</b> ..... | <b>17</b> |
| How to Use CyberCop Server .....                            | 17        |
| CyberCop Server Functionality .....                         | 18        |
| CyberCop Server Security Policy Categories .....            | 18        |
| Administration Stanzas .....                                | 18        |
| Incident Stanzas .....                                      | 19        |
| Responses .....   | 20        |
| Notifications .....   | 20        |
| Security Policy Portability .....                           | 21        |
| Security Policy Distribution .....                          | 22        |
| Default Security Policy .....                               | 22        |
| Security Policy Validation .....                            | 22        |
| CyberCop Server ARMs .....                                  | 23        |
| Fixit ARM .....   | 23        |
| ARM for Cisco PIX Firewall .....                            | 24        |
| Tivoli TME 10 ARM .....                                     | 24        |
| How the CyberCop Server Uses Auditing .....                 | 24        |
| Audit Events .....  | 24        |
| Audit Trails .....  | 25        |
| The Importance of Audit Trails .....                        | 25        |

|   |           |
|---|-----------|
| UNIX Audit Trails .....   | 26        |
| Windows NT Audit Trails .....   | 26        |
| Using the CyberCop Server to Monitor Audit Trails .....               | 27        |
| <b>Chapter 2. Installation Instructions for CyberCop Server .....</b> | <b>29</b> |
| Evaluation Version of CyberCop Server .....                           | 29        |
| Preinstallation Requirements .....                                    | 29        |
| CyberCop Server CD .....  | 29        |
| Hardware requirements .....   | 30        |
| Supported operating systems .....                                     | 30        |
| Privileged access .....   | 30        |
| Installing CyberCop Server for Windows NT .....                       | 30        |
| Installing the CyberCop Server for Solaris .....                      | 32        |
| Installing ARMs After CyberCop Server Installation .....              | 33        |
| Installing ARMs for Windows NT .....                                  | 34        |
| Installing ARMs for Solaris .....                                     | 34        |
| <b>Chapter 3. Configuring the Security Policy .....</b>               | <b>35</b> |
| Security Policy Stanzas .....   | 35        |
| Stanza Format .....   | 36        |
| Creating Your Security Policy .....                                   | 37        |
| UNIX .....  | 37        |
| Windows NT .....  | 38        |
| Configuring Your Security Policy .....                                | 39        |
| Pager Script and SNMP Script .....                                    | 39        |
| Configuring the Pager Script .....                                    | 39        |
| Configuring the SNMP Script .....                                     | 39        |
| BusinessHours Stanza .....  | 40        |
| Defaults Stanza .....   | 41        |
| Agents Stanza .....   | 42        |
| Agents Stanza .....   | 43        |
| Responses in the Incident Stanzas .....                               | 43        |
| Illegal Login Stanza .....  | 44        |
| Illegal Privilege Escalation Stanza (UNIX Only) .....                 | 46        |
| Illegal Jumper Stanza .....   | 48        |



---

|  |           |
|--|-----------|
| Self Defense Stanza .....                                | 50        |
| Illegal File Access Stanza .....                         | 51        |
| Password Rattling Stanza .....                           | 54        |
| System Access Stanza .....                               | 56        |
| System Exploitation Stanza .....                         | 58        |
| System Attack Stanza .....                               | 60        |
| System Probe Stanza (UNIX Only) .....                    | 62        |
| System Misuse Stanza .....                               | 64        |
| User Covering Tracks Stanza .....                        | 66        |
| <b>Appendix A. CyberCop Server Features .....</b>        | <b>69</b> |
| <b>Appendix B. Keywords .....</b>                        | <b>71</b> |
| Keywords .....   | 72        |
| <b>Appendix C. Platform Limitations Per Stanza .....</b> | <b>77</b> |
| Stanzas Per Platform .....                               | 77        |
| <b>Appendix D. Policy Validation Errors .....</b>        | <b>81</b> |
| <b>Glossary .....</b>                                    | <b>85</b> |



# Preface

## About this Manual

This manual documents the features and capabilities of CyberCop Server. It contains the following chapters and appendixes:

- Chapter 1, Introduction to CyberCop Server, describes the features of the product. It describes the CyberCop Server security categories and ARMs, gives an overview of the auditing features of operating systems and how the CyberCop Server can use these features.
- Chapter 2, Installation Instructions for CyberCop Server, provides installation and upgrade instructions for the operating systems supported by the CyberCop Server.
- Chapter 3, Configuring the Security Policy, provides a detailed description of the format of the stanzas in the text-based security policy and how to configure them. It also gives the procedure for how to validate, apply, and enable the security policy for the CyberCop Server.
- Appendix A, CyberCop Server Features, lists the products Security Categories, Responses, and Notifications.
- Appendix B, Keywords, gives a list of the keywords used in the security policy.
- Appendix C, Platform Limitations Per Stanza, lists the signature categories used in the security policy.
- Appendix D, Error Messages, lists the routine and validation error messages and their meanings.
- The Glossary provides terms that are used in conjunction with the CyberCop Server.

## Related Documentation

This guide contains all the information you need to learn and use the CyberCop Server. The following documents are also available:

- Release Notes, which include additions to this guide, changes in this release, known limitations, and bugs
- Installation procedures in HTML and TXT format
- ARM help files in HTML and TXT format

# Navigational Aids Used in This Manual

This manual uses a procedure format, notes, and warning boxes to help you locate important information as explained below:

---

**Procedure format:**

1. Procedures in text are denoted like this.
2. The top line is always followed by a series of steps for accomplishing a particular task.

- 
- **NOTE:** This describes valuable information. Be certain to read it carefully before you proceed.
- 

- 
- I **TIP:** This offers you helpful information for using and applying the product.
- 

- 
- + **WARNING:** Within these lines is information that you must know to avoid damage to files, hardware devices, or personnel.
- 

- 
- E **IMPORTANT:** This message conveys essential information.
- 

# Conventions Used in This Manual

The following describes the conventions used in this manual:

|                        |  |
|------------------------|--|
| <b>Bold</b>            | Menus, fields, options, and buttons are in bold typeface. An example follows:<br><br>Select the <b>Clear</b> option from the <b>Edit</b> menu. |
| <i>Sans-serif font</i> | Pathnames, filenames, icon names, screen text, and special keys on the keyboard are shown in a sans-serif font.                                |
| <b>Keystrokes</b>      | Keystrokes that you enter are shown in bold sans-serif type.   |
| <i>Variables</i>       | Command-line text for which you must supply a value is shown in italic sans-serif type.  |

## Operating System Information

Throughout this guide you will see the name of an operating system in bold with following text that indicates information specific to that operating system:

**SOLARIS:** Indicates that the following information is specific to the Sun Microsystems Solaris operating system only.

**UNIX:** Indicates that the following information is specific to the Solaris variant of the UNIX operating system only.

**WINDOWS NT:** Indicates that the following information is specific to the Microsoft Windows NT operating system only.

# How to Contact Network Associates, Inc.

## Customer Service

To order products or obtain product information, contact the Network Associates Customer Care department.

You can contact Customer Care at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

**Phone** (408) 988-3832

**Fax** (408) 970-9727

Or write to:

Network Associates, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
U.S.A.

## Technical Support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and encryption information.

**World Wide Web** <http://www.nai.com>

Technical Support for your Network Associates product is also available through these channels:

**Phone** (970) 522-2952

**Fax** (408) 970-9727

**Email** [support@nai.com](mailto:support@nai.com)

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name
- Product version
- Computer platform and CPU type
- Amount of available memory (RAM)
- Network operating system and version
- Content of any status or error message displayed on screen, or appearing in a log file (not all products produce log files)

## Training

Network Associates offers a comprehensive set of training courses focused on hands-on network analysis, monitoring, and troubleshooting using Network Associates products. Courses can be conducted at your site, at central locations throughout the globe, or at training centers in Menlo Park and Anaheim, California; Chicago, Illinois; and Atlanta, Georgia. For more information about these courses, contact your sales representative or call Network Associates.





# Introduction to CyberCop Server

# 1

CyberCop Server 1.0 is a host-based intrusion-detection application that detects misuse incidents and responds to them in real time. CyberCop Server first analyzes the operating system's audit trail in real time for misuse incidents, then responds according to the configuration in your security policy. The CyberCop Server text-based security policy is where you define the misuse incidents, as well as the responses and notifications that CyberCop Server will take in the event of a policy violation. When a misuse incident occurs, CyberCop Server detects it, and then reacts with a built-in response based on your security policy configuration or with a response from an active response module (ARM). An *ARM* is an application that allows CyberCop Server to interoperate with another application that you are using on your system.

The text-based security policy can be edited with a standard text editor. For more information, see [Chapter 3, “Configuring the Security Policy.”](#)

This chapter describes the following features of CyberCop Server:

- How to Use CyberCop Server
- CyberCop Server Security Policy Categories
- CyberCop Server ARMs
- How CyberCop Server Uses Auditing

## How to Use CyberCop Server

Install CyberCop Server on any systems that you want to monitor for intrusion or any other kind of suspicious activity, or on any systems that contain important sensitive data. After the installations, configure the security policy to meet your security needs. Validate the policy to make sure there are no errors. Then copy the policy to the Solaris or NT machines on which the CyberCop Server is installed. You can then enable CyberCop Server to apply the policy. Afterward, check to make sure the policy is securing the systems in the way that you intended, and make sure that the policy is configured to suit your needs.

For detailed information on the above procedures, [See “Creating Your Security Policy” on page 37.](#)

## CyberCop Server Functionality

CyberCop Server provides a complete set of notifications and active responses including ARM support. In addition, CyberCop Server can kill processes, terminate logins, and shun (disable) accounts. When used in a UNIX environment, the product also retains audit trail information for analysis. See Appendix A for a complete list of features.

## CyberCop Server Security Policy Categories

The security policy for CyberCop Server is built around administration and incident stanzas. *Stanzas* are lines of arguments that tell CyberCop Server which security categories to monitor, which notifications to send, and to whom to send notifications.

The administration stanzas identify the hours that CyberCop Server monitors the system, and the defaults for users and addresses that receive the notifications.

The incident stanzas identify CyberCop Server's notifications and responses. For detailed information on how to configure the individual stanzas in the security policy, see [Chapter 3, "Configuring the Security Policy."](#)

## Administration Stanzas

The two administration stanzas are at the beginning of the security policy—Business Hours and Defaults.

- **Business Hours.** Used to configure the hours that you want CyberCop Server to monitor your system. You configure the business ("daytime") hours; all other hours are considered nonbusiness ("nighttime") hours.
- **Defaults.** Used to configure some defaults for who receives notifications about CyberCop Server policy violations, and what kinds of notifications they receive. You can configure the following categories:
  - Email address of the person receiving the notifications
  - Report file in which violations can be logged
  - Message prepended to the system log message that will identify the violations
  - Pager script so that someone can be paged when a violation occurs
  - Simple Network Management Protocol (SNMP) script to allow SNMP Traps (an *SNMP Trap* is a message sent from an SNMP agent to advise you that a significant violation has occurred)
  - The duration of shun intervals (that is, the amount of time that will pass whenever a login is shunned; the default value is 15 minutes)

## Incident Stanzas

You configure the incident stanzas to protect your system and its files, and to detect intruders and misuses by using specific keywords for the incident, filter, parameter, and value fields in each stanza.

See Appendix B “Keywords” for tables listing the keywords that are valid for the filter, parameter, and value fields of the stanzas.

