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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2003–2015 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## PREFACE

Preface ix  
Change History ix  
About This Guide ix  
Audience x  
Organization of This Guide x  
Related Documents xi  
Obtaining Documentation and Submitting a Service Request xi  
Field Alerts and Field Notices xii  
Documentation Feedback xii  
Conventions xii

## CHAPTER 1

### Encryption Support 1

User and Agent Passwords 1  
Call Variables and Extended Call Variables 1  
Internet Script Editor 1  
CTIOS C++/COM Toolkit 2  
Cisco Contact Center SNMP Management Service 2  
Additional Encryption 3

## CHAPTER 2

### IPsec and NAT Support 5

About IPsec 5  
Support for IPsec in Tunnel Mode 6  
Support for IPsec in Transport Mode 6  
System Requirements 6  
Supported Communication Paths 7  
IPsec Policy Configuration 7
Batch Deployment 35
Network Isolation Utility Command-Line Syntax 35
Troubleshoot Network Isolation IPsec Policy 41

CHAPTER 5  
Windows Server Firewall Configuration 43  
Windows Server Firewall 43  
Cisco Firewall Configuration Utility Prerequisites 44  
Run Cisco Firewall Configuration Utility 44  
Verify New Windows Firewall Settings 45  
Windows Server Firewall Communication with Active Directory 46  
Domain Controller Port Configuration 46  
Restrict FRS Traffic to Specific Static Port 46  
Restrict Active Directory Replication Traffic to Specific Port 46  
Configure Remote Procedure Call (RPC) Port Allocation 47  
Windows Firewall Ports 47  
Test Connectivity 48  
Validate Connectivity 48  
CiscoICMfwConfig_exc.xml File 49  
Windows Firewall Troubleshooting 50  
Windows Firewall General Troubleshooting Notes 50  
Windows Firewall Interferes with Router Private Interface Communication 50  
Windows Firewall Shows Dropped Packets Without Unified CCE Failures 50  
Undo Firewall Settings 50

CHAPTER 6  
SQL Server Hardening 53  
SQL Server Hardening Considerations 53  
Top SQL Hardening