



Access Security for IT Administrators

- Secure all Citrix Presentation Server and Password Manager Components
- Learn how to implement effective countermeasures for every type of threat
- Understand secure deployment scenarios and administrative best practices

Citrix Product Development Team



Osborne

Foreword by Brad Pedersen, Chief Architect and
Senior Fellow, Citrix Systems, Inc.

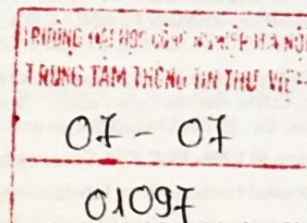
Citrix® Access Security for IT Administrators

CITRIX PRODUCT DEVELOPMENT TEAM



GIFT OF THE ASIA FOUNDATION
NOT FOR RE-SALE

QUÀ TẶNG CỦA QUỸ CHÂU Á
KHÔNG ĐƯỢC BÁN LẠI



**Mc
Graw
Hill**

New York ~~Chicago~~ San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi San Juan Seoul Singapore Sydney Toronto

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, Professional Publishing, McGraw-Hill, Two Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.

Citrix® Access Security for IT Administrators

Copyright © 2007 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

1 2 3 4 5 6 7 8 9 0 DOC DOC 0 1 9 8 7 6

ISBN-13: 978-0-07-148543-2

ISBN-10: 0-07-148543-0

Sponsoring Editor

Wendy Rinaldi

Editorial Supervisor

Janet Walden

Project Manager

Patricia Wallenburg

Acquisitions Coordinator

Mandy Canales

Copy Editor

Eric Lowenkron

Proofreader

Paul Tyler

Indexer

Karin Arrigoni

Production Supervisor

Jean Bodeaux

Technical Editor

Kyle Randolph

Composition

Patricia Wallenburg

Illustration

Patricia Wallenburg

Art Director, Cover

Jeff Weeks

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill, or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

This Volume is for informational purposes only, and is primarily geared toward users of Citrix brand products located in North America. As the user may know, data security, in addition to being a practical concern, is fast becoming an issue of legal compliance. This Volume does not constitute legal advice and should not be relied upon for legal compliance purposes.

CITRIX MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THIS VOLUME FOR ANY PURPOSE. THIS VOLUME IS PROVIDED "AS IS." CITRIX HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS VOLUME AND THE INFORMATION CONTAINED HEREIN, INCLUDING ALL WARRANTIES AND CONDITIONS OF ACCURACY, TIMELINESS, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. THE CONTENT, ADVICE AND STRATEGIES IN THIS VOLUME MAY NOT BE APPROPRIATE FOR EVERY SITUATION OR LEGAL JURISDICTION. CITRIX IS NOT IN THE BUSINESS OF RENDERING PROFESSIONAL LEGAL OR LEGAL COMPLIANCE ADVICE. USERS ARE URGED TO CONSULT WITH OUTSIDE LEGAL PROFESSIONALS IF NECESSARY. IN NO EVENT SHALL CITRIX BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION AVAILABLE IN THIS VOLUME. THIS VOLUME MAY MAKE REFERENCE TO OTHER PRODUCTS, SERVICES OR WEB SITES. CITRIX DOES NOT ENDORSE ANY OTHER PRODUCT, SERVICE OR SOURCE OF INFORMATION. THIS VOLUME COULD INCLUDE TECHNICAL INACCURACIES OR ERRORS. CITRIX MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE SERVICES AND PROGRAM(S) DESCRIBED IN THIS VOLUME AT ANY TIME.

Citrix, ICA (Independent Computing Architecture), and Program Neighborhood are registered trademarks, and Citrix Presentation Server, Citrix Access Suite, Citrix Password Manager, Citrix Developer Network, and SpeedScreen are trademarks of Citrix Systems, Inc. in the United States and other countries.

RSA Encryption © 1996–1997 RSA Security Inc. All Rights Reserved.

DB2 is a registered trademark of International Business Machines Corp. in the U.S. and other countries.

Java is a registered trademark of Sun Microsystems, Inc. in the U.S. and other countries. Solaris is a registered trademark of Sun Microsystems, Inc. Sun Microsystems, Inc. has not tested or approved this product.

Microsoft, MS-DOS, Windows, Windows Media Player, Windows Server, Windows NT, Win32, Outlook, Outlook Express, Internet Explorer, ActiveX, Active Directory, Access, SQL Server, SQL Server Express Edition, and DirectShow are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle database is a registered trademark of Oracle Corporation.

All other trademarks and registered trademarks are the property of their owners.