The incident stanza list includes the following:

- **Illegal Login.** Used to configure the responses CyberCop Server takes when someone illegally logs into the system. This stanza identifies the users that are allowed to login, and the addresses they are allowed to login from. Reports remote and local logins.
- **Illegal Privilege Escalation (UNIX only).** Used to configure the responses that CyberCop Server takes when a user illegally transitions to root. Illegal Privilege Escalation reports transitions to super user and specifies which users are allowed.
- **Illegal Jumper.** Used to configure the responses taken when a user who has logged in remotely jumps to another system. Illegal Jumpers reports telnets, ftps, and so forth, by remote sessions, and specifies which users are allowed.
- **Self Defense.** Used to configure whether you want to know if the CyberCop Server configuration has been compromised.
- **Illegal File Access.** Used to configure the responses taken when a user illegally modifies files in a given directory. Illegal File Access reports accesses to specified file system objects and specifies which users are allowed access to these objects.
- **Password Rattling.** Used to configure the responses taken when a user attempts to gain access to a machine by trying the password several times. Password Rattling reports multiple failed attempts to log in or to switch to a different user.
- **System Access.** Used to configure the responses taken when a user gains access by password rattling or by using an outside file system mount.
- **System Exploitation.** Used to configure the responses taken when system vulnerabilities are exploited.
- **System Attack.** Used to configure responses taken when attack scenarios, such as a Trojan horse program, are attempted.
- **System Probe (UNIX only).** Used to configure responses to usage of the Security Analysis Tool for Auditing Networks (SATAN) scanner against the machine.
- **User Covering Tracks.** Used to configure responses to a user covering his tracks, such as someone attempting to change the audit userid.

## Responses

CyberCop Server can make the following responses when a violation to your security policy occurs:

- **Kill Process.** Used to configure CyberCop Server to kill the offending process.
  - **Kill Login.** Used to configure CyberCop Server to kill the offending login, that is, CyberCop Server will log the user off the system.
- 
- **NOTE:** For more complete protection, use Kill Login with Disable Login.
- 
- **Disable Login.** Used to configure CyberCop Server to disable the offending user's ability to log in again.
- 
- **NOTE:** Choose either Disable Login or Shun Login in a particular incident stanza. Do not use them together.
- 
- **Shun Login.** Used to configure CyberCop Server to disable the offending user from executing a login for a period of time. An incident specific shun interval can be supplied for each particular incident stanza, otherwise the default shun response is used from the Defaults stanza.

## Notifications

CyberCop Server can send the following notifications when a violation to your security policy occurs:

- **SNMP Trap.** Sends an SNMP trap to your SNMP console. For instructions to configure the SNMP Trap script, [See “Configuring the SNMP Script” on page 39.](#)
- **Pager.** Pages the administrator by calling a pager script. For instructions to configure the pager script, [See “Configuring the Pager Script” on page 39.](#)
- **Syslog.** Used to configure CyberCop Server to log incidents to the system log. Messages are prepended with the default system log message. As an alternative, you can specify the syslog text as an argument to Syslog.
- **Email.** Used to configure CyberCop Server to send an email message to whomever you specify in the security policy. The default email address is used unless you specify an incident-specific email address as an argument to email.
- **Report File.** Used to configure CyberCop Server to log incidents to a report file. The default report file is used unless you specify an incident-specific report file name as an argument to ReportFile. The report file is found in the <CyberCop Server Home Directory>/report directory on both UNIX and Windows NT.

- **Popup Message.** Used to configure CyberCop Server to send popup messages to the desktop on which CyberCop Server is installed whenever a violation to the security policy occurs.

**UNIX:** If no one is logged in, the popup message is not displayed.

**WINDOWS NT:** If no one is logged in, the popup message is queued until someone logs in.

## Security Policy Portability

The configuration policy can be ported to other systems; however, be aware of the following situations:

- Users specified in the security policy, but which are not valid for the system, are ignored. Unknown user names produce an error message, but the incident group with which they are associated is still applied.
- Files names specified in the policy, but which do not exist on the system, are ignored. Unknown file names produce an error message and the incident group with which they are associated is ignored.
- Invalid values in the response section of the stanza do not invalidate the other responses in the stanza.

To increase the portability of the security policy across systems, use the following variables when configuring your security policy:

- *\$administrator*. The default administration account as defined in **.email-target**. If email-target does not exist, root is used under UNIX and the administration account is used under Windows NT.
- *\$hostname*. The hostname of the system.
- *\$windir*. Under Windows NT, the directory in which the operating system is located. This is typically C:\winnt. This variable is ignored under UNIX.
- *\$cybercopserverdir*. This variable contains the full installation directory path to the CyberCop Server installation.
- *\$systemdrive*. Under Windows NT, this variable is the drive letter and colon that identify where the operating system is installed. This is typically C: or D:. This variable is ignored under UNIX.

---

+ **WARNING:** While it is likely that a carefully-constructed security policy will be usable on different UNIX platforms, there will be some limitations. Security policies are not interchangeable between UNIX and Windows NT.

---

## Security Policy Distribution

There is no automatic distribution mechanism for security policies in this release. Each security policy must be copied to the CyberCop Server system manually to <CyberCop Server Home Directory>/tmp/security.txt (UNIX and Windows NT). Notify CyberCop Server to apply the new security policy with the commands listed below.

**UNIX:** Type in the following command: **cybercopserver config**

**WINDOWS NT:** Restart CyberCop Server from the program group by going to **Start-->Programs-->CyberCop Server-->Restart CyberCop Server.**

## Default Security Policy

A default security policy is available to be used immediately. This security policy contains a basic set of widely-applicable security incidents. The default security policy does not contain any active responses, and provides notification only via email.

- 
- **NOTE:** We recommend that you customize this security policy before applying it. For detailed information on customizing the security policy, see [Chapter 3, “Configuring the Security Policy.”](#)
- 

## Security Policy Validation

You can check the correctness of a security policy on an intended system by copying the security policy to the system and using the following command from the command line:

```
cybercopserver validate <full path to your new policy file>
```

This command causes the security policy to be checked on the system for any inconsistencies in user names, file names, and licensing options. Errors are reported on the command line only. If validation errors occur when the security policy is applied, messages will be mailed to the default administrator address.

---

**NOTE:** It is recommended that you always check your security policies using the validation command before you apply them.

---

## CyberCop Server ARMs

CyberCop Server includes ARMs that allow the CyberCop Server to interact with third-party software. This add-on software integrates the notification and response features of third-party software with the security features of the CyberCop Server, thus adding another layer of security. The ARMs Kit allows you to create response modules for any third-party applications that you might want to interoperate with the CyberCop Server. See the CyberCop Server ARM Developer's Guide for more information.

- 
- **NOTE:** The CyberCop Server ARM Development Kit is not included with this release. Check the Network Associates Web page ([www.nai.com](http://www.nai.com)) for availability of the CyberCop Server ARM Development Kit and the CyberCop Server ARM Development Kit guide.)
- 

Three ARMs are available for installation on the CyberCop Server CD: the Fixit ARM, the ARM for the Cisco PIX Firewall, and the Tivoli TME 10 ARM. These ARMs can be installed as part of the CyberCop Server installation or added later. See the section titled [See “Installing ARMs After CyberCop Server Installation” on page 33](#) for instructions.

For detailed information on how to configure the ARMs stanzas in your security policy, [See “Configuring Your Security Policy” on page 39](#). If you have not already installed the ARMs, see the ARM help files (in HTML or TXT format) available on the CyberCop CD for more information.

Check the Network Associates Web page (<http://www.nai.com>) periodically for new ARMS.

## Fixit ARM

The Fixit ARM allows the CyberCop Server to manage protected files that have been illegally modified or created by using the following file protection responses:

- **Move corrupt files.** When a user violates the security policy by creating or modifying a protected file in a protected directory, the Fixit ARM copies the illegal version of the file into a protected area for later analysis. This file can be used as evidence against malicious users.
- **Restore files.** Files that should not be changed can be kept in the Fixit cache. The files can be automatically restored from the cache when a security violation to a protected file occurs.
- **Delete bad files.** When a user causes an incident by creating a new file in a monitored directory, the new file can be automatically deleted by the Fixit ARM. See the help file ([fixit.html](#) or [fixit.txt](#)) in the **arm/fixit** directory for details on how to cache files for the Fixit ARM to use.

## ARM for Cisco PIX Firewall

The ARM for the PIX firewall allows the CyberCop Server to reconfigure the Cisco Private Internet Exchange (PIX) firewall when a violation to your security policy occurs. In the CyberCop Server security policy, the ARM can be configured to tell the PIX firewall to either block or shun an outside IP address.

The PIX firewall keeps intruders out of the internal network while allowing regulated conduit access through the firewall for such services as email, telnet, ftp, SNMP, and World Wide Web use. The PIX Firewall ARM adds further protection by telling the firewall to deny access to an IP address that has violated the CyberCop Server's security policy. The firewall conduit normally allows all IP addresses in, but the ARM enables the firewall to block out a specific IP address. Once an incident is associated with a certain IP address, the information to block or shun that IP address is sent to the firewall via the ARM.

See the help file (**pix.html** or **pix.txt**) in the **arm/pix** directory for details on how to configure the Cisco PIX Firewall ARM.

## Tivoli TME 10 ARM

The Tivoli ARM allows the CyberCop Server to notify the Tivoli TME 10 Framework when a violation to your security policy occurs. The CyberCop Server sends notices via the ARM to Tivoli TEC, to the Notice Board, or to the Management Console when violations to any of the CyberCop Server's security categories occur (if you have them configured to use the TME ARM as a response).

See the help file (**tme.html** or **tme.txt**) in the **arm/tme** directory for details on how to configure the Tivoli TME 10 ARM.

## How the CyberCop Server Uses Auditing

The UNIX and Windows NT operating systems have built-in mechanisms to track and record administrative and system events. As this information is collected, it is written to the audit trail files on UNIX systems or to the security event log in Windows NT. The CyberCop Server's daemon (UNIX) or service (Windows NT) reads the audit trail files in real time, analyzing the data for security policy violations.

This system of collecting and sorting information can be used to form a powerful detection and response system.

## Audit Events

In most operating systems, the system calls record audit events such as failed login attempts or opened files. Most operating systems categorize audit events into a small number of broad classes, each containing related event types.



**UNIX:** The operating system collects audit event information and writes it to the audit trail files. The CyberCop Server's daemon searches the data in real time for violations to the security policy.

**WINDOWS NT:** The operating system records events in the security event log. Auditing can be manually enabled from the Audit Policy dialog of User Manager. However, the CyberCop Server automatically turns on auditing when the CyberCop Server's service is enabled. Both system-wide events and object access can be audited under Windows NT.

## Audit Trails

Audit events are individual records of activities performed by the operating system kernel by means of system calls. An audit trail is a set of those events. These records are preserved as an inventory of user logon, subsequent activities, and resource utilization. The CyberCop Server analyzes the output of this information collection system by comparing userids and session processes against the users and uses allowed by your security policy.

The CyberCop Server's analysis results can then be routed automatically to email, reports, and responses.

## The Importance of Audit Trails

Audit trails provide a very rich source of information about all system activities. They can tell you who is on your system and what is being done, down to the most minute details of file openings, modifications, and deletions. This information is very useful to track authorized and unauthorized user logins, as well as to pinpoint possible damage to your valuable data assets.

You can also look for illegal connections from machines outside your network, since the audit trails typically contain the IP address from which logins originate. Then you can track down from where users logged in and which processes they initiated. These facts can help you determine if intruders have entered your system, where they came from, and what mischief they may have done.

Audit trails also tell you the outcome of individual audit events, such as if a login was successful or if a file write failed. These events provide clues to help track intruders who may have replaced mission-critical applications with malicious programs. Manual inspection of raw audit trail records is very time-consuming, but considered worthwhile when serious security violations are suspected.

Audit trails for both the UNIX and Windows NT operating systems provide user accountability by associating activities on the system with the individuals and their userids.

