Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted

ICM Software Releases 7.x(y)

October 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

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

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

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

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

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Table of Contents

Preface 1
- Purpose 1
- Audience 2
- Organization 2
- Related Documentation 3
- Conventions.....4
- Obtaining Documentation and Submitting a Service Request.....4
- Documentation Feedback.....5

1. Encryption Support.....7
- User and Agent Passwords.....7
- Call Variables and Extended Call Variables.....7
- Internet Script Editor, Agent Reskilling and WebView.....8
- CTI OS C++/COM Toolkit.....8
- Cisco Contact Center SNMP Management Service.....9
- Cisco Support Tools.....9
- Additional Encryption.....9

2. IPSec and NAT Support.....11
- About IPSec.....11
- About NAT.....12
- Support for IPSec (IP Security) in Tunnel Mode.....12
- Support for IPSec (IP Security) in Transport Mode.....13
  - System Requirements.....13
  - Supported Communication Paths 13
  - Configuring IPSec Policy.....15
- IPSec Connection to Cisco CallManager.....17
- Monitoring IPSec Activity.....17
  - IPSec Monitor.....17
  - IPSec Logging.....17
  - Network Monitoring.....18
  - System Monitoring 18
- Securing Support Tools Using IPSEC.....19
- Support Tools IPSEC Configuration Example.....?
- Support for NAT (Network Address Translation).....20
- NAT and CTI OS.....20
- IPSec and NAT Transparency.....21
- Additional IPSec References.....21

3. Applying IPSec with the Network Isolation Utility.....23
- About IPSec.....23
- Deploying IPSec Manually Versus Deploying It Via the Network Isolation Utility.....24
- About the Cisco Network Isolation Utility.....24
- An Illustration of Network Isolation Utility Deployment.....25
- How the Network Isolation Utility Works.....25
  - IPSec Terminology.....25
  - The Network Isolation Utility Process.....26
- About Encrypting Traffic.....27
- How to Deploy the Network Isolation Feature.....27
  - Important Deployment Tips.....28

Sample Deployment.....28
Devices That Must Communicate with One Another.....33
Typical Boundary Devices.....34
Caveats.....36
How to Do a Batch Deployment.....37
How to Run the Network Isolation Utility from the Command Line.....37
How to Monitor the Network Security.....42
Troubleshooting the Network Isolation IPSec Policy.....42

4. Windows Server 2003 Firewall Configuration.....43
Cisco Firewall Configuration Utility Prerequisites.....44
Using the Cisco Firewall Configuration Utility.....45
Verifying New Windows Firewall Settings.....45
Configuring Windows Server 2003 Firewall to Communicate With Active Directory.....46
Configuring Domain Controller Ports.....46
Restrict FRS Traffic to a Specific Static Port.....46
Restrict Active Directory replication traffic to a specific port.....47
Configure Remote Procedure Call (RPC) port allocation.....47
Windows Server 2000 and 2003 Firewall Ports.....47
Testing Connectivity.....48
Validating Connectivity.....48
Understanding the CiscoICMfwConfig_exc.xml File.....49
Troubleshooting Windows Firewall.....50
General Troubleshooting Notes.....50
Windows Firewall Interferes with Router Private Interface Communication.....50
Windows Firewall Shows Dropped Packets but no ICM or IPCC Failures are Evident.....50
Undo Firewall Settings.....51

5. Automated Security Hardening Settings on Windows Server 2003.....53
Applying/Removing Cisco ICM Security Settings.....54
Applying Cisco ICM Security Settings During Setup.....54
Manually Installing Cisco ICM Security Settings.....55
Rolling Back Security Settings.....55
Account Policies Settings.....56
Password Policy.....56
Account Lockout Policy.....57
Kerberos Policy.....57
Local Policies.....57
Audit Policy.....57
User Rights Assignment.....58
Security Options.....61
Event Log.....70
System Services.....70
Settings for System Services.....71
Registry.....77
File System.....78

6. Applying Security with the Cisco Unified Contact Center Security Wizard.....81
About the Cisco Unified Contact Center Security Wizard.....81
Configuration and Restrictions.....82
How to Install the Wizard.....82
How to use the Wizard.....83
Example Security Wizard Usage.....85

Example Security Hardening Configuration Panels....86
Example Windows Firewall Configuration Panels....88
Example Network Isolation Configuration Panels....92

7. Updating Microsoft Windows 97
Microsoft Security Updates....97
Microsoft Service Pack Policy....98
Configuring the Server to use an Alternate Windows Update Server....99

8. SQL Server Hardening....101
SQL Server Hardening Suggestions....101
Top Hardening Suggestions....101
SQL Server Users and Authentication....104
SQL Server 2005 Security Considerations....105
Automated SQL 2005 Hardening....105
SQL Server Security Hardening Utility....106
Manual SQL 2005 Server Hardening....107

9. Cisco SSL Encryption Utility....109
About the SSL Encryption Utility....109
Installing SSL During Setup....110
SSL Encryption Utility in Standalone Mode....110
Enabling the Transport Layer Security (TLS) 1.0 Protocol....112

10. Intrusion Prevention and Cisco Security Agent....113
What are Cisco Security Agent Policies?....113
Types of Agents....114
Managed Agent....114
Standalone Agent....114

11. Microsoft Baseline Security Analyzer (MBSA)....115
Security Update Scan Results....116
Windows Scan Results....116
Internet Information Services (IIS) Scan Results....117
SQL Server Scan Results....118
Desktop Application Scan Results....119

12. Auditing 121
How to View Auditing Policies....121
Security Log....122
Real-Time Alerts....122
SQL Server Auditing Policies....122
SQL Server C2 Security Auditing....122
Active Directory Auditing Policies....123

13. General Anti-Virus Guidelines and Recommendations....125
Guidelines and Recommendations....126
ICM/IPCC Software Maintenance Parameters....127
Logger Recommendations 127
Distributor Recommendations....127
Router and PG Recommendations....128
Other Scheduled Tasks Recommendations....128
File Type Exclusion Recommendations....128

14. Remote Administration....129

Windows Terminal Services (Remote Desktop)....129
Remote Desktop....130
Securing the RDP-TCP Connection....130
Per-User Terminal Services Settings....131
pcAnywhere....131
Restricting access to internal machines....132
Preventing unauthorized connections to a pcAnywhere host....132
Protecting the data stream during a remote control session....134
Preventing unauthorized changes to the installed product....134
Identifying security risks....134
Logging events during a remote control session....135
VNC....135
TRIDIA VNC Pro....135

15. Additional Security Best Practices....137
Additional Cisco Call Center Applications....137
Cisco ICM WebView....137
Cisco ICM CTI Object Server (CTI OS)....138
Cisco Agent Desktop (CAD)....138
Cisco ICM Router....138
Peripheral Gateways (PGs) and IPCC Enterprise Agent Login....139
CTI OS and Monitor Mode Connection....139
Microsoft Internet Information Server (IIS)....139
Hardening IIS for use with WebView and Internet Script Editor on Windows 2000 Platforms....139
Sybase EAServer (Jaguar) Hardening....142
Starting Jaguar Manager....142
Changing Jaguar Password....143
Restart WebView/Services....144
RMS Listener Hardening....144
WMI Service Hardening....145
WMI namespace-level security:....145
Additional WMI Security Considerations....146
SNMP Hardening....146
Toll Fraud Prevention....147
Syskey....148
Third-Party Security Providers....148
Third-Party Management Agents....148

List of Figures

Figure 1: Example Network Isolation Deployment....25

Figure 2: Example Contact Center Enterprise System....29

Figure 3: Example Phase 1 - Step 1 IPSec Deployment....29

Figure 4: Example Tusted Device Isolation....30

Figure 5: Example Phase 1 - Step 2 IPSec Deployment....30

Figure 6: Example Phase 1 - Step 3 IPSec Deployment....31

Figure 7: Example Phase 2 - Step 1 IPSec Deployment....31

Figure 8: Example Phase 2 - Step 2 IPSec Deployment....32

Figure 9: Example IPSec Deployment - Overall Design....32

Figure 10: Example Security Wizard Welcome Panel....85

Figure 11: Example Security Hardening Introduction Panel....86

Figure 12: Example Security Hardening Template Options Panel....86

Figure 13: Example Security Hardening Confirmation Panel....87

Figure 14: Example Security Hardening Status Panel....88

Figure 15: Example Windows FireWall Wizard Introduction Panel....88

Figure 16: Example Firewall Configuration Options Panel....89

Figure 17: Example Firewall Confirmation Panel....90

Figure 18: Example Firewall Status Panel....91

Figure 19: Example Network Isolation Introductory Panel....92

Figure 20: Example Trusted Devices Configuration Panel....93

Figure 21: Example Boundary Device Panel....94

Figure 22: Example Network Isolation Confirmation Panel....95

Figure 23: Example Network Isolation Status Panel....95

Figure 24: SSL Config Utility - Configuration Tab....111

Figure 25: SSL Config Utility - Certificate Administration Tab....111

Preface

Purpose

This document describes security hardening configuration guidelines for Cisco ICM Software Release 7.x(y) on Windows Server 2003. The term "ICM software" includes: IP Contact Center (IPCC) Enterprise and Hosted Editions, System IPCC, and ICM Enterprise and Hosted Editions. Optional ICM applications applying to these server configurations are also addressed here, with the exception of the following: Web Collaboration Option Collaboration Server, Media Blender (when not co-resident with a PG; if co-resident with a PG then these best practices are applicable), Dynamic Content Adapter and E-mail Manager Option. References throughout this document to "ICM/IPCC" will assume the aforementioned configurations. Any accompanying applications making up the customer's particular solution, whether Cisco provided - such as PSO applications - or provided by a Cisco partner, have not been approved for use with these security hardening recommendations. Special testing and qualification must be considered to ensure that recommended security configurations do not hinder the operation of those applications.

The configurations presented in this document represent parameters used internally within Cisco to develop and test the applications. Other than the base Operating System and applications' installations, any deviation from this set cannot be guaranteed to provide a compatible operating environment. It is important to note recommendations contained in this document will not always be uniformly implemented; some implementations - as based on corporate policy, specific IT utilities (e.g., backup accounts) or other external guidelines - may modify or limit the application of these guidelines.

Note: Security Hardening for Release 7.x(y) is supported on Windows 2003 only when the server has been hardened using the 6.0 guidelines. You cannot upgrade a non-hardened Windows 2000 server from ICM 5.0 or 6.0 to ICM 7.x(y) and then apply hardening. First harden the Windows 2000 Server running a previous version of ICM before upgrading to 7.x(y). The other option is to upgrade the Operating System to Windows Server 2003 after upgrading the ICM/IPCC software and then applying the automated hardening described in this guide.

Audience

This document is primarily intended for server administrators and OS and application installers.

It is assumed that the target reader of this document is an experienced administrator familiar with Windows 2003 and Windows Server 2003 installations. It is further assumed that the reader is fully familiar with the applications making up the ICM/IPCC solution, as well as with the installation and administration of these systems. It is the intent of these best practices to additionally provide a consolidated view of securing the various third-party applications on which the Cisco contact center applications depend. Should vendor recommendations differ from these guidelines, following such recommendations may result in systems that are not protected from malicious attacks.

Organization

This document is organized into the following chapters:

Chapter	Description
Encryption Support	A brief overview of the encryption methods used in ICM/IPCC
IPSec and NAT Support	Security Best Practices of deploying IPSec and NAT in an ICM/IPCC Environment.
Windows Server 2003 Firewall Configuration	The use of Windows Firewall and details about Cisco's Windows Firewall configuration script.
Automated Security Hardening Settings on Windows Server 2003	Specific details of the settings changed when using the Cisco Security Template.
Updating Microsoft Windows	Security Best Practices to use when updating Windows Server 2003.
SQL Server Hardening	Security Best Practices for SQL Server
Cisco SSL Encryption Utility	Details on using the SSL Encryption Utility
Intrusion Prevention and Cisco Security Agent	Using Cisco Security Agent for Host Intrusion Detection.
Microsoft Baseline Security Analyzer (MBSA)	Example of what to expect when running MBSA on a typical ICM Server.
Auditing	Security Best Practices for setting Auditing Policies on ICM/IPCC Servers.
General Anti-Virus Guidelines and Recommendations	General Anti-Virus Guidelines and Recommendations

Chapter	Description
Remote Administration	Security Best Practices to consider when using various remote administration applications.
Additional Security Best Practices	Additional Security Best Practices on: • Additional Cisco Call Center Applications • Microsoft Internet Information Server • Sybase EAServer (Jaguar) • RMS Listener Hardening • WMI Service Hardening • SNMP Service Hardening • Toll Fraud Prevention • Syskey • Third-party Security Providers • Third Part Management Agents

Related Documentation

The recommendations contained herein are based in part on hardening guidelines published by Microsoft, such as those found in the Windows Server 2003 Security Hardening Guide, as well as other third-party vendors' hardening recommendations. A number of recommendations are made fully consistent with supporting Microsoft guidelines; our intent is to further interpret and customize those guidelines as specifically applicable to the ICM/IPCC server products.

This document should be used in conjunction with the Planning and Staging Guides that are part of the ICM/IPCC documentation. It should further be used as a reference standard for all customers requiring verification that certain security configuration changes to the base operating system and contact center application servers have been certified for use with the ICM/IPCC applications. The average time to execute the majority of the steps has been reduced significantly due to the automation and integration with the impacted products installation programs.

More information can be found in the following documents:

- *Staging Guide: Cisco ICM/IPCC Enterprise & Hosted Editions*
- **Microsoft Windows Server 2003 Security Hardening Guide** (http://www.microsoft.com/technet/security/prodtech/windowsserver2003/W2003HG/SGCH00.mspx)

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Chapter 1

Encryption Support

This section describes the types of encryption used in the ICM system. The concepts should aid you in understanding how encryption is used in the ICM/IPCC environment.

This chapter contains the following topics:

- User and Agent Passwords, page 7
- Call Variables and Extended Call Variables, page 7
- Internet Script Editor, Agent Reskilling and WebView, page 8
- CTI OS C++/COM Toolkit, page 8
- Cisco Contact Center SNMP Management Service, page 9
- Cisco Support Tools, page 9
- Additional Encryption, page 9

User and Agent Passwords

Cisco ICM/IPCC systems are highly distributed applications composed of many node and server applications. Applications users' and contact center agents' passwords are stored in the Cisco ICM Logger databases as well as the Distributor databases as an RSA Data Security, Inc. MD5 Message-Digest Algorithm hash. When passed from one server node to another, such as from a Peripheral Gateway to a Router, or from a Distributor to a Router or a Logger, they are passed as MD5 hashes as opposed to clear text.

Call Variables and Extended Call Variables

To protect data sent in call variables or ECC variables, Cisco ICM relies on IPSec and the deployment of IPSec policies between servers running Windows Server 2003. In an IPCC environment, the establishment of an IPSec channel between the Cisco Call Manager and the Peripheral Gateway is also supported. The recommended integrity algorithm is SHA-1 and the encryption algorithm is 3DES. The recommended IKE security algorithm is a minimum of Diffie-Hellman Group 2 for a 1024-bit key or 2048-bit key if processing power allows it.

See Also

IPSec and NAT Support on page 11

Internet Script Editor, Agent Reskilling and WebView

Release 7.x(y) of Cisco ICM supports, as a default on Windows 2003 Server, the encryption of traffic for users accessing the ICM Internet Script Editor, Agent Reskilling, and WebView applications so that all user logins and optionally session traffic done from a remote machine are protected from snooping. The applications are HTTP based that implement the SSL v3.0 protocol using the OpenSSL libraries.

The Agent Reskilling and Internet Script Editor web applications will also be deployed and enabled for 128-bit SSL encryption in IIS 6.0 as a default so that all supervisor logins, user logins, and data exchanged is protected across the network.

For WebView, the authentication phase is encrypted with 128-bit encryption by default. As an option, users may decide to encrypt the entire session which may be done during installation or afterwards using the SSL Encryption Utility.

For more information on enabling certain Cipher Suites in IIS see: **http://support.microsoft.com/?kbid=245030**

See Also

Cisco SSL Encryption Utility on page 109
Cisco WebView Documentation

CTI OS C++/COM Toolkit

The CTI OS (C++/COM toolkit) and CAD agent desktops implement TLS v1.0 protocol using the OpenSSL libraries to protect data exchanged from the agent desktop to the CTI Object Server. A Cipher suite is used for authentication, key exchange, and stream encryption. The Cipher suite is as follows:

- Key exchange: Diffie-Hellman
- Authentication: RSA
- Encryption: AES (128)
- Message digest algorithm: SHA1

Refer to the CTI OS System Manager's Guide and Cisco CAD Installation Guide for more configuration details.

Cisco Contact Center SNMP Management Service

The ICM/IPCC software includes an SNMP v3 agent to support authentication and encryption (privacy) provided by *SNMP Research International*. Cisco's implementation exposes the configuration of the communication with a management station to be authenticated using the MD5 or SHA-1 digest algorithms, and for all SNMP messages to be encrypted using one of the following three protocols: 3DES, AES-192, or AES-256.

See Also

SNMP Hardening on page 146
SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions

Cisco Support Tools

The Cisco Support Tools for Cisco IPCC is a serviceability application that is deployed with SSL enabled by default. This ensures all data exchanged from the browser to the server and vice versa as well as user logins are encrypted with 128-bit encryption.

Additional Encryption

In addition to the various areas of application level encryption provided in the Cisco ICM suite of applications, Cisco supports the deployment of the solution across sites running Cisco IOS(TM) IPSec in Tunnel Mode with HMAC-SHA1 Authentication (ESP-SHA-HMAC) and 3DES Encryption (ESP-3DES).

See Also

IPSec and NAT Support on page 11

Chapter 2

IPSec and NAT Support

About IPSec

Internet Protocol security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services.

Note: IPSec can be deployed in many different ways. The purpose of this chapter is to explain what IPSec is and how to secure **selected communication paths** using IPSec. The chapter on Applying IPSec with the Network Isolation Utility (page 23) explains a specific, more restricted, but automated way of applying IPSec to secure the **entire** traffic to and from the server. The Network Isolation Utility can also save you a lot of work in applying IPSec. However, if you use that utility to apply IPSec, you should also read this chapter to understand the various IPSec deployment options and to use the one that is the most beneficial for your environment.

For more information, see **http://www.cisco.com/go/ipsec** and **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_IPSECtopnode.asp**

Implementing IPSec in an ICM or IPCC environment means finding a balance between ease of deployment and usability, and protecting sensitive information from unauthorized access.

Finding the proper balance requires:

- Assessing the risk and determining the appropriate level of security for your organization.
- Identifying valuable information.
- Defining security policies that use your risk management criteria and protect the identified information.
- Determining how the policies can best be implemented within the existing organization.

- Ensuring that management and technology requirements are in place.

Security considerations are also influenced by the way the application will be used or deployed. For example, the required security might differ, depending on whether certain ICM/IPCC servers will be deployed in a single data center or across a number of sites which may or may not communicate across trusted networks. The security framework in Windows Server 2003 is designed to fulfill the most stringent security requirements. However, software alone might be less effective without careful planning and assessment, effective security guidelines, enforcement, auditing, and sensible security policy design and assignment.

About NAT

Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As its name implies, NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network.

The section in this chapter beginning with Support for NAT (Network Address Translation) (page 20) describes the ICM and IPCC NAT support.

Support for IPSec (IP Security) in Tunnel Mode

Due to increased security concerns in the deployment of data and voice networks alike, ICM and IPCC Enterprise deployments now add support for IPSec between Central Controller sites and remote Peripheral (PG) sites. This secure network implementation implies a distributed model where the WAN connection is secured via IPSec tunnels. The testing undertaken in this release was limited to configuration of Cisco IOS(TM) IPSec in Tunnel Mode, meaning only the Cisco IP Routers (IPSec peers) between the two sites were part of the secure channel establishment. All data traffic is encrypted across the WAN link but un-encrypted on the local area networks. In tunnel mode, traffic flow confidentiality is ensured between IPSec peers which, in this case, are the IOS Routers connecting a central site to a remote site.

The qualified specifications for the IPSec configuration are as follows:

- HMAC-SHA1 Authentication (ESP-SHA-HMAC)
- 3DES Encryption (ESP-3DES)

We **highly** recommend that hardware encryption be used in order to avoid a **significant** increase in IP Router CPU overhead and throughput impact. There are also some latency implications, so it is important to size the network infrastructure (network hardware and physical links) accordingly. There are also considerations that must be taken for QoS networks. The common recommendation is to classify and apply QoS features based on packet header information before traffic is tunnel encapsulated and/or encrypted.

More detailed resources on Cisco IOS IPSec functionality can be found at **http://www.cisco.com/go/ipsec**

Support for IPSec (IP Security) in Transport Mode

System Requirements

System Requirements for IPSec Support in Transport Mode

- Cisco ICM Release 7.x
- Microsoft®) Windows®) Server 2003
- Intel PRO/100 S Server Adapter P/N PILA8470C3

Note:

- IPSec offload network adapters accelerate the cryptographic operations used to secure IPSec packets, therefore minimizing the performance costs for encryption. As a result, IPSec - secured TCP/IP connections can achieve similar throughput as TCP/IP connections that are not secured using IPSec. If the hardware acceleration cards cannot be used, then IPSec encryption will increase CPU load, and decrease throughput.
- ICM Release 7.x support for IPSec is contingent on the use of network interface cards which support IPSec offloads. The card listed in the System Requirements list is what has been tested and is recommended.

See Also

For more information about the benefits of using IPSec hardware offload adapters, see "Intel PRO/100S Network Adapter, IPSec Offload Performance and Comparison," at **http://www.veritest.com/clients/reports/intel/intelps.pdf**.

Supported Communication Paths

ICM Release 7.x supports deploying IPSec in a Windows Server 2003 operating environment to secure server to server communication. The support is limited to the following list of nodes which exchange customer sensitive data.

1. NAM Router - CICM Router
2. ICM Router Side A - ICM Logger Side A (visible path)
3. ICM Router Side B - ICM Logger Side B (visible path)
4. ICM Router Side A - ICM Router Side B (private path)
5. ICM Logger Side A - ICM Logger Side B (private path)

6. ICM Router - ICM Peripheral Gateway (PG)
   a. ICM Router Side A - ICM PG Side A
   b. ICM Router Side A - ICM PG Side B
   c. ICM Router Side B - ICM PG Side A
   d. ICM Router Side B - ICM PG Side B
7. ICM Router - ICM Real-time Distributor (Primary/Secondary)
   a. ICM Router Side A - ICM Real-time Distributor (Primary/Secondary)
   b. ICM Router Side B - ICM Real-time Distributor (Primary/Secondary)
8. ICM Logger - ICM Real-time Distributor (Primary/Secondary) with HDS
   a. ICM Logger Side A - ICM Real-time Distributor (Primary/Secondary) with HDS
   b. ICM Logger Side B - ICM Real-time Distributor (Primary/Secondary) with HDS
9. ICM PG Side A - ICM PG Side B
   a. visible path
   b. private path
10. ICM PG Side A/B - Cisco CallManager (IPCC)

For the server communication paths identified, the following security level should be considered a general basis for planning an IPSec deployment:

- **High security**

  Computers that contain highly sensitive data are at risk for data theft, accidental or malicious disruption of the system, or any public network communications. Secure Server (Require Security), a default policy, requires IPSec protection for all traffic being sent or received (except initial inbound communication) with stronger security methods. Unsecured communication with a non-IPSec-aware computer is not allowed.

See Also

Be sure to consult the Microsoft Knowledge Base article **IPSec default exemptions are removed in Windows Server 2003** (http://support.microsoft.com/kb/810207/EN-US/) for important information about changes in Windows Server 2003 IPSec support from Windows 2000 Server support of IPSec.

Configuring IPSec Policy

Windows Server 2003 IPSec policy configuration is the translation of security requirements to one or more IPSec policies.

Each IPSec policy consists of one or more IPSec rules. Each IPSec rule consists of:

- A selected filter list.
- A selected filter action.
- Selected authentication methods.
- A selected connection type.
- A selected tunnel setting.

There are multiple ways to configure IPSec policies but the following is the most direct method:

Create a new policy and define the set of rules for the policy, adding filter lists and filter actions as required. In this method, an IPSec policy is created first and then rules are added and configured. Filter lists (specifying traffic types) and filter actions (specifying how the traffic is treated) are added during rule creation.

An IPSec Security Policy must be created for each communication path and on each end (on every server). The following will need to be provided when creating and editing the properties of each IPSec policy using the IP Security Policy Wizard.

1. Name
2. Description (optional)
3. Do not Activate the default response rule
4. IP Security Rule - Add Rule using the Add Wizard
   - Tunnel Endpoint: Do not specify a tunnel
   - Network Type: All network connections
5. IP Filter List
   - Name
   - Description (optional)
   - Add IP Filter using the Add Wizard

     Description (optional)

Source address: A specific IP Address (differs based on the path)

Source address: A specific IP Address (differs based on the path)

Destination address: A specific IP Address (differs based on the path)

IP Protocol type: Any

– Add Filter Action using the Add Wizard

Name

Description (optional)

Filter Action General Options: Negotiate security

Do not communicate with computers that do not support IPSec

IP Traffic Security: Integrity and encryption - Integrity algorithm: SHA1 - Encryption algorithm: 3DES

– Authentication Method: Active Directory _Kerberos V5 protocol (Default)

Note:

- X509 certificates can also be used in a production environment depending on customers' preference. With ICM requiring Active Directory in all deployment models, relying on Kerberos as the authentication method will not require any extra security credential management. For PG to CCM connections an X509 pre-shared key should be used.

- For enhanced security, the use of pre-shared key authentication is not recommended because it is a relatively weak authentication method. In addition, pre-shared keys are stored in plaintext. It is recommended that you use pre-shared keys only for testing. For more information, see Pre-shared key authentication at **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_IPSec_Und4.asp**

6. Key Exchange Security Method - IKE Security Algorithms (Defaults)

– Integrity algorithm: SHA1

– Encryption algorithm: 3DES

– Diffie-Hellman group: Medium (DH Group 2, 1024-bit key)

Note:

- For enhanced security, do not use Diffie-Hellman Group 1, which provides 768 bits of keying strength. For maximum security, use Group 2048 (high), which provides 2,048 bits of keying strength. Strong Diffie-Hellman groups combined with longer key lengths increase the computational difficulty of determining a secret key. For more information, see Key exchange methods at **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_IPSECkeyexchgsm.asp**

- For information about general best practices for security, see Best practices for security at **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_SEconceptsbp.asp**
- Using key lengths results in more CPU processing overhead.

IPSec Connection to Cisco CallManager

On IPCC Systems, when the CallManager is not in the same domain as the ICM system, you are unable to use kerberos for authentication. You must use X.509 certificates.

Monitoring IPSec Activity

IPSec Monitor

IP Security Monitor (ipsecmon) can be used to monitor IPSec on a Windows Server 2003 operating system. Details on the use of IPSec Monitor can be found at **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/IPSEC_Mon_Node.asp**

IPSec Logging

If your policies do not work correctly, you might need to enable the logging of the IPSec security association process. This is called an Oakley log. The log is difficult to read, but it can help you track down the location of the failure in the process. The following steps walk you through the steps for enabling IPSec logging.

Step 1 Select Start, Run. Type Regedt32 and click OK to get into the Registry Editor.

Step 2 Double-click HKEY_LOCAL_MACHINE.

Step 3 Navigate to System\CurrentControlSet\Services\PolicyAgent.

Step 4 Double-click Policy Agent.

Step 5 Right-click in the right-hand pane and select Edit, Add Key.

Step 6 Enter Oakley as the key name (case sensitive).

Step 7 Double-click Oakley. Then right-click in the left-hand pane and select New, DWORD Value.

Step 8 Enter the value name EnableLogging (case sensitive)

Step 9 Double-click the value and set the DWORD to 1. Click OK.

Step 10 Go to a command prompt and type net stop policyagent & net start policyagent.

Step 11 Find the log in %windir%\debug\Oakley.log

Network Monitoring

The Network Monitor component (netmon) that ships with Windows Server 2003 can capture frames that are sent to or from the computer on which Network Monitor is installed. For more information, refer to Microsoft documentation at **http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_netmnintro.asp**

System Monitoring

The built-in Performance console (perfmon) provides the ability to monitor network activity along with the other performance data on the system. Treat network components as another set of hardware resources to observe as part of your normal performance-monitoring routine.