AT A GLANCE



▼ 1	Introduction	1
▼ 2	Secure Deployments	11
▼ 3	Administrative Best Practices	31
▼ 4	Secure Gateway	43
▼ 5	Web Interface	65
▼ 6	Password Manager	91
▼ 7	Presentation Server	125
▼ 8	Presentation Server Client	191
▼ 9	License Server	213
▼ A	Other Citrix Solutions	231

▼ B	Checklists	239
▼ C	Additional Resources	245
▼ D	SSL/TLS Certificate Installation	251
▼	Index	255

CONTENTS

Foreword	xv
▼ 1 Introduction	1
How to Use This Book	2
Threat Modeling	2
Components	3
Assets	3
Security Characteristics	4
Confidentiality	4
Integrity	4
Countermeasures	7
Security Technologies	8
Cryptography	8
Digital Certificates	8
Auditing	9
Summary	9
▼ 2 Secure Deployments	11
Authentication	12
Password	13
Smart Card	13

Token	13
Biometric	13
Authentication Protocols	14
Secure Communications	14
SSL/TLS	14
HTTPS	15
IPsec	15
Secure Deployments	15
Web Interface in a DMZ with Secure Gateway for Windows Deployment	16
Secure Gateway in Front of Web Interface in a Single DMZ	19
Web Interface, Secure Gateway, and Secure Gateway Proxy in Two DMZs	22
Web Interface in DMZ with SSL Relay	24
Intranet Deployment	27
Summary	29
▼ 3 Administrative Best Practices	31
People	32
Physical Security	32
Password Policies	32
Least Privilege	33
Separation of Duties	33
Processes	33
Security Patch Management	34
Backup Policies	34
Incident Response Policies	35
Auditing Policies	36
Technology	36
Antivirus Software	37
Firewall Placement	37
Secure the File System	39
Windows Group Policy	39
Certificate Management	40
Summary	41
▼ 4 Secure Gateway	43
Deployments	44
Components	44
Secure Gateway	44
Secure Gateway Proxy	47
Secure Gateway Assets	47
Threats and Countermeasures	49

Service Disruption	49
Unauthorized Access to the Secure Gateway	50
Compromise of Client to Gateway Session Data	51
Compromise of Secure Gateway to Presentation Server Session Data	51
Compromise of Session Data Between Secure Gateway and Secure Gateway Proxy	52
Compromise of Session Data Between Secure Gateway/ Secure Gateway Proxy and Secure Ticket Authority	52
Compromise of Session Data Between Secure Gateway and the Web Interface	53
Compromise of Session Data Between Client Web Browser and Web Interface	53
Tampering with Secure Gateway Configuration	53
Unauthorized Access to Log Files	54
Worms, Viruses, and Other Malicious Software	55
Steps for Securing Secure Gateway	56
Secure the Operating System	56
Install Secure Gateway as a Nonprivileged User	58
Configure the Secure Gateway Configuration Wizard	58
Restrict Access to Secure Gateway	60
Enable IPsec Between Secure Gateway and Presentation Server	61
Protect Log Files	61
Configure Auditing	61
Verify Secured Configuration	62
Summary	63
▼ 5 Web Interface	65
Deployments	66
Components	69
Web Interface	69
Web Interface Configuration File	69
Access Suite Console	69
ICA File	69
Assets	72
Threats and Countermeasures	72
Unauthorized Access to Web Interface	72
Service Disruption	73
Disclosure of ICA File	74
Tampering with Configuration Files	75
Profiling	75
Worms, Viruses, and Other Malicious Software	76

Steps for Securing Web Interface Server	77
Secure the Operating System	77
Restrict Access to Web Interface Server	82
Configure Authentication	82
Secure Link between Web Interface and Presentation Server	83
Secure Link between Web Interface and Secure Gateway	85
Secure Web Interface for Use with Program Neighborhood Agent	85
Protect Log Files	86
Configure Auditing	87
Verify Secured Configuration	87
Summary	90
▼ 6 Password Manager	91
Deployments	92
Components	92
Password Manager Agent	92
Central Store	97
Password Manager Console	97
Password Manager Service	97
Password Manager Application Definition Tool	98
Assets	98
Threats and Countermeasures	99
Tampering with Administrative Data on Password Manager Agent	99
Disclosure of Secondary Credentials to Attackers	100
Disclosure of Secondary Credentials to Users	100
Tampering with Administrative Data in Transit	100
Tampering with Secondary Credentials in Transit	101
Disclosure of Secondary Credentials on Central Store	101
Tampering with Secondary Credentials on Central Store	102
Disclosure of Password Manager Service Data	102
Disclosure of Secondary Credentials in Transit	103
Service Disruption	103
Steps for Securing Password Manager Agent	104
Configure Password Manager with Smart Cards	104
Create Secure User Configuration	105
Configure Secure User Configuration	106
Create Secure Password Policy	109
Steps for Securing Password Manager Service	110
Secure the Operating System	110
Enable Data Integrity Module	114