## UNIX Audit Trails

Audit events are created in the UNIX kernel through invocation of system calls such as audit, audit svc, auditlog, and auditwrite. A typical UNIX audit event record contains standard audit information such as time stamp, event type, userid, and processid. Raw audit trail data generated by the operating system is often difficult to interpret, since events are appended to the audit file as they occur (Figure 1-1). The events are not ordered by userid or processid, so many varied activities are recorded in the file.

```
15:45:57.99960500:13:09:96,6159,P7,s(0:0),1021:1021:0,10:10,S280,-1,,success for user
jsmith
15:51:01.949961000:13:09:96,6155,P43,s(0:0),1021:1021:1021,10:10,S43,-1,(pts/10:n:"000
0,-1,-1":0:c6332e67:-1:0:0),successful login
15:51:13.69955500:13:09:96,6155,P69,s(0:0),2003:2003:2003,10:10,S69,-1,(pts/10:n:"0000
,-1,-1":0:c6332e67:-1:0:0),successful login
15:51:23.359957500:13:09:96,6,P90,s(0:0),2003:2003:2003,10:10,S69,-1,(/opt/nai-ccsvr/t
mp/CCSERVER2.ndx:f:"0666,0,10":0:0:0:357252:8388631)
15:51:23.759960500:13:09:96,6,P90,s(0:0),2003:2003:2003,10:10,S69,-1,(/opt/nai-ccsvr/t
mp/ccserver.exe:f:"0666,0,10":0:0:0:357251:8388631)
15:51:28.989959500:13:09:96,23,P102,s(0:0),2003:2003:2003,10:10,S69,-1,(/usr/bin/ftp:f
:"0555,2,2":0:0:0:3385:8388622),ftp,host 1
15:52:04.669960500:13:09:96,4,P114,s(0:3),2003:2003:2003,10:10,S69,-1,(/opt/nai-ccsvr/
tmp/CCSERVER2.ndx:f:"0666,2003,10":0:0:0:357251:8388631)
15:52:07.439958500:13:09:96,4,P122,s(0:3),2003:2003:2003,10:10,S69,-1,(/opt/nai-ccsvr/
tmp/ccserver.exe:f:"0666,2003,10":0:0:0:357252:8388631)
15:52:09.529960000:13:09:96,23,P129,f(13:1),2003:2003:2003,10:10,S69,-1,(/opt/nai-ccsv
r/tmp/ccserver.exe:f:"0666,2003,10":0:0:0:357252:8388631)
```

**Figure 1-1. Sample Audit Trail Data**

## Windows NT Audit Trails

Event Viewer is the Windows NT tool used to monitor events on a system. There are three types of event logs: system, security, and application. As events such as logon, logoff, policy change, privilege use, system event, object access, detailed tracking, and account management occur, they are logged into the Event Viewer.

The format and contents of the Windows NT audit event records are based on the design of Event Viewer, which uses information from the Registry to locate message files and present the audit records. Event Viewer looks for event source modules from each installed application that generates audit event records. The event source module adds audit event records to the security log information in the Registry.

A typical Windows NT audit event record contains standard audit information such as date, time, source, category, event, user, and computer.

Details about the event are found in the Event Detail window of the Event Viewer. Figure 1-2 shows a sample Event Detail window.



Figure 1-2. Windows NT Event Detail

## Using the CyberCop Server to Monitor Audit Trails

Without tools to interpret the valuable information in audit trails, the key facts are often obscured by the sheer volume of audit data. The CyberCop Server uses audit trails created by the operating system as its data source for detecting system misuse. Using patented technology, the CyberCop Server analyzes the audit trails for:

- User activities
- Resource utilization
- Attacks and misuse

The system administrator receives email or a report when misuse is detected, and then can respond immediately to protect the system. The CyberCop Server reports show the security incident that was detected, and the who, what, when, and where of the intrusion that occurred.

# Installation Instructions for CyberCop Server

## 2

This chapter describes how to install the CyberCop Server on the following operating systems:

- Windows NT 4.0 with Service Pack 3
- Sun Microsystems Solaris 2.5 or later

## Evaluation Version of CyberCop Server

If you have an evaluation version of the CyberCop Server CD, you can install a copy of the Cybercop Server on each system that you want to monitor. The installation expires at the end of the evaluation period.

If you experience problems installing the evaluation version of the CyberCop Server, see the Network Associates Web site (<http://www.nai.com>) for more information.

To find out if you have an evaluation or permanent version of the CyberCop Server, run `cybercopserver version` at the command line; this command returns version information. See Figure 2-1 for the Windows NT example.

**Figure 2-1. Windows NT Version Example**

CyberCop Server Version 1.0 (August 31, 1998)

Copyright (c) 1998 Network Associates, Inc.

All rights reserved.

## Preinstallation Requirements

### CyberCop Server CD

Both the evaluation and permanent versions of the CD contain all the required software for all supported operating systems. The evaluation version can be installed one time on each system, and expires at the end of the evaluation period.

- 
- **NOTE:** Contact your sales representative for information about upgrading to new versions of the CyberCop Server.
-

## Hardware requirements

- 50 MB of available hard-disk space
  - 32 MB of memory
  - Local drive for installation
- 
- NOTE: The CyberCop Server must be installed on a local disk, not a drive mounted on NFS™ or another sharing scheme.
- 

## Supported operating systems

- Windows NT 4.0 with Service Pack 3
  - Solaris 2.5 or later
- 
- NOTE: Under UNIX, if you are running Network Information Service (NIS or NIS+), the CyberCop Server must be able to query NIS for userids and groupids.
- 

## Privileged access

The CyberCop Server must be installed by root or administrator, because the executable must be able to access protected configuration and audit trail data files

## Installing CyberCop Server for Windows NT

The CyberCop Server takes control over management of the Windows NT audit event log.

- 
- NOTE: Before you install a permanent version of CyberCop Server on a system, you must uninstall any existing evaluation versions that reside on that system.
- 

- 
- + WARNING: Do not install the CyberCop Server on a FAT drive, a remotely shared disk, or a mapped drive of your Windows NT system. The CyberCop Server must be installed on a local NTFS partition. If content files are placed on a FAT drive, a remotely shared disk, or a mapped drive, the CyberCop Server is unable to detect or respond to changes made to these files.
- 

1. Log in as the Administrator or as a member of the Administrator's group.
2. Insert the CyberCop Server CD into the CD-ROM drive.

The Welcome screen appears.

3. Read the Software License Agreement.  
If you accept the terms of the agreement, click Yes and continue the installation.
  4. Type in your name and company name.
  5. Select the destination directory for the CyberCop Server program files. The default is as follows:  
**C:\Program Files\Network Associates\CyberCop Server**
- 
- NOTE: The destination directory should be on a local NTFS drive, not a network drive.
- 
6. Type in the SMTP Gateway. This entry is required if you want to be notified of security incidents by email.
- 
- NOTE: Contact your system administrator for assistance if you do not know the SMTP Gateway. Use a fully qualified domain name or an IP address for the SMTP gateway.
- 
7. Type in the email address of the security policy administrator.  
The security policy administrator will receive email whenever the CyberCop Server detects errors while validating the security policy.
  8. Click yes to install the socket replacement libraries.
- 
- NOTE: The mssock.dll and ws2\_32.dll must be replaced by the DLLs so that network connections are more completely reported.
- 
9. Choose the ARMs you want to install by clicking the check boxes.  
The following ARMs are available (see [Chapter 1, “Introduction to CyberCop Server](#) for more information):
    - Fixit ARM
    - ARM for Cisco PIX Firewall
    - Tivoli TME 10 ARM
  10. To install the CyberCop Server’s SNMP option, click the check box.
  11. Select the CyberCop Server’s Program Folder. The default is “**CyberCop Server.**”
  12. Click Next for setup to copy the CyberCop Server files from the CD.
  13. If you chose the SNMP server option in step 9, restart the SNMP server when prompted.
  14. Setup is complete. If you chose the socket replacement libraries in step 7, you will be asked to reboot your system for the configuration changes to take effect.

You are now ready to configure your security policy. See [Chapter 3, “Configuring the Security Policy,”](#) for detailed information on how to configure, validate, and apply your security policy.

## Installing the CyberCop Server for Solaris

You must have root access and the root password to install the CyberCop Server:

- 
- **NOTE:** Before you install a permanent version of CyberCop Server on a system, you must uninstall any existing evaluation versions that reside on that system.
- 

1. Insert the CyberCop Server CD into the CD-ROM drive.
2. Log in as root and type in the password.
3. To add the CyberCop Server, type in the following:  
`/usr/sbin/pkgadd -d /cdrom/cybercopserver/solaris`
4. Choose the CyberCop Server from the list of packages to add.
5. Type in the path to the installation directory:  
**EXAMPLE:** `/opt /<????>`
6. Answer `y` to continue with the installation.
7. **Type `q` to quit after the files have been copied.**
8. Run the CyberCop Server installation script.
  - a. Change to the CyberCop Server installation directory if you are not already there:  
`cd ./<CyberCop Server directory>`
  - b. Run the installation script to install the CyberCop Server:  
`./INSTALL`
9. Answer `y` if you accept the terms of the software license agreement.
10. Answer `y` if you want to install any ARMs.

The following ARMs are available (see [Chapter 1, “Introduction to CyberCop Server”](#) for more information):

  - Fixit ARM
  - ARM for Cisco PIX Firewall
  - Tivoli TME 10 ARM
11. Type in the email address of the security policy administrator.

The security policy administrator will receive email whenever the CyberCop Server detects errors while validating the security policy.
12. Reboot the system to start the CyberCop Server.



- NOTE: The CyberCop Server will load with the default policy (security.txt) in the ./tmp directory.
- 

You are now ready to configure your security policy. See [Chapter 3, “Configuring the Security Policy,”](#) for detailed information on how to configure, validate, and apply your security policy.

## Installing ARMs After CyberCop Server Installation

If you chose not to install the ARMs during CyberCop Server installation, you can install them later by following the procedure below. Each ARM has to be installed separately. Three ARMs are available for the CyberCop Server:

- Fixit ARM
- ARM for Cisco Pix Firewall
- Tivoli TME 10 ARM

See [“Agents Stanza” on page 42](#) and [“Agents Stanza” on page 43](#) in [Chapter 3](#) for more information on configuring the ARMS available for the CyberCop Server. Help files for each ARM are available on the CyberCop Server CD in the arm directory.

Periodically, NAI develops additional new ARMs for the CyberCop products. Check the NAI Web page (<http://www.nai.com>) for new ARMs that you can download from the Web page.

## Installing ARMs for Windows NT

1. Log in as the administrator or as a member of the administrator's group.
2. Insert the CyberCop Server CD into the CD-ROM drive.
3. Cancel the CyberCop Server installation.
4. Go to a DOS prompt.
5. **Go to the `./armname` directory on the CD.**  
EXAMPLE: `cd \winnt\arms\nt\ armname`
6. **Within the `./armname` directory, run the installation script by typing:**  
EXAMPLE: `install.bat .\<????>`  
This installs the ARM.
7. Repeat steps 5 and 6 for each ARM that you want to install.

The ARM is now installed and ready to be configured to operate with the CyberCop Server. See [“Agents Stanza” on page 42](#) and [“Agents Stanza” on page 43](#) in [Chapter 3](#) for more information on configuring the ARMS stanzas.

## Installing ARMs for Solaris

1. Log in as root.
2. Insert the CyberCop Server CD.
3. **Go to the `./armname` directory:**  
EXAMPLE: `cd /cdrom/cybercopserver/arms/Solaris/ armname`
4. **Within the `./armname` directory, run the installation script by typing:**  
EXAMPLE: `install.sh /opt/<????>`  
This installs the ARM.
5. Repeat steps 3 and 4 for each ARM that you want to install.

The ARMs are now installed and ready to be configured to operate with the CyberCop Server. See [“Agents Stanza” on page 42](#) and [“Agents Stanza” on page 43](#) in [Chapter 3](#) for more information on configuring the ARMS stanzas.

This chapter provides information about the following topics:

- Security Policy Stanzas
- Creating Your Security Policy
- Configuring Your Security Policy

A default security policy can be found in the policies directory. Make a copy of it or print it, and take a look at this .txt file to familiarize yourself with the format of the security policy.