Network activity can influence the performance not only of your network components but also of your system as a whole. You should monitor other resources along with network activity, such as disk, memory, and processor activity. System Monitor enables you to track network and system activity using a single tool. Use the following counters as part of your normal monitoring configuration:

Cache\Data Map Hits %
Cache\Fast Reads/sec
Cache\Lazy Write Pages/sec
Logical Disk\% Disk Space
Memory\Available Bytes
Memory\Nonpaged Pool Allocs
Memory\Nonpaged Pool Bytes
Memory\Paged Pool Allocs
Memory\Paged Pool Bytes

Processor(_Total)\% Processor Time
System\Context Switches/sec
System\Processor Queue Length
Processor(_Total)\Interrupts/sec

Securing Support Tools Using IPSEC

Support Tools uses a different architecture than ICM/IPCC. The Support Tools Server uses a client-policy with a filter that *requests* security. The Support Tools Node Agents uses a client-policy that *requires* security.

The filter does not monitor one-to-one connections. Instead, the filter monitors all incoming IP traffic that uses the default Support Tools TCP Port (39100). The Support Tools Server, by requesting but not requiring IPSEC from each Node Agent, does not deny traffic from a Node Agent that is unable to use IPSEC.

Support Tools uses the ESP protocol (Encapsulating Security Payload) for authentication but does not use encryption. ESP is used to authenticate instead of the AH protocol (Authentication Header) for the ability to support NAT.

Support Tools uses SHA1 for the integrity algorithm in ESP. The policy uses Kerberos in order to support authentication when components reside within the same Active Directory as the server. The policy uses X.509 certificates when components reside in a different Active Directory domain . This means that the policy for the Support Tools server should be configured to support both Kerberos and Certification authentication. Kerberos should be the preferred method and thus listed first in the Authentication Methods list.

A filter should be added complying with the above listed recommendations when securing a Support Tools component that resides on a system with a one-to-one IPSEC policy. The filter should be added to the filter list of the existing policy and listed second.

A configuration example follows:

Support Tools IPSEC Configuration Example

```
Client Policy
   IP Filter
      From any IP address / TCP port
      To any IP address / specific TCP port (39100, Support
      Tools default)
   Filter Action
      Request Security on Support Tools Server
      Require Security on Node Agent
         Negotiate security
```

```
          ESP with SHA1 Integrity and no encryption
Authentication Mode (Both should be listed on Support
Tools server)
   Kerberos
   Certification (On machines where Kerberos is not
   available)
```

Support for NAT (Network Address Translation)

NAT is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). NAT also translates the incoming traffic "legal" delivery addresses to the IP addresses within the inside network.

Release 7.x continues support for deployment of IP Phones (IPCC) across NAT. Cisco has also tested locating remote Peripheral (PG) servers on a NAT network remote from the Central Controller servers (Routers and Loggers). The qualification of NAT support for PG servers was limited to a network infrastructure implementing Cisco IP Routers with NAT functionality.

Agent Desktops are supported in a NAT environment, except when silent monitoring is used. Silent Monitoring is not supported under NAT, see the section on NAT and CTI OS below.

More detailed resources on how to configure NAT can be found at **http://www.cisco.com/**

More details on how to deploy IP Phones across NAT can be found at the following link: **http://cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products_feature_guide09186a008008052e .html**

NAT and CTI OS

CTI OS Silent Monitor does not work in a production environment when all of the servers of the IP Contact Center Solution (AW, PG , CTI OS Server and Call Manager) are located on a remote data center with a private addressing scheme and the agent/supervisor desktops and hard IP-phones are on the call center network that also has its own address scheme while both networks (data center and call center) are joined together using Network Address translation (NAT).

The two main problems that are identified in this environment are as follows:

- The CTI toolkit Agent Desktop cannot sniff any VoIP packets from the PC port on the IP Phone, because the IP address used on the packet filter is the translated address sent by Cisco Call Manager. The problem is that the address belongs to the address scheme at the data center network and not on the call center network space. Note that the problem identified in this bullet is not particular to CTI OS but also affects applications written using GED-188 directly that rely on the RTP Stated/Stop events.
- The IP address the CTI toolkit Supervisor Desktop provides the CTI toolkit Agent Desktop for it to forward sniffed VoIP packets is an address on the data center address space. The

CTI toolkit Supervisor Desktop obtains its IP address from the eClientIdentifyEvent sent by CTI OS Server to the supervisor workstation when it initiates its session with CTI OS Server. The IP address included in the event is the translated address in the data center network versus that of the call center network.

IPSec and NAT Transparency

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPSec. NAT Traversal (NAT-T) is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Software Release 12.2(13)T and above. If both VPN devices are NAT-T capable, then NAT-T is auto detected and auto negotiated.

Additional IPSec References

Additional IPSec references can be found on the web at:

- IPSec Architecture - **http://www.microsoft.com/technet/itsolutions/network/security/ipsecarc.mspx**
- Windows Server 2003 IPSec Documentation - **http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_IPSECtopnode.asp**
- Intel PRO/100S Network Adapter, IPSec Offload Performance and Comparison - **http://www.veritest.com/clients/reports/intel/intelps.pdf**

Chapter 3

Applying IPSec with the Network Isolation Utility

This chapter contains the following topics:

- About IPSec, page 23
- Deploying IPSec Manually Versus Deploying It Via the Network Isolation Utility, page 24
- About the Cisco Network Isolation Utility, page 24
- An Illustration of Network Isolation Utility Deployment, page 25
- How the Network Isolation Utility Works, page 25
- About Encrypting Traffic, page 27
- How to Deploy the Network Isolation Feature, page 27
- Caveats, page 36
- How to Do a Batch Deployment, page 37
- How to Run the Network Isolation Utility from the Command Line, page 37
- How to Monitor the Network Security, page 42
- Troubleshooting the Network Isolation IPSec Policy, page 42

About IPSec

IPSec (Internet Protocol Security) is a security standard developed jointly by Microsoft, Cisco Systems, and many other IETF (Internet Engineering Task Force) contributors. It provides integrity(authentication) and encryption between any two nodes, which could be either an endpoint or a gateway. IPSec is application independent as it works at layer 3 of the network. This is particularly useful for large and distributed applications like ICM since it provides security between the application nodes independently of the application.

For some introductory information on IPSec, see:

- **Frequently Asked Questions** (http://www.microsoft.com/technet/network/ipsec/ipsecfaq.mspx)

- **A white paper you can download: Internet Protocol Security for Microsoft Windows Server 2003 http** (//www.microsoft.com/downloads/details.aspx?familyid=E6590330-D903-4BDD-965581B86DF655E4&displaylang=en)

Deploying IPSec Manually Versus Deploying It Via the Network Isolation Utility

The Network Isolation Utility, described in this chapter, automates much of the work you need to do to secure an ICM or IPCC environment using IPSec. The Network Isolation utility deploys a preconfigured IPSec policy on Unified ICM and Unified Contact Center Enterprise servers that secures the **entire** network traffic to or from those servers. Network connectivity is restricted to only those severs that share the same policy or are explicitly listed as exceptions. If you wish to secure network traffic only between **selected communication paths**, then refer to the manual steps described in the chapter on IPSec and NAT Support (page 11).

About the Cisco Network Isolation Utility

The Cisco Network Isolation Utility uses the Windows IPSec feature to isolate ICM devices (for example, the router, the logger, and the peripheral gateway device) from the rest of the network. The utility creates a Network Isolation IPSec policy, which, once deployed, sets ICM devices as Trusted and authenticates and optionally encrypts all traffic between Trusted Devices. Traffic between Trusted Devices continues to flow normally without any additional configuration. All traffic to or from devices outside the Trusted Devices is denied unless it is classified as coming from or going to a Boundary Device.

A Boundary Device is a device without an IPSec policy that is allowed access to a Trusted Device. These devices typically include the Domain Controller, the Cisco Unified Communications Manager, default gateway devices, CTIOS desktops, WebView clients, serviceability devices, and remote access computers.

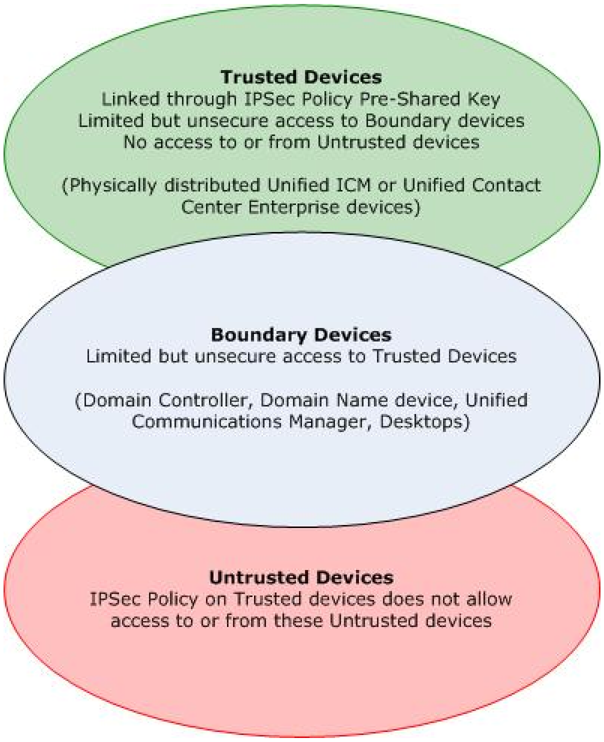
Each Trusted Device has its own list of Boundary Devices, which is defined either by separate IP addresses or subnets or ports.

The Network Isolation policy uses the IPSec ESP (Encapsulating Security Payload) protocol for integrity and encryption. The cipher suite deployed is as follows:

- IP Traffic Security:
  - Integrity algorithm: SHA1
  - Encryption algorithm: 3DES
- Key Exchange Security:
  - Integrity algorithm: SHA1
  - Encryption algorithm: 3DES (optional)
  - Diffie-Hellman group: High (2048-bit key)

An Illustration of Network Isolation Utility Deployment

Figure 1: Example Network Isolation Deployment


Trusted Devices
Linked through IPSec Policy Pre-Shared Key
Limited but unsecure access to Boundary devices
No access to or from Untrusted devices
(Physically distributed Unified ICM or Unified Contact Center Enterprise devices)
Boundary Devices
Limited but unsecure access to Trusted Devices
(Domain Controller, Domain Name device, Unified Communications Manager, Desktops)
Untrusted Devices
IPSec Policy on Trusted devices does not allow access to or from these Untrusted devices

How the Network Isolation Utility Works

To understand the Network Isolation Utility design and how it works, you should understand the following:

- IPSec Terminology (page 25)
- The Network Isolation Utility Process (page 26)

IPSec Terminology

- **Policy**

  An IPSec policy is a collection of one or more rules that determine IPSec behavior. In Windows Server 2003, multiple policies can be created but only one policy can be assigned (active) at a time.

- **Rules**

Each rule is made up of a FilterList, FilterAction, Authentication Method, TunnelSetting, and ConnectionType.

- **Filter List**

  A set of filters that match IP packets based on source and destination IP address, protocol, and port.

- **Filter Action**

  A filter action, identified by a Filter List, defines the security requirements for the data transmission.

- **Authentication Method**

  An authentication method defines the requirements for how identities are verified in communications to which the associated rule applies.

For fuller definitions of Microsoft Windows IPSec terminology, see **Overview of IPsec Policy Concepts** (http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecapa.mspx).

The Network Isolation Utility Process

The Network Isolation Utility must be run separately on each Trusted Device. Do **not** run the utility on Boundary Devices.

To allow traffic to or from Boundary Devices, the Boundary Devices list on each Trusted Device must be configured manually.

Once the Network Isolation IPSec policy is deployed on a device, that device is set as Trusted and traffic flows freely between it and any other Trusted Device without any additional configuration.

When run, the Network Isolation Utility does the following:

1. Removes any IPSec policies already on that computer. This is to avoid conflicts so the new policy matches on all ICM devices for a successful deployment.

2. Creates a Cisco Unified Contact Center (Network Isolation) IPSec policy in the Windows IPSec policy store.

3. Creates the following two rules for the policy:

   a. **Trusted Devices Rule**

      Trusted Devices Filter List: all traffic. One filter that matches all traffic.

      Trusted Devices Filter Action: Require security. Authenticate using the integrity algorithm SHA1 and optionally encrypt using encryption algorithm 3DES.

Authentication Method: The authentication method used to create trust between computers is a Preshared Key.

The Preshared Key can be a string of words, numbers, or characters except the double quote symbol. The minimum length for this key is 36 characters.

b. **Boundary Devices Rule**

Boundary Devices Filter List: (empty by default)

Boundary Devices Filter Action: Permit traffic without IPSec policy. Boundary Devices do not require IPSec to communicate with Trusted Devices.

4. Stores a copy of the Cisco Unified Contact Center IPSec policy in an XML file located in Network Isolation utility folder:**`<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML`**

   The XML files stores the policy state and the Boundary Device list. It does not store the pre-shared key.

5. Logs all commands and actions in a log file at: **`<SystemDrive>:\CiscoUtils\NetworkIsolation\Logs\CiscoICMNetworkIsolation.log`**

   The utility keeps one copy of the log file and appends all commands and actions to any previously created logs.

About Encrypting Traffic

The Network Isolation policy allows only those computers having the same pre-shared key to interact. However, if encryption is not enabled, then, although an outside hacker cannot access a trusted computer, the hacker might be able to see the traffic coming and going from that computer. Therefore, you can also encrypt that traffic if you want to.

Note:

- You cannot encrypt traffic to one Trusted Device alone. You must either encrypt traffic on all Trusted Devices or none. The reason is that if only one computer has encrypted traffic, then none of the other Trusted Devices will understand it.

- Cisco strongly recommends the use of encryption offload network interface cards when IPSec is enabled with encryption so that performance is not impacted by the encryption software. See IPSec and NAT Support (page 11) for more details.

How to Deploy the Network Isolation Feature

You should be aware of the following when designing your deployment plan for the Network Isolation feature:

- Important Deployment Tips (page 28)
- Sample Deployment (page 28)
- Devices That Must Communicate with One Another (page 33)
- Typical Boundary Devices (page 34)

Important Deployment Tips

No configuration is needed on Boundary Devices. All the configuration is done on Trusted Devices. The Network Isolation Utility configures Trusted Devices to interact with other Trusted Devices and with Boundary Devices.

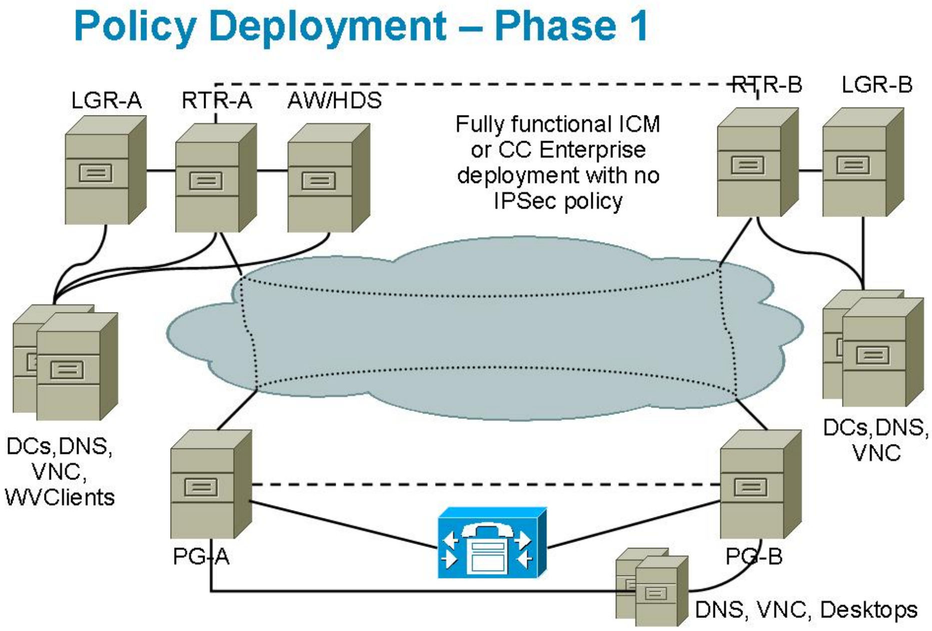
Since the network isolation feature is applied on one device at a time, and since this feature instantly limits communication with other devices once it is applied, you need to carefully plan how to deploy this feature before using it or you could accidentally stop your network from working. It is advisable to write a deployment plan before you implement the Network Isolation feature. You should deploy this feature therefore only during a maintenance window and you should review the Caveats (page 36) before writing your deployment plan.

Sample Deployment

The following is one sample deployment. Phase one of the deployment is to deploy the policy on the ICM Router, Logger, and AW and to put the Peripheral Gateway (PG) subnets in the ICM Router's Boundary Devices list. Phase two of the deployment is to remove the PGs from the ICM Router's Boundary Device list simultaneously as the policy is deployed on the PGs.

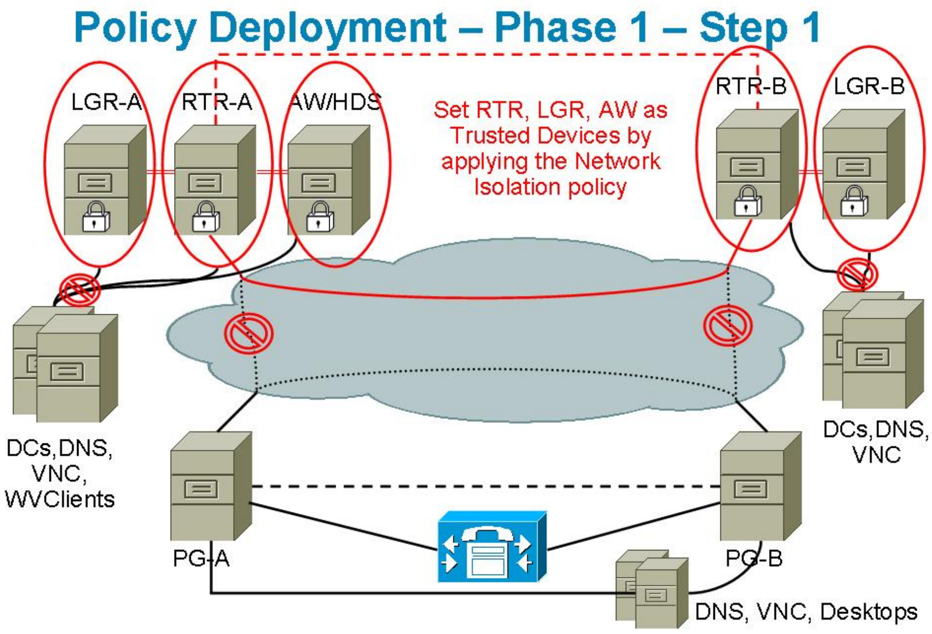
1. Start with a fully functional Unified ICM or Cisco Unified Contact Center Enterprise system that has no IPSec policy deployment.

Figure 2: Example Contact Center Enterprise System


Policy Deployment – Phase 1
LGR-A
RTR-A
AW/HDS
RTR-B
LGR-B
Fully functional ICM or CC Enterprise deployment with no IPSec policy
DCs,DNS, VNC, WVClients
DCs,DNS, VNC
PG-A
PG-B
DNS, VNC, Desktops

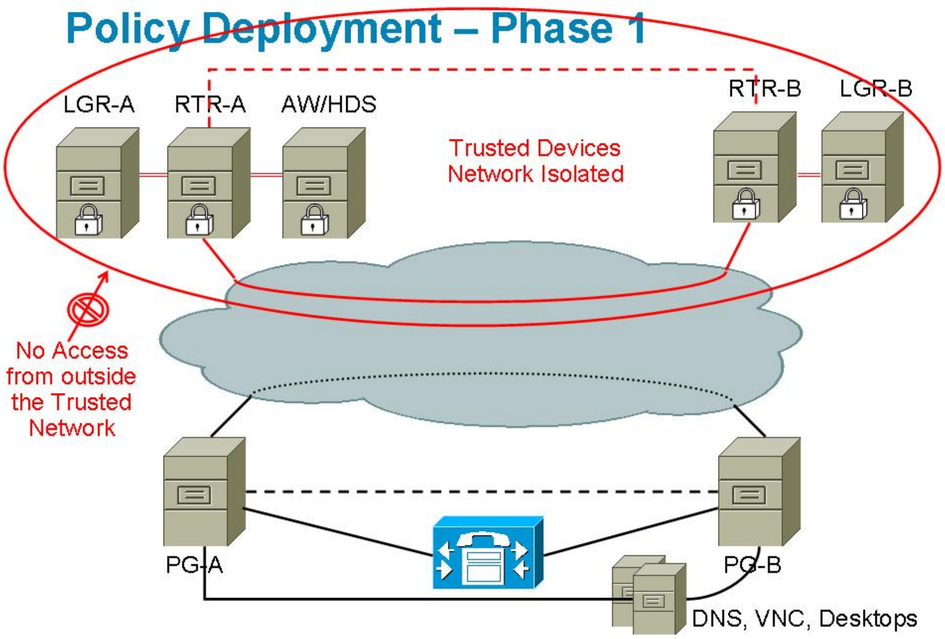
2. Set the ICM Router, the Logger, and the Admin Workstation as Trusted Devices by running the Network Isolation Utility on each of them.

Figure 3: Example Phase 1 - Step 1 IPSec Deployment


Policy Deployment – Phase 1 – Step 1
LGR-A
RTR-A
AW/HDS
RTR-B
LGR-B
Set RTR, LGR, AW as Trusted Devices by applying the Network Isolation policy
DCs,DNS, VNC, WVClients
DCs,DNS, VNC
PG-A
PG-B
DNS, VNC, Desktops

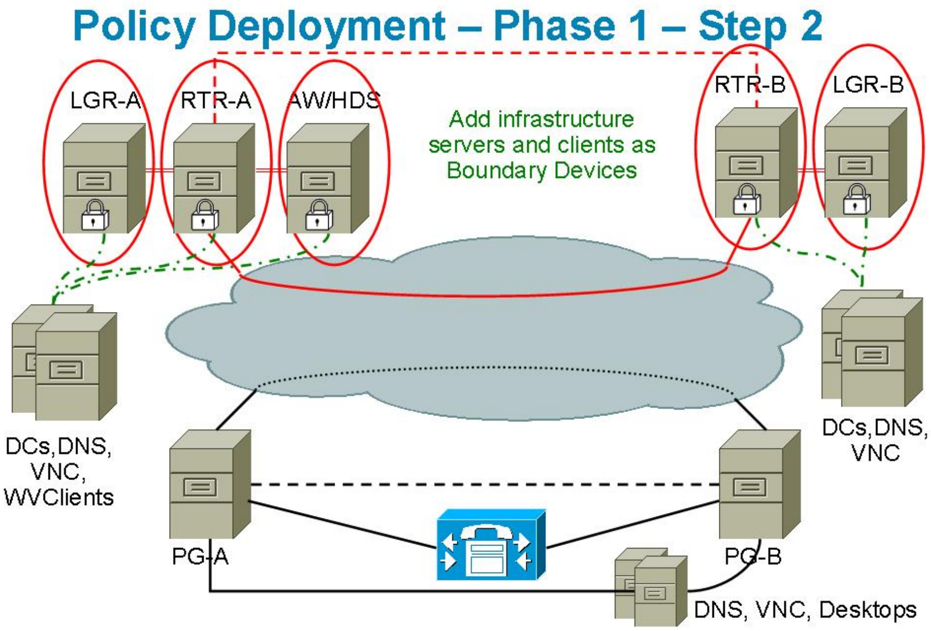
This process leaves the Trusted Devices as network isolated.

Figure 4: Example Tusted Device Isolation



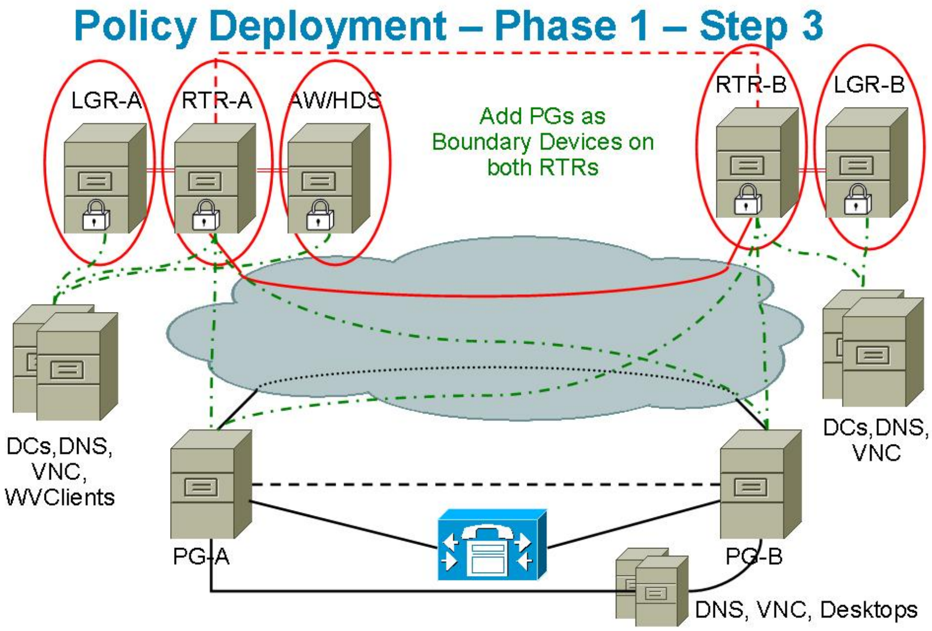
3. Add the infrastructure servers and clients as Boundary Devices.

Figure 5: Example Phase 1 - Step 2 IPSec Deployment



4. Put the Peripheral Gateway (PG) subnets in the ICM Router’s Boundary Devices list.

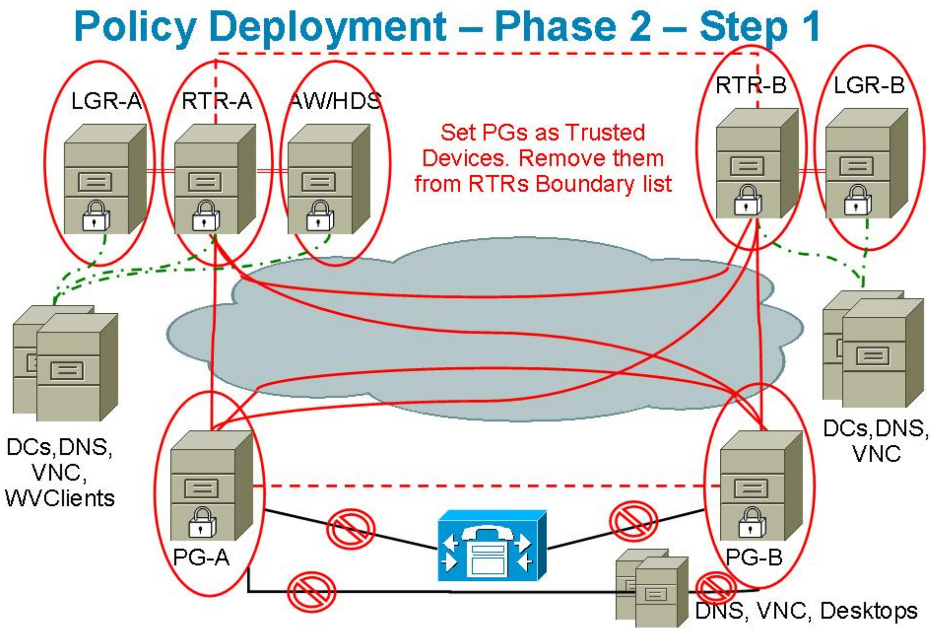
Figure 6: Example Phase 1 - Step 3 IPSec Deployment



5. Then set the PGs as Trusted Devices and simultaneously remove them from the Router's Boundary list.

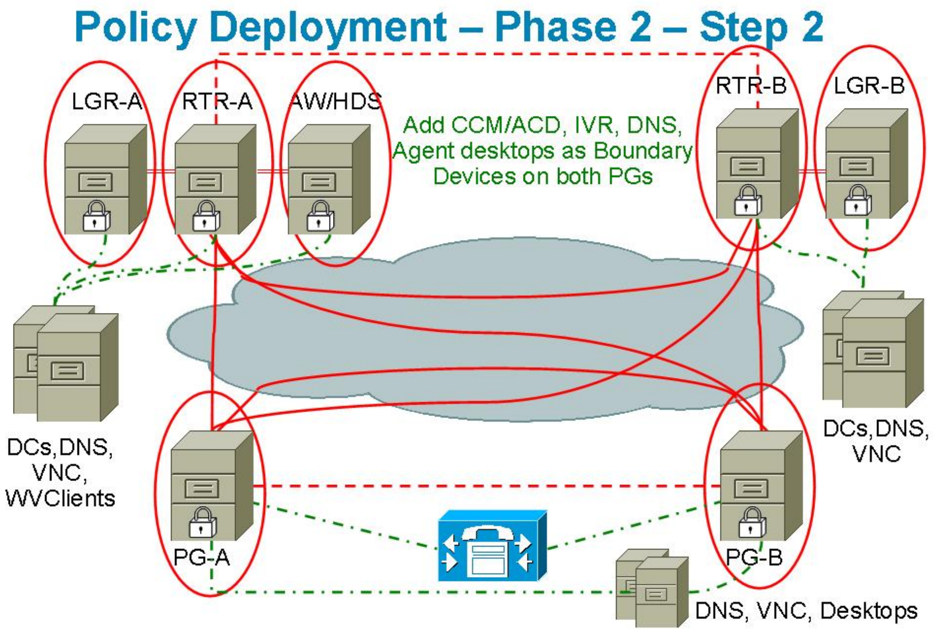
   Note: Once the policy is deployed on a PG, that PG is a Trusted Device. Therefore, it is imperative that the PG be removed from the Router's Boundary Device list since a communication path (in this case, between the router and the PG) cannot be set as both Trusted and Boundary.