Configure Auditing	114
Secure Password Manager Service Data	115
Steps for Securing Central Store	115
Secure the Operating System	115
Secure NTFS Network Share Central Store	118
Secure Active Directory Container Central Store	119
Verify Secured Configuration	123
Summary	123
▼ 7 Presentation Server	125
Deployments	126
Session Reliability	126
Components	126
Access Suite Console	127
Citrix Connection Configuration Utility	130
Configuration Manager	130
CPU Utilization Manager	130
Client Network	131
Diagnostic Facility COM Server	131
Encryption Service	131
Independent Management Architecture Service	131
Installation Manager	131
Citrix WMI Service	131
Load Manager	131
Memory Optimization	132
MFCOM	132
Network Manager	132
Pass-Through Client	132
Presentation Server Console	132
Presentation Server Management Pack for Microsoft	
Operations Manager	133
Print Manager Service	133
Resource Manager	133
Secure Ticket Authority	134
SSL Relay	134
Suite Monitoring and Alerting Service	134
Windows Management Instrumentation Provider	134
XML Service	134
XTE Server	134
Accounts	135
Anonymous Accounts	135
Service Accounts	135
Citrix Administrator	135

Assets	136
Presentation Server	136
Presentation Server Machine	137
ICA Session	138
Threats and Countermeasures	138
Presentation Server	138
Presentation Server Machine	141
ICA Session	143
Steps for Securing the Presentation Server	145
Secure the Operating System	145
Configure Authentication	149
Configure Secure Communications	152
Configure Client Drive Mapping	156
Configure Clipboard Mapping	157
Configure Client Device Mapping	159
Secure the IMA Data Store	161
Configure Citrix Administration Accounts	162
Configure Citrix Connection Configuration	164
Configure Terminal Services Configuration	165
Configure Presentation Server Policies	166
Configure Group Policy for the Presentation Server	171
Secure the SNMP Configuration	177
Secure IMA Communication	178
Access the Presentation Server Console Only as a Published Application	178
Access the Access Suite Console Only as a Published Application	178
Secure Printer Connections	179
Configure Installation Manager Deployments	180
Secure the XML Service and Secure Ticket Authority	181
Only Launch Published Applications	183
Secure the Pass-Through Client	184
Run Published Applications Only as a Nonprivileged User	184
Remove Remote Desktop Protocol Access	184
Disable Administrative Shares	185
Configure Auditing	185
Verify the Secured Configuration	187
Summary	190
▼ 8 Presentation Server Client	191
Deployments	192
Components	192

Pass-Through Client	192
Program Neighborhood	196
Program Neighborhood Agent	196
Web Client	196
Assets	196
Threats and Countermeasures	197
Disclosure of Password	197
Disclosure of ICA Session Data	198
Disclosure of Client Files	198
Malicious Servers	198
Unauthorized Access to Client Devices	198
Tampering with Client Files	199
Tampering with Client Configuration	199
Disclosure of Password	198
Steps for Securing Presentation Server Client	200
Configure Authentication	200
Configure Secure Communications	204
Run the Client Only as a Nonprivileged User	208
Disable Client Drive Mapping	208
Disable Undesired Device Mappings	208
Disable Bitmap Disk Cache	210
Verify the Secured Configuration	210
Summary	211
▼ 9 License Server	213
Deployments	214
Components	214
Citrix License Server	214
License Files	214
License Management Console	214
License Administration Commands	216
License Server Options File	216
Assets	216
Threats and Countermeasures	216
Service Disruption	217
Unauthorized Access to the License Server Service	217
Worms, Viruses, and Other Malicious Software	218
Steps for Securing the Citrix License Server	219
Secure the Operating System	219
Download License Files	222
Protect the License Files	223
Protect the Log Files	224
Restrict Access to the License Management Console	225

Isolate the Citrix License Server Behind a Firewall	227
Configure Auditing	228
Verify the Secured Configuration	229
Summary	230
▼ A Other Citrix Solutions	231
▼ B Checklists	239
▼ C Additional Resources	245
▼ D SSL/TLS Certificate Installation	251
▼ Index	255