---

+ **WARNING:** Modification of the CyberCop Server's security policy should only be performed by highly competent CyberCop Server system administrators.

---

## Security Policy Stanzas

The security policy contains stanzas that are made up of lines of arguments that tell the CyberCop Server which security categories to monitor, which responses to take when a violation occurs, which notifications to send, and who to send the notifications to. The stanzas can be listed in any order, but should only be listed once.

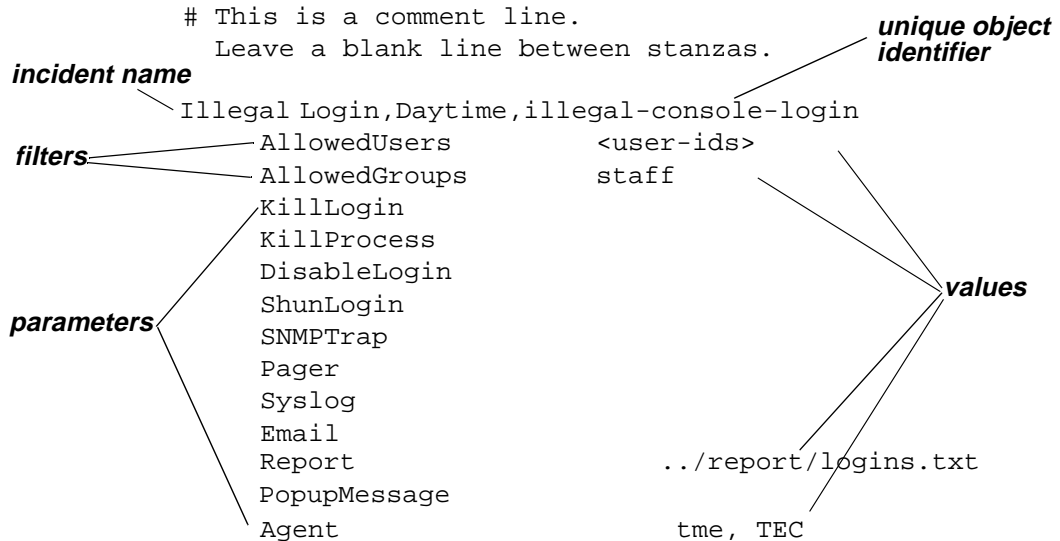
A stanza consists of the name of the incident, the unique object identifier, and the keywords in the filter, parameter, and value fields that tell the CyberCop Server actions to take. See Appendix B, "Keywords," for a list of keywords that are valid for the CyberCop Server's security incidents.

See the Glossary for definitions of these terms.

## Stanza Format

The format of the stanza is strict. It is made up of lines of keywords in the filter, parameter, and value fields. See [Figure 3-1](#) for a sample stanza.

**Figure 3-1. Sample Stanza Format**



The incident title (Illegal Login) is followed by the hours keyword (Daytime) and the unique object identifier (illegal-console-login). The filters (AllowedLoginUsers and AllowedLoginGroups) are listed first under the incident title with their values, (user id and staff). Under the filters come the parameters (KillLogin, DisableLogin, and so forth) with any values that apply to them. The parameters consist of the notifications and responses that apply to that particular incident.

The following characteristics apply:

- The keywords and parameters are not case-sensitive, but the values are.
- Use a pound sign (#) to begin a comment. Comments that extend from the # to the end of the line are ignored by the CyberCop Server's parser.
- Separate multiple items with commas.
- Stanzas must contain at least one notification (SNMPTrap, Pager, Syslog, Email, Report, or PopupMessage).
- Separate each stanza with a blank line. Blank lines signal the end of a stanza.

See Appendix B for a table that lists the keywords that are valid for the incident name, filter, parameter, and value fields.

## Creating Your Security Policy

The following procedures give the high-level steps for creating a security policy for the UNIX and Windows NT platforms.

### UNIX

1. Go to the CyberCop Server installation directory (./<????>).
2. There are two text files in this directory: advpolicy.txt and defpolicy.txt.

- For full monitoring capability, copy the advpolicy.txt file and rename it.
- For minimal monitoring, copy the defpolicy.txt file and rename it.

Choose a name that is distinctive so that you will always know which policy you are using. For example, you might want to name the policies by dates: january.txt, monday.txt, or weekend.txt.

3. Modify the stanzas in the file to meet your security needs and save the file.

See the following sections on the individual stanzas for detailed information on how to modify them.

- 
- **NOTE:** The default security policy comes with most lines commented out (#). Remove the # and change any values of any parameters as needed.
- 

4. **IMPORTANT:** Before enabling the CyberCop Server, validate the policy to make sure that it is correct by typing:

```
cybercopserver validate <full path to your new policy file>
```

5. Copy the \*.txt file to ./<????>/tmp/security.txt.

6. Enable the CyberCop Server by typing:

```
cybercopserver config
```

The security policy is automatically validated again whenever the CyberCop Server is enabled. Any runtime validation errors are emailed to the policy administrator.

- 
- **NOTE:** To disable the CyberCop Server, enter shutdown instead of config.
- 

7. Repeat this procedure for each machine on which the CyberCop Server is installed.

## Windows NT

1. Go to the CyberCop Server's installation directory (C:\Program Files\Network Associates\CyberCop Server).

2. There are two text files in this directory: advpolicy.txt and defpolicy.txt.

- For full monitoring capability, copy the advpolicy.txt file and rename it.
- For minimal monitoring, copy the defpolicy.txt file and rename it.

Choose a name that is distinctive so that you will always know which policy you are using. For example, you might want to name the policies by dates: january.txt, monday.txt, or weekend.txt.

3. Modify the stanzas in the file to meet your security needs and save the file.

See the following sections on the individual stanzas for detailed information on how to modify them.

- 
- NOTE: The default security policy comes with most lines commented out (#). Remove the # and change any values of any parameters as needed.
- 

4. Before enabling the CyberCop Server, validate the policy to make sure that it is correct by typing:

```
cybercopserver validate <full path to your new policy file>
```

Validation errors are emailed to the address specified in the security policy.

5. Copy your new policy to \CyberCop Server\tmp\security.txt.
6. Restart the CyberCop Server by going to Start-->Programs-->Cyber Cop Server-->Restart CyberCop Server.

The security policy is automatically validated again whenever the CyberCop Server is enabled.

7. Repeat this procedure for each machine on which the CyberCop Server is installed.

# Configuring Your Security Policy

The following section gives guidelines and instructions for configuring each CyberCop Server stanza in the security policy.

## Pager Script and SNMP Script

If you are planning to use the pager and SNMP methods of notification, you must configure the Pager and SNMP scripts before you configure your security policy.

### Configuring the Pager Script

**WINDOWS NT:** The pager script is found in .\CyberCop Server\utils. To allow the CyberCop Server to interact with your pager, you must replace the following lines in the pager.bat file with whatever program you use, so that the CyberCop Server can call your paging system:

```
echo %EMAIL_BODY% > tmp.txt ..\bin\hlisntp.exe -s
%EMAIL_SUBJECT% -f
tmp.txt %EMAIL_ADDRESS%
del tmp.txt
```

**UNIX:** The pager script is found in ./CyberCop Server/utils. To allow the CyberCop Server to interact with your pager, you need to replace the following lines in the pager.sh file with whatever program you use, so that the CyberCop Server can call your paging system:

```
echo "$EMAIL_BODY" | mail -s "$EMAIL_SUBJECT"
$EMAIL_ADDRESS_____
```

### Configuring the SNMP Script

**UNIX:** To enable the CyberCop Server to send SNMP Traps, make the following changes to the snmp.sh file. The Gateway Name must be changed in the following lines to wherever you want to send the SNMP Traps. You can change the remaining lines to whatever is appropriate to your environment. The common defaults are listed below.

```
GATEWAY_NAME = "NONE"
COMMUNITY_NAME = "public"
TRAP_TYPE = "6"
SPECIFIC_TYPE = "0"
```

**WINDOWS NT:** You do not need to change the SNMP script for Windows NT since it is already configured when you set up SNMP. See your Windows NT documentation for information on installing SNMP.

- NOTE: Some Network Managers display CyberCop Server SNMP trap messages in HEX instead of readable ASCII. The CUM-based SNMP Network Managers normally display these messages in the readable format.
- 

## BusinessHours Stanza

**Figure 3-2. BusinessHours Stanza**

```
BusinessHours
Sun
Mon
Tue      8-18, 14, 16-20
Wed      8-18
Thu      8-18
Fri      8-18
Sat
```

- 
- NOTE: 8-18 designates 8 am to 6:59 pm on Monday through Friday as the daytime hours.
- 

The BusinessHours stanza allows you to set the daytime hours or “business” hours for the CyberCop Server. Hours specified in this stanza are considered daytime hours. All other times are assumed to be nighttime hours. Time is entered in military (24-hour) time. If this stanza or any part of it is not entered, then the hours are assumed to be nighttime hours.

The valid parameters for the BusinessHours stanza are:

- Three-letter abbreviations for the days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun)

The valid values for the parameters are:

- Hours or ranges of hours separated by commas

Several ranges can be specified for one day, but the ranges must all appear on the same line.

- 
- NOTE: Days can only appear once in the BusinessHours stanza.
-



## Defaults Stanza

Figure 3-3. Defaults Stanza

```
Defaults
EmailAddress      $administrator
ReportFile        ..\report\cybercopserver.txt
SyslogName        CyberCopServer
PagerScript       ..\utils\pager.nt
SNMPScript        ..\utils\snmp.nt
ShunInterval      15
```

In the Defaults stanza, you configure the default response targets to be used when no targets are specified in the individual stanzas. The following parameters allow you to configure these default values:

- **EmailAddress** - Type in the email address of the person who is monitoring the emails generated by the CyberCop Server.  
For example, you may want the company address listed as the default email address during the day, but you may want a home address listed in the individual stanzas for nighttime and weekend hours. Separate the entries by a comma.
- **ReportFile** - The file in which all incident reports are stored.  
This file can grow to be very large rather quickly, so you may want to save these reports periodically into another directory. Naming them by times or dates, for example 3\_13\_98.txt, is helpful if you ever need to retrieve information as evidence of intrusion.
- **SyslogName** - Choose the message that is prepended to syslog entries. The default is **CyberCopServer**.
- **PagerScript** - Have the pager script invoked whenever an incident occurs.  
If you elect to use this option, configure the script and then uncomment the line (that is, remove the pound sign (#) from the beginning of the line). If you do not configure the script first, you will receive error messages when your policy is validated.

**UNIX:** The pager script file is pager.sh.

**WINDOWS NT:** The pager script file is pager.bat.

- **SNMPScript** - Have an SNMP Trap sent, for example, to the administrator or to a central console whenever incidents occur.

If you elect to use this option, configure the script and then uncomment the line (that is, remove the pound sign (#) from the beginning of the line). If you do not configure the script first, you will receive error messages when your policy is validated.

**UNIX:** The SNMP script file is `snmp.sh`.

**WINDOWS NT:** The SNMP script file is `snmp.bat`.

- **ShunInterval** - Configure the amount of time that will pass whenever a login is shunned. The default value is 15 minutes.

## Agents Stanza

**Figure 3-4. Agents Stanza**

```
Agents
Agents      fixit,pix,tme
Config      fixit #no parameters for fixit
Config      pix,<firewall name>,<internal IP address>,<login
            pass-word>,<enable password>,<Global IP address>,<shun
            interval>
Config      tme,<server name>,<notice group>,<priority>*
```

\* Choose one of the following values for <priority>: CRITICAL, ERROR, WARNING, DEBUG, or NOTICE

The Agents stanza configures ARM agents. ARMs are programs that allow the CyberCop Server to interact with other applications. See [Chapter 1](#) for more information on CyberCop Server ARMs.