Figure 7: Example Phase 2 - Step 1 IPSec Deployment


Policy Deployment – Phase 2 – Step 1
LGR-A
RTR-A
AW/HDS
Set PGs as Trusted Devices. Remove them from RTRs Boundary list
RTR-B
LGR-B
DCs,DNS, VNC, WVClients
DCs,DNS, VNC
PG-A
PG-B
DNS, VNC, Desktops

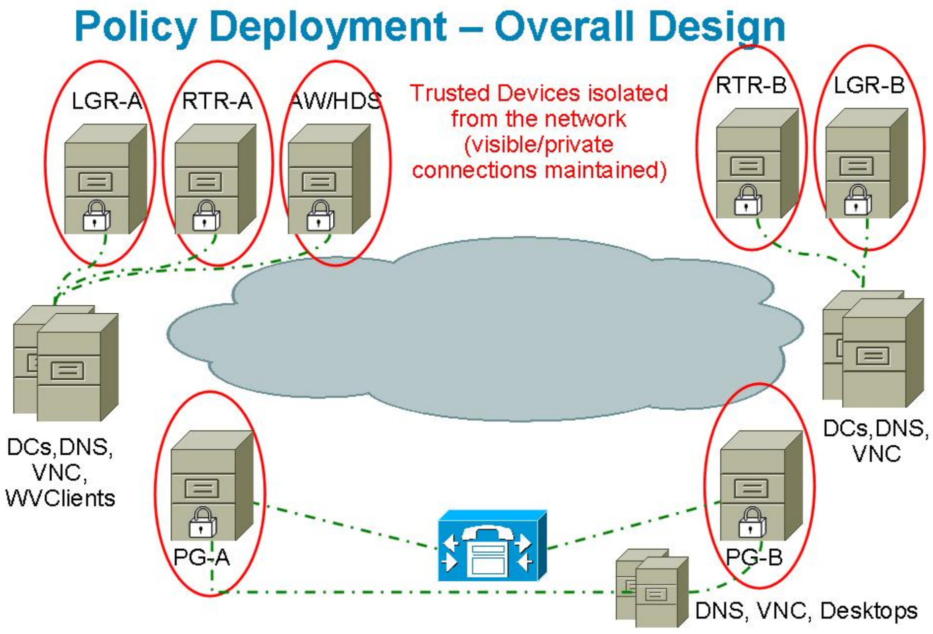
6. Add the Unified Communication Manager or ACD server, the DNS, and the agent desktops as Boundary Devices on both PGs.

Figure 8: Example Phase 2 - Step 2 IPSec Deployment


Policy Deployment – Phase 2 – Step 2
LGR-A
RTR-A
AW/HDS
RTR-B
LGR-B
Add CCM/ACD, IVR, DNS, Agent desktops as Boundary Devices on both PGs
DCs,DNS, VNC, WVClients
DCs,DNS, VNC
PG-A
PG-B
DNS, VNC, Desktops

When you are finished, all ICM Trusted Devices will communicate with ONLY each other and their respective Boundary Devices (the domain controller, the DNS, the Unified Communications Manager, and so on). Any network attack from outside will not reach the Trusted Devices, unless routed through the Boundary Devices.

Figure 9: Example IPSec Deployment - Overall Design


Policy Deployment – Overall Design
LGR-A
RTR-A
AW/HDS
Trusted Devices isolated from the network (visible/private connections maintained)
RTR-B
LGR-B
DCs,DNS, VNC, WVClients
DCs,DNS, VNC
PG-A
PG-B
DNS, VNC, Desktops

Devices That Must Communicate with One Another

Each device in the following list must be able to have two-way communication with each device in its sublist. These devices can be set as either Trusted or Boundary Devices:

- Router
  - Router (on the other side in a duplex system)
  - Logger
  - Admin Workstation/ Historical Database Server
  - NAM Router
  - Peripheral Gateway (on both sides in a duplex system)
  - Application Gateway
  - Database Server
  - Network Gateway
- Logger
  - Historical Database Server/ Admin Workstation
  - Router
  - Campaign Manager
  - Dialer
- Peripheral Gateway
  - Multichannel/Multimedia Server
  - Router (on both sides in a duplex system)
  - Peripheral Gateway (on the other side in a duplex system)
  - Cisco Communications Manager
  - Admin Workstation legacy PIMS/switches
- CTIOS Server and CTIOS Clients
  - CTIOS Server (on the other side in a duplex system)
  - Peripheral Gateway

  - CTIOS Agent desktops
  - Cisco Agent Desktop
  - All CTI Clients
- Silent Monitor Server
  - CTIOS Server (on the other side in a duplex system)
  - Peripheral Gateway
  - CTIOS Agent desktops
  - Cisco Agent Desktop
  - All CTI Clients
- Admin Workstation/Historical Database Server
  - Multichannel/Multimedia Server
  - Router
  - Logger
  - WebView Server
  - Custom Application Server
  - CON API Clients
  - Internet Script Editor Clients/ Webskilling
  - 3rd Party Clients/ SOL party
- WebView Server
  - Admin Workstation/Historical Database Server
  - Clients
  - 3rd Party Software Server
  - Open Software Server

Typical Boundary Devices

The following is a list of Boundary Devices that you will typically need to allow normal functioning of an ICM system:

- **Domain Controllers for RTR, LGR, AW or HDS, and PGs**

  Configuration Example:

  Boundary Device(s): Domain Controller IP Address(s)

  Traffic Direction: Outbound

  Protocol: Any

  Port: Not Applicable

- **DNS, WINS, Default Gateway**

- **Remote Access or Remote Management for every Trusted Device (VNC, pcAnywhere, Remote Desktop Connection, SNMP)**

  Configuration Example for VNC:

  Boundary Device(s): Any host

  Traffic Direction: Inbound

  Protocol: TCP

  Port: 5900

- **Communications Manager Cluster for PGs**

  Configuration Example:

  Boundary Device(s): A specific IP Address (or Subnet)

  Traffic Direction: Outbound

  Protocol: TCP

  Port: All ports

- **Agent Desktops**

  Configuration Example for CTIOS Server:

  Boundary Device(s): A Subnet

  Traffic Direction: Inbound

  Protocol: TCP

  Port: 42028

- **WebView Clients**

Configuration Example for WebView Server:

Boundary Device(s): A Subnet

Traffic Direction: Inbound

Protocol: TCP

Port: 80 and 443

The Support Tools 2.1 or greater server does not need to be added to the Boundary Server list if its policy has the same preshared key as the policy created by the Network Isolation Utility.

Caveats

You must carefully plan deployments so that the policy is applied to all machines at the same time. Otherwise, you can accidentally isolate a device.

- **Important**: Enabling the policy remotely will block remote access unless a provision is made in the Boundary Device list for remote access. You must add a Boundary Device for remote access before enabling the policy remotely.
- **Important**: You must add all domain controllers as Boundary Devices or your domain login will fail and your ICM services will also fail to start or you may see delayed login times. This list of domain controllers should include all domains in which the ICM application is installed as well as all domains in which ICM setup, configuration and Webview users and supervisors exist.
- Adding a new device as Boundary Device (for example, a new Domain Controller) requires a change to the policy on all Trusted Devices which need access to this new device without IPSec.
- A change in the Preshared Key must be invoked on all Trusted Devices.
- If you enable encryption on only one Trusted Device, then that device will not be able to communicate with the other Trusted Devices since it's network traffic will be encrypted. Encryption should be enabled on all or none of the Trusted Devices.
- You should avoid the use the Windows IPSec Policy MMC plug-in to make any changes to the IPSec policy. The Network Isolation utility maintains its own copy of the policy, and, whenever executed, the utility reverts to its last saved configuration, ignoring any changes made outside the utility (or the Security Wizard).
- When you install the Cisco Support Tools, 2.1 or later on a device, an IPsec policy is automatically applied to that device. If you then run the Network Isolation Utility on that same device, the Support Tools IPSec policy will be deleted and replaced by the Network Isolation IPSec policy.

The Cisco Unified Contact Center (Network Isolation) IPSec policy supercedes the Cisco Unified Contact Center (Support Tools) IPSec policy. This means that the Support Tools Installation will not overwrite or modify the Network Isolation IPSec policy.

As long as the preshared key is the same for all the Trusted Devices and the Support Tools server, the Support Tools server will continue to work and connect to the Support Tools Node Agents on the Trusted Devices using IPSec.

- While the Network Isolation Utility does not interfere with applications that run on the network, it should be run only during the application maintenance window since it can potentially disrupt connectivity when you are setting up the network security.
- If your network is behind a firewall, then you must configure the firewall to:
  - Allow IP protocol number 50, which is the ESP (Encapsulating Security Protocol).
  - Allow UDP source and destination traffic on port 500 for the IKE (Internet Key Exchange) protocol.
- If you are using the NAT (Network Address Translation) protocol, then you must configure the firewall to forward traffic on UDP source and destination port 4500 for UDP-ESP encapsulation.
- Any changes made to the application port usage, such as a web server port, must also be reflected in the policy.
- The Network Isolation Policy should be deployed after the ICM or the Unified Contact Center application is configured and confirmed to be working.

How to Do a Batch Deployment

You can use the XML file (<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML), containing the list of Boundary Devices and policy state, on one Trusted Device to replicate the policy on other Trusted Devices. This can help to speed up deployment when a common set of Boundary Devices must be added to all Trusted Devices.

For example, when setting up your PGs as Trusted Devices, you may first want to complete configuring one ICM PG. Next, you can copy the XML file from that configured PG to the rest of your ICM PGs, and then run the Isolation Utility (or the Security Wizard) on the other PGs to replicate the same Boundary Device list on all your PGs.

How to Run the Network Isolation Utility from the Command Line

You can run the Network Isolation Utility either from the command line or from the Unified Contact Center Security Wizard.

Note: It is recommended that you use the Security Wizard for initial policy creation or modification. You can use the command line for batch deployment.

To run the utility from the command line, go to the C:\CiscoUtils\NetworkIsolation directory, where the utility is located, and run it from there:

C:\CiscoUtils\NetworkIsolation>

The following is the command-line syntax for enabling the policy on Trusted Devices:

```
cscript ICMNetworkIsolation.vbe <arguments>
```

Note: You must use **cscript** to invoke the script.

You can add Boundary Devices with multiple filters. You can filter them by:

- **IP Address**: Individual IP addresses or by an entire subnet of devices
- **Dynamically detected devices**: DNS, WINS, DHCP, Default Gateway

  Windows dynamically detects the IP address of these devices and keeps the filter list updated
- **Direction of traffic**: inbound or outbound
- **Protocol**: TCP, UDP, ICMP, or any protocol
- **Port** (only if TCP or UDP is selected): a specific port or all ports

In the syntax:

- angle brackets < > = required
- square brackets [ ] = optional
- a pipe or bar | = any one of the items between the bar(s)

The following table lists the command syntax for all uses of the command.

Table 1: The Network Isolation Utility Command Syntax for Each Argument

Argument Name	Syntax and Example	Function
HELP	cscript ICMNetworkIsolation.vbe /?	Displays the syntax for the command.
ENABLE POLICY	cscript ICMNetworkIsolation.vbe /enablePolicy <36+ characters PreSharedKey in double quotes> [/encrypt] **Note:** The only non-supported character for use in the PresharedKey is double quotes since that character marks the beginning and end of the key. You can enter any other character within the key.	Creates a new policy or enables an existing one from the stored policy XML file. Optionally enables encryption of the network traffic data. Creates a new policy in Windows IPSec policy store and adds all Boundary Devices listed in

Argument Name	Syntax and Example	Function
	For Example: **cscript ICMNetworkIsolation.vbe / enablePolicy “myspecialpresharedkey123456789mnbvcx”**	the XML file. If the XML file does not exist, then it creates a new XML file. The /encrypt option overrides the value set in the XML file.
Note: The add, remove, and delete arguments make a backup of the xml file and name it xml.lastconfig before carrying out their function.		
ADD BOUNDARY	cscript ICMNetworkIsolation.vbe /addBoundary DNS|WINS|DHCP|GATEWAY For example: **cscript ICMNetworkIsolation.vbe / addBoundary DNS** This example adds the DNS server to the Boundary Device list.	Adds to the Boundary Device list the type of device specified. The type can be specified as DNS, WINS, DHCP, or GATEWAY. The utility recognizes DNS, WINS, DHCP, and GATEWAY as the Domain Name System (DNS) device, the Windows Internet Name Service (WINS) device, the Dynamic Host Configuration Protocol (DHCP) device, and the default Gateway (GATEWAY) device respectively. The Windows operating system dynamically detects a change in IP address for each of the preceding types of devices and dynamically updates the Boundary filter list accordingly.
	cscript ICMNetworkIsolation.vbe /addAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber> For example: **cscript ICMNetworkIsolation.vbe / addAnyHostBoundary Inbound TCP 5900** This example allows VNC access from all machines.	Adds to the Boundary Device list any device that matches the following criteria: • One of the specified traffic directions (outbound or inbound). • One of the specified protocols Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). • The specified port.
	cscript ICMNetworkIsolation.vbe /addIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: **cscript ICMNetworkIsolation.vbe / addIPAddrBoundary 10.86.121.160 Outbound Any**	Adds to the Boundary Device list the IP address of a device that has the following configuration: • (required) The specified IP address. • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (required): Transmission Control Protocol (TCP), User Datagram Protocol (UDP),

Argument Name	Syntax and Example	Function
	This example allows all outbound traffic to a device with the specified IP address.	Internet Control Message Protocol (ICMP), or any protocol. • (optional) any port or a specified port if the selected protocol is TCP or UDP.
	cscript ICMNetworkIsolation.vbe /addSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: **`cscript ICMNetworkIsolation.vbe / addSubnetBoundary 10.86.0.0.255.255.0.0 Inbound TCP 42028`** This example allows a CTIOS Server to listen for agent desktops on the 10.86.x.x network.	Adds to the Boundary Device list the subnet that has the following configuration: • (required) The starting IP address of the following specified range. • (required) The specified subnet mask (a range of logical addresses within an address space). • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or any protocol. • (optional) any port or a specified port if TCP or UDP is selected as the protocol.
REMOVE BOUNDARY	cscript ICMNetworkIsolation.vbe /removeBoundary DNS|WINS|DHCP|GATEWAY For example: **`cscript ICMNetworkIsolation.vbe / removeBoundary GATEWAY`**	Removes from the Boundary Device list the type of device specified. The type can be specified as DNS, WINS, DHCP, or GATEWAY. The utility recognizes DNS, WINS, DHCP, and GATEWAY as the Domain Name System (DNS) device, the Windows Internet Name Service (WINS) device, the Dynamic Host Configuration Protocol (DHCP) device, and the default Gateway (GATEWAY) device respectively. The Windows operating system dynamically detects a change in IP address for each of the preceding types of devices and dynamically updates the Boundary filter list accordingly.
	cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber>	Removes from the Boundary Device list any host device at the specified IP address that matches the following criteria:

Argument Name	Syntax and Example	Function
	For example: **cscript ICMNetworkIsolation.vbe / removeAnyHostBoundary Inbound TCP 5900**	• One of the specified traffic directions (outbound or inbound). • One of the specified protocols (TCP or UDP). • The specified port number for internet traffic.
	cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: **cscript ICMNetworkIsolation.vbe / removeIPAddrBoundary 10.86.121.160 Outbound Any**	Removes from the Boundary Device list the device at the specified IP address that has the following configuration: • (required) The specified IP address. (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (TCP, UDP, ICMP, or any protocol). • (optional) any port or a specified port if TCP or UDP is the specified protocol.
	cscript ICMNetworkIsolation.vbe /removeSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: **cscript ICMNetworkIsolation.vbe / removeSubnetBoundary 10.86.0.0.255.255.0.0 Inbound Any**	Removes from the Boundary Device list all the devices at the specified IP address that have the following configuration: • (required) The starting IP address of the following specified range. • (required) The specified subnet mask. • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (TCP, UDP, ICMP, or any protocol). • (optional) any port or a specified port.
DISABLE POLICY	**cscript ICMNetworkIsolation.vbe / disablePolicy**	Disables the ICM Network Isolation IPSec policy on the computer. However, the policy is not deleted and it can be re-enabled. This option is helpful when troubleshooting network problems. If you are having a network connectivity problem with your contact center application, and you do not know what is causing the problem, you might want to disable the policy

Argument Name	Syntax and Example	Function
		to help you clarify the source of your problem. If you are still having the problem with the policy disabled, then the policy is not the cause of your problem.
DELETE POLICY	`cscript ICMNetworkIsolation.vbe /deletePolicy`	Deletes the ICM Network Isolation Security policy from the Windows IPSec policy store and renames the XML file to CiscoICMIPsecConfig.xml.lastconfig.

How to Monitor the Network Security

IP Security Monitor (ipsecmon) can be used to monitor IPSec on a Windows device 2003 operating system. Details on the use of IPSec Monitor can be found at **http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/IPSEC_Mon_Node.asp**

Troubleshooting the Network Isolation IPSec Policy

- Disable the policy and confirm whether the network problem you experienced still exists.

  Shutting down the policy might not be an option on a highly distributed system. So, it is very important that policy is deployed after the ICM application is completely configured and tested.

- Check if an IP address or port specified in the Boundary Device list was modified after the policy was deployed.

- Check whether a communication path is set as Trusted and Boundary.

  An overlap of both will cause communication to fail.

- Confirm by looking in the <system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML file whether the required Boundary Devices are listed as Boundary Devices. Preferably, use the Security Wizard (see Applying Security with the Cisco Unified Contact Center Security Wizard (page 81)) to check the Boundary Devices.

- Changes made to the IPSec policy directly from the Windows MMC console are not reflected in the utility (or in the Security Wizard) .

  The Enable Policy option will always overwrite the IPSec policy store with the configuration stored in the XML file.

- Check for the caveats listed in Caveats (page 36).

Chapter 4

Windows Server 2003 Firewall Configuration

Windows Server 2003 (Service Pack 1) includes Windows Firewall. Windows Firewall is a stateful host firewall which drops all unsolicited incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic), or unsolicited traffic that has NOT been specified as allowed (excepted traffic). This behavior of Windows Firewall provides a level of protection from malicious users and programs that use unsolicited incoming traffic to attack computers.

More information can be found in Microsoft's **Windows Firewall Operations Guide** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/c52a765e-5a62-4c28-9e3f-d5ed334cadf6.mspx).

If you are using IPSec, you should also consult the following Microsoft TechNet article on **Managing IPSec and Multicast Settings** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/6955d995-7b77-47cf-8749-cd906afc46d9.mspx).

Note: Windows Firewall is disabled by default on systems that have been upgraded to SP1. Systems that have a new installation of Windows Server 2003 that already include SP1 (known as a slipstream installation) have Windows Firewall **enabled** by default.

You may enable Windows Firewall on your ICM/IPCC Servers, however, you must ensure that all required ports are open so that the ICM/IPCC components installed on the server can function properly.

Cisco provides a utility to automatically allow all traffic from ICM/IPCC applications on a Windows Server 2003 SP1 server. Additionally, the utility is developed so that it can open ports for common 3rd party applications used in the ICM/IPCC environment. The script reads the list of ports in the file **`%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`** and uses the directive contained therein to modify the firewall settings. See below for more information on the CiscoICMfwConfig_exc.xml file.

The utility allows all traffic from ICM/IPCC applications by adding the relevant applications to the list of excepted programs and services. When the excepted application runs, Windows

Firewall monitors the ports on which the program listens and automatically adds those ports to the list of excepted traffic.

The script can allow traffic from the third party applications by adding the application's *port number* to the list of excepted traffic. However, you must edit the **`CiscoICMfwConfig_exc.xml`** file to enable these ports.

Ports/Services Enabled by default:

- 80/TCP and 443/TCP - HTTP/HTTPS (when IIS is installed)
- Microsoft Remote Desktop
- File and Print Sharing Exception (See Microsoft's technet article **Enable or disable the File and Printer Sharing exception** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/267c6000-957e-4fb4-8698-e41d4439fb58.mspx).

Ports than can be optionally opened:

- 5900/TCP - VNC (optional)
- 5800/TCP - Java Viewer (optional)
- 21800/TCP - Tridia VNC Pro (encrypted remote control) (optional)
- 5631/TCP and 5632/UDP - pcAnywhere(optional)

Note: The XML file may be configured to add port based exceptions outside of this list.

This chapter contains the following topics:

- Cisco Firewall Configuration Utility Prerequisites, page 44
- Using the Cisco Firewall Configuration Utility, page 45
- Verifying New Windows Firewall Settings, page 45
- Configuring Windows Server 2003 Firewall to Communicate With Active Directory, page 46
- Understanding the CiscoICMfwConfig_exc.xml File, page 49
- Troubleshooting Windows Firewall, page 50

Cisco Firewall Configuration Utility Prerequisites

The following must be installed before using the Firewall configuration utility:

1. Windows Server 2003 Service Pack 1 (if you are not doing a slipstream install that includes Windows Server 2003 SP1)
2. ICM/IPCC Version 7.x component(s)

Note: Any subsequent installation of any new component to the Application installation will require re-configuring the Windows Firewall. This involves removing the configuration previously applied and re-running the windows firewall configuration utility.

Using the Cisco Firewall Configuration Utility

You can run the Cisco Firewall Configuration Utility either from the command line or from the Unified Contact Center Security Wizard. For how to run it from the Security Wizard, see Applying Security with the Cisco Unified Contact Center Security Wizard (page 81).

Warning: If you attempt to run this utility from a remote session, such as VNC, you may be "locked out" once the firewall starts. If possible, perform any firewall related work at the computer, as network connectivity may be severed for some remote applications.

Use the Cisco Firewall Configuration utility on each server running an ICM component. To use the utility:

Step 1 Stop all application services.

Step 2 From a command prompt, run **cscript %SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig.vbe**

Step 3 If this is the first time the script has run then it will run `register.bat` and ask you to rerun the application using the same command as above. Rerun the script as if instructed to do so.

Note: If you subsequently rerun the script and it says that it is (again) running for the first time, and to (again) rerun the script, then manually run the `register.bat` file from the command line.

Step 4 A confirmation Dialog appears. Click OK.

The script verifies the Windows Firewall service is installed, then starts it if it is not running.

It then updates the firewall with the ports and services specified in the file `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`

Step 5 Reboot the server.

Verifying New Windows Firewall Settings

You can verify that the ICM components and ports have been added to the Windows Firewall exception list by:

Step 1 Select **Start** > **Settings** > **Control Panel** > **Windows Firewall**.

The Windows Firewall dialog box appears.

Step 2 Select the **Exceptions** tab of the Windows Firewall dialog box.

Step 3 Scroll through the list of excepted applications. Several ICM executables now appear on the list as well as any ports or services defines in the configuration file.

Configuring Windows Server 2003 Firewall to Communicate With Active Directory

You need to open up the ports used by domain controllers (DCs) for communication via LDAP and other protocols to ensure Active Directory is able to communicate through a firewall.

Be sure to consult the Microsoft Knowledge Base (KB) **KB179442** (http://support.microsoft.com/kb/179442/en-us) for important information about configuring firewall for Domains and Trusts.

To establish secure communications between DCs and ICM Services you need to define the following ports for outbound and inbound exceptions on the firewall:

- Ports that are already defined
- Variable ports (high ports) for use with Remote Procedure Calls (RPC)

Configuring Domain Controller Ports

The following port definitions must be defined on *all* DCs within the demilitarized zone (DMZ) that might be replicating to external DCs. It is important that you define the ports on all DCs in the domain.

Restrict FRS Traffic to a Specific Static Port

Be sure to consult the Microsoft Knowledge Base (KB) **KB319553** (http://support.microsoft.com/kb/319553/en-us) for more information about restricting File Replication service (FSR) traffic to a specific static port.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters**

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port Assignment**
- Value: **10000 (decimal)**

Restrict Active Directory replication traffic to a specific port

Be sure to consult the Microsoft Knowledge Base (KB) KB224196 (http://support.microsoft.com/kb/224196/en-us) for more information about restricting Active Directory replication traffic to a specific port.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port**
- Value: **10001 (decimal)**

Configure Remote Procedure Call (RPC) port allocation

Be sure to consult the Microsoft Knowledge Base (KB) KB154596 (http://support.microsoft.com/kb/154596/en-us) for more information about configuring RPC port allocation.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry: **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc**

Step 3 Add the **Internet** key.

Step 4 Add the following registry values:

- Ports: **MULTI_SZ: 10002-10200**
- PortsInternetAvailable: **REG_SZ : Y**
- UseInternetPorts: **REG_SZ : Y**

Windows Server 2000 and 2003 Firewall Ports

Be sure to consult the Microsoft Knowledge Base (KB) KB179442 (http://support.microsoft.com/kb/179442/en-us) for a detailed description of the ports that are used to configure a firewall for domains and trusts.

Server Port	Protocol	Protocol	Service
135	TCP	RPC	RPC Connector Helper (machines connect to determine which high port to use)
137	TCP	UDP	NetBIOS Name
138		UDP	NetBIOS NetLogon and Browsing
139			NetBIOS Session
123		UDP	NTP
389	TCP		LDAP
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
42			Wins Replication
53	TCP	UDP	DNS
88	TCP	UDP	Kerberos
445	TCP	UDP	SMB over IP (Microsoft-DS)
10000	TCP		RPC NTFRS
10001	TCP		RPC NTDS
10002 - 10200	TCP		RPC - Dynamic High Open Ports
	ICMP		

Testing Connectivity

To test connectivity and show the FRS configuration in Active Directory, use the Ntfrsult tool.

Step 1 From the command line, run the Windows File Replication utility: **Ntfrsutl version** <server_name>.

When communications between the domain controllers are configured properly, the ntfrsutl output shows the FRS configuration in Active Directory.

Validating Connectivity

To validate connectivity between the domain controllers, use the Portqry tool.

Visit the following Microsoft Web site: **http://download.microsoft.com/download/3/f/4/3f4c6a54-65f0-4164-bdec-a3411ba24d3a/PortQryUI.exe (http://download.microsoft.com/download/3/f/4/3f4c6a54-65f0-4164-bdec-a3411ba24d3a/portqryui.exe)** to obtain the tool.

Step 1 Download the **PortQryUI.exe** and run the tool.

Step 2 Select the destination CD or PDC.

Step 3 Select **Domains and Trusts**.

Step 4 Use the response from PortQry to verify the ports are open.

Be sure to consult the Microsoft Knowledge Base (KB) **KB832919** (http://support.microsoft.com/kb/832919/en-us) for more information about PortQry features and functionality.

Understanding the CiscoICMfwConfig_exc.xml File

The CiscoICMfwConfig_exc.xml file is a standard XML file that contains the list of applications, services and ports that the Cisco Firewall Script uses to modify the Windows Firewall so that the firewall works properly in the ICM/IPCC environment.

The file consists of three main parts:

- Services - The services that are allowed access through the firewall.
- Ports - The ports that the firewall should open.

  This is conditional depending on the installation of IIS in the case of TCP/80 and TCP/443.
- Applications - The applications that are **not** allowed access through the firewall.

  The script automatically excludes all of the applications listed in the **`CiscoICMfwConfig_exc.xml`** file.

  Note: The behavior of the Applications section is opposite to that of the other two sections in the file. The Ports and Services sections ALLOW access, whereas the Application section DENIES access.

You can manually add additional services or ports to the CiscoICMfwConfig_exc.xml file and rerun the script to reconfigure Windows Firewall, for example, if you wanted to allow your **Jaguar** server connections from port 9000 (CORBA), then you could add a line within the **`<Ports>`** part of the file to open port 9000 on the Windows Firewall:

```
<Port Number="9000" Protocol="TCP" Name="CORBA" />.
```

Note: This would only be needed if remote Jaguar administration is required. In most cases this is not needed.

You could also use the standard Windows Firewall mechanism to add or deny the ports or applications by selecting the Exceptions tab of the Windows Firewall Control Panel Applet and clicking **Add Port...** or **Add Program...**.

Some commonly used ports are listed in the file, however they are commented out. In XML, comments (ignored code) is surrounded by the **<!--** and **-->** tags respectively. Anything within those tags is ignored. You can easily enable one of the commonly used ports by cutting it out of the commented section and pasting it *after* the closing comment tag (**-->**), but *before* the **</Ports>** tag.

Troubleshooting Windows Firewall

The following notes and tasks can aid you if you have trouble with Windows Firewall.

General Troubleshooting Notes

Some general troubleshooting notes for Windows Firewall:

1. Running the CiscoICMfwConfig application for the first time requires that it be run twice to allow for the registration of FirewallLib.dll. In some cases, a time lapse is needed for the registration to complete, especially on a slower system.

2. If the registration fails, it's possible the .NET framework isn't installed correctly. Verify the following path and files exist:

   `%windir%\Microsoft.NET\Framework\v1.1.4322\regasm.exe`

   `%windir%\Microsoft.NET\Framework\v1.1.4322\gacutil.exe`

3. Change **`%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\Register.bat`** as needed to meet the environment.

Windows Firewall Interferes with Router Private Interface Communication

Indication: The MDS fails to connect from the Side-A router to Side-B router on the private interface IP Addresses (Isolated) only when the Windows Firewall is enabled.

Problem: Windows Firewall is preventing the application (mdsproc.exe) from sending traffic to the remote host on the private network.

Recommended Action: Configure static routes on both Side-A and Side-B routers for the private addresses (high and non high).

Windows Firewall Shows Dropped Packets but no ICM or IPCC Failures are Evident

Indication: The Windows Firewall Log shows dropped packets but the ICM and IPCC applications do not exhibit any application failures.

Problem: The Windows Firewall is designed to log any and all traffic destined to the host when it either isn't allowed or it is sent to a port that no allowed application is listening on.

Recommended Action: Review the pfirewall.log file closely to determine the source and destination IP Addresses and Ports. Use **`netstat`** or **`tcpview`** to determine what processes listen/connect on what ports.

Undo Firewall Settings

You can use the firewall configuration utility to undo the last application of the firewall settings. You will need the **`CiscoICMfwConfig_undo.xml`** file.

Note: The undo file is only written if the configuration completes successfully. Manual cleanup may be necessary using the Windows Firewall Control Panel Applet in case this file does not exist for the undo operation to complete.

To undo the firewall settings:

Step 1 Stop all application services.

Step 2 Open a command window by selecting **`Start > Run`** and entering **`CMD`** in the dialog window. Click OK.

Step 3 **`cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig`**

Step 4 Type: **`cscript CiscoICMfwConfig.vbe undo`**

Step 5 Reboot the server.

Chapter 5

Automated Security Hardening Settings on Windows Server 2003

The ICM and System IPCC Setup programs can automatically apply a majority of the Cisco recommended Windows hardening settings on Windows Server 2003 Systems with Service Pack 1 or greater.

ICM/IPCC is qualified to work only on a standard, Retail (or OEM) packaged installation of Windows Server 2003 (Standard or Enterprise), with or without Cisco Security Hardening. Cisco provides its own security hardening policy to secure the standard Windows image for ICM/IPCC. Cisco does not support ICM/IPCC on a customized Windows image (that is, a corporate image) or when custom security hardening has been applied. Customized image of the Windows operating system or customer security hardening can cause the ICM/IPCC application to fail.

The settings detailed below are automatically applied when you choose to use the automated hardening feature in setup. All of the following settings appear under the **Computer Configuration > Windows Settings > Security Settings** category of settings.

In addition to automatically applying the settings during setup, the script can be used to upgrade the current Cisco ICM security template if there is one already installed, and it can rollback the template to previous versions of the Cisco ICM security settings. The script can also rollback the security settings to the settings originally on the server before any Cisco ICM security settings were applied.

Note: The 7.2(1) or later Security Hardening template enables FIPS complaint encryption policy. This impacts the following areas of the operating system that can impact ICM operation:

- Microsoft Internet Information Services (IIS)
- Microsoft Internet Explorer.
- Terminal Services using the Remote Desktop Connection.

For more information on how FIPS compliancy affects:

- The Microsoft operating system, see the Microsoft Knowledge Base (KB) article **KB811833** (http://support.microsoft.com/kb/811833)
- ICM software, see Cisco SSL Encryption Utility (page 109).
- Terminal Services, see Remote Administration (page 129).

The Customer Voice Portal 4.0.1 Security Hardening template is the same as ICM 7.0 Security Hardening template except for two settings and the template name:

- SecondaryLogonService: Automatic (CVP); Disabled(ICM)
- MinimumPasswordAge: 0 (CVP); 1 (ICM)
- Template name: Cisco_Security_Template.inf (CVP); CiscoICM_Security_Template.inf (ICM)

Note: Servers running Cisco Collaboration Server (CCS), Cisco Email Manager (CEM), Cisco Dynamic Content Adapter (DCA), and Remote Monitoring Suite (RMS) are not supported for use with the automated hardening script.

This chapter contains the following topics:

- Applying/Removing Cisco ICM Security Settings, page 54
- Account Policies Settings, page 56
- Local Policies, page 57
- Event Log, page 70
- System Services, page 70
- Registry, page 77
- File System, page 78

Applying/Removing Cisco ICM Security Settings

There are several ways in which you can install, upgrade, and rollback security settings:

Applying Cisco ICM Security Settings During Setup

The ICM and System IPCC Setup applications determine if Cisco ICM Security Hardening is applied, and if not, prompt you to apply Cisco ICM security settings during ICM installation. Choosing **Yes** applies the Cisco ICM security settings as defined in the current security template. Choosing **No** results in no security setting changes.

If Cisco ICM Security Hardening is already applied, but the template version of the security settings is older than the one available to ICM Setup, Setup prompts you to update the security settings to the new template version. Choosing **YES** applies the new version of the security settings, while at the same time creating a rollback script so you can revert to the earlier template settings at a later time. Choosing **No** results in no security settings being changed.

Manually Installing Cisco ICM Security Settings

You can run the Security Hardening Utility either from the command line or from the Unified Contact Center Security Wizard. For how to run it from the Security Wizard, see Applying Security with the Cisco Unified Contact Center Security Wizard (page 81).

You can manually install the latest Cisco ICM security settings template at any time by running the ICMSecurityHardening VBS script. The script is located in **`%SYSTEMDRIVE%\CiscoUtils\SecurityTemplates`**.

Note: You must use **`cscript`** from the command line to invoke the script.

To manually apply a Cisco ICM Security Setting template:

Step 1 From the command line type in **`cscript %SYSTEMDRIVE%\CiscoUtils\SecurityTemplates\ICMSecurityHardening.vbe HARDEN`**

Step 2 Reboot the server.

Rolling Back Security Settings

You can manually rollback to a previous version of the system's security settings to prior security state by using the ICMSecurityHardening script. Each time the security hardening script is run a rollback file is created. The "1" extension denotes that it is the baseline settings for the server before hardening was applied. A new rollback file is created with each subsequent update of the security template. The are numbered consecutively, "2", "3", "4", etc.

Warning: The ICMSecurityHardening script cannot rollback changes made to Registry Values and File System security settings.

To roll back to a previous version of the security settings:

Step 1

If: You want to rollback all the settings contained in a security template:

Then: From the command line type in **`cscript %SYSTEMDRIVE%\CiscoUtils\SecurityTemplates\ICMSecurityHardening.vbe ROLLBACK <ROLLBACKFILE>`**

If: You want to only rollback settings in a particular area:

Then: From the command line type in **`cscript %SYSTEMDRIVE%\CiscoUtils\SecurityTemplates\ICMSecurityHardening.vbe ROLLBACK <ROLLBACKFILE> <AREA>`**

Where **<ROLLBACKFILE>** is the name of the file from which you want to rollback the settings. and **<AREA>** is one of the following section names; SECURITYPOLICY, USER_RIGHTS, SERVICES

Step 2 Reboot the server.

See Also

Account Policies Settings on page 56
Local Policies on page 57
Event Log on page 70
System Services on page 70

Account Policies Settings

The following Settings are applied in **Computer Configuration** > **Windows Settings** > **Account Policies**.

Note: Account policies are overwritten by the domain policy by default. Applying the Cisco ICM Security Template does not take effect. These settings are only significant when the machine is not a member of a domain. Cisco Recommends that you set the Default Domain Group Policy with these settings.

When a value is listed as **Not Defined** then it means that the setting is not changed from what was previously set before the automated hardening script runs.

The security settings can be viewed in the Local Security Policy Snap-in.

Password Policy

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Enforce password history	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	90 days
Minimum password age	2 days	1 days
Minimum password length	12 characters	12 characters
Passwords must meet complexity requirements	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled

Account Lockout Policy

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Account lockout duration	15 minutes	15 minutes
Account lockout threshold	10 invalid logon attempts	3 invalid logon attempts
Reset account lockout counter after	15 minutes	15 minutes

Kerberos Policy

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Enforce user logon restrictions	Not Defined	Not Defined
Maximum lifetime for service ticket	Not Defined	Not Defined
Maximum lifetime for user ticket	Not Defined	Not Defined
Maximum lifetime for user ticket renewal	Not Defined	Not Defined
Maximum tolerance for computer clock synchronization	Not Defined	Not Defined

Local Policies

Audit Policy

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Success, Failure	Not defined
Audit logon events	Success, Failure	Success, Failure

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Audit object access	Success, Failure	Failure
Audit policy change	Success	Success, Failure
Audit privilege use	Success, Failure	Failure
Audit process tracking	No auditing	Not defined
Audit system events	Success	Success, Failure

User Rights Assignment

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Access this computer from the network (SeNetworkLogonRight)	Not Defined	Not Defined
Act as part of the operating system (SeTcbPrivilege)	Not Defined	Not Defined
Add workstations to domain (SeMachineAccountPrivilege)	Administrators	Administrators
Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)	LOCAL SERVICE,NETWORK SERVICE,Administrators	LOCAL SERVICE,NETWORK SERVICE, Administrators
Allow logon locally (SeInteractiveLogonRight)	Not Defined	Null
Allow logon Through Terminal Services (SeRemoteInteractiveLogonRight)	Administrators	Administrators
Back up files and directories (SeBackupPrivilege)	Not Defined	Administrators
Bypass traverse checking (SeChangeNotifyPrivilege)	Not Defined	Users
Change the system time (SeSystemTimePrivilege)	Administrators	Administrators

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Create a pagefile (SeCreatePagefilePrivilege)	Administrators	Administrators
Create a token object (SeCreateTokenPrivilege)	Not Defined	Null
Create global objects (SeCreateGlobalPrivilege)	Not Defined	Not Defined
Create permanent shared objects (SeCreatePermanentPrivilege)	Not Defined	Null
Debug programs (SeDebugPrivilege)	Not Defined	Administrators
Deny access to this computer from the network (SeDenyNetworkLogonRight)	ANONYMOUS LOGON; Built-in Administrator; Guest; Guests; Support_388945a0;	ANONYMOUS LOGON; Built-in Administrator; Guest; Guests; Support_388945a0;
Deny logon as a batch job (SeDenyBatchLogonRight)	Guest; Guests; Support_388945a0	Guest; Guests; Support_388945a0
Deny logon as a service (SeDenyServiceLogonRight)	Not Defined	Null
Deny logon locally (SeDenyInteractiveLogonRight)	Not Defined	Guests
Deny log on Through Terminal Services (SeDenyRemoteInteractiveLogonRight)	Built-in Administrator; Guest; Guests; Support_388945a0	Built-in Administrator; Guest; Guests; Support_388945a0
Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)	Not Defined	Administrators
Force shutdown from a remote system (SeRemoteShutdownPrivilege)	Administrators	Administrators
Generate security audits (SeAuditPrivilege)	LOCAL SERVICE,NETWORK SERVICE	LOCAL SERVICE,NETWORK SERVICE

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Impersonate a client after authentication (SeImpersonatePrivilege)	Not Defined	Not Defined
Increase scheduling priority (SeIncreaseBasePriorityPrivilege)	Administrators	Administrators
Load and unload device drivers (SeLoadDriverPrivilege)	Administrators	Administrators
Lock pages in memory (SeLockMemoryPrivilege)	Administrators	Administrators
Log on as a batch job (SeBatchLogonRight)	Not Defined	Null
Log on as a service (SeServiceLogonRight)	Not Defined	Not Defined
Manage auditing and security log (SeSecurityPrivilege)	Administrators	Administrators
Modify firmware environment values (SeSystemEnvironmentPrivilege)	Administrators	Administrators
Perform Volume Maintenance Tasks (SeManageVolumePrivilege)	Administrators	Administrators
Profile single process (SeProfileSingleProcessPrivilege)	Administrators	Administrators
Profile system performance (SeSystemProfilePrivilege)	Administrators	Administrators
Remove computer from docking station (SeUndockPrivilege)	Administrators	Administrators
Replace a process level token (SeAssignPrimaryTokenPrivilege)	Not Defined	LOCAL SERVICE,NETWORK SERVICE
Restore files and directories (SeRestorePrivilege)	Administrators	Administrators

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Shut down the system (SeShutdownPrivilege)	Administrators	Administrators
Synchronize directory service data (SeSynchAgentPrivilege)	Not Defined	Null
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	Not Defined	Administrators

Security Options

Most of these settings can be viewed by running **`secpol.msc`** on a Windows 2003 Server. However, not all MSS settings are shown by default. You should consult the document **Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP** available from microsoft.com for details on viewing all of the available security settings in the Microsoft Local Security Settings console.

Note: Beginning with release 7.2(1), Security Hardening will rename the local Administrator account to xAdministrator. Hence, any service running under the local Administrator account will fail to start after the system is hardened. As a secure practice, avoid using the local Administrator account for any service. However, if you must use the local Administrator account, then you need to change the account username for the service to continue function after hardening is applied.

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Accounts: Administrator account status	Not Defined	Not Defined
Accounts: Guest account status	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled
Accounts: Rename administrator account	Not Defined	xadministrator
Accounts: Rename guest account	Not Defined	xguest
Audit: Audit the access of global system objects	Disabled	Disabled

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Audit: Audit the use of Backup and Restore privilege	Disabled	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled	Not defined
Devices: Allow undock without having to log on	Disabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Administrators
Devices: Prevent users from installing printer drivers	Enabled	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled	Enabled
Devices: Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined	Not Defined
Domain controller: LDAP server signing requirements	Not Defined	Not Defined
Domain controller: Refuse machine account password changes	Not Defined	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined	Not Defined
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled
Domain member: Disable machine account password changes	Disabled	Disabled
Domain member: Maximum machine account password age	30 days	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabled
Interactive logon: Do not display last user name	Enabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled
Interactive logon: Message text for users attempting to log on	This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted.	This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted.
Interactive logon: Message title for users attempting to log on	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION.	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION.
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 logons	0 logons
Interactive logon: Prompt user to change password before expiration	14 days	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	Enabled
Interactive logon: Require smart card	Not Defined	Not Defined

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Interactive logon: Smart card removal behavior	Lock Workstation	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined	Enabled
Network access: Allow anonymous SID/Name translation	Disabled	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled	Enabled

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled
Network access: Named Pipes that can be accessed anonymously	Not Defined	Not Defined
Network access: Remotely accessible registry paths	Not Defined	Not Defined
Network access: Remotely accessible registry paths and subpaths	Not Defined	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled
Network access: Shares that can be accessed anonymously	Not Defined	Not Defined
Network access: Sharing and security model for local accounts	Not Defined	Classic - local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled
Network security: Force logoff when logon hours expire	Enabled	Enabled
Network security: LAN Manager authentication level	Send LM & NTLM - use NTLMv2 session security if negotiated	Send NTLMv2 response only\refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Not Defined	Require 128-bit encryption
Network security: Minimum session security for NTLM SSP	Not Defined	Require 128-bit encryption

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
based (including secure RPC) servers		
Recovery console: Allow automatic administrative logon	Disabled	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Enabled	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled
Shutdown: Clear virtual memory pagefile	Enabled	Enabled
System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined	Enabled
System objects: Default owner for objects created by members of the Administrators group	Not Defined	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not Defined	Not Defined
MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to	10	10

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
create when additional connections are necessary for Winsock applications (10 recommended) **Note:** MSS settings are not displayed by default in the Local Security Policy or Security Templates snap-in. Manual configuration is required to implement this.		
MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)	Enabled	Enabled
MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications	20000	20000
MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)	20	20
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled	Disabled
MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)	Disabled	Disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest Protection, source routing is automatically disabled.	Highest Protection, source routing is automatically disabled.

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)	Undefined	Enabled
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	Disabled	Disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled	Disabled
MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)	Disabled	Disabled
MSS: (Hidden) Hide Computer From the Browse List	**Not Defined -** (not recommended except for highly secure environments)	**Not Defined -** (not recommended except for highly secure environments)
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	300000 or 5 minutes (recommended)	300000 or 5 minutes (recommended)
MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)	Not Defined	Not Defined
MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives	255, disable autorun for all drives	255, disable autorun for all drives
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled	Enabled
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames	Disabled	Disabled

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)	Disabled	Disabled
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled	Enabled
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	0	0
MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)	Connections time sooner if a SYN attack is detected by the server	Connections time sooner if a SYN attack is detected by the server
MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 & 6 seconds, half-open connections dropped after 21 seconds	3 & 6 seconds, half-open connections dropped after 21 seconds
MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3	3
MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)	5	5
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	90%	90%

Event Log

Setting	Value: 7.0(0) & 7.1(1)	Value: 7.2(1) & 7.5(1)
Maximum application log size	16384 kilobytes	81920 kilobytes
Maximum security log size	81920 kilobytes	81920 kilobytes
Maximum system log size	16384 kilobytes	81920 kilobytes
Restrict guest access to application log	Enabled	Enabled
Restrict guest access to security log	Enabled	Enabled
Restrict guest access to system log	Enabled	Enabled
Retain application log	Not Defined	7 days
Retain security log	Not Defined	7 days
Retain system log	Not Defined	7 days
Retention method for application log	As Needed	As Needed
Retention method for security log	As Needed	As Needed
Retention method for system log	As Needed	As Needed

System Services

Note: The service startup settings for 7.0(0) and 7.2(1) or later are the same [with the exception of Distributed Transaction Coordinator, see the table below]. However, the 7.2(1) or later security template modifies permissions for the Alerter and ClipBook services. The Administrators group and the SYSTEM group permissions for the Alerter and ClipBook services are set to allow full control; all other permissions are revoked.

Settings for System Services

Full Service Name	Service Name	Startup Type
.NET Framework Support Service	CORRTSvc	Disabled
Alerter	Alerter	Disabled
Application Layer Gateway Service	ALG	Disabled
Application Management	AppMgmt	Disabled
ASP .NET State Service	aspnet_state	Disabled
Automatic Updates	wuauserv	Automatic
Background Intelligent Transfer Service	BITS	Manual
Certificate Services	CertSvc	Disabled
Client Service for NetWare	NWCWorkstation	Disabled
ClipBook	ClipSrv	Disabled
Cluster Service	ClusSvc	Disabled
COM+ System Application	COMSysApp	Manual
COM+Event Services	EventSystem	Automatic
Computer Browser	Browser	Disabled
Cyrptographic Services	CryptSvc	Automatic
DCOM Server Process Launcher	DcomLaunch	Automatic
DHCP Client	Dhcp	Automatic
DHCP Server	DHCPServer	Disabled
Distributed File System	Dfs	Disabled
Distributed Link Tracking Client	TrkWks	Disabled

Full Service Name	Service Name	Startup Type
Distributed Link Tracking Server	TrkSvr	Disabled
Distributed Transaction Coordinator	MSDTC	Disabled (prior to Release 7.5) Manual (Release 7.5)
DNS Client	Dnscache	Automatic
DNS Server	DNS	Disabled
Error Reporting Service	ERSvc	Disabled
Event Log	Eventlog	Automatic
Fast User Switching Compatibility	FastUserSwitchingCompatibility	Disabled
Fax Service	Fax	Disabled
File Replication	NtFrs	Disabled
File Server for Macintosh	MacFile	Disabled
FTP Publishing Service	MSFtpsvc	Disabled
Help and Support	helpsvc	Disabled
HTTP SSL	HTTPFilter	Not Defined
Human Interface Device Access	HidServ	Disabled
IAS Jet Database Access	IASJet	Disabled
IIS Admin Service	IISADMIN	Not Defined
IMAPI CD-Burning COM Service	ImapiService	Disabled
Indexing Service	cisvc	Disabled
Infrared Monitor	Irmon	Disabled
Internet Authentication Service	IAS	Disabled

Full Service Name	Service Name	Startup Type
Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)	SharedAccess	Automatic
Intersite Messaging	IsmServ	Not Defined
IP Version 6 Helper Service	6to4	Disabled
IPSec Policy Agent (IPSec Service)	PolicyAgent	Automatic
Kerberos Key Distribution Center	Kdc	Not Defined
LED/LCD Manager	SALDM	Disabled
License Logging Service	LicenseService	Disabled
Logical Disk Manager	dmserver	Manual
Logical Disk Manager Administrative Service	Dmadmin	Manual
Message Queuing	msmq	Not Defined
Message Queuing Down Level Clients	mqds	Disabled
Message Queuing Triggers	Mqtgsvc	Disabled
Messenger	Messenger	Disabled
Microsoft POP3 Service	POP3SVC	Disabled
MS Software Shadow Copy Provider	SwPrv	Manual
MSSEARCH	MSSEARCH	Disabled
MSSQL$UDDI	MSSQL$UDDI	Disabled
MSSQLServerADHelper	MSSQLServerADHelper	Disabled
Netlogon	Netlogon	Automatic
NetMeeting Remote Desktop Sharing	mnmsrvc	Disabled

Full Service Name	Service Name	Startup Type
Network Connections	Netman	Manual
Network DDE	NetDDE	Disabled
Network DDE DSDM	NetDDEdsdm	Disabled
Network Location Awareness (NLA)	NLA	Manual
Network News Transfer Protocol (NNTP)	NntpSvc	Disabled
Network Provisioning Service	xmlprov	Disabled
NTLM Security Support Provider	NtLmSsp	Automatic
Performance Logs and Alerts	SysmonLog	Manual
Plug and Play	PlugPlay	Automatic
Portable Media Serial Number	WmdmPmSN	Disabled
Print Server for Macintosh	MacPrint	Disabled
Print Spooler	Spooler	Not Defined
Protected Storage	ProtectedStorage	Automatic
Remote Access Auto Connection Manager	RasAuto	Disabled
Remote Access Connection Manager	RasMan	Manual
Remote Administration Service	srvcSurg	Disabled
Remote Desktop Help Session Manager	RDSessMgr	Disabled
Remote Installation	BINLSVC	Disabled
Remote Procedure Call (RPC)	RpcSs	Automatic
Remote Procedure Call (RPC) Locator	RpcLocator	Not Defined

Full Service Name	Service Name	Startup Type
Remote Registry Service	RemoteRegistry	Automatic
Remote Server Manager	appmgr	Disabled
Remote Server Monitor	Appmon	Disabled
Remote Storage Notification	Remote_Storage_User_Link	Disabled
Remote Storage Server	Remote_Storage_Server	Disabled
Removable Storage	NtmsSvc	Manual
Resultant Set of Policy Provider	RSoPProv	Disabled
Routing and Remote Access	RemoteAccess	Disabled
SAP Agent	nwsapagent	Disabled
Secondary Logon	seclogon	Disabled
Security Accounts Manager	SamSs	Automatic
Server	lanmanserver	Automatic
SharePoint Timer Service	SPTimer	Disabled
Shell Hardware Detection	ShellHWDetection	Disabled
Simple Mail Transport Protocol (SMTP)	SMTPSVC	Disabled
Simple TCP/IP Services	SimpTcp	Disabled
Single Instance Storage Groveler	Groveler	Disabled
Smart Card	SCardSvr	Disabled
SNMP Service	SNMP	Disabled
SNMP Trap Service	SNMPTRAP	Disabled
Special Administration Console Helper	Sacsvr	Disabled

Full Service Name	Service Name	Startup Type
SQLAgent$* (* UDDI or WebDB)	SQLAgent$WEBDB	Not Defined
System Event Notification	SENS	Automatic
Task Scheduler	Schedule	Automatic
TCP/IP NetBIOS Helper Service	LmHosts	Automatic
TCP/IP Print Server	LPDSVC	Disabled
Telephony	TapiSrv	Not Defined
Telnet	TlntSvr	Disabled
Terminal Services	TermService	Manual
Terminal Services Licensing	TermServLicensing	Disabled
Terminal Services Session Directory	Tssdis	Disabled
Themes	Themes	Disabled
Trivial FTP Daemon	tftpd	Disabled
Uninterruptible Power Supply	UPS	Not Defined
Upload Manager	Uploadmgr	Disabled
Virtual Disk Service	VDS	Disabled
Volume Shadow Copy	VSS	Manual
Web Element Manager	elementmgr	Disabled
WebClient	WebClient	Disabled
Windows Audio	AudioSrv	Disabled
Windows Firewall/Internet Connection Sharing	SharedAccess	Not Defined
Windows Image Acquisition (WIA)	StiSvc	Disabled
Windows Installer	MSIServer	Manual

Full Service Name	Service Name	Startup Type
Windows Internet Name Service (WINS)	WINS	Disabled
Windows Management Instrumentation	winmgmt	Automatic
Windows Management Instrumentation Driver Extensions	Wmi	Manual
Windows Media Connect	WmcCds	Disabled
Windows Media Connect (WMC) Helper Service	WmcCdsLs	Disabled
Windows Media Services	WMServer	Disabled
Windows System Resource Manager	WindowsSystemResourceManager	Disabled
Windows Time	W32Time	Automatic
Windows User Mode Driver Framework	UMWdf	Disabled
WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Disabled
WinSIP	WinSIP	Disabled
Wireless Configuration	WZCSVC	Disabled
WMI Performance Adapter	WmiApSrv	Manual
Workstation	lanmanworkstation	Automatic
World Wide Web Publishing Service	W3SVC	Not Defined

Registry

The 7.2(1) or later security template modifies the access auditing for the following registry keys. These changes do not apply to earlier template versions.

Warning: The ICMSecurityHardening script cannot rollback changes made to Registry auditing.

Object Name	Group or User Name	Auditing
HKLM\Software	Everyone	Access Failure
HKLM\System	Everyone	Access Failure

File System

The 7.2(1) or later security template modifies the access auditing for the following files. These changes do not apply to earlier template versions.

Warning: The ICMSecurityHardening script cannot rollback changes made to File System access permissions.