During CyberCop Server installation, you can add any of the currently available ARMs:

- Fixit ARM (fixit)
- ARM for Cisco Pix Firewall (pix)
- Tivoli TME 10 Framework ARM (tme)

To find out how to install ARMs after you have installed the CyberCop Server, see “Installing ARMs After CyberCop Server Installation” on page 33. Check the NAI Web page (<http://www.nai.com>) for newly available ARMs.

There are two steps to configure the ARMs: the Agents stanza and the Agent response in the incident stanzas.

## Agents Stanza

In the Agents stanza, the keywords Agents and Config in the parameter field allow you to specify the name and default values for each agent.

The valid values are:

- Agents - fixit,pix,tme  
List all of the ARMs that you want to configure on the same line separated by a comma.
- Config - The values for Config depend on your environment. See Figure 3-4 for the variable values for each ARM.

## Responses in the Incident Stanzas

In the individual stanzas for the security incidents, add the ARM responses that you want for each incident. The Fixit ARM response applies to the Illegal File Access incident. The PIX and TME ARM responses can apply to all of the incident stanzas (provided you have a PIX firewall or Tivoli TME 10 Framework installed). See the help files (in HTML and TXT format in each ARM directory) for more information on configuring each ARM to work with the CyberCop Server. The following table lists the values for the Agent parameter in the incident stanzas.

**Figure 3-5. Agent Response Values**

| Parameter Field | Value Field*                   |
|-----------------|--------------------------------|
| Agent           | fixit,SAVE_BAD FIX_BAD DEL_NEW |
| Agent           | pix,SHUN BLOCK                 |
| Agent           | tme,TEC NOTICE BCAST           |

\* All ARM values are separated by spaces rather than by commas.

## Illegal Login Stanza

**Figure 3-6. Illegal Login Stanza**

```
Illegal Logins,Daytime,illegal-remote-login
AllowedRemoteUsers                fred, john
AllowedRemoteGroups                administrators,testers
AllowedRemoteAddrs
KillLogin
DisableLogin
ShunLogin                        15
SNMPTrap
Pager
Syslog
Email
Report
Popup Message
Agent                            tme,TEC
```

The Illegal Login stanza configures the responses taken when a user illegally logs into the system during the day or night. The stanza line has the incident title (Illegal Login) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (illegal-console-login or illegal-remote-login).

Configure a separate stanza for daytime and nighttime for each category (illegal-console-login or illegal-remote-login). Uncomment the lines that you want to activate in the security policy by removing the #, and change the values to suit your needs.

See Figure 3-1 for the sample stanza with the terms (keywords, parameters, values) called out.

The filters allowed for illegal-console-login are:

- **AllowedUsers** - In the values field, list the users that are allowed to login to the console during the given hours. Separate each user name with a comma.
- 
- **NOTE:** The Windows NT administrator account is automatically added to the AllowedUsers filter rules in the illegal-console-login stanza.
- 
- **AllowedGroups** - In the values field, list the groups that are allowed to login to the console during the given hours. Separate each user name with a comma.

The filters allowed for illegal-remote-login are:

- AllowedRemoteUsers - In the values field, list the users that are allowed to log into the system during the given hours. Separate each user name with a comma.
- 
- NOTE: To use the AllowedRemoteUsers filter in a illegal-remote-login stanza, you must also specify the AllowedRemoteAddrs filter.
- 
- NOTE: The Windows NT administrator account is automatically added to the AllowedRemoteUsers filter rules in the illegal-remote-login stanza.
- 
- AllowedRemoteGroups - In the values field, list the groups that are allowed to log into the system during the given hours. Separate each group name with a comma.
  - AllowedRemoteAddrs - In the values field, list the TCP/IP addresses that users are allowed to log in from during the given hours. Separate each address with a comma.

The following responses and notifications parameters are available:

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.
  - SNMPTrap - Uncomment this line to have the CyberCop Server generate an SNMP trap.
  - Pager - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
  - Syslog - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
  - Email - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.

- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## Illegal Privilege Escalation Stanza (UNIX Only)

**Figure 3-7. Illegal Privilege Escalation Stanza**

|  |                  |
|--|------------------|
| Illegal Privilege Escalation,Daytime,illegal-root-transition |                  |
| AllowedUsers   | fred, john       |
| AllowedGroups  | staff, testers   |
| KillLogin  |                  |
| KillProcess  |                  |
| DisableLogin   |                  |
| ShunLogin  | 15               |
| SNMPTrap   |                  |
| Pager  |                  |
| Syslog   |                  |
| Email  | fred@company.com |
| Report   |                  |
| Popup Message  |                  |
| Agent  | tme, TEC         |

The Illegal Privilege Escalation stanza configures the responses taken when a user illegally transitions to root during the day or night. The stanza line has the incident title (Illegal Privilege Escalation) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (illegal-root-transition).

The filters allowed are:

- **AllowedUsers** - In the values field, list the users that are allowed to transition to root during the given hours

- AllowedGroups - In the values field, list the groups that are allowed to transition to root during the given hours

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
- KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
- DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.

---

• NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.

---

- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.
- SNMPTrap - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- Pager - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- Syslog - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- Email - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- Report - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- PopupMessage - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- Agent - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## Illegal Jumper Stanza

**Figure 3-8. Illegal Jumper Stanza**

```
Illegal Jumper,Nighttime,illegal-jumper
AllowedUsers      Administrator
AllowedGroups
KillLogin
KillProcess
DisableLogin
ShunLogin         15
SNMPTrap
Pager
Syslog
Email             fred@home.com
Report
Popup Message
Agent            tme,TEC
```

The Illegal Jumper stanza configures the responses taken when a remotely logged-in user jumps (logs into another computer) during the day or night. The stanza line has the incident title (Illegal Jumper) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (illegal-jumper).

The filters allowed are:

- **AllowedUsers** - In the values field, list the users that are allowed to jump during the given hours
- **AllowedGroups** - In the values field, list the groups that are allowed to jump during the given hours

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- **KillLogin** - Uncomment this line to have the CyberCop Server kill the illegal login.
- **KillProcess** - Uncomment this line to have the CyberCop Server terminate the offending process.
- **DisableLogin** - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.



- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 

- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.
- SNMPTrap - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- Pager - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- Syslog - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- Email - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- Report - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- PopupMessage - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- Agent - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## Self Defense Stanza

**Figure 3-9. Self Defense Stanza**

```
Self Defense,Daytime,self-defense
KillLogin
KillProcess
DisableLogin
ShunLogin                15
SNMPTrap
Pager
Syslog
Email                    fred@company.com
Report
Popup Message
```

The Self Defense stanza indicates the responses taken when the databases of the CyberCop Server are altered during the day or night. The stanza line has the incident title (Self Defense) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (self-defense).

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.
  - SNMPTrap - Uncomment this line to have the CyberCop Server generate an SNMP trap.

- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## Illegal File Access Stanza

**Figure 3-10. Illegal File Access Stanza**

```
Illegal File Access,Daytime,illegal-file-access-1
ProtectPathOnly      c:\temp
AllowedUsers         fred
Syslog
Email
Reportfile
Agents               fixit,SAVE_BAD FIX_BAD DEL_NEW
```

The Illegal File Access stanza configures the responses taken when a user illegally accesses a given directory during the day or night. The stanza line has the incident title (Illegal File Access) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (illegal-file-access- n where n is any unique string).

You can use the variable n to number each stanza, since each directory that you want to protect must have its own stanza.

Configure a separate stanza for daytime and nighttime for each directory (illegal-file-access- n) you want to protect. Uncomment the lines that you need and change the values to suit your security needs.

- 
- + **WARNING:** You must have a separate stanza for each directory that you want the CyberCop Server to protect.
- 

The filters allowed are:

- **ProtectPathOnly** - In the values field, list the name of the path to protect. The CyberCop Server does not protect the subdirectories of this path.
  - **ProtectPathSubdirs** - In the values field, list the name of the path to protect. The CyberCop Server will protect the path and all of its subdirectories.
- 
- **NOTE:** Each Illegal File Access stanza must have either the **ProtectPathOnly** or the **ProtectPathSubdirs** filter, but cannot include both filters.
- 

The parameters allowed are

- **AllowedUsers** - In the values field, list the users that are allowed to modify the file during the given hours.
- **AllowedGroups** - In the values field, list the groups that are allowed to modify the file during the given hours.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- **KillLogin** - Uncomment this line to have the CyberCop Server kill the illegal login.
  - **KillProcess** - Uncomment this line to have the CyberCop Server terminate the offending process.
  - **DisableLogin** - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- **NOTE:** Choose either **DisableLogin** or **ShunLogin** in a particular stanza.
- 
- **ShunLogin** - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.
  - **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.

- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
  - **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
  - **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
  - **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
  - **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
  - **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.
- 
- **NOTE:** The Fixit ARM is used with Illegal File Access to replace or delete damaged files.
-

## Password Rattling Stanza

**Figure 3-11. Password Rattling Stanza**

```
Password Rattling,Daytime,password-rattling
KillLogin #Reserved for future use
KillProcess #Reserved for future use
DiableLogin #Reserved for future use
ShunLogin #Reserved for future use
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The Password Rattling stanza configures the responses taken when a user attempts to gain access to a password (for example, failed attempts to log in or to switch user) during the day or night. The stanza line has the incident title (Password Rattling) followed by the hours (Daytime or Nighttime) and the unique object identifier keyword (password-rattling).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.

- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## System Access Stanza

**Figure 3-12. System Access Stanza**

```
System Access,Daytime,system-access
KillLogin
KillProcess
DisableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The System Access stanza configures the responses taken when a user succeeds in password rattling or outside file system mounts during the day or night. The stanza line has the incident title (System Access) followed by the hours keyword (Daytime or Night-time) and the unique object identifier (system-access).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.



- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## System Exploitation Stanza

**Figure 3-13. System Exploitation Stanza**

```
System Access,Daytime,system-access
KillLogin
KillProcess
DiableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The System Exploitation stanza configures the responses taken against attempted system vulnerabilities (for example, writing system executables or accessing the password file) during the day or night. The stanza line has the incident title (System Exploitation) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (system-exploitation).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.

- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## System Attack Stanza

**Figure 3-14. System Attack**

```
System Attack,Daytime,system-attack
KillLogin
KillProcess
DisableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The System Attack stanza configures the responses taken when attack scenarios are attempted (for example, planting a Trojan horse or writing to other .rhosts files) during the day or night. The stanza line has the incident title (System Attack) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (system-attack).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.

- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## System Probe Stanza (UNIX Only)

**Figure 3-15. System Probe Stanza**

```
System Probe,Daytime,system-probe
KillLogin
KillProcess
DisableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The System Probe stanza configures the responses taken when the SATAN scanner is used against the machine during the day or night. The stanza line has the incident title (System Probe) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (system-probe).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
- KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
- DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.

---

• NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.

---

- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.

- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## System Misuse Stanza

**Figure 3-16. System Misuse Stanza**

```
System Attack,Daytime,system-attack
KillLogin
KillProcess
DisableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The System Misuse stanza configures the responses taken when misuses (such as inappropriate file deletion) are recognized during the day or night. The stanza line has the incident title (System Misuse) followed by the hours keyword (Daytime or Nighttime) and the unique object identifier (system-misuse).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.



- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.

## User Covering Tracks Stanza

**Figure 3-17. User Covering Tracks**

```
System Attack,Daytime,system-attack
KillLogin
KillProcess
DiableLogin
ShunLogin
SNMPTrap
Pager
Syslog
Email
Report
PopupMessage
```

The User Covering Tracks stanza configures the responses taken when activity that looks like a user trying to cover his tracks is recognized during the day or night. The stanza line has the incident title (User Covering Tracks) followed by the hours keyword (Day-time or Nighttime) and the unique object identifier (user-covering-tracks).

Configure a separate stanza for daytime and nighttime for this category. Uncomment the lines that you need and change the values to suit your security policy.

There are no filters associated with this category.