Object Name	Group or User Name	Permissions
%SystemDrive%	Administrator, SYSTEM	Full Control (This folder, subfolders and files)
%SystemDrive%	CREATOR OWNER	Full Control (Subfolders and files only)
%SystemDrive%	Users	Read and Execute (This folder, subfolders and files)
arp.exe	Administrator, SYSTEM	Full Control
at.exe	Administrator, SYSTEM	Full Control
attrib.exe	Administrator, SYSTEM	Full Control
cacls.exe	Administrator, SYSTEM	Full Control
debug.exe	Administrator, SYSTEM	Full Control
edlin.exe	Administrator, SYSTEM	Full Control
eventtriggers.exe	Administrator, SYSTEM	Full Control
ftp.exe	Administrator, SYSTEM	Full Control
nbtstst.exe	Administrator, SYSTEM	Full Control
net.exe	Administrator, SYSTEM	Full Control
net1.exe	Administrator, SYSTEM	Full Control
netsh.exe	Administrator, SYSTEM	Full Control
netstat.exe	Administrator, SYSTEM	Full Control
nslookup.exe	Administrator, SYSTEM	Full Control
ntbackup.exe	Administrator, SYSTEM	Full Control
rcp.exe	Administrator, SYSTEM	Full Control
reg.exe	Administrator, SYSTEM	Full Control
regedt.exe	Administrator, SYSTEM	Full Control

Object Name	Group or User Name	Permissions
regini.exe	Administrator, SYSTEM	Full Control
regsvr32.exe	Administrator, SYSTEM	Full Control
rexec.exe	Administrator, SYSTEM	Full Control
route.exe	Administrator, SYSTEM	Full Control
rsh.exe	Administrator, SYSTEM	Full Control
sc.exe.exe	Administrator, SYSTEM	Full Control
secedit.exe	Administrator, SYSTEM	Full Control
subst.exe	Administrator, SYSTEM	Full Control
systeminfo.exe	Administrator, SYSTEM	Full Control
telnet.exe	Administrator, SYSTEM	Full Control
tftp.exe	Administrator, SYSTEM	Full Control
tlntsvr.exe	Administrator, SYSTEM	Full Control

Chapter 6

Applying Security with the Cisco Unified Contact Center Security Wizard

This chapter contains the following topics:

- About the Cisco Unified Contact Center Security Wizard, page 81
- Configuration and Restrictions, page 82
- How to Install the Wizard, page 82
- How to use the Wizard, page 83
- Example Security Wizard Usage, page 85
- Example Security Hardening Configuration Panels, page 86
- Example Windows Firewall Configuration Panels, page 88
- Example Network Isolation Configuration Panels, page 92

About the Cisco Unified Contact Center Security Wizard

The Cisco Unified Contact Center Security Wizard is a new security deployment tool for Cisco Unified ICM and the Cisco Unified Contact Center Enterprise, introduced after the publication of Unified ICM 7.2, that simplifies security configuration through its step-by-step wizard based approach.

The Security Wizard is a new graphical user interface to configure security by means of the Unified ICM and Unified Contact Center Enterprise security command-line utilities:

- The Security Hardening Utility
- The Windows Firewall Utility
- The Network Isolation Utility

The Security Hardening and Windows Firewall utility are two command-line security utilities that have existed since the 7.0 release. The Network Isolation Utility was introduced after the ICM 7.2 release.

The Cisco Unified Contact Center Security Wizard works with ICM 7,0, 7.1, 7.2, and 7.5. That is, all three security utilities within the wizard (the Security Hardening utility, the Windows Firewall utility, and the Network Isolation utility) can be used in ICM 7.0, 7.1, 7.2, and 7.5.

For the respective individual descriptions of each of these utilities, see the following chapters in this guide:

- Automated Security Hardening Settings on Windows Server 2003 (page 53)
- Windows Server 2003 Firewall Configuration (page 43)
- Applying IPSec with the Network Isolation Utility (page 81)

Configuration and Restrictions

The following are Security Wizard restrictions:

- While the Security Wizard does not interfere with applications that run on the network, it should be run only during the application maintenance window since it can potentially disrupt connectivity when you are setting up the network security.
- The Security Wizard works only
  – with ICM 7.x
  – on a Windows 2003 platform
- The Firewall Configuration Utility and the Network Isolation Utility require that they be configured after ICM is installed on the network. For more details, see Windows Server 2003 Firewall Configuration (page 43) and Applying IPSec with the Network Isolation Utility (page 23).

How to Install the Wizard

To install the wizard, run the file UCCSecurityWizard.exe and follow the online instructions.

When installed:

- The Security Wizard is placed in the “%SYSTEMDRIVE%\CiscoUtils\UCCSecurityWizard” directory.
- The Network Isolation Utility is placed in the “%SYSTEMDRIVE%\CiscoUtils\NetworkIsolation” directory

The Security Hardening Utility and the Windows Firewall utility and are both installed during the ICM or Unified Contact Center installation on all ICM or Unified Contact Center servers, releases 7.x(y).

When installed:

- The Security Hardening Utility is placed in the "%SYSTEMDRIVE%\CiscoUtils\SecurityTemplates" directory
- The Windows Firewall Utility is placed in the "%SYSTEMDRIVE%\CiscoUtils\FirewallConfig" directory

Note: If a security utility is not installed, the Security Wizard will still display the introductory page for that tool, the Next button is disabled and a note explaining the reason is displayed on the Introductory page for that tool.

How to use the Wizard

You must be a server administrator to use the features in the Security Wizard.

You can run the wizard using the shortcut installed under **Start > Programs > Cisco Unified Contact Center > Security Wizard**

Note:

- When you run the wizard, CSA service must be stopped.
- Before you use the wizard, you should read the chapters in this guide on each of the utilities included in the wizard to make sure you understand what the utilities do.

When running the Security Wizard, you are provided with a menu list of the security utilities (the Security Hardening, the Windows Firewall, and the Network Isolation Utility), and you run each, one at a time.

You can go back and forth on any menu selection to understand what each one contains. However, once you click the Next button for any particular feature, then you must either complete configuring or cancel to go back to the Welcome page.

The wizard is self explanatory with each utility having an introductory panel, configuration panel(s), a confirmation panel, and a status panel:

- **Introductory** panel:
  - Briefly describes what the specific utility does.
  - Warns if security utility files are missing or not installed.
  - Allows you to switch between utilities until you click the Next button.

- **Configuration** panel(s): Lists the options you can select to configure the utility and gathers your configuration input.
- **Confirmation** panel: Allows you to confirm your configuration choices or to go back and make changes.

  After you have entered all the required input, the confirmation panel is displayed and the Next button is replaced with the Finish button. This indicates that this is your last chance to make a change to your configuration selections.

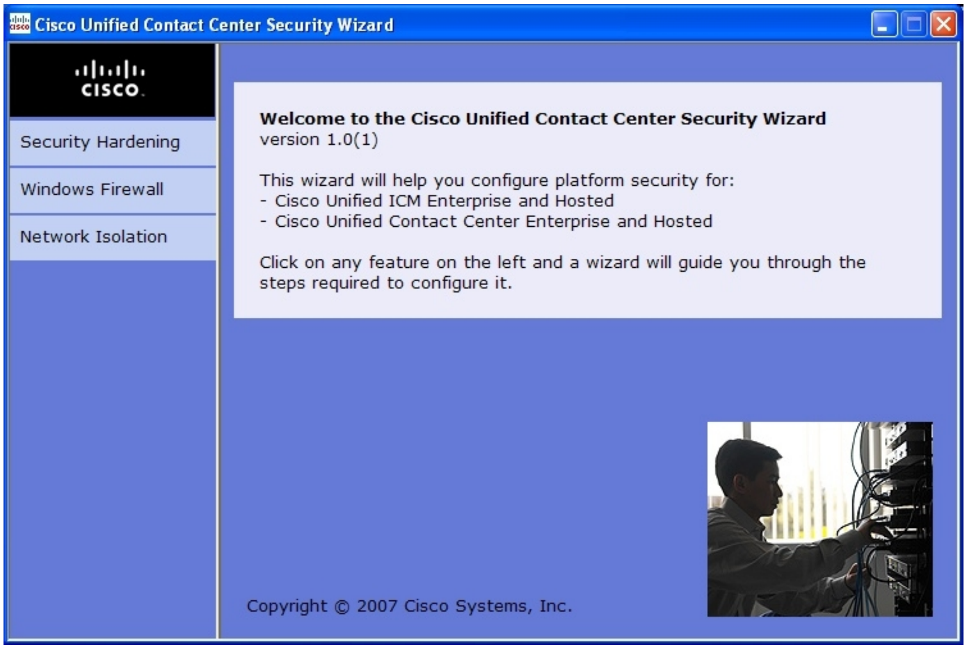
  Once you click finish, you can no longer go back.
- **Status** panel:
  - Displays the configuration command with all its required arguments.
  - Displays the streaming output of the configuration command while it is executing in the background.
  - Displays "Configuration Complete" and enables the "Go back to Welcome Panel' button once the command execution is complete.

The defaults are set to the recommended values and warnings are displayed if you make a selection that could cause a problem.

In the rare event of the back-end utility script dying, a temporary text file, created in the UCCSecurityWizard folder and containing the command-line output, is not deleted. You can use this text file to debug the issue.

Example Security Wizard Usage

Figure 10: Example Security Wizard Welcome Panel



Welcome to the Cisco Unified Contact Center Security Wizard
version 1.0(1)

This wizard will help you configure platform security for:
- Cisco Unified ICM Enterprise and Hosted
- Cisco Unified Contact Center Enterprise and Hosted

Click on any feature on the left and a wizard will guide you through the steps required to configure it.

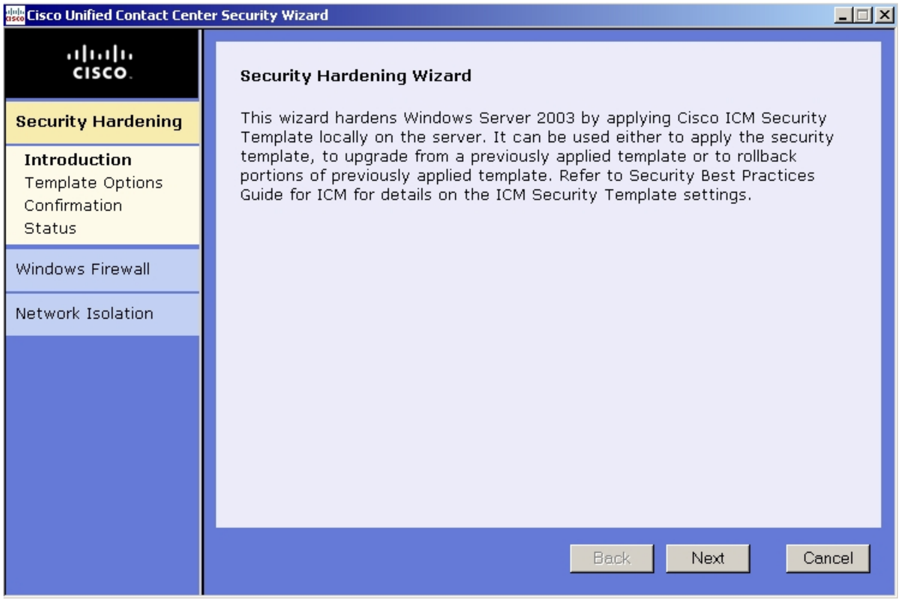
Copyright © 2007 Cisco Systems, Inc.

The Security Wizard requires the command line utilities to be installed on the system to configure security. It will detect if a utility is not installed and notify the user if it is not installed.

The Security Wizard can execute on all Unified ICM or Unified Contact Center Enterprise servers but will not execute on a Domain Controller.

Example Security Hardening Configuration Panels

Figure 11: Example Security Hardening Introduction Panel



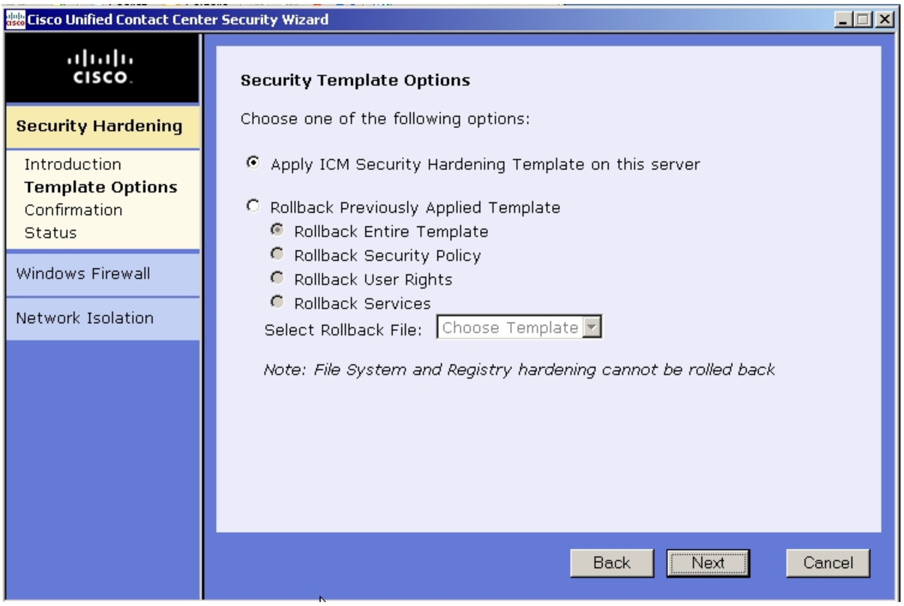
Security Hardening Wizard

This wizard hardens Windows Server 2003 by applying Cisco ICM Security Template locally on the server. It can be used either to apply the security template, to upgrade from a previously applied template or to rollback portions of previously applied template. Refer to Security Best Practices Guide for ICM for details on the ICM Security Template settings.

You can switch between utilities until you click the Next button at the bottom of the utility panel.

Bolded titles in the left menu bar indicate the selected utility and the selected step within that utility.

Figure 12: Example Security Hardening Template Options Panel



Security Template Options

Choose one of the following options:

● Apply ICM Security Hardening Template on this server

○ Rollback Previously Applied Template
- ● Rollback Entire Template
- ○ Rollback Security Policy
- ○ Rollback User Rights
- ○ Rollback Services

Select Rollback File: Choose Template

Note: File System and Registry hardening cannot be rolled back

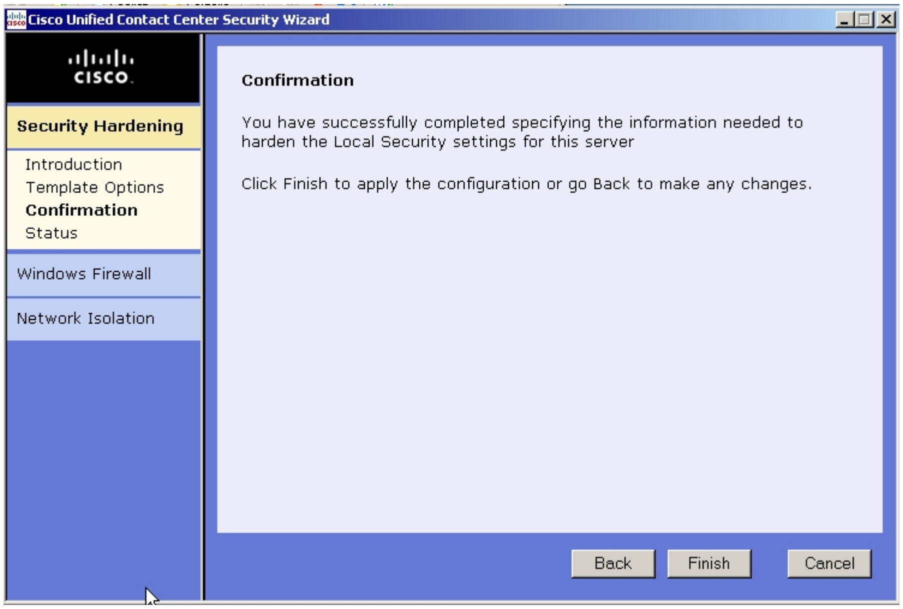
In the Security Hardening configuration window, you can:

- Apply the ICM Security Hardening template.
- Roll back part of or all of a previously applied ICM Security Hardening template.

See Automated Security Hardening Settings on Windows Server 2003 (page 53) for complete descriptions of the preceding configuration options.

The Rollback File selection list is dynamically populated.

Figure 13: Example Security Hardening Confirmation Panel



Cisco Unified Contact Center Security Wizard

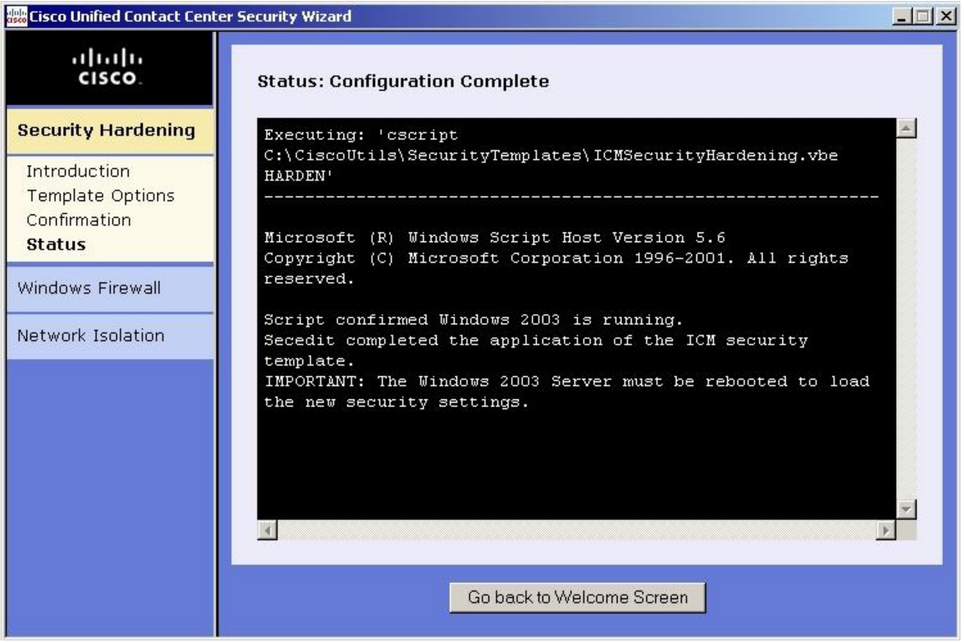
Confirmation

You have successfully completed specifying the information needed to harden the Local Security settings for this server

Click Finish to apply the configuration or go Back to make any changes.

At this point, you can still change any configuration selections. Once you click **Finish**, you can no longer change your selections.

Figure 14: Example Security Hardening Status Panel



Status: Configuration Complete

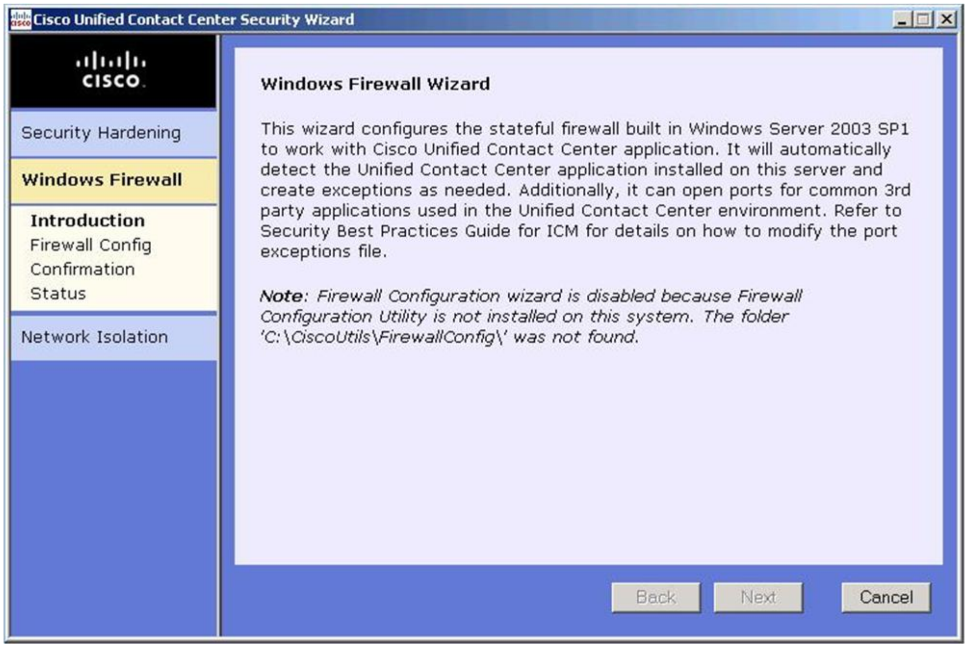
```
Executing: 'cscript
C:\CiscoUtils\SecurityTemplates\ICMSecurityHardening.vbe
HARDEN'
-----------------------------------------------------------

Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights
reserved.

Script confirmed Windows 2003 is running.
Secedit completed the application of the ICM security
template.
IMPORTANT: The Windows 2003 Server must be rebooted to load
the new security settings.
```

The status bar at the top of the panel tells you when the configuration is complete.

You may see some command-line windows open and close. That is normal in some command windows as different commands are executed.

Example Windows Firewall Configuration Panels

Figure 15: Example Windows FireWall Wizard Introduction Panel



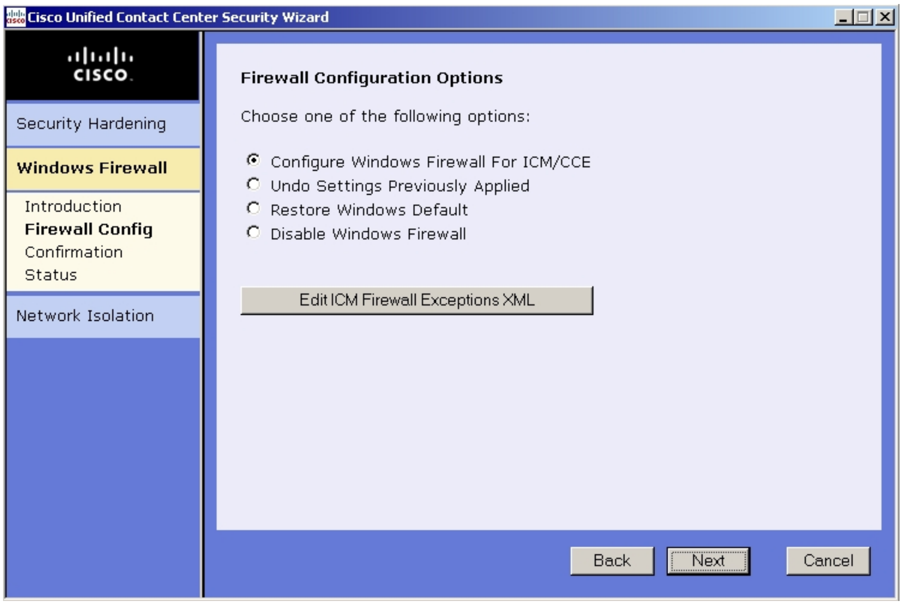
Windows Firewall Wizard

This wizard configures the stateful firewall built in Windows Server 2003 SP1 to work with Cisco Unified Contact Center application. It will automatically detect the Unified Contact Center application installed on this server and create exceptions as needed. Additionally, it can open ports for common 3rd party applications used in the Unified Contact Center environment. Refer to Security Best Practices Guide for ICM for details on how to modify the port exceptions file.

Note: Firewall Configuration wizard is disabled because Firewall Configuration Utility is not installed on this system. The folder 'C:\CiscoUtils\FirewallConfig\' was not found.

If the selected utility has not been installed on your system, you will get a message in this panel saying that.

Figure 16: Example Firewall Configuration Options Panel



Cisco Unified Contact Center Security Wizard

Firewall Configuration Options

Choose one of the following options:

● Configure Windows Firewall For ICM/CCE
○ Undo Settings Previously Applied
○ Restore Windows Default
○ Disable Windows Firewall

In the Security Wizard Firewall Configuration panel, you can:

- Configure a Windows firewall for your Unified ICM or Unified Contact Center Enterprise system
- Undo firewall configuration settings previously applied.
- Restore to Windows Default

Warning: The Default Windows firewall configuration is not compatible with the ICM application.

- Disable the Windows firewall.
- Edit the ICM Firewall Exceptions XML file. Clicking on the **Edit ICM Firewall Exceptions XML** button opens that XML file in Notepad. You must save the file and close it before continuing with the wizard.

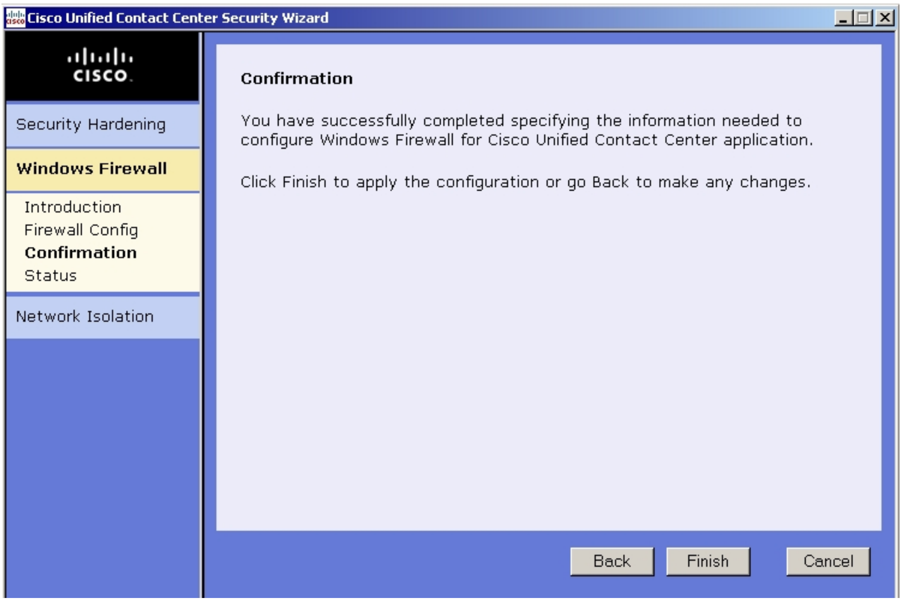
The Window Firewall Configuration Utility:

- Automatically detects ICM components installed and configures the Windows Firewall accordingly.

  Must be executed **after** the ICM application is installed.
- Can add custom exceptions such as an exception for VNC.
- Is installed by default on all Unified ICM and Unified Contact Center Enterprise servers.

See Windows Server 2003 Firewall Configuration (page 43) for a complete description of these configuration options.

Figure 17: Example Firewall Confirmation Panel

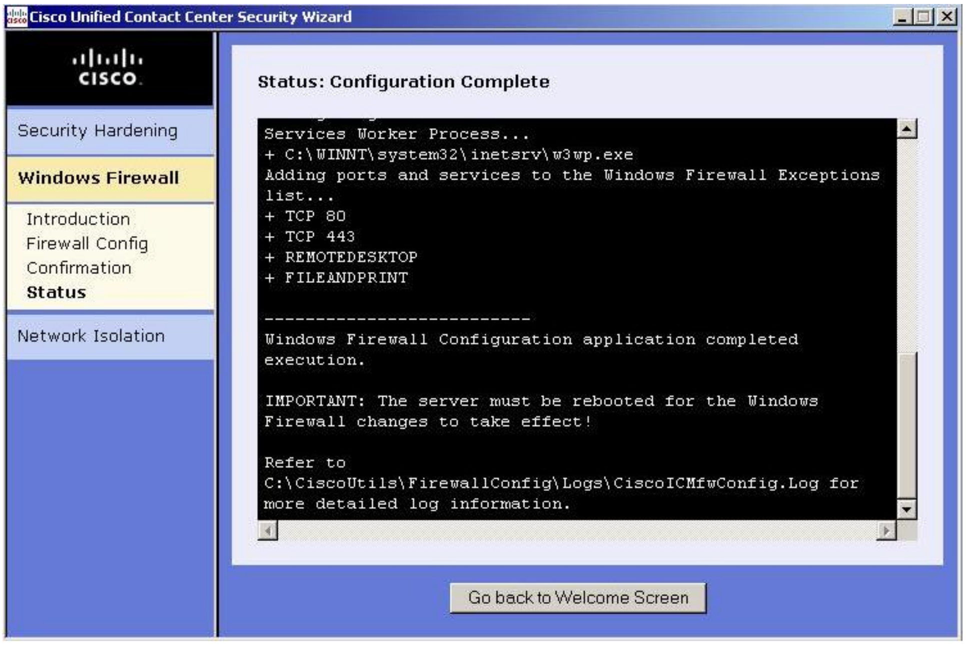


Confirmation

You have successfully completed specifying the information needed to configure Windows Firewall for Cisco Unified Contact Center application.

Click Finish to apply the configuration or go Back to make any changes.

Figure 18: Example Firewall Status Panel

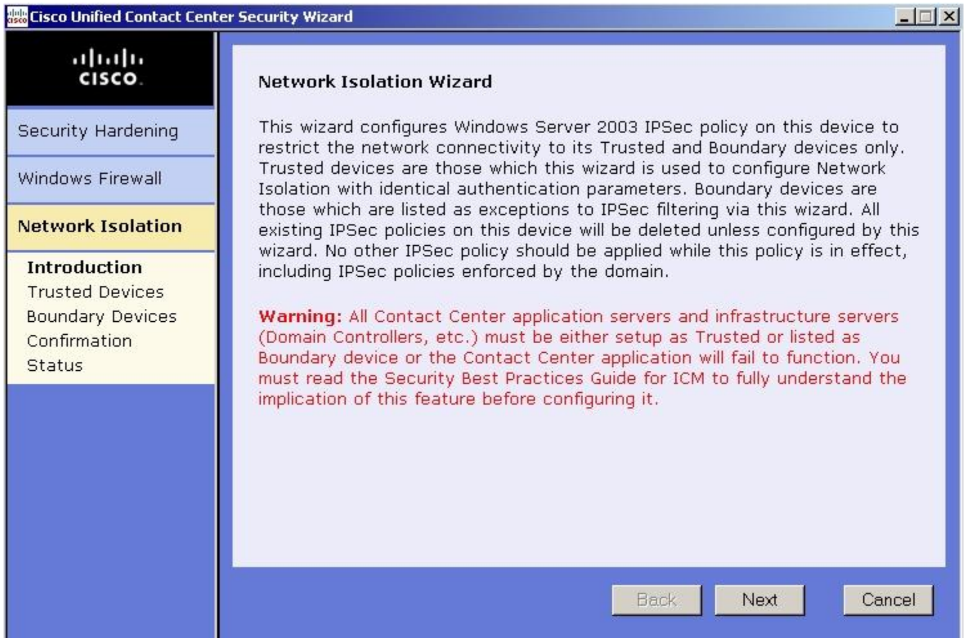


Status: Configuration Complete

```
Services Worker Process...
+ C:\WINNT\system32\inetsrv\w3wp.exe
Adding ports and services to the Windows Firewall Exceptions
list...
+ TCP 80
+ TCP 443
+ REMOTEDESKTOP
+ FILEANDPRINT

--------------------------
Windows Firewall Configuration application completed
execution.

IMPORTANT: The server must be rebooted for the Windows
Firewall changes to take effect!

Refer to
C:\CiscoUtils\FirewallConfig\Logs\CiscoICMfwConfig.Log for
more detailed log information.
```

Example Network Isolation Configuration Panels

Figure 19: Example Network Isolation Introductory Panel



Network Isolation Wizard

This wizard configures Windows Server 2003 IPSec policy on this device to restrict the network connectivity to its Trusted and Boundary devices only. Trusted devices are those which this wizard is used to configure Network Isolation with identical authentication parameters. Boundary devices are those which are listed as exceptions to IPSec filtering via this wizard. All existing IPSec policies on this device will be deleted unless configured by this wizard. No other IPSec policy should be applied while this policy is in effect, including IPSec policies enforced by the domain.

Warning: All Contact Center application servers and infrastructure servers (Domain Controllers, etc.) must be either setup as Trusted or listed as Boundary device or the Contact Center application will fail to function. You must read the Security Best Practices Guide for ICM to fully understand the implication of this feature before configuring it.

The preferred choice for deploying the Network Isolation Utility when configuring it for the first time or when editing an existing policy is through the Security Wizard.

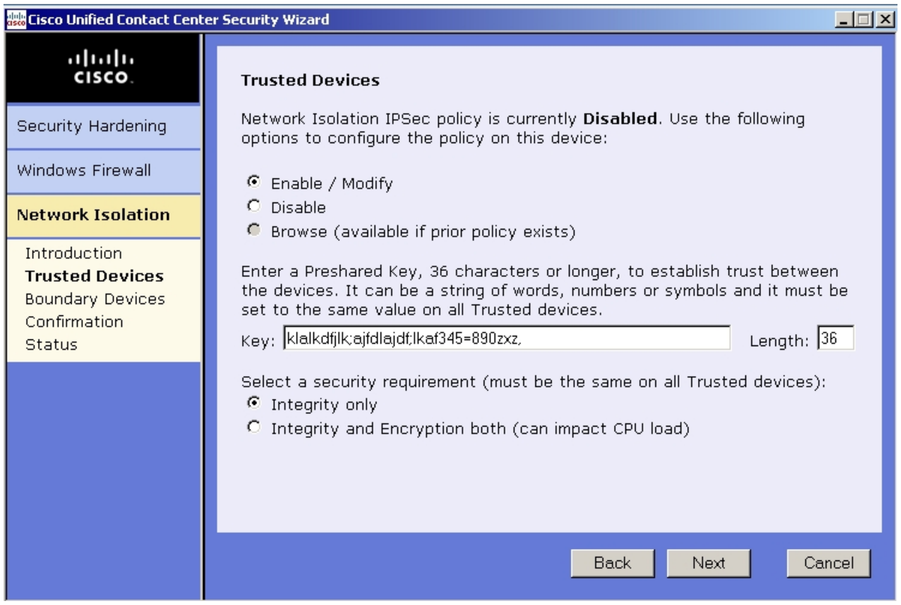
The reason for this is the following advantages not available in the command line interface. Through the Security Wizard interface:

- You can be guided with configuration panels that dynamically change according your input.
- You can browse the current policy.
- You can see the current Network Isolation configuration and edit it if you need to.
- You can add multiple Boundary Devices through a single Security Wizard panel whereas in the command line interface you need to create a separate command for each device you want to add.

The Network Isolation Utility must be run on every server that should be set as a Trusted Device. There is no need to run the utility on Boundary Devices.

For a complete description of the Network Isolation Utility, see Applying IPSec with the Network Isolation Utility (page 23)

Figure 20: Example Trusted Devices Configuration Panel



Trusted Devices

Network Isolation IPSec policy is currently **Disabled**. Use the following options to configure the policy on this device:

- ● Enable / Modify
- ○ Disable
- ○ Browse (available if prior policy exists)

Enter a Preshared Key, 36 characters or longer, to establish trust between the devices. It can be a string of words, numbers or symbols and it must be set to the same value on all Trusted devices.

Key: klalkdfjlk;ajfdlajdf;lkaf345=890zxz, Length: 36

Select a security requirement (must be the same on all Trusted devices):

- ● Integrity only
- ○ Integrity and Encryption both (can impact CPU load)

This panel and the next panel are loaded from the last configuration saved in the XML Network Isolation configuration file (not the Windows IPSec policy store), if it is available.

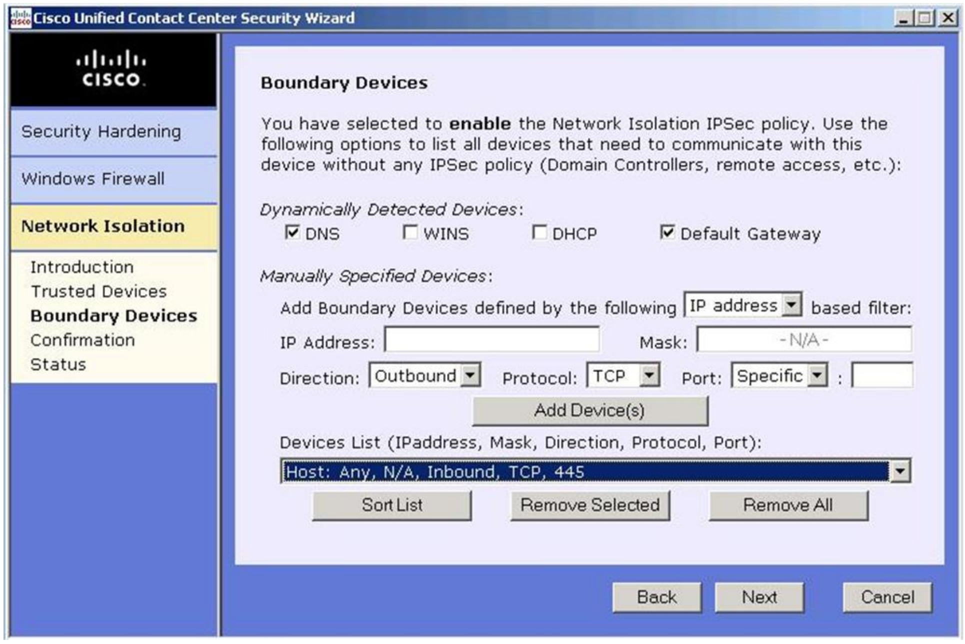
The Trusted Devices Panel:

- Shows the current status of the policy.
- Can be used to enable, modify, browse, or disable the policy.

> **Note:**
>
> - To enable or modify a device as Trusted you must enter a Preshared Key of 36 characters or more. The length of the key typed in is displayed and updated as you enter it to help you enter the correct length.
> - You can permanently delete the Network Isolation Utility policy only through the command line.

You must use the same Preshared Key on all Trusted Devices or else network connectivity between the Trusted Devices will fail.

Figure 21: Example Boundary Device Panel



Boundary Devices

You have selected to **enable** the Network Isolation IPSec policy. Use the following options to list all devices that need to communicate with this device without any IPSec policy (Domain Controllers, remote access, etc.):

Dynamically Detected Devices:

☑ DNS ☐ WINS ☐ DHCP ☑ Default Gateway

Manually Specified Devices:

Add Boundary Devices defined by the following IP address based filter:

IP Address: Mask: -N/A-

Direction: Outbound Protocol: TCP Port: Specific :

Devices List (IPaddress, Mask, Direction, Protocol, Port):

Host: Any, N/A, Inbound, TCP, 445

This panel and the previous panel are loaded from the last configuration saved in the XML Network Isolation configuration file (not the Windows IPSec policy store), if it is available.

In the Boundary Devices panel:

- The content of the panel is dynamically modified based on the selection made in the previous panel:
  - If in the previous panel, you have disabled the policy, then the panel elements displayed here are disabled.
  - If in the previous panel, you have selected the browse option, then only the Boundary List of devices is enabled for browsing purposes.
- You can add or remove multiple boundary devices.
- You can add dynamically detected devices through check boxes.
- You can add manually specified devices through a port, an IP address, or a subnet. After specifying the device, you must click **Add Device** to add the device.

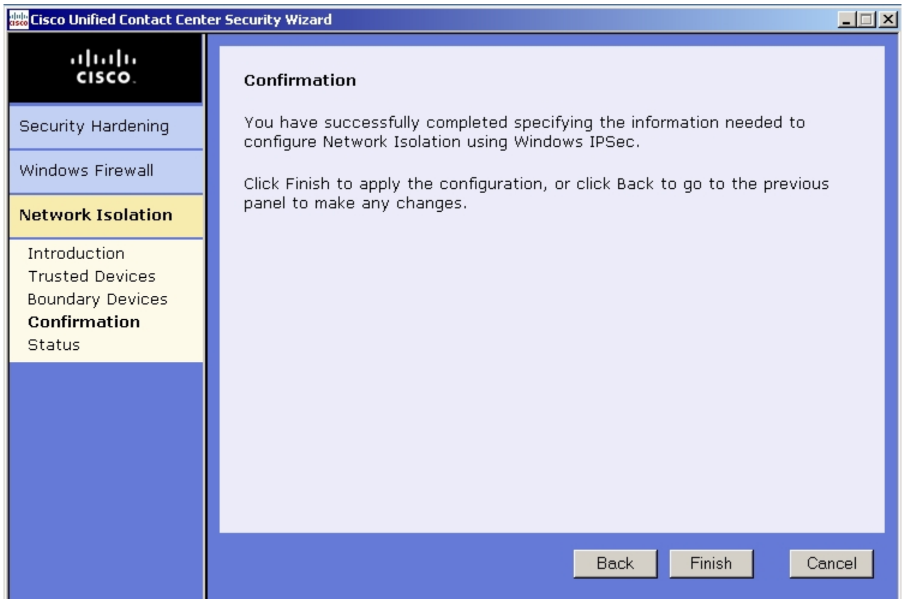
  The Add button validates the data and checks for duplicate entries before proceeding further.
- You can remove a device from the Boundary Devices by selecting it in the Devices List and clicking **Remove Selected**.

You can narrow down the exception based on:

- Direction of traffic: Outbound or Inbound
- Protocol: TCP, UDP, ICMP

- Any Port (only if TCP or UDP selected)
- A specific port or All ports

Figure 22: Example Network Isolation Confirmation Panel

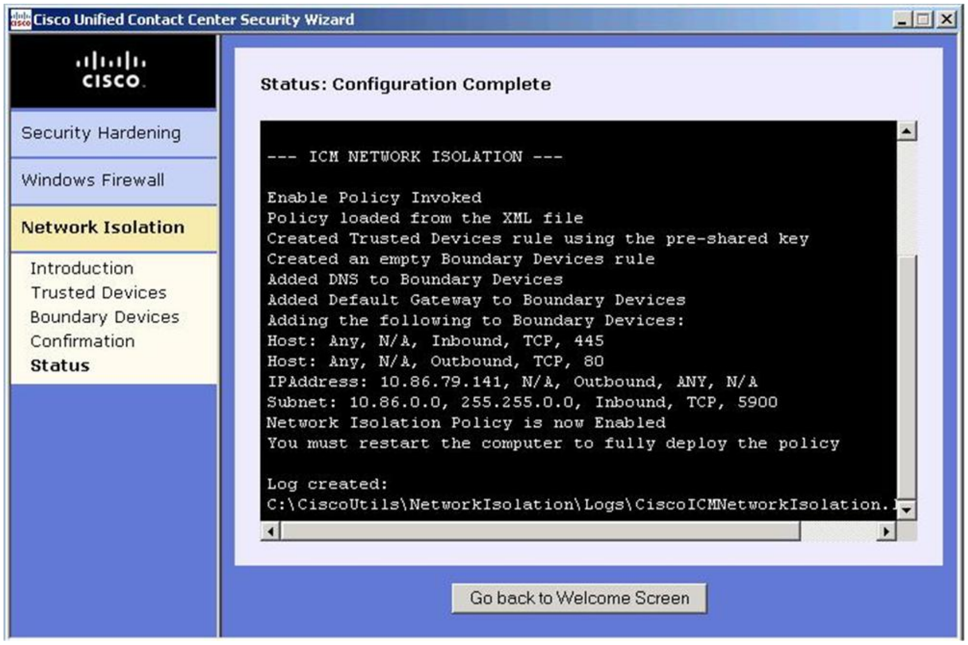


Confirmation

You have successfully completed specifying the information needed to configure Network Isolation using Windows IPSec.

Click Finish to apply the configuration, or click Back to go to the previous panel to make any changes.

Figure 23: Example Network Isolation Status Panel



Status: Configuration Complete

```
--- ICM NETWORK ISOLATION ---

Enable Policy Invoked
Policy loaded from the XML file
Created Trusted Devices rule using the pre-shared key
Created an empty Boundary Devices rule
Added DNS to Boundary Devices
Added Default Gateway to Boundary Devices
Adding the following to Boundary Devices:
Host: Any, N/A, Inbound, TCP, 445
Host: Any, N/A, Outbound, TCP, 80
IPAddress: 10.86.79.141, N/A, Outbound, ANY, N/A
Subnet: 10.86.0.0, 255.255.0.0, Inbound, TCP, 5900
Network Isolation Policy is now Enabled
You must restart the computer to fully deploy the policy

Log created:
C:\CiscoUtils\NetworkIsolation\Logs\CiscoICMNetworkIsolation.
```

Chapter 7

Updating Microsoft Windows

Note: For the currently supported Windows operating system software, see the latest **Hardware and System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise and Hosted Editions** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

This chapter contains the following topics:

- Microsoft Security Updates, page 97
- Microsoft Service Pack Policy, page 98

Microsoft Security Updates

Automatically applying security and software update patches from third-party vendors is not without risk. Although the risk is generally small, subtle changes in functionality or additional layers of code may alter the overall performance of Cisco Contact Center products.

Cisco recommends that Contact Center customers assess all security patches released by Microsoft and install those deemed appropriate for their environments. Customers are specifically cautioned not to automatically enable Microsoft Windows Update. The update schedule can conflict with other ICM/IPCC activity. Customers should consider using Microsoft Software Update Service or similar patch management products to selectively apply Critical and Important security patches and follow Microsoft's guidelines regarding when and how they should apply these updates.

Cisco provides a complimentary service of assessing the impact of Microsoft security patches and, where necessary, qualifying higher severity security patches that may be relevant to the ICM/IPCC Enterprise and ICM/IPCC Hosted software products. The impact assessment process results in the application of one of three categorical ratings to the updates:

1. **Impacting**

Microsoft labels the update as critical, important, or otherwise of special interest, and it directly affect the Cisco Unified Customer Contact software product. In other words, the update affects some software component or function (or is basic to the operating system and affects all operations for any software), or it applies to the latest supported Cisco Unified Customer Contact software product qualified service pack(s). Cisco recommends installing such an update. In the unlikely event that problems are found with a particular update, Cisco tests and qualifies the faults before approving the use of the security update with Cisco Unified Customer Contact software products.

2. **Deferred**

   Microsoft labels the update as critical, important, or is otherwise of special interest, but it does not directly affect Cisco Unified Customer Contact software product components or functions during regular use of the software. Qualification testing is typically deferred and performed with the next maintenance release of the product. The release notes of the maintenance release describe the applicability of all security updates relative to that maintenance release.

3. **Not Applicable**

   The update does not apply to the latest supported Cisco Unified Customer Contact software product, regardless of product applicability or Microsoft rated severity. Cisco performs no additional qualification testing.

Until April 2008, all Microsoft security update assessment notices were sent as Field Notices. Starting May 2008, the Impact Assessment bulletin is published on Cisco Security Center as well as being available as a free RSS feed. You can obtain the Impact Assessment bulletin by visiting Cisco Security Center at **http://www.cisco.com/security**, click on IntelliShield Event Responses, select the month/year of the bulletin required, and then look for Contact Center Impact Assessment section. You can also subscribe to the IntelliShield Event Responses RSS feed at **http://tools.cisco.com/security/center/eventResponses_20.xml**. Please note, the IntelliShield Event Responses bulletin is made available on the same day when Microsoft releases the security update, which is typically the second Tuesday of the month. However, the Contact Center Impact Assessment section is added to the bulletin typically a few days after that.

Note: Cisco recommends that Contact Center customers assess the security exposure of the critical security patches released by Microsoft for Windows, IIS and SQL and apply critical security patches as deemed necessary for their site ahead of the Impact Assessment bulletin.

See Cisco Customer Contact Software Policy for Third-Party Software/Security Updates at **http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_bulletins_list.html**

Microsoft Service Pack Policy

Do not automatically apply Microsoft Service Packs for the Operating system or SQL Server. Cisco qualifies service packs through extensive testing and defines compatible service packs in each product's Bill of Materials.

The Microsoft Windows Automatic Update Client can be configured to poll a server that is running Microsoft Software Update Services (SUS) or Windows Server Update Services in place of the default Windows Update Web site to retrieve updates.

This is the recommended approach to be able to selectively approve updates and determine when they get deployed on production servers.

To use Automatic Updates with a server that is running Software Update Services, see the Software Update Services Deployment white paper. To view this white paper, visit the following Microsoft Web site: **http://www.microsoft.com/windowsserversystem/updateservices/techinfo/previous/susdeployment.mspx**

Configuring the Server to use an Alternate Windows Update Server

To configure the server to use an alternate Windows Update server:

Step 1 Select **Start** > **Run** and type `regedit` in the dialog. Click OK.

Warning: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

Step 2 In regedit, locate and then click the following key in the registry:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU`

Step 3 Edit (or add) the following setting:

Value name: UseWUServer

Registry Value Type: Reg_DWORD

Value data: Set this value to 1 to configure Automatic Updates to use a server that is running Software Update Services instead of Windows Update.

Step 4 To determine the server that is running SUS that your client computers and servers go to for their updates, add the following registry values to the registry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\`

Value name: WUServer

Registry Value Type: Reg_SZ

This value sets the SUS server by HTTP name (for example, http://IntranetSUS).

Value name: WUStatusServer

Registry Value Type: Reg_SZ

This value sets the SUS statistics server by HTTP name

Chapter 8

SQL Server Hardening

SQL Server Hardening Suggestions

Top Hardening Suggestions

Top Hardening Suggestions:

1. Do not install SQL Server on an Active Directory Domain Controller.

2. In a multi-tier environment, run Web logic and business logic on separate computers. For example, WebView servers can be deployed on a dedicated server not shared with an Admin Workstation.

3. Install latest applicable SQL Server service pack and security updates. Refer to the *Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted* for the compatible service pack for your product.

4. Set a strong password for the ‘sa' account before installing the ICM software (see SQL Server Users and Authentication (page 104)).

5. Always install SQL Server service to run using a least privilege account. Never install SQL Server to run using the built in Local System account. Follow the steps below to modify the SQL Server service account.

   Note: The following assumes the SQL Server has been installed prior with the service configured to run as the ‘LocalSystem' Account. It's possible these steps can be shortened if the SQL Server is installed initially to run using a least privileged account. See the ICM Staging Guide for more information on how to properly install SQL Server using a Domain User Account to run the MSSQL Server service.

a. Create a Windows domain user account (e.g., <domain>\SQLServiceAcct>). (See Staging Guide for details). Appropriate file system permissions (Modify) must be given to this user account for the \mssql\data directory to be able to create, expand or delete databases as needed by the ‘icmdba' application.

b. Configure Security Account Delegation in Active Directory (Users folder) for this account:

   From the ‘Account' property page, select ‘Account is trusted for delegation'.

   Make sure ‘Account is sensitive and cannot be delegated' is NOT selected.

c. Configure Security Account Delegation in Active Directory (Computers folder) for each machine that has SQL (or MSDE) installed:

   Select ‘Trust computer for delegation' on the ‘General' property page.

d. Have a Domain Administrator configure Security Account Delegation using the SetSPN utility from the Windows 2000 resource kit to set a Service Principal Name as follows:

   List the existing SPN for the machine by typing the following at a command prompt: **`setspn -L <machine>`**

   Delete any existing SPN for the MSSQLSvc entry by typing the following at a command prompt: **`setspn -D "MSSQLSvc/<machine:port> <serviceaccountname>" <machine>`**[1]

   Create a new SPN entry for the MSSQLSvc entry by typing the following at a command prompt: **`setspn -A "MSSQLSvc/<machine:port> <serviceaccountname>" <machine>`**

e. Add the domain user account created in Step a. to the NTFS permissions for the Operating System and data partitions at the root level (e.g., C:\). Allow all permissions, except Full Control.

   Note: In Release 7.5, the SQL Server 2005 automated hardening utility, as well as the ICMDBA tool, will automatically ensure this permission is appropriately granted.

f. Finally, add this domain user account created in Step a. to the Registry permissions for the HKEY_LOCAL_MACHINE\Software, HKEY_LOCAL_MACHINE\System and HKEY_USERS hives, giving it Full Control.

g. From the SQL Server Enterprise Manager (for SQL Server 2000), or from the SQL Server Configuration Manager (for SQL Server 2005), configure the SQL Server service to run as the domain user account created in Step a. (e.g., <domain>\SQLServiceAcct>).

[1] The string inside quotes must match exactly what is seen in the List command:: setspn -L <machine>

6. For releases earlier than Release 7.5, SQL Server Agent Service may be disabled if not used. However, in Release 7.5, SQL Server Agent Service **MUST** be enabled and set to Automatic for database maintenance functioning in ICM.

   Note: Applying SQL Server security updates or hotfixes may require that the SQL Server Agent service be disabled. It is recommended that this service should be reset to 'disabled' before performing the update. When the update has completed, stop the service and set it back to 'enabled'.

7. In all releases prior to 7.5, the Distributed Transaction Coordinator, MSDTC, is disabled (this is done by default by the automated server hardening in the Cisco ICM Security Template Settings shipped with 7.0, 7.1, and 7.2).

   However, in Release 7.5, MSDTC services must be set to manual (done by default by the automated server hardening in the Cisco ICM Security Template shipped with 7.5).

   Note: The SQLServerAgent and MSDTC services may be used for 3rd Party Backup solutions therefore we recommend checking the Backup Agents' system requirements before disabling these services.

8. Use NTFS directory security with EFS for SQL Server data directories. EFS must be set while logged in under the account credentials that the SQL service will run under (e.g., <domain>\SQLServiceAcct>). From the Local Policy editor, temporarily grant 'logon locally' privileges to this account to enable EFS then remove this right after logging off.

Warning: EFS should only be enabled if there is a concern with data theft as there will be a performance impact.

   Note: In order to copy and send the data to other parties, it will be necessary to backup the database to a different directory that is not encrypted to ensure that the receiving party is able to read the data in the backup. This can be accomplished by backing up the database from the SQL Server Enterprise Manager.

9. Disable the SQL guest account.

10. Restrict sysadmin membership to your ICM administrators.

11. Block TCP port 1433 and UDP port 1434 at the firewall except for when the ICM distributor or administrative workstation is not in the same security zone as the ICM Logger.

12. Protection by good housekeeping:

    a. Run the KillPwd utility to remove password data from setup files. Detailed instructions on how to run this utility can be found in KB Article Q263968 at **http://support.microsoft.com/default.aspx?scid=kb;en-us;263968**

    b. Delete or secure old setup files: Delete or archive the following files after installation: sqlstp.log, sqlsp.log, and setup.iss in the <systemdrive>:\Program Files\Microsoft SQL Server\MSSQL\Install folder for a default installation, and the <systemdrive>:\Program Files\Microsoft SQL Server\ MSSQL$<Instance Name>\Install folder for named instances.

If the current system is an upgrade from SQL Server 7.0, delete the following files: setup.iss in the %Windir% folder, and sqlsp.log in the Windows Temp folder.

13. Change the recovery actions of the Microsoft SQL Server service to restart after a failure.
14. Remove all sample databases, e.g., Pubs and Northwind.
15. Enable auditing for failed logins.

SQL Server Users and Authentication

When creating a user for the SQL Server account, create Windows accounts with the lowest possible privileges for running SQL Server services. It is preferable that this be done during the installation of SQL Server.

The local user or the domain user account that is created to function as SQL Server service account follows the Windows or domain password policy respectively. It is imperative that a strict password policy is applied on this account. However, the password should not be set to expire else SQL Server service will cease to function and that in turn will cause ICM to fail.

The password and account settings may be governed by the site requirements. At the least, the following is recommended:

Setting	Value
Enforce Password History	24 passwords remembered
Minimum Password Length	12 characters
Password Complexity	Enabled
Minimum Password Age	1 day
Account Lockout Duration	15 minutes
Account Lockout Threshold	3 invalid logon attempts
Reset Account Lockout Counter After	15 minutes

Note: The service account password must *explicitly* be set to Not expire.

Use **Windows Only** authentication if possible. Cisco Contact Center applications use Windows authentication to access SQL Server. Cisco understands that some third party applications may require SQL Server authentication to run properly, but if you are not using any third party products to access SQL Server, then you should use **Windows Only** authentication, rather than mixed mode authentication.

Note: Windows Only authentication is enforced through SQL Server 2005 automated hardening introduced in Release 7.5.

Using mixed mode authentication can increase security risks.

During ICM setup, if the sa password is found to be blank, then a randomly generated strong password is generated and used to secure the sa account. **This randomly generated sa password is displayed only once during the install. Make note of the password as it is not presented**

again. Resetting of the sa account password may be done after installation by logging on to the SQL Server using a Windows Local Administrator account.

SQL Server 2005 Security Considerations

Microsoft SQL Server 2005 is far more secure by design, default, and deployment than Microsoft SQL Server 2000. Microsoft SQL Server 2005 provides a much more granular access control, a new utility to manage attack surface, and runs with lower privileges. To make the best out of the security features provided by Microsoft SQL Server 2005, it is necessary that the database administrator follow the best practices as described below in the "Automated SQL 2005 Hardening" and the "Manual SQL 2005 Hardening" sections.

Automated SQL 2005 Hardening

The first step in securing the deployment is to install and enable only those components or features that are required all the time. If a feature is required only for certain limited activity, then that feature should be disabled during regular operation and enabled only as needed.

Cisco provides the SQL Server Security Hardening utility to automatically disable unwanted SQL Server services and features. ICM/IPCC Setup and Upgrade prompt the user to run the SQL Server Security Hardening utility in the same manner as it does for Windows Security Hardening.

SQL Server 2005 breaks down the server functionality into more granular services. The following table lists them with the secure deployment recommendations -- which are automatically set by the SQL Server Security Hardening utility:

Service	Startup Type
SQL Server Database Engine	Automatic
SQL Server Active Directory Helper	Disabled
SQL Server Agent	Automatic
SQL Server FullText Search	Automatic
SQL Server Browser	Disabled
SQL Server VSS Writer	Disabled

The above settings can be viewed or modified using *SQL Server Surface Area Configuration – Services and Connection* tool.

The following table lists the various features available in SQL Server 2005 and the state that they must be configured in to secure the deployment for ICM. These are automatically set by the SQL Server Security Hardening utility:

Feature	Enabled
Ad-hoc Remote Queries (use of OPENROWSET and OPENDATASOURCE)	N
CLR Integration	N

Feature	Enabled
DAC (Dedicated Administrator Connection for remote access)	N
Database Mail	N
Native XML Web Service (access over HTTP)	N
OLE Automation	N
Service Broker (to communicate between instances)	N
SQL Mail	N
Web Assistant (Deprecated in SQL Server 2005)	N
Xp_cmdshell	N

The above settings can be viewed or modified using *SQL Server Surface Area Configuration – Features* tool.