The following responses and notifications parameters are available (if a certain response or notification is not appropriate for this incident, you will receive an error message to that effect):

- KillLogin - Uncomment this line to have the CyberCop Server kill the illegal login.
  - KillProcess - Uncomment this line to have the CyberCop Server terminate the offending process.
  - DisableLogin - Uncomment this line to have the CyberCop Server disable the offending user's ability to log in again.
- 
- NOTE: Choose either DisableLogin or ShunLogin in a particular stanza.
- 
- ShunLogin - Uncomment this line to have the CyberCop Server disable the offending user from executing a login for default shun time. In the values field, specify an incident-specific shun time in minutes.

- **SNMPTrap** - Uncomment this line to have the CyberCop Server generate an SNMP trap.
- **Pager** - Uncomment this line to have the CyberCop Server page the administrator by running the default pager script. In the values field, specify an incident-specific paging script.
- **Syslog** - Uncomment this line to have the CyberCop Server log the incident to the system log. The message will be prepended with the default syslog message or you can specify the syslog text in the values field.
- **Email** - Uncomment this line to have the CyberCop Server send an email message to the person that you designate. The default email address is used unless you specify an incident-specific email address in the values field.
- **Report** - Uncomment this line to have the CyberCop Server log the incident to the report file. The default report file is used unless you specify an incident-specific report file name in the values field.
- **PopupMessage** - Uncomment this line to have the CyberCop Server send a popup message to the monitor or console when an incident is detected.
- **Agent** - Uncomment this line to have the CyberCop Server activate an ARM response when an incident is detected. List the appropriate ARM keywords in the values field.



The following table lists the CyberCop Server's features.

See the NAI Web page (<http://www.nai.com>) for information on obtaining an upgrade from an evaluation version to a permanent version of the CyberCop Server.

## **Security Categories**

- Business Hours
- Defaults
- Illegal Login
- Illegal Privilege Escalation (UNIX)
- Illegal Jumper
- Self-Defense
- Illegal File Access
- Password Rattling
- System Exploitation
- System Probe (UNIX)
- System Attack
- System Misuse
- User Covering Tracks

## **Responses**

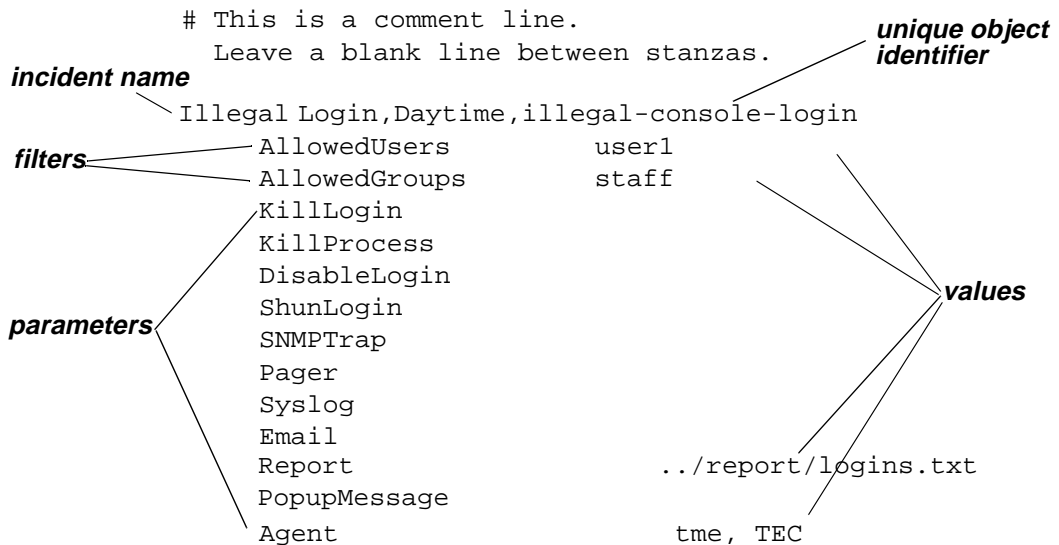
- Kill Process
- Kill Login
- Shun Login
- Disable Login
- ARM Support (fixit, pix, tme)
- Email
- Report File
- SNMP Trap
- Syslog
- Popup Message
- Disable Login

### Notifications

- Email
- Report File
- Syslog
- SNMP Trap
- Popup Message

This appendix includes information about valid keywords for the stanza title, filters, parameters, and values fields in the stanzas. It is important to use the exact forms of the keywords listed below.

Figure B-1 gives an example of the format of a stanza. You can see the correct placement of the filters, unique object identifiers, parameters, values, and comments. If your stanzas do not follow this strict format, you will receive an error message specifying which keywords are incorrect. See Appendix D for a list of CyberCop Server error messages.



**Figure B-1. Stanza Format**

Table B-1 lists the keywords that are valid for each field in each security category stanza.

Make sure that all are spelled correctly in the security policy, otherwise the security policy parser will return an error.

See Appendix D for a list of the error messages that the CyberCop Server sends when the parser encounters something invalid in the security policy.

# Keywords

| Incident Title | Filters             | Parameters        | Values                                      |
|----------------|---------------------|-------------------|---|
| BusinessHours  |                     | Sun               | use numbers between<br>0 and 23             |
|                |                     | Mon               |   |
|                |                     | Tue               |   |
|                |                     | Wed               |   |
|                |                     | Thu               |   |
|                |                     | Fri               |   |
|                |                     | Sat               |   |
| Defaults       |                     | EmailAddress      | \$administrator                             |
|                |                     | ReportFile        | ./report/report.txt                         |
|                |                     | SyslogName        |   |
|                |                     | PagerScript       |   |
|                |                     | SnmpScript        | 15 minutes (default)                        |
| Agents 1       |                     | ShunInterval      |   |
|                |                     | Agents            | fixit/pix/tme                               |
|                |                     | Config            | <configuration<br>arguments>                |
| Illegal Login  | AllowedUsers        | Daytime/Nighttime |   |
|                | AllowedGroups       | KillLogin         |   |
|                | AllowedRemoteUsers  | DisableLogin      |   |
|                | AllowedRemoteGroups | ShunLogin         |   |
|                | AllowedRemoteAddrs  | SNMPTrap          |   |
|                |                     | Pager             |   |
|                |                     | Syslog            |   |
|                |                     | Email             |   |
|                |                     | Report            |   |
|                |                     | PopupMessage      |   |
|                |                     | Agent             |   |
|                |                     | Agent             |   |
|                |                     |                   | pix,SHUN BLOCK<br>tme,TEC NOTICE<br>BCAST 2 |



| Incident Title            | Filters       | Parameters        | Values         |
|---------------------------|---------------|-------------------|----------------|
| Illegal Privilege         | AllowedUsers  | Daytime/Nighttime |                |
| Escalation<br>(UNIX only) | AllowedGroups | KillLogin         |                |
|                           |               | KillProcess       |                |
|                           |               | DisableLogin      |                |
|                           |               | ShunLogin         |                |
|                           |               | SNMPTrap          |                |
|                           |               | Pager             |                |
|                           |               | Syslog            |                |
|                           |               | Email             |                |
|                           |               | Report            |                |
|                           |               | PopupMessage      |                |
|                           |               | Agent             |                |
|                           |               | Agent             | pix,SHUN BLOCK |
| Illegal Jumper            | AllowedUsers  | Daytime/Nighttime |                |
|                           | AllowedGroups | KillLogin         |                |
|                           |               | KillProcess       |                |
|                           |               | DisableLogin      |                |
|                           |               | ShunLogin         |                |
|                           |               | SNMPTrap          |                |
|                           |               | Pager             |                |
|                           |               | Syslog            |                |
|                           |               | Email             |                |
|                           |               | Report            |                |
|                           |               | PopupMessage      |                |
|                           |               | Agent             |                |
|                           |               | Agent             | pix,SHUN BLOCK |
| Self Defense              |               | Daytime/Nighttime |                |
|                           |               | KillLogin         |                |
|                           |               | KillProcess       |                |
|                           |               | DisableLogin      |                |
|                           |               | ShunLogin         |                |
|                           |               | SNMPTrap          |                |
|                           |               | Pager             |                |
|                           |               | Syslog            |                |

| Incident Title      | Filters  | Parameters        | Values                             |
|---------------------|--|-------------------|------------------------------------|
| Illegal File Access | ProtectPathOnly<br>ProtectPathSubdirs<br>AllowedUsers<br>AllowedGroups | Email             |                                    |
|                     |  | Report            |                                    |
|                     |  | PopupMessage      |                                    |
|                     |  | Daytime/Nighttime |                                    |
|                     |  | KillLogin         |                                    |
|                     |  | KillProcess       |                                    |
|                     |  | DisableLogin      |                                    |
|                     |  | ShunLogin         |                                    |
|                     |  | SNMPTrap          |                                    |
|                     |  | Pager             |                                    |
| Password Rattling   |  | Syslog            |                                    |
|                     |  | Email             |                                    |
|                     |  | Report            |                                    |
|                     |  | PopupMessage      |                                    |
|                     |  | Agent             | fixit, SAVE_BAD<br>FIX_BAD DEL_NEW |
|                     |  | Daytime/Nighttime |                                    |
|                     |  | Kill Login        |                                    |
|                     |  | KillProcess       |                                    |
|                     |  | DisableLogin      |                                    |
|                     |  | ShunLogin         |                                    |
| System Access       |  | SNMPTrap          |                                    |
|                     |  | Pager             |                                    |
|                     |  | Syslog            |                                    |
|                     |  | Email             |                                    |
|                     |  | Report            |                                    |
|                     |  | Popup Message     |                                    |
|                     |  | Daytime/Nighttime |                                    |
|                     |  | Kill Login        |                                    |
|                     |  | KillProcess       |                                    |
|                     |  | DisableLogin      |                                    |
|                     |  | ShunLogin         |                                    |
|                     |  | SNMPTrap          |                                    |
|                     |  | Pager             |                                    |
|                     |  | Syslog            |                                    |
|                     |  | Email             |                                    |

| Incident Title              | Filters | Parameters        | Values |
|-----------------------------|---------|-------------------|--------|
| System Probe<br>(UNIX only) |         | Report            |        |
|                             |         | Popup Message     |        |
|                             |         | Daytime/Nighttime |        |
|                             |         | Kill Login        |        |
|                             |         | KillProcess       |        |
|                             |         | DisableLogin      |        |
|                             |         | ShunLogin         |        |
|                             |         | SNMPTrap          |        |
|                             |         | Pager             |        |
|                             |         | Syslog            |        |
| System Attack               |         | Email             |        |
|                             |         | Report            |        |
|                             |         | Popup Message     |        |
|                             |         | Daytime/Nighttime |        |
|                             |         | Kill Login        |        |
|                             |         | KillProcess       |        |
|                             |         | DisableLogin      |        |
|                             |         | ShunLogin         |        |
|                             |         | SNMPTrap          |        |
|                             |         | Pager             |        |
| System<br>Exploitation      |         | Syslog            |        |
|                             |         | Email             |        |
|                             |         | Report            |        |
|                             |         | Popup Message     |        |
|                             |         | Daytime/Nighttime |        |
|                             |         | Kill Login        |        |
|                             |         | KillProcess       |        |
|                             |         | DisableLogin      |        |
|                             |         | ShunLogin         |        |
|                             |         | SNMPTrap          |        |
|                             |         | Pager             |        |
|                             |         | Syslog            |        |
|                             |         | Email             |        |
|                             |         | Report            |        |
|                             |         | Popup Message     |        |
|                             |         | Daytime/Nighttime |        |
|                             |         | Kill Login        |        |
|                             |         | KillProcess       |        |
|                             |         | DisableLogin      |        |
|                             |         | ShunLogin         |        |

| Incident Title | Filters | Parameters        | Values |
|----------------|---------|-------------------|--------|
| System Misuse  |         | Daytime/Nighttime |        |
|                |         | Kill Login        |        |
|                |         | KillProcess       |        |
|                |         | DisableLogin      |        |
|                |         | ShunLogin         |        |
|                |         | SNMPTrap          |        |
|                |         | Pager             |        |
|                |         | Syslog            |        |
|                |         | Email             |        |
|                |         | Report            |        |
| User Covering  |         | Popup Message     |        |
|                |         | Daytime/Nighttime |        |
| Tracks         |         | Kill Login        |        |
|                |         | KillProcess       |        |
|                |         | DisableLogin      |        |

See the help files (in HTML and TXT format) on the CD for information on configuring the ARMs. If you have Tivoli's TME 10 Framework, you can add the TME 10 ARM responses for each incident stanza.