The SQL Server Security Hardening utility also:

- Enforces Windows Only authentication mode.
- Verifies that the named pipe (np) is listed before tcp ip (tcp) in the SQL Server Client Network Protocol Order.

SQL Server Security Hardening Utility

The SQL Server Security Hardening utility allows you to Harden or Rollback the SQL Server security on ICM Logger and AW/HDS components. The Harden option disables unwanted services and features, as explained in the "Automated SQL 2005 Hardening" section above. If the latest version of the security settings are already applied, then the Harden option does not change anything. The Rollback option allows you to return to the state of SQL services and features that existed prior to your applying the last hardening.

The SQL Server Security Hardening utility is launched via Setup, by default, to harden the SQL Server security. However, you can run it manually, as described below.

Utility Location

The utility is located at:

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity
```

Harden SQL Server

From the command line type in

```
Perl ICMSQLSecurity.pl HARDEN
```

Note: The current SQL Server configuration will be backed up to <ICMInstallDrive>:\CiscoUtils\SQLSecurity\ICMSQLSEcurity.bkp before applying the SQL Server hardening.

Rollback SQL Server Security Hardening

The ROLLBACK command rolls back to the previous SQL Server configuration, if hardening was applied before.

To rollback to the previous SQL Server configuration, from the command line type in

```
Perl ICMSQLSecurity.pl ROLLBACK
```

No Argument

If no argument is used with the command line, usage help is displayed.

Output Log

All output logs are saved in the file:

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity\Logs\ICMSQLSecurity.log
```

Manual SQL 2005 Server Hardening

By default, SQL Server 2005 disables VIA endpoint and limits the Dedicated Administrator Connection (DAC) to local access. Also, by default, all logins have GRANT permission for CONNECT using Shared Memory, Named Pipes, TCP/IP and VIA end points. ICM requires only Named Pipes and TCP/IP endpoints.

- Enable both Named Pipes and TCP/IP endpoints during SQL Server 2005 setup. Make sure Named Pipes has a higher order of priority than TCP/IP.

  Note: The SQL Server Security Hardening utility will check for the availability and order of these endpoints.

- Disable access to all endpoints that are not required. For instance: Deny connect permission to VIA endpoint for all users/groups who have access to the database

Chapter 9

Cisco SSL Encryption Utility

About the SSL Encryption Utility

In ICM release 7.x(y), ICM web servers are configured for secure access (HTTPS) using SSL. Cisco provides an application called the SSL Encryption Utility (SSLUtil.exe) to help with the task of configuring web servers for use with SSL.

Note: This utility is only supported on servers running Windows Server 2003.

The operations performed by the SSL encryption utility can also be accomplished by the operating system facilities such as IIS, however the Cisco utility simplifies the process.

SSLUtil.exe is located in the <ICMInstallDrive>\icm\bin folder. The SSL Encryption Utility can be invoked in either standalone mode or automatically as part of setup.

The SSL Encryption Utility generates log messages pertaining to the operations that it performs. When running as part of setup, log messages are written to the setup log file. In standalone mode, the log messages are only displayed on the SSL Utility Window.

The SSL Encryption Utility performs two major functions:

- SSL Configuration
- SSL Certificate Administration

SSL is only available for ICM web applications installed on Windows Server 2003. The ICM/IPCC web applications that can be configured for SSL are:

- WebView
- IPCC Web Administration (System IPCC)

- Internet Script Editor
- Agent Re-skilling

Installing SSL During Setup

By default, setup enables SSL for IPCC Web Administration, Internet Script Editor and Agent Re-skilling applications. SSL can be configured for WebView during setup. By default, Authentication mode is selected for WebView during setup. For more detail on SSL for WebView application, refer to "SSL Configuration at ICM Setup" in *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*. If the SSL settings are changed via other means such as IIS manager while the SSL Configuration Utility is open, those changes are not reflected in the SSL Configuration Utility unless it is closed and reopened.

The SSL Configuration Utility also facilitates creation of self-signed certificates and installation of the created certificate in IIS. A certificate may also be removed from IIS using this tool. When invoked as part of setup, the SSL Configuration Utility sets SSL port in IIS to 443 if it is found to be blank.

If you want to use SSL for Agent Reskilling or Internet Script Editor, then you can just accept the default settings during installation and the supported servers will use SSL.

If you want to use SSL in WebView, leave **Enable Encryption** selected. You can further specify session encryption (all traffic is encrypted, not just the authentication process) during the WebView setup process; note that this increases server load significantly.

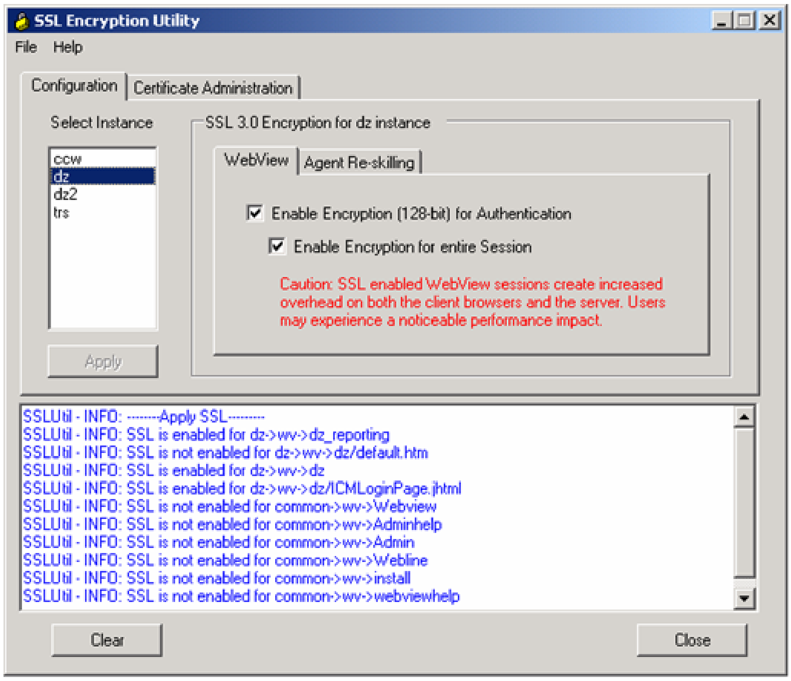
When the utility runs during setup a self-signed certificate is generated (using OpenSSL), imported into the Local Machine Store, and installed on the web server. Virtual directories are enabled and configured for SSL with 128-bit encryption.

Note: During setup, if a certificate exists or the Web Server is found to have an existing server certificate installed, a log entry is added and no changes take effect. Any certificate management changes must be done using the utility in standalone mode or directly using the IIS Services Manager.

SSL Encryption Utility in Standalone Mode

In standalone mode, the SSL Configuration Utility displays the list of the ICM instances installed on the local machine. When an ICM instance is selected, the web applications installed and their SSL settings are displayed. You can then alter the SSL settings for the web application.

Figure 24: SSL Config Utility - Configuration Tab



SSL 3.0 Encryption for dz instance

☑ Enable Encryption (128-bit) for Authentication

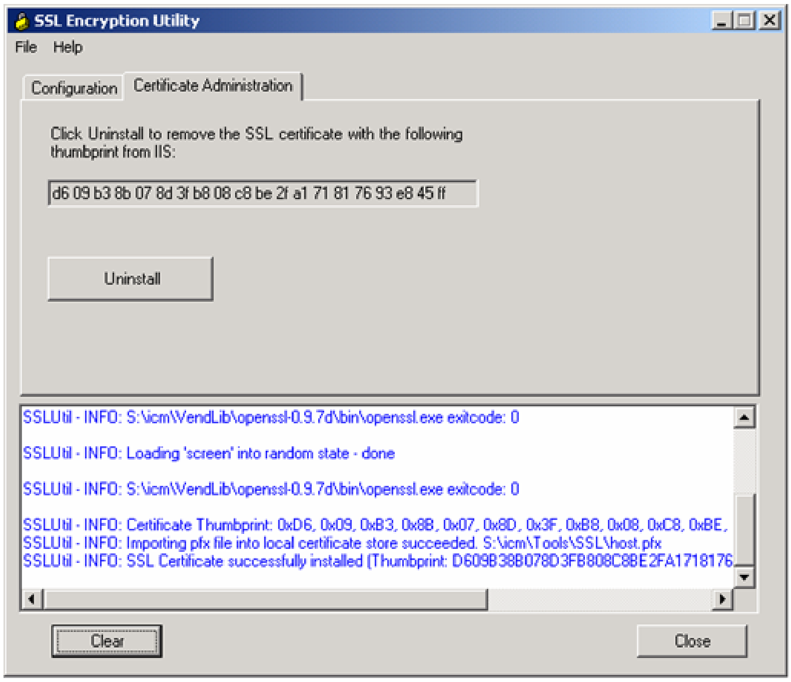
☑ Enable Encryption for entire Session

Caution: SSL enabled WebView sessions create increased overhead on both the client browsers and the server. Users may experience a noticeable performance impact.

```
SSLUtil - INFO: --------Apply SSL---------
SSLUtil - INFO: SSL is enabled for dz->wv->dz_reporting
SSLUtil - INFO: SSL is not enabled for dz->wv->dz/default.htm
SSLUtil - INFO: SSL is enabled for dz->wv->dz
SSLUtil - INFO: SSL is enabled for dz->wv->dz/ICMLoginPage.jhtml
SSLUtil - INFO: SSL is not enabled for common->wv->Webview
SSLUtil - INFO: SSL is not enabled for common->wv->Adminhelp
SSLUtil - INFO: SSL is not enabled for common->wv->Admin
SSLUtil - INFO: SSL is not enabled for common->wv->Webline
SSLUtil - INFO: SSL is not enabled for common->wv->install
SSLUtil - INFO: SSL is not enabled for common->wv->webviewhelp
```

The SSL Configuration Utility also facilitates creation of self-signed certificates and installation of the created certificate in IIS. A certificate may also be removed from IIS using this tool. When invoked as part of setup, the SSL Configuration Utility sets SSL port in IIS to 443 if it is found to be blank.

Figure 25: SSL Config Utility - Certificate Administration Tab



Click Uninstall to remove the SSL certificate with the following thumbprint from IIS:

d6 09 b3 8b 07 8d 3f b8 08 c8 be 2f a1 71 81 76 93 e8 45 ff

```
SSLUtil - INFO: S:\icm\VendLib\openssl-0.9.7d\bin\openssl.exe exitcode: 0

SSLUtil - INFO: Loading 'screen' into random state - done

SSLUtil - INFO: S:\icm\VendLib\openssl-0.9.7d\bin\openssl.exe exitcode: 0

SSLUtil - INFO: Certificate Thumbprint: 0xD6, 0x09, 0xB3, 0x8B, 0x07, 0x8D, 0x3F, 0xB8, 0x08, 0xC8, 0xBE,
SSLUtil - INFO: Importing pfx file into local certificate store succeeded. S:\icm\Tools\SSL\host.pfx
SSLUtil - INFO: SSL Certificate successfully installed (Thumbprint: D609B38B078D3FB808C8BE2FA1718176
```

Enabling the Transport Layer Security (TLS) 1.0 Protocol

In ICM release 7.2(1) or later, hardening settings on Windows Server 2003 secure the IIS webserver by default. Specifically, the security template enables FIPS compliant strong encryption, which requires the TLS 1.0 protocol be enabled instead of SSL 2.0 or SSL 3.0. TLS 1.0 is enabled on Internet Explorer 7.0 by default, but is not enabled on Internet Explorer 6.0. To ensure Web browser connectivity to a hardened Webview, Dynamic Reskilling (Agent Reskilling), or SIPCC Webconfig server over HTTPS using Internet Explorer 6, you need to enable TLS 1.0 protocol.

Step 1 Launch **Internet Explorer 6.0**.

Step 2 On the **Tools** menu, click **Internet Options**.

Step 3 Select the **Advanced** tab.

Step 4 Scroll to **Security** and select the **Use TLS 1.0** checkbox.

Be sure to consult the Microsoft Knowledge Base (KB)**KB811833** (http://support.microsoft.com/kb/811833)for additional information about security settings.

Note: If security hardening is applied using the 7.2(1) or later template but Internet Explorer is *not* configured to support the TLS 1.0 protocol, the Web browser will not be unable to connect to the Web server. An error message indicates that the page is either unavailable or that the Web site might be experiencing technical difficulties.

Chapter 10

Intrusion Prevention and Cisco Security Agent

The Cisco Security Agent (CSA) provides Host Intrusion Detection and prevention for servers. As high-visibility network security attacks such as Code Red and the SQL Slammer worm have shown, traditional host and desktop security technologies are limited in their capability to combat the effects of new and evolving virus attacks. Unlike traditional signature matching security technologies, CSA analyzes virus behavior to provide robust protection with reduced operational costs. By identifying and preventing malicious behavior before it occurs, CSA removes potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications.

Note: You should not view CSA as providing complete security for servers running Cisco ICM software. Rather, you should view CSA as an additional line of defense which, when used with other standards defenses such as virus scanning software, firewalls, and the documented guidelines, as providing enhanced security for ICM software servers.

This chapter contains the following topics:

- What are Cisco Security Agent Policies?, page 113
- Types of Agents, page 114

What are Cisco Security Agent Policies?

The Cisco Security Agent provides protection for Windows platforms based on a set of rules, or policies, that you set. Policies define which actions on the system and network are allowed and denied. Cisco Security Agent checks actions that use system or network resources and blocks denied actions.

You define policies to control access to system and network resources based on the following parameters:

- Which resource is being accessed

- Which operation is being invoked
- Which process is invoking the action

Cisco has defined a policy for CSA to protect servers without interfering with the normal operations of ICM software. You can download this policy from the **Cisco Web site** (www.cisco.com).

Note: If you do use CSA, then consult the following guide for important information regarding installing ICM/IPCC applications using their default paths. Installing ICM/IPCC application to their default paths minimizes any issues that may arise out of using CSA with supported applications that have been installed in non-default locations.

See Also

Cisco Security Agent Installation/Deployment Guide for ICM/IPCC Enterprise & Hosted Editions

Types of Agents

You can use Cisco Security Agent as either a Standalone Agent or a Managed Agent.

Managed Agent

A Managed Agent reports all significant events to a centralized Management Center.

The Management Center serves multiple agents and servers simultaneously. The Management Center allows you to monitor and protect multiple servers using a browser-based console.

The Managed Agent is appropriate if you are using third-party software that is not approved by Cisco for ICM servers. If this is the case, it is recommended that you purchase and install the CSA Management Center, then import the ICM policy (page 113) and customize it to allow the third-part applications to operate.

Standalone Agent

The CSA Standalone Agent provides the same protections and the Managed Agent, but does not report events back to the Management Center. Furthermore, the Standalone Agent uses a static policy (page 113) that you cannot modify.

The Standalone Agent for ICM software is available free of charge from Cisco.

See Also

Cisco Security Agent on the Cisco Web Site (www.cisco.com/go/csa)

Chapter 11

Microsoft Baseline Security Analyzer (MBSA)

The Microsoft Baseline Security Analyzer checks computers running Microsoft Windows(R) Server 2003, Windows XP, Windows 2000, or Windows NT(R) 4.0 for common security mis-configurations.

The following are the scanning options selected for Cisco ICM Real-Time Distributor running one or more web applications (e.g. Internet Script Editor, WebView, or Agent-Reskilling).

- Windows operating system (OS) checks
- IIS checks
- SQL checks
- Security update checks
- Password checks

This report is provided to show an example of the results of running the MBSA tool against a Cisco ICM server that is running the majority of Microsoft Server Applications supported by the tool.

This chapter contains the following topics:

- Security Update Scan Results, page 116
- Windows Scan Results, page 116
- Internet Information Services (IIS) Scan Results, page 117
- SQL Server Scan Results, page 118
- Desktop Application Scan Results, page 119

Security Update Scan Results

Score	Issue	Result
✓	Windows Security Updates	No critical security updates are missing.
✓	IIS Security Updates	No critical security updates are missing.
✓	SQL Server/MSDE Security Updates	Instance (default): No critical security updates are missing.
✓	MDAC Security Updates	No critical security updates are missing.
✓	MSXML Security Updates	No critical security updates are missing.
	Office Security Updates	No Microsoft Office products are installed.

Windows Scan Results

Table 2: Vulnerabilities

Score	Issue	Result
ℹ	Automatic Updates	Automatic Updates are managed through Group Policy on this computer.
✗	Administrators	More than 2 Administrators were found on this computer. **Note:** This warning can be ignored given that the Cisco ICM application requires the addition of certain groups to the Local Administrators group, therefore triggering this event. It is recommended that you review the Result Details and remove any known unnecessary accounts.
✗	Password Expiration	Some user accounts (1 of 7) have non-expiring passwords. **Note:** When the server is properly configured to require expiring passwords, this warning will typically find the Guest account to have a non-expiring password even though the account is disabled. This warning can be ignored.
ℹ	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.
✓	Local Account Password Test	Some user accounts (1 of 7) have blank or simple passwords, or could not be analyzed.

Score	Issue	Result
✓	File System	All hard drives (1) are using the NTFS file system.
✓	Autologon	Autologon is not configured on this computer.
✓	Guest Account	The Guest account is disabled on this computer.
✓	Restrict Anonymous	Computer is properly restricting anonymous access.

Table 3: Additional System Information

Score	Issue	Result
✱	Auditing	Logon Success and Logon Failure auditing are both enabled.
✱	Services	Some potentially unnecessary services are installed.
ℹ	Shares	2 share(s) are present on your computer.
ℹ	Windows Version	Computer is running Windows 2000 or greater.

Internet Information Services (IIS) Scan Results

Table 4: Vulnerabilities

Score	Issue	Result
✓	IIS Lockdown Tool	The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations running IIS 6.0.
✓	Sample Applications	IIS sample applications are not installed.
✓	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
✓	Parent Paths	Parent paths are not enabled.
✓	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.

Table 5: Additional System Information

Score	Issue	Result
✱	Domain Controller Test	IIS is not running on a domain controller.
✱	IIS Logging Enabled	All web and FTP sites are using the recommended logging options.

SQL Server Scan Results

Instance (default)

Table 6: Vulnerabilities

Score	Issue	Result
✗	Sysadmin role members	BUILTIN\Administrators group is part of sysadmin role. **Note:** This is acceptable because the Cisco ICM application adds certain groups to the local Administrators account on the server which require dbo access to the database.
✓	Sysadmins	No more than 2 members of sysadmin role are present.
✓	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.
✓	Exposed SQL Server/MSDE Password	The 'sa' password and SQL service account password are not exposed in text files.
✓	Domain Controller Test	SQL Server and/or MSDE is not running on a domain controller.
✓	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to Windows Only.
✓	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
✓	CmdExec role	CmdExec is restricted to sysadmin only.
✓	Folder Permissions	Permissions on the SQL Server and/or MSDE installation folders are set properly.

Score	Issue	Result
✓	Guest Account	The Guest account is not enabled in any of the databases.
	SQL Server/MSDE Account Password Test	The check was skipped because SQL Server and/or MSDE is operating in Windows Only authentication mode.

Desktop Application Scan Results

Table 7: Vulnerabilities

Score	Issue	Result
✓	IE Zones	Internet Explorer zones have secure settings for all users.
✓	IE Enhanced Security Configuration for Administrators	The use of Internet Explorer is restricted for administrators on this server.
✓	IE Enhanced Security Configuration for Non-Administrators	The use of Internet Explorer is restricted for non-administrators on this server.
	Macro Security	No Microsoft Office products are installed

Chapter 12

Auditing

You can set auditing policies to track significant events, such as account logon attempts. Local policies should also always be set.

Note: Domain auditing policies always overwrite local auditing policies. The two sets of policies should be identical where possible.

To set local auditing policies, select **Start > Programs > Administrative Tools > Local Security Policies**.

Note: Automated Security Hardening on Windows 2003 (as described in Chapter 4) configures the ICM/IPCC server with the recommended auditing settings. See Local Policies - Audit Policy (page 57)

This chapter contains the following topics:

- How to View Auditing Policies, page 121
- Security Log, page 122
- Real-Time Alerts, page 122
- SQL Server Auditing Policies, page 122
- Active Directory Auditing Policies, page 123

How to View Auditing Policies

Step 1 Select **Start** > **Programs** > **Administrative Tools** > **Local Security Policies**.

the Local Security Settings window opens.

Step 2 In the tree in the left pane, select and expand **Local Policies**.

Step 3 In the tree under Local Policies, select **Audit Policy**.

The different auditing policies appear in the left pane.

Step 4 View or change the auditing policies by double-clicking the policy name.

Security Log

After setting auditing policies, it is recommended that you view the security log once a week. You need to look for unusual activity such as Logon failures or Logon successes with unusual accounts.

To view the Security Log, select**Start> Programs > Administrative Tools > Event Viewer**

Real-Time Alerts

MSFT Windows provides the SNMP Event Translator facility, which lets you translate events in the Windows eventlog into real-time alerts by converting the event into an SNMP trap. Use evntwin.exe or evntcmd.exe to configure SNMP traps.

Be sure to consult Microsoft TechNet **http://technet2.microsoft.com/windowsserver/en/library/978683e3-b1d9-4733-98a2-31085c43c1171033.mspx?mfr=true** (http://technet2.microsoft.com/windowsserver/en/library/978683e3-b1d9-4733-98a2-31085c43c1171033.mspx?mfr=true)for additional information about configuring the translation of events to traps.

Refer to the *Cisco SNMP Installation and Basic Configuration* guide for information about configuring SNMP trap destinations.

SQL Server Auditing Policies

For general SQL Server auditing policies, see **SQL server Auditing at Microsoft** (http://www.microsoft.com/technet/security/prodtech/sqlserver/sql2kaud.mspx).

SQL Server C2 Security Auditing

C2 security is a government rating for security in which the system has been certified for discretionary resource protection and auditing capability.

Cisco does not support C2 auditing for SQL Server in the ICM/IPCC environment. Cisco cannot guarantee that enabling C2 auditing on SQL Server will not have significant negative impact on the system. For more information on C2 Auditing, see **SQL Server 2000 C2 Administrator's and User's Security Guide** (http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sqlc2.mspx).

Active Directory Auditing Policies

It is recommended that you audit Active Directory account management and logins, and monitor audit logs for unusual activity.

The following table contains the recommended and default DC Audit policies.

Table 8: Active Directory Audit Policy Recommendations

Policy	Default Setting	Recommended Setting	Comments
Audit account logon events	No auditing	Success and Failure	Account logon events are generated when a domain user account is authenticated on a Domain Controller.
Audit account management	Not defined	Success	Account management events are generated when security principal accounts are created, modified, or deleted.
Audit directory service access	No auditing	Success	Directory services access events are generated when an Active Directory object with a system access control list (SACL) is accessed.
Audit logon events	No auditing	Success and Failure	Logon events are generated when a domain user interactively logs onto a Domain Controller or when a network logon to a Domain Controller is performed to retrieve logon scripts and policies.
Audit object access	No auditing	(No change)	
Audit policy change	No auditing	Success	Policy change events are generated for changes to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	No auditing	(No change)	
Audit process tracking	No auditing	(No change)	
Audit system events	No auditing	Success	System events are generated when a user restarts or shuts down the Domain Controller or when an event occurs that affects either the system security or the security log.

Chapter 13

General Anti-Virus Guidelines and Recommendations

Cisco recommends that you only use the approved Anti-Virus (AV) software products with ICM/IPCC software, as described in this part.

Warning: Often, the default AV configuration settings increase CPU load and memory and disk usage, adversely affecting software performance. Therefore it is critical that you follow the guidelines in this part when using AV software with ICM/IPCC software.

Viruses are unpredictable and Cisco cannot assume responsibility for the consequences of virus attacks on mission-critical applications. Particular care should be taken for systems that use Microsoft Internet Information Server (IIS) such as WebView.

Note:

- Your corporate Anti-Virus strategy should include specific provisions for any server positioned outside the corporate firewall or subject to frequent connections to the public Internet.

- Refer to the Bill of Materials for the application and version qualified and approved for your release of ICM/IPCC.

Many of the default AV configuration settings can adversely affect product performance as a result of increased CPU load, memory, and disk usage by the Anti-Virus software program. Cisco tests specific configurations to maximize product performance.

This chapter contains the following topics:

- Guidelines and Recommendations, page 126
- ICM/IPCC Software Maintenance Parameters, page 127
- File Type Exclusion Recommendations, page 128

Guidelines and Recommendations

Anti-virus applications have numerous configuration options that allow very granular control of what and how data should be scanned on a server.

With any anti-virus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. The role of the system administrator is to determine what the optimal configuration requirements will be for installing an anti-virus application within a particular environment. Refer to your particular anti-virus product documentation for more detailed configuration information.

The following list highlights some general best practices:

- Update AV software scanning engines and definition files on a regular basis, following your organization's current policies.

- Upgrade to the latest supported version of the third-party anti-virus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.

- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Where possible, each of these remote machines should have its own anti-virus software installed, thus keeping all scanning local. With a multi-tiered anti-virus strategy, scanning across the network and adding to the network load should not be required.

- Schedule full scans of systems by AV software **only** during scheduled maintenance windows, and when the AV scan will not interrupt other ICM maintenance activities.

- Do not set AV software to run in an automatic or background mode for which all incoming data or modified files are scanned in real time.

- Due to the higher scanning overhead of heuristics scanning over traditional anti-virus scanning, use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).

- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This is the default setting for most anti-virus applications. Implementing on-access scanning on file reads will yield a higher impact on system resources than necessary in a high-performance application environment.

- While on-demand and real-time scanning of all files gives optimum protection, this configuration does have the overhead of scanning those files that cannot support malicious code (for example, ASCII text files). Cisco recommends excluding files or directories of files, in all scanning modes, that are known to present no risk to the system.

- Schedule regular disk scans only during low usage times and at times when application activity is lowest. To determine when application purge activity is scheduled, refer to the Security Best Practices guides listed in the previous item.

- Disable the email scanner if the server does not use email.
- Additionally, set the AV software to block port 25 to block any outgoing email.**(Do not block port 25 on Cisco Email Manager Servers, if CEM uses the default port 25 to send email)**
- Block IRC ports.
- If your AV software has spyware detection and removal then enable this feature. Clean infected files, or if they cannot be cleaned delete them.
- Enable logging in your AV application. Limit the log size to 2 MB.
- Set your AV software to scan compressed files.
- Set your AV software to not use more than 20% CPU utilization at any time.
- When a virus is found, the first action should be to clean the file, the second to delete or quarantine the file.
- If available in your AV software, enable buffer overflow protection.
- Set your AV software to start on system startup.

ICM/IPCC Software Maintenance Parameters

Before scheduling AV software activity on Cisco ICM/IPCC Servers, note that a few parameters that control the application's activity at specific times. Anti-Virus software configuration settings should avoid scheduling "Daily Scans," "Automatic DAT Updates," and "Automatic Product Upgrades" during the times specified below.

Logger Recommendations

Do not schedule AV software activity to coincide with the time specified in the following Logger registry keys:

- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\Purge\Schedule\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

Distributor Recommendations

Do not schedule AV software activity to coincide with the time specified in the following Distributor registry keys:

- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

Router and PG Recommendations

On the ICM Router and Peripheral Gateway (PG), do not schedule AV program tasks:

- During times of heavy or peak call load.
- At the half hour and hour marks, as ICM processes increase during those times.

Other Scheduled Tasks Recommendations

You can find other scheduled ICM process activities on Windows by inspecting the Scheduled Tasks Folder. Scheduled AV program activity should not conflict with those ICM scheduled activities

File Type Exclusion Recommendations

There are a number of binary files that are written to during the operation of ICM processes that have little risk of virus infection.

Omit files with the following file extensions from the drive and on-access scanning configuration of the AV program:

- *.hst applies to PG.
- *.ems applies to ALL.

Chapter 14

Remote Administration

This section describes recommended practices for remote administration.

Note:

- Use of any remote administration applications can cause adverse effects during load.
- Use of remote administration tools that employ encryption can impact server performance. The performance level impact is tied to the level of encryption used. More encryption results in more impact to the server performance.

This chapter contains the following topics:

- Windows Terminal Services (Remote Desktop), page 129
- pcAnywhere, page 131
- VNC, page 135
- TRIDIA VNC Pro, page 135

Windows Terminal Services (Remote Desktop)

Terminal Services permits users to remotely execute applications on Microsoft Windows Server 2003 from a wide range of devices over virtually any type of network connection. It can be enabled to run in either Application Server or Remote Administration modes. ICM/IPCC only supports Remote Administration mode.