# Platform Limitations Per Stanza



## Stanzas Per Platform

The following table shows which stanzas, which are made up of groups of signatures, are valid for each platform. See Appendix A for a listing of stanzas.

| Number | Signature                                  | Solaris | NT |
|--------|--|---------|----|
|        | <b>Password Rattling</b>                   |         |    |
| 0003   | General doorknob rattling                  | x       | x  |
| 0013   | General su rattling                        | x       |    |
|        | <b>System Access</b>                       |         |    |
| 0006   | Successful doorknob rattling               | x       | x  |
| 0010   | Suspicious login                           | x       |    |
| 0014   | Successful su rattling                     | x       |    |
| 0036   | Remote user executing restricted program   | x       |    |
| 0052   | Audit userid changed                       | x       |    |
| 0057   | File system mounted by outside network     | x       | x  |
|        | <b>System Attack</b>                       |         |    |
| 0001   | Installing system-level Trojan horse       | x       |    |
| 0002   | Malicious manipulation of other user files | x       |    |
| 0007   | Setuid Trojan horse                        | x       |    |
| 0008   | Exploration                                | x       |    |
| 0011   | Planting bogus su executable               | x       |    |
| 0012   | Executing bogus su program                 | x       |    |
| 0031   | Write to other <b>.rhosts</b>              | x       |    |
| 0032   | Attempted write to other <b>.rhosts</b>    | x       |    |
| 0037   | Executing known rogue program              | x       | x  |

| Number | Signature   | Solaris | NT |
|--------|---|---------|----|
| 0039   | Attempt to open /dev/nit                              | x       |    |
|        | <b>System Exploitation</b>                            |         |    |
| 0017   | Writing world executable to system space              | x       |    |
| 0019   | Linking write world executable to system space        | x       |    |
| 0020   | Attempting to write world executable to system space  | x       |    |
| 0022   | Attempting to link world executable into system space | x       |    |
| 0023   | Modify system time                                    | x       | x  |
| 0024   | Attempt to modify system time                         | x       |    |
| 0038   | Attempt root login via local host                     | x       |    |
| 0061   | Bosperf dash x vulnerability                          |         |    |
| 0062   | Rout login via -froot                                 |         |    |
| 0083   | User added Administrators Group                       |         | x  |
| 0084   | Illegal access to user information                    |         | x  |
| 0085   | Detect add/remove users/groups                        |         | x  |
| 0088   | Illegal TCP/IP jumper                                 |         | x  |
| 0089   | Illegal use of regedit                                |         | x  |
|        | <b>System Misuse</b>                                  |         |    |
| 0009   | Malicious intruder                                    | x       |    |
| 0015   | Inappropriate file deletion                           | x       |    |
| 0016   | Illegally named file                                  | x       |    |
| 0029   | Writing to lost + found                               | x       |    |
| 0030   | Attempting to write to lost + found                   | x       |    |
| 0050   | User touched tagged file                              | x       |    |
| 0051   | User manipulated tagged file                          | x       |    |
|        | <b>System Probe</b>                                   |         |    |
| 0044   | SATAN normal scan                                     | x       |    |
| 0045   | SATAN heavy scan                                      | x       |    |
| 0046   | SATAN finger scan (normal, heavy)                     | x       |    |

| Number | Signature                             | Solaris | NT |
|--------|---------------------------------------|---------|----|
| 0047   | SATAN tcpscan (normal, heavy)         | x       |    |
| 0048   | SATAN udpscan (heavy)                 | x       |    |
| 0049   | SATAN tcpscan plus (heavy)            | x       |    |
|        | <b>User Covering Tracks</b>           |         |    |
| 0053   | Attempt to change audit userid        | x       |    |
| 0054   | Illegal audit state change            | x       | x  |
| 0055   | Attempted audit state change          | x       |    |
| 0056   | Auditing disabled                     | x       | x  |
| 0058   | Audit event timestamp out of range    | x       | x  |
| 0059   | Remote user connecting to remote node | x       |    |
| 0060   | Remote user connecting to source node | x       |    |





This appendix lists CyberCop Server security policy validation error messages in alphabetical order and provides explanations and suggestions for each message.

Erroneous data: DATA

The data in the error message contains an error that the CyberCop Server could not specifically identify. Change the security policy file so that the data conforms to the syntax specified in this document.

Errors parsing configuration file FILENAME

Problems were encountered by the security policy parser during validation of the file [FILENAME]. This message should be followed by a list of the errors that were found. Correct the errors in the security policy in order to bypass this message. Note that the CyberCop Server will still run even if errors have been detected in the security policy file—it simply ignores bad information.

Incomplete data: DATA

The parser expected to find additional data, but none was found. Verify that the syntax of [DATA] is correct and that it conforms to the parsing rules.

Invalid keyword: KEYWORD

The keyword [KEYWORD] is not valid for the current stanza and cannot be used. To correct this problem, check for misspelling in the keyword or remove the keyword from the stanza. See Appendix B for a list of valid keywords.

Invalid stanza title: STANZA

The value [STANZA] is not recognized by the policy parser as being a valid stanza title. See Appendix B for a list of valid stanza title keywords.

Invalid value: VALUE

The value [ *VALUE*] is either syntactically incorrect or is a value that the CyberCop Server knows to be wrong. For example, supplying the directory name "**2;j{h3m**" would result in this message: CyberCop Server can verify that this cannot possibly represent a valid directory name. The CyberCop Server can perform similar validation on users, email addresses, days of the week, and numerical values.

Keyword not supported on this platform: KEYWORD

The keyword [ *KEYWORD*] is not supported for the current stanza on this platform. Limitations in the underlying system prevent the CyberCop Server from correctly implementing this keyword. The keyword should thus not be used—upgrading the product level will have no effect. Refer to Appendix C for a list of stanzas supported for each CyberCop Server platform.

No alarms specified: STANZA

Stanzas are required to have at least one alarm, that is, notification (SNMP Trap, Email, for example), otherwise they should be omitted from the security policy file.

Redundant data: DATA

The data displayed in the error message has occurred more than once in the security policy file. To avoid confusion, the CyberCop Server security policy parser treats this situation as an error. To correct the problem, ensure that your security policy file contains only one instance of a given stanza, and verify that only one instance of a given keyword is present within a stanza.

Specified directory does not exist: DIRECTORY

The CyberCop Server cannot find the specified directory. Make sure that the directory exists and that no misspelling exists in the directory path.

Stanza not supported on this platform: STANZA

The supplied stanza type is not supported on the current platform and cannot be used. Refer to Appendix C for information on which stanzas (groups of signatures) are supported on each platform.

subsequent line(s) ignored

The parser is skipping lines that have been made unusable by a previous error.

Too many errors have occurred. Error logging has been stopped.

The security policy parser has run out of memory to store errors. For reasons of efficiency, the parser sets a limit of 2000 characters on the amount of error information that it will record.

Unlicensed incident creation: INCIDENT

The current level of the product is not authorized to create new incidents. To enable new incident creation, upgrade the product as described in the section titled “Upgrading From the Evaluation to the Permanent Version of CyberCop Server” in Chapter 2.

Unlicensed response selection: RESPONSE

The current version of the product is not authorized to perform this response. Either choose a different response or upgrade the product as described in the section titled “Upgrading From the Evaluation to the Permanent Version of CyberCop Server” in Chapter 2.

Value not required: DATA

The value specified in [DATA] is unnecessary and will be ignored by the CyberCop Server. To reduce confusion, the specified value should be removed.

Value required: KEYWORD

The keyword specified in the policy file must be followed by a value.

(WARNING) Response not recommended for this incident type:  
RESPONSE

The specified response should not be used with the current incident type. Unpredictable results could result from the use of the response.



# Glossary

|                           |   |
|---------------------------|---|
| <b>agent</b>              | A computer generating audit trail data. A machine whose audit data is analyzed by talker.   |
| <b>ARM</b>                | Active Response Module. An external program that the CyberCop Server can invoke as a response to an incident.   |
| <b>audit events</b>       | Instances of system calls or services by system utilities that are recorded in the audit trail.   |
| <b>audit file</b>         | A file containing audit events created by the system audit daemon.  |
| <b>audit flag</b>         | The selection of which audit events or classes of audit events are to be recorded in the audit trail.   |
| <b>audit ID</b>           | Unique arithmetic value (maintained separate from the userid) that identifies each authorized user to the auditing operation.   |
| <b>audit trail</b>        | An ordered timestamped log of audit events.   |
| <b>authorization</b>      | Right granted to an identified user to perform an action that would be otherwise prohibited.  |
| <b>console</b>            | The terminal or display located near the system unit providing access to the system and display-ing messages for system errors and other problems requiring intervention.   |
| <b>daemon</b>             | A UNIX program that operates in the background and provides system services; for example, inetd is the network daemon and provides TCP/IP network services; auditd is the audit daemon and writes audit events to the audit trail file. |
| <b>distributed system</b> | Set of workstations administered as a unit in UNIX.   |
| <b>effective groupid</b>  | The groupid that is used by the operating system to determine access permissions for an execut-ing process.   |

|                         |   |
|-------------------------|---|
| <b>effective userid</b> | The userid that is used by the operating system to determine access permissions for an executing process.   |
| <b>event</b>            | A collection of information describing a single operating system function.  |
| <b>event attributes</b> | Information logged for an audit event; includes timestamp, event type, description of event sub-ject, description of event object, and more.  |
| <b>event class</b>      | Convenient grouping of audit event types provided by the operating system; for example, all audit events associated with writing files are included in the <code>data_write</code> event class. The number of event classes available is determined by the client operating system.                                   |
| <b>event type</b>       | The narrowest category of events, such as <code>execute chmod service</code> or <code>open file for read</code> . The number of event types available are determined by the client operating system.  |
| <b>file access mode</b> | The type of access requested in a system service request; usually made of a combination of read, write, and execute; at runtime the file access mode is compared with an object's permission mode to determine if access will be granted; for further information, see the man page for <code>chmod(1v)</code> [Sun]. |
| <b>file system ID</b>   | Part of the description of an object in an audit event; the operating system assigned identifier for the device on which the object is physically located.  |
| <b>filters</b>          | A user-controlled data reduction operation whereby a user can set the criteria for which events or objects are valid and invalid. For example, the filter <code>AllowedUsers root</code> specifies that root is a valid user.   |
| <b>groupid</b>          | Identifier of a UNIX group; every userid belongs to at least one group; a convenient way to make files and programs accessible to all members of a group or project.  |
| <b>incident</b>         | An instance of an attack or misuse that is detected.  |
| <b>Internet</b>         | A worldwide collection of interconnected TCP/IP networks.   |