Remote Desktop can be used for remote administration of ICM-CCE-CCH server **if** used with /admin option (or /console in older version clients), only. The /admin (aka /console) connects to the local console session.

Using the Remote Desktop Console session, you can:

- Run Configuration Tools

- Run Script Editor, though the recommended approach is to use Internet Script Editor

  Note: Remote Desktop without the console option is not supported.

Note: If you apply Cisco ICM Security Hardening 7.2(1) or later to your system, then you need to upgrade your Remote Desktop Clients to 5.2 or later. Remote Desktop Client 5.2 or later is required to connect to a server with FIPS Compliant algorithms enabled. Older versions of Remote Desktop client do not support FIPS compliant algorithms which the Cisco ICM Security Hardening utility 7.2(1) or later enables. For more information about FIPS compliant algorithms and security settings, see the Microsoft Knowledge Base articles **KB11770** (http://support.microsoft.com/kb/811770) and **KB81183** (http://support.microsoft.com/kb/811833) .

Remote Desktop

Communication between the server and the client will use native Remote Desktop Protocol (RDP) encryption. By default, all data sent is protected by encryption based on the maximum key strength supported by the client.

RDP is the preferred remote control protocol due to its security and low performance impact

Windows Server 2003 Terminal Services provides the ability to connect to and shadow a console session thereby replacing the need to pcAnywhere or VNC. From a command line:

```
mstsc -v:servername /F -console
```

Securing the RDP-TCP Connection

You can configure the properties of the terminal server's RDP-TCP connection to provide better protection. Run Terminal Services Configurator, select Connections, and then select RDP-TCP.

Step 1 Restrict the number of client sessions that can remain active on the server.

From the Network Adapter tab, select Maximum connections and set the limit on the number of concurrent connections.

Step 2 Set session time limits.

From the Sessions tab, check the first of three Override User Settings check box and set values for each of the following (all values are recommendations; use values that work best within your organization):

1. End a disconnected session, 1 or 5 minutes.
2. Active session limit, 1 or 2 days.
3. Idle session limit, 30 minutes.

Step 3 Set permissions for users and groups on the terminal server.

Use the Permissions tab to add users, groups and computers access limits and permissions. Click Add, select the user, group or computer name, and then set one of three basic permissions:

1. Full Control (given to administrators and the system; allows logging onto the terminal server, modifying the connection parameters, connecting to a session, getting session info, resetting or ending a session, logging off other users, remotely controlling other users' sessions, sending messages to other users, and disconnecting sessions).

2. User Access (given to ordinary users; allows logging onto the terminal server, getting session info, connecting to a session or sending messages to other user sessions).

3. Guest Access (for restricted users; allows logging onto the terminal server).

Step 4 Optionally, restrict reconnections of a disconnected session to the client computer from which the user originally connected.

From the Sessions tab, check the last of three Override User Settings check boxes and set Allow reconnection from previous client.

Step 5 Optionally, configure encryption levels to High.

From the General tab, set Encryption level to High. Use this option only if there is a risk that communications can be eavesdropped.

Per-User Terminal Services Settings

You can configure a number of per-user terminal services settings for each user. Using Active Directory Users and Computers, right click on a user and then select properties

Step 1 On the Terminal Services Profile tab, set a user's right to logon to terminal server by setting the Allow logon to terminal server checkbox. Optionally, create a profile and set a path to a terminal services home directory.

Step 2 On the Sessions tab, set session active and idle time outs.

Step 3 On the Remote Control tab, set whether a remote session can be remotely viewed and controlled by administrators and whether a user's permission is required.

pcAnywhere

NOTE: The following discussion applies to all approved versions of pcAnywhere.[2]

Security is one of the most important considerations in implementing a remote control solution.

[2] Refer to the Bill of Materials for the versions qualified and approved for your release of ICM.

pcAnywhere addresses security in the following ways:

1. Restricting access to internal machines
2. Preventing unauthorized connections to a pcAnywhere host
3. Protecting the data stream during a remote control session
4. Preventing unauthorized changes to the installed product
5. Identifying security risks
6. Logging events during a remote control session

pcAnywhere is a trademark of Symantec, Inc. For details, see **http://www.symantec.com/pcanywhere/**.

Restricting access to internal machines

One of the best ways to ensure security is to restrict connections from outside your organization. pcAnywhere is the only remote control product to provide the following two ways to accomplish this objective:

- Limiting connections to a specific TCP/IP address range - pcAnywhere hosts can be configured to only accept TCP/IP connections that fall within a specified range of addresses.
- Serialization - A feature that enables the embedding of a security code into the pcAnywhere host and remote objects created. This security code must be present on both ends for a connection to be made.

Preventing unauthorized connections to a pcAnywhere host

The first line of defense in creating a secure remote computing environment is to prevent unauthorized users from connecting to the host. pcAnywhere provides a number of security features to help you achieve this objective.

Authentication	Authentication is the process of taking a user's credentials and verifying them against a directory or access list to determine if the user is authorized to connect to the system.
Mandatory passwords	pcAnywhere now requires a password for all host sessions. This security feature prevents users from inadvertently launching an unprotected host session.
Callback security (for dial-up connections)	pcAnywhere lets dial-up users specify a call-back number for remote control sessions. In a normal pcAnywhere session, the remote connects to the host, and the session begins. When callback is enabled, the remote calls the host, but then the host drops the connection and calls back the remote at the specified phone number.

Table 9: General pcAnywhere Security Settings

Settings	Default	Change to	Description
Restrict connections after an end of session	no	(optional)	With pcAnywhere, host users can prevent remote users from reconnecting to the host if the session is stopped due to a normal or abnormal end of session.
Wait for anyone	Yes	Yes	
and secure by	no	Yes (lock computer)	

Table 10: Security Options - Connection Options

Settings	Default	Change to	Description
Prompt to confirm connection	no	(optional)	This feature prompts the host user to acknowledge the remote caller and permit or reject the connection. By enabling this feature, users can know when someone is connecting to their host computer. This will depend on the remote administration policy of whether users must be physically present at the server being remotely accessed.

Table 11: Security Options - Login Options

Settings	Default	Change to	Description
Make password case sensitive	no	yes	Lets you use a combination of uppercase and lowercase letters in a password. This setting applies to pcAnywhere Authentication only.
Limit login attempts per call	3	3	pcAnywhere lets host users limit the number of times a remote user can attempt to login during a single session to protect against hacker attacks.
Limit time to complete login	3	1	Similarly, host users can limit the amount of time that a remote user has to complete a login to protect against hacker and denial of service attacks.

Table 12: Security Options - Session Options

Settings	Default	Change to	Description
Disconnect if inactive	no	Yes (2 Minutes)	Limits time of connection. pcAnywhere lets host users limit the amount of time that a remote caller can stay connected to the host to protect against denial of service attacks and improper use.

Protecting the data stream during a remote control session

Encryption prevents the data stream (including the authorization process) from being viewed using readily available tools.

pcAnywhere offers three levels of encryption:

- pcAnywhere encryption
- Symmetric encryption
- Public key encryption

Table 13: Encryption Configuration

Settings	**Default**	**Change to**	**Description**
Level	<none>	Symmetric	Lists the following encryption options: **None**: Sends data without encrypting it. **pcAnywhere encoding**: Scrambles the data using a mathematical algorithm so that it cannot be easily interpreted by a third party. **Symmetric**: Encrypts and decrypts data using a cryptographic key. **Public key**: Encrypts and decrypts data using a cryptographic key. Both the sender and recipient must have a digital certificate and an associated public/private key pair.
Deny lower encryption level	no	Yes	Refuses a connection with a computer that uses a lower level of encryption than the one you selected.
Encrypt user ID and password only	no	no	Encrypts only the remote user's identity during the authorization process. This option is less secure than encrypting an entire session.

Preventing unauthorized changes to the installed product

Integrity checking is a feature that, when enabled, verifies that the host and remote objects, DLL files, executables, and registry settings have not been changed since the initial installation. If pcAnywhere detects changes to these files on a computer, pcAnywhere will not run. This security feature guards against hacker attacks and employee changes that might hurt security.

Identifying security risks

Symantec's Remote Access Perimeter Scanner (RAPS) lets administrators scan their network and telephone lines to identify unprotected remote access hosts and plug security holes. This tool provides administrators with a way to access the vulnerability of their network in terms of remote access products. Using RAPS, you can automatically shut down an active pcAnywhere host that is not password protected and inform the user.

Logging events during a remote control session

You can log every file and program that is accessed during a remote control session for security and auditing purposes. Previous versions only tracked specific pcAnywhere tasks such as login attempts and activity within pcAnywhere. The centralized logging features in pcAnywhere let you log events to pcAnywhere log, NT Event Log (NT, Windows 2000, Windows Server 2003), or an SNMP monitor.

VNC

SSH Server allows the use of VNC through an encrypted tunnel to create secure remote control sessions. However, this configuration is currently not supported by Cisco. The performance impact of running an SSH server has not been determined.

TRIDIA VNC Pro

Tridia VNC Pro provides the same level of use a regular VNC but adds additional security features such as enhanced password security, viewer logs and 1024-bit encryption. For more information about TRIDIA VNC Pro see **http://www.tridiavncpro.com/**.

Chapter 15

Additional Security Best Practices

This chapter lists additional security best practices.

In addition to these, you can find other Unified ICM security considerations in the chapter on such in the *Setup and Configuration Guide for Cisco Unified ICM Hosted Edition* at **Cisco Unified Contact Center Hosted Install and Upgrade Guides** (http://www.cisco.com/en/US/products/sw/custcosw/ps5053/prod_installation_guides_list.html) .

This chapter contains the following topics:

- Additional Cisco Call Center Applications, page 137
- Microsoft Internet Information Server (IIS), page 139
- Sybase EAServer (Jaguar) Hardening, page 142
- RMS Listener Hardening, page 144
- WMI Service Hardening, page 145
- SNMP Hardening, page 146
- Toll Fraud Prevention, page 147
- Syskey, page 148
- Third-Party Security Providers, page 148
- Third-Party Management Agents, page 148

Additional Cisco Call Center Applications

Security best practices for additional Cisco Call Center applications are as follows:

Cisco ICM WebView

The Cisco ICM/IP Contact Center Enterprise Edition WebView Installation and Administration Guide contains the following security related documentation:

- "Creating a WebView Administrator", "Supervisors and WebView Reports", and "Setting Up WebView Users" which describes login, domain, and password security for WebView users.
- "Supervisors and WebView Reports" also describes how a supervisor can only see his or her own agents.
- "WebView User's Password Expiration and Domain Security Settings" describes WebView (ICM) users as taking their security setting from the domain on which they are created. The domain also sets the expiration date on the password.
- WebView online help:

  Under saving reports: From the Security pull-down menu, select either Shared or Private. If you select Shared, all WebView users can access the report. If you select Private, only you can access the report. Under Viewing graphical reports and using the Job Scheduler is a discussion of the mechanics involved in order to allow viewing graphical reports and use of the Job Scheduler in a Microsoft Internet Explorer browser — which requires that all ActiveX Controls and plug-ins be enabled in the browser's security settings.

Note: Starting in release 7.0(0), WebView now supports SSL for both Sessions and/or Authentication.

Cisco ICM CTI Object Server (CTI OS)

In the Cisco ICM Software CTI OS System Manager's Guide

- Desktop Users: the section "Desktop User Accounts" contains instructions for configuring privileges for desktop users.

Cisco Agent Desktop (CAD)

The Cisco Agent Desktop Documentation, found within the IPCC Documentation Set - **http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/index.htm** - Privileges: Required privileges of various kinds are discussed in the CAD Installation Guide and the CAD Administrator User's Guide.

Cisco ICM Router

The file **dbagent.acl** is an internal file that users should not edit. This file, however, must have READ permission so that it can allow users to connect to the router's real-time feed. The file works in the background without users being aware of it.

Peripheral Gateways (PGs) and IPCC Enterprise Agent Login

As of release 7.5(1), there is a rate limit of IPCC Enterprise agent login attempts with incorrect password. By default, the agent account is disabled for 15 minutes on 3 incorrect password attempts, counted over a period of 15 minutes.

This default can be changed through the use of registry keys. The registry keys are under:

HKLM\SOFTWARE\Cisco Systems,
Inc.\\ICM\<inst>\PG(n)[A/B]\PG\CurrentVersion\PIMS\pim(n)\EAGENTData\Dynamic

AccountLockoutDuration - Default 15 - Once the account is locked out as a result of unsuccessful login attempts, these are the number of minutes the account will remain locked out.

AccountLockoutResetCountDuration - Default 15 - Number of minutes before the AccountLockoutThreshold count goes back to zero. This is applicable when the account does not get locked out, but you have unsuccessful login attempts which are less than AccountLockoutThreshold.

AccountLockoutThreshold - Default 3 - Number of unsuccessful login attempts after which the account is locked out.

CTI OS and Monitor Mode Connection

As of release 7.5(1), there is a rate limit on Monitor Mode connection. When TLS is enabled and a password is required, then Monitor Mode is disabled for 15 minutes after 3 incorrect password attempts (configurable). Counter resets on a valid login. See the *CTI OS System Manager's Guide* for more information.

Microsoft Internet Information Server (IIS)

Internet Information Server (IIS) is only required for two applications making up the ICM/IPCC solution targeted in this document, WebView and Internet Script Editor. The service should not be installed, or should be disabled, on any other node except for the Distributor. There are some exceptions in multi-media configuration of the solution. In this case, product documentation and system requirements must be followed.

Hardening IIS for use with WebView and Internet Script Editor on Windows 2000 Platforms

Note: These hardening suggestions only apply to Windows 2000 Server. Windows 2003 Server's version of IIS is more secure than the version of IIS found in Windows 2000 Server.

Top Hardening Suggestions:

Step 1 IIS is used as an intranet-only http server for the ICM product. It is expected that a firewall is deployed to protect external connections to the server.

Step 2 Install the most recent compatible service pack and updates.

Note: Refer to the Bill of Materials for the compatible service pack for your product.

Step 3 Disable the following non essential services:

- File Transfer Service
- E-mail Service
- News Service

Note: This can be accomplished using the IIS Lockdown tool as described below. However, Windows Server 2003 does not enable these extra services by default when installing IIS. Verify that are not installed or they are disabled.

The following sub-components of Internet Information Services (IIS) must be selected during the installation of the web server:

- Common Files
- Internet Information Services Snap-In - for management purposes
- Internet Services Manager (HTML) - for management purposes
- World Wide Web Server

Step 4 Run the IISLockDown tool:

1. Select Static Web server template and select "View template settings" checkbox.

   Note: On systems that do not require IIS you can use this tool to disable IIS by selecting the ‘Server that does not require IIS' template option.

2. Disable all services except Web service.
3. Disable all unneeded script extensions.
4. Select all additional security options except for "Scripts".

   Note: Note that all selected virtual directories must be removed with the exception of the "Scripts" virtual directory.

5. Install URLScan.

Step 5 Click Finish to complete the wizard.

Edit <system_directory>\system32\inetsrv\urlscan\urlscan.ini as follows:

1. Change "AllowDotInPath=0" to "AllowDotInPath=1"
2. Add "POST" to the [AllowVerbs] section

3. Remove all entries under [DenyUrlSequences] section.

In addition to the above edits, the following additional changes are required depending on whether WebView or Internet Script Editor or both are going to be running on the computer.

WebView Only - No Changes Requires

Internet Script Editor Only:

1. Change "UseAllowExtensions=0" to "UseAllowExtensions=1"
2. Add these entries to [AllowExtensions]
   - .dll
   - .ese

WebView and Internet Script Editor:

1. Change "UseAllowExtensions=0" to "UseAllowExtensions=1"
2. Add these entries to [AllowExtensions]
   - .jhtml
   - .jsp
   - .AdminServlet
   - .js
   - .css
   - .cab
   - .psr
   - .xml
   - .zip
   - .jar
   - .

     Note: This entry is a "dot".
   - .exe
   - .dll

Step 6 Setting Registry permissions

Warning: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

Use RegEdt32 to set the permissions depending on whether only WebView or only Internet Script Editor or both are going to be running on the computer.

1. WebView Only:

   Add the "IUSR_<machine_name>" account to have Read only rights to the HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINE\System hives.

2. Internet Script Editor Only:

   Add the "IWAM_<machine_name>" account to have Read only rights to the HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINE\System hives.

3. WebView and Internet Script Editor:

   Implement both of the "WebView Only" and "Internet Script Editor Only" sections above.

Sybase EAServer (Jaguar) Hardening

Jaguar is used by some ICM/IPCC Enterprise products such as WebView. Use these guidelines for hardening Jaguar with WebView after the installation of the ICM and 3rd Party Tools

Starting Jaguar Manager

To start Jaguar Manager:

Step 1 Launch "Jaguar Manager" Application from Start > Program > Sybase > EAServer 5.1 > Jaguar Manager from the WebView Server Machine.

Step 2 Once the Jaguar Manager has started, click on Tools > Connect > Jaguar Manager.

Step 3 In the resulting dialog replace "localhost" in the "Host Name" field with the actual hostname or host IP address.

Step 4 Click the ‘Connect' button.

Changing Jaguar Password

The password used to connect to the Jaguar service is changed in Jaguar Administration and in the jagconnection.properties file. The guidelines provided below to accomplish this are also provided in the reporting documentation (See WebView Installation Guide).

Note: If the password is changed, any subsequent reinstallation of ICM on a WebView server will prompt the user for the Jaguar Password.

The ‘jagadmin' password is modified in two steps:

Step 1 Modify ‘jagadmin' password on EAServer

1. Using the tree on the left pane of Jaguar Manager, navigate to Jaguar Manager > Servers > Jaguar
2. After selecting ‘Jaguar' node, click on File->Server Properties… menu
3. On the server properties dialog box, select ‘Security' tab
4. Click on ‘Set jagadmin Password' button.
5. On the ‘Administrator Password' dialog box
   - Leave ‘Old jagadmin Password' blank.
   - Enter new password in the ‘New jagadmin Password' and ‘Verify N jagadmin Password' fields.
6. Click ‘OK'

Step 2 Modify ‘jagadmin' password at WebView

1. Using Windows Explorer, navigate to ‘**`<Sybdase Home>\EAServer\html\classes\com\cisco\atg`** is typically ‘C:\Program Files\Sybase').
2. Open file ‘jagconnection.properties' using Notepad or WordPad.
3. Locate ‘JAGCONNECT_JAGUAR_ADMIN_PWD' key in the properties file. By default it is blank.
4. Enter the new jagadmin password from step 1 above in clear text. The modified key should look like ‘JAGCONNECT_JAGUAR_ADMIN_PWD=<new password>'

Note: The password entered in clear text gets encrypted when WebView runs for first time after the change.

Restart WebView and Jaguar after you have changed the password. See below:

Restart WebView/Services

Step 1 Close Jaguar Manager.

Step 2 Restart ‘Jaguar' service from Windows Services panel.

Step 3 Restart ‘IIS Admin' service from Windows Services panel (this will also restart ‘World Wide Web' service automatically).

See Also

The Windows Firewall may block port 9000 (Jaguar Manager Tool - CORBA). If you wish to open port 9000 see Understanding the CiscoICMfwConfig_exc.xml File (page 49) to learn how to use the Cisco Firewall tool to open the port.

RMS Listener Hardening

The RMS Listener receives data from remote Logger or SDDSN nodes using either a TCP/IP LAN connection or a RAS dial-up modem connection and NetBEUI. The data is transferred using a file copy process over this connection. As a result, a writeable file share must be configured on the RMS Listener.

Note: Servers running RMS are not supported for use with Automated Security Hardening.

General hardening recommendations follow:

1. It is assumed that you have followed the general hardening procedures in this document.
2. It is also assumed that you have two NTFS partitions. One for the OS and one for the remote data transfer.
3. The OS partition should be hardened to allow only <machine>\Administrators and SYSTEM accounts for file system and registry permissions as described earlier in this document.
4. Create a local group called <machine>\ListenerAccounts.
5. Create a local account for the duplex Listener to use to connect to this Listener with basic user rights (e.g., <machine>\ListenerAcct).
6. Add this account to the <machine>\ListenerAccounts group and remove this account from <machine>\Users group.
7. From the ListenCfg utility configure the other Listener to connect to this Listener using this account. Note: The domain would be the name of this machine. For example, if this is the side A Listener and the machine name was **`ListenerSideA`**, you would configure the side B Listener to connect to **`ListenerSideA\ListenerAcct`**.

8. For each customer system that will connect to the RMS Listener, create a local account with basic user rights (e.g., <machine>\Acme_ICMUser). Note: If remote access (modem) is used, this account will need dial-in permissions.

9. Add these customers to the local <machine>\ListenerAccounts group and remove these accounts from the <machine>\Users group.

10. No registry access is needed for this group

11. Create the identical group and accounts on both Side A and Side B RMS Listener systems.

12. The root of the remote data partition (e.g., F:\) should be configured to allow the SYSTEM account Full Control.

13. At the root of the remote data partition (e.g., F:\), the <machine>\Administrators and <machine>\ListenerAccounts groups should have ONLY: 'List Folder Contents', 'Read' and 'Write' permissions. Do NOT give 'Full', 'Modify' or 'Read & Execute' rights. This will prevent inadvertent launching of a virus that might have been copied from a remote system to the RMS Listener.

14. The logical share to the remote data partition (e.g., ‘FF') should be configured for Full Control with the <machine>\ListenerAccounts and SYSTEM accounts having access. Note that the NTFS permissions will further restrict the physical access to this share.

15. Enable Remote Access logging if a RAS connection via modem is used.

16. Configure the Domain and Backup domain in the Logger or SDDSN ‘Phone Home' setup screen to use the Listener Side A and B machine names respectively.

Refer to the RMS documentation for additional information about configuration.

WMI Service Hardening

Windows Management Instrumentation (WMI) is used to manage Windows systems. WMI security is an extension of the security subsystem built into Windows operating systems. WMI security includes: WMI namespace-level security; Distributed COM (DCOM) security; and Standard Windows OS security.

WMI namespace-level security:

To configure the WMI namespace-level security:

Step 1 Launch the %SYSTEMROOT%\System32\Wmimgmt.msc MMC control.

Step 2 Right click on the WMI Control icon and select properties.

Step 3 Select the ‘Security' properties page.

Step 4 Select the ‘Root' folder and press the ‘Security' button.

Step 5 Remove EVERYONE from the selection list then press the ‘OK' button.

Only <machine>\Administrators should have ALL rights.

Additional WMI Security Considerations

The WMI services are set to ‘Manual' startup by default. These services are used by 3rd Party Management agents as well as Cisco Support Tools Node Agent to capture system data and should not be disabled unless specifically required.

DCOM security configuration should be performed in a manner that is consistent with your scripting environment. Refer to the WMI security documentation for additional details on using DCOM security.

Additional References:

- **How to Set WMI Namespace Security in Windows Server 2003asp** (http://support.microsoft.com/default.aspx?scid=kb;en-us;325353)
- **Securing a Remote WMI Connection** (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/securing_a_remote_wmi_connection.asp)

SNMP Hardening

See the *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for details on installation, setting the community names, user names, and trap destinations.

Although the Microsoft Management and Monitoring Tools sub-components are necessary for SNMP manageability, the Microsoft native SNMP service will be disabled during ICM Setup and its functionality replaced by a more secure agent infrastructure. The administrator should not attempt to re-enable the Microsoft SNMP service as this may cause conflicts with the Cisco installed SNMP agents.

The Microsoft SNMP trap service should be explicitly disabled. It is not recommended that ICM/IPCC Enterprise servers run management software for collecting SNMP traps, thus, the Microsoft SNMP trap service is not necessary.

Versions 1 and 2c of the SNMP protocol are less secure than version 3. SNMP version 3 features a significant step forward in security. For ICM Enterprise and IPCC Enterprise hosts located on internal networks behind corporate firewalls, it is desirable to enable SNMP manageability by performing the additional configuration and hardening recommendations listed below:

1. Create SNMP v1/v2c community strings or SNMP v3 user names using a combination of upper- and lower-case characters. DO NOT use the common "public" and/or "private" community strings. Create names that are difficult to guess.

2. Use of SNMP v3 is highly preferred. Always enable authentication for each SNMP v3 user name. The use of a privacy protocol is also encouraged.
3. Limit the number of hosts that are allowed to connect to SNMP manageable devices.
4. Configure community strings and user names on manageable devices to accept SNMP requests only from those hosts running SNMP management applications. (This is done via the SNMP agent configuration tool when defining community strings and user names.)
5. Enable sending of SNMP traps for authentication failures. This will alert you to potential attackers trying to "guess" community strings and/or user names.

SNMP manageability is installed on ICM/IPCC Enterprise servers and is executing by default. However, for security reasons, SNMP access is denied until the configuration steps enumerated above have been completed.

As an alternative that provides a much higher level of security, customers may choose to configure IPSec filters and an IPSec policy for SNMP traffic between an SNMP management station and SNMP agents. Follow Microsoft's recommendations on how to accomplish this. For more information on IPSec policy for SNMP traffic refer to Microsoft knowledge base article: Q324261.

Toll Fraud Prevention

Toll fraud is a serious issue in the Telecommunications Industry. The fraudulent use of telecommunications technology can be very expensive for a company, and it is essential that the Telecom Administrator take the necessary precautions to prevent this. For IPCC environments, resources are available on Cisco.com providing some basic information to lock down CallManager systems and to mitigate against toll fraud.

In ICM, the primary concern would be in using dynamic labels in the label node of an ICM script. If the dynamic label is constructed from information entered by a caller (such as with Run External Script), then it is possible to construct labels of the form.

- 9.....
- 9011....
- etc.

These labels might cause the call to be sent to outside lines or even to international numbers. If the dial plans configured in the routing client would allow such numbers to go through, and the customer does not want such labels to be used, then the ICM script must check for valid labels before using them.

A simple example would be an ICM script that prompts the caller with "If you know your party's extension, enter it now", and then uses the digits entered blindly in a dynamic label node. It is possible that the call could be transferred anywhere. If this behavior is not desired, then either the ICM routing script or the routing client's dial plan must check for and disallow invalid numbers.

An example of an ICM script check might be an "If" node that use an expression such as

```
substr (Call.CallerEnteredDigits, 1, 1) = "9"
```

The "True" branch of this node would then branch back to ask the caller again. The false branch would allow the call to proceed. This is, of course, only an example. Each customer must decide what is allowed, or not, based on their own environment.

ICM does not normally just transfer calls to arbitrary phone numbers. Numbers have to be explicitly configured as legal destinations, or alternatively the ICM routing script can contain logic which causes the call to be transferred to a phone number which is contained in a script variable. It is possible for a script to be written in such a way that a caller enters a series of digits and the script treats it as a destination phone number and asks the routing client to transfer the call to that number. Our recommendation would be to add logic to such a script to make sure the requested destination phone number is reasonable.

Syskey

Syskey enables the encryption of the account databases. It is recommended that you use Syskey to secure any local account database.

Note: When configuring Syskey, you must use the System Generated Password and Store Startup Key Locally options in the Startup Key dialog box.

Third-Party Security Providers

Cisco has qualified ICM software with the Operating System implementations of NTLM, Kerberos V and IPSec security protocols.

Cisco does not support other third-party security provider implementations.

Third-Party Management Agents

Some server vendors include in their server operating system installations agents to provide convenient server management and monitoring.

For example:

- HP's ProLiant Servers run Insight Management Agents for Windows.
- IBM provides the IBM Director Agent.

These and other agents enable the gathering of detailed inventory information about servers, including operating system, memory, network adapters, and hardware.

While Cisco recognizes such agents can be of value, due to performance impact considerations, Cisco does not currently support their use on mission critical IPCC/ICM servers.

Warning: You must configure agents in accordance to the Anti-Virus policies (page 125) described in this document. Polling or intrusive scans should not be executed during peak hours, but rather scheduled during maintenance windows.

Note: You should install SNMP services as recommended by these third-party management applications to take full advantage of the management capabilities provided with your servers. Failing to install, or disabling, SNMP prevents enterprise management applications from receiving hardware pre-failure alerts and disables certain application functions such as advanced ProLiant status polling, inventory reporting, and version control in HP Insight Manager.

See Also

HPInsight Management Agents User Guide (ftp://ftp.compaq.com/pub/products/servers/management/imaug.pdf) **HP Software Security Customer Advisories** (http://h18013.www1.hp.com/products/servers/management/mgtsw-advisory.html)