|                                  |   |
|----------------------------------|---|
| <b>local terminal</b>            | The non-console terminal directly connected to the client. See also “console.”  |
| <b>misuse</b>                    | A misuse is any activity that would be deemed unacceptable and undesirable were it known to the party responsible for the security of the site  |
| <b>misuse signatures</b>         | Machine-readable patterns of events used by the CyberCop Server to find instances of misuse in audit data.  |
| <b>name service</b>              | Identification and authentication mechanism for network account usersids. NIS and NIS+ are supported.   |
| <b>Network File System (NFS)</b> | A protocol developed by Sun used to provide remote network access to files on different kinds of machines. NFS servers also provide kernels and swap files to diskless clients so they can operate. |
| <b>network terminal</b>          | A network based connection to the agent; that is, not directly attached to the agent.   |
| <b>NIS</b>                       | Network Information Service (formerly “Yellow Pages”), see also “name service.”   |
| <b>notification</b>              | When an incident occurs, the CyberCop Server can inform system administrators via email and paging or through other applications (SNMP Trap).   |
| <b>object</b>                    | Something acted on in an audit event; usually a UNIX file or device.  |
| <b>object attributes</b>         | Information logged for an object in an audit event; includes name, type of object, its ownership, and other characteristics.  |
| <b>object name</b>               | The human-readable name of an object; usually a file name or the name of a device; for example, /etc/passwd or /dev/ttya.   |
| <b>object type</b>               | A category of objects; for example, files, devices, directories, links, shared memory segments.   |
| <b>optional data</b>             | Information included in the audit event that is not part of the standard format, and which varies by event type.  |

|                           |   |
|---------------------------|---|
| <b>outcome</b>            | Whether an event completed successfully (pass) or not (fail); failed outcomes (like failed attempts to open files) are often more interesting than successful ones.   |
| <b>owning groupid</b>     | The group to which an object (file, device) belongs; every UNIX object has ownership consisting of a userid and a groupid.  |
| <b>owning userid</b>      | The individual userid to which an object (file, device) belongs; every UNIX object has ownership consisting of a userid and a groupid.  |
| <b>parent process ID</b>  | The unique number assigned to a UNIX process that generates a process ID; it is included in each audit trail event logged from that process. See also “process ID.”   |
| <b>permission mode</b>    | The permissions attached to a file or other object which control who may access it; at runtime the file access mode is compared with the object’s permission mode to determine if access should be granted; for further information, see the man page for <code>chmod(1v)</code> [Sun].   |
| <b>privilege</b>          | Right granted to a TCB process to perform an action that would otherwise be prohibited; for example, the right to generate audit data or to override discretionary access checks. A privilege is granted to a trusted process. Typically, the trusted process enables the privilege just before needing it and disables it just after using it. |
| <b>process ID</b>         | The unique number assigned to a UNIX process; it is included in each audit trail event logged from that process.  |
| <b>real groupid</b>       | The groupid that is used by the operating system for accounting purposes on an executing process; may or may not be the same as the effective groupid.  |
| <b>real userid</b>        | The userid that is used by the operating system for accounting purposes on an executing process; may or may not be the same as the effective userid.  |
| <b>regular expression</b> | A pattern matching technique used by the CyberCop Server and often used in UNIX; for further information, see <code>grep(1v)</code> [Sun].  |



|   |   |
|---|---|
| <b>SNMP trap</b>  | A message sent from an SNMP agent to advise you that a significant violation has occurred.  |
| <b>Security Analysis Tool for Auditing Networks (SATAN)</b> | Written in shell, perl, expect, and C, SATAN gathers information from a remote host by probing NIS, finger, NFS, ftp and tftp, rexd, and other services. SATAN obtains network information and looks for security flaws and known bugs in system and network utilities.   |
| <b>response</b>   | An action resulting from an incident. This can be a built-in response or an ARM response.   |
| <b>session</b>  | The collection of audit trail events attributable to a single user between the original login event (authentication event) and the final logout; includes all activities in all windows and shells that were created by that login session; if two people log in with the same userid and password, CyberCop Server will interpret their behavior as two separate sessions. |
| <b>session ID</b>   | Unique ID that the CyberCop Server assigns to each session.   |
| <b>shun</b>   | An active response that keeps a user from being able to log onto the protected machine for a period of minutes. Note that this response does not kill any current logins  |
| <b>signature</b>  | See “misuse signatures.”  |
| <b>stanza</b>   | A section of the security policy. Stanzas define daytime hours, default response targets, or incidents. The stanza has a strict format made up of fields for filters, parameters, and values.   |
| <b>subject</b>  | The individual on whose behalf an event occurs; usually a human user.   |
| <b>subject attributes</b>                                   | Information logged for a subject in an audit event; includes the audit/real/effective userids and the real/effective groupids.  |

|                                 |   |
|---------------------------------|---|
| <b>switchover</b>               | The process by which the audit daemon closes the current audit file and opens a new audit file in the current audit directory: for further information, see the man page for audit(8)[Sun].           |
| <b>time stamp</b>               | The date and time at which an event occurs.   |
| <b>unique object identifier</b> | The unique object identifier field selects one of the prepackaged security incidents for use and Customizing in the policy for either daytime and nighttime. Do not change this case-sensitive field. |
| <b>userid</b>                   | A unique (numerical) identifier for an authorized user login.   |
| <b>username</b>                 | The name associated with a userid; there may be more than one username associated with a single userid.   |

# Index

## Symbols

\$administrator variable [21](#)  
\$cybercopserverdir variable [21](#)  
\$hostname variable [21](#)  
\$systemdrive [21](#)  
\$windir variable [21](#)

## A

active response module (ARM) [17](#)  
administration stanzas [18](#)  
    Business Hours [18](#)  
    Defaults [18](#)  
Agent response [46](#) to [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#),  
    [63](#), [65](#), [67](#)  
Agents stanza [42](#) to [43](#)  
AllowedGroups filter [44](#), [47](#) to [48](#)  
AllowedGroups parameter [52](#)  
AllowedRemoteAddrs filter [45](#)  
AllowedRemoteGroups filter [45](#)  
AllowedRemoteUsers filter [45](#)  
AllowedUsers filter [44](#), [46](#), [48](#)  
AllowedUsers parameter [52](#)  
ARM  
    definition [17](#)  
    for Cisco PIX Firewall [24](#)

arm directory [33](#)  
armname directory [34](#)  
audit events [24](#)  
audit trail files [24](#)  
audit trails [25](#)  
auditing [24](#)

## B

Business Hours stanza [18](#), [40](#)

## C

copying security policies [22](#)  
Customer Care  
    contacting [xiv](#)  
CyberCop Server ARM  
    Developer's Guide [23](#)

---

## D

default security policy [22](#)

Defaults stanza [18](#), [41](#)

DisableLogin response [20](#), [45](#), [47](#) to [48](#), [50](#), [52](#), [54](#),  
[56](#), [58](#), [60](#), [62](#), [64](#), [66](#)

distributing security policies [22](#)

## E

Email notification [20](#)

Email response [45](#), [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#), [63](#),  
[65](#), [67](#)

EmailAddress in Defaults stanza [41](#)

evaluation version [29](#)

Event Viewer [26](#)

## F

filters

    AllowedGroups [44](#)

    AllowedRemoteAddrs [45](#)

    AllowedRemoteGroups [45](#)

    AllowedRemoteUsers [45](#)

    AllowedUsers [44](#)

Fixit ARM [23](#)

    delete bad files [23](#)

    move corrupt files [23](#)

    restore files [23](#)

fixit.html [23](#)

fixit.txt [23](#)

## H

hardware requirements [30](#)

## I

Illegal File Access stanza [19](#), [51](#)

Illegal Jumper stanza [19](#), [48](#)

Illegal Login stanza [19](#), [44](#)

Illegal Privilege Escalation Stanza (UNIX Only) [46](#)

Illegal Privilege Escalation stanza (UNIX Only) [19](#)

incident stanzas [18](#) to [19](#)

    Illegal File Access [19](#)

    Illegal Jumper [19](#)

    Illegal Login [19](#)

    Illegal Privilege Escalation [19](#)

    Password Rattling [19](#)

    Self-Defense [19](#)

    System Access [19](#)

    System Attack [19](#)

    System Exploitation [19](#)

    System Probe [19](#)

    User Covering Tracks [19](#)

installing ARMs

    Solaris [34](#)

    Windows NT [34](#)

installing ARMs after Server installation [33](#)

installing the Server

    Solaris [32](#)

    Windows NT [30](#)

## K

KillLogin response [20](#), [45](#), [47](#) to [48](#), [50](#), [52](#), [54](#), [56](#), [58](#), [60](#), [62](#), [64](#), [66](#)  
KillProcess response [20](#), [47](#) to [48](#), [50](#), [52](#), [54](#), [56](#), [58](#), [60](#), [62](#), [64](#), [66](#)

## M

manual conventions [xii](#)

## N

Network Associates  
    contacting  
        Customer Care [xiv](#)  
        within the United States [xiv](#)

NIS [30](#)

notifications [20](#)  
    Email [20](#)  
    Pager [20](#)  
    PopupMessage [21](#)  
    ReportFile [20](#)  
    SNMPtrap [20](#)  
    Syslog [20](#)

## O

online Help [xiii](#)  
operating system kernel [25](#)  
operating systems, supported [30](#)

## P

Pager notification [20](#)  
Pager response [45](#), [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#), [63](#), [65](#), [67](#)  
pager script  
    configuring [39](#)  
    configuring, UNIX [39](#)  
    configuring, Windows NT [39](#)

PagerScript in Defaults stanza [41](#)

Password Rattling stanza [19](#), [54](#)

permanent version [29](#)

pix.html [24](#)

pix.txt [24](#)

PopupMessage notification [21](#)

PopupMessage response [46](#) to [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#), [63](#), [65](#), [67](#)

preinstallation requirements [29](#)

privileged access [30](#)

ProtectPathOnly filter [52](#)

ProtectPathSubdirs filter [52](#)

## R

Report response [46](#) to [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#), [63](#), [65](#), [67](#)

ReportFile in Defaults stanza [41](#)

ReportFile notification [20](#)

responses [20](#)

    DisableLogin [20](#)

    KillLogin [20](#)

    KillProcess [20](#)

    ShunLogin response [20](#)

responses in incident stanzas [43](#)

## S

security event log [24](#)

security policy [18](#)

    configuring [39](#)

    creating [37](#)

    creating, UNIX [37](#)

    creating, Windows NT [38](#)

    stanzas [35](#)

    validating [22](#)

---

security.txt [33](#)  
Self Defense stanza [19](#), [50](#)  
ShunInterval in Defaults stanza [42](#)  
ShunLogin response [20](#), [45](#), [47](#), [49](#) to [50](#), [52](#), [54](#), [56](#),  
[58](#), [60](#), [62](#), [64](#), [66](#)  
SNMP script  
    configuring [39](#)  
    configuring, UNIX [39](#)  
    configuring, Windows NT [39](#)  
SNMPScript  
    in Defaults stanza [42](#)  
SNMPtrap notification [20](#)  
SNMPTrap response [45](#), [47](#), [49](#) to [50](#), [52](#), [55](#), [57](#), [59](#),  
[61](#), [63](#), [65](#), [67](#)  
stanza format [36](#)  
stanzas  
    definition [18](#)  
Syslog notifications [20](#)  
Syslog response [45](#), [47](#), [49](#), [51](#), [53](#), [55](#), [57](#), [59](#), [61](#),  
[63](#), [65](#), [67](#)  
SyslogName in Defaults stanza [41](#)  
System Access stanza [19](#), [56](#)  
System Attack stanza [19](#), [60](#)  
system calls [25](#) to [26](#)  
System Exploitation stanza [19](#), [58](#)  
System Misuse stanza [64](#)  
System Probe stanza (UNIX only) [19](#), [62](#)

## T

technical support  
    e-mail address [xiv](#)  
    information needed from user [xv](#)  
    online [xiv](#)

Tivoli TME 10 ARM [24](#)  
tme.html [24](#)  
tme.txt [24](#)

## U

UNIX  
    new security policy [22](#)  
    Popup Message notification [21](#)  
UNIX audit trails [26](#)  
User Covering Tracks stanza [19](#), [66](#)

## V

validating security policy [22](#)  
variables  
    \$administrator [21](#)  
    \$cybercopserverdir [21](#)  
    \$hostname [21](#)  
    \$systemdrive [21](#)  
    \$windir [21](#)

## W

Windows NT  
    new security policy [22](#)  
    Popup Message notification [21](#)  
Windows NT audit trails [26](#)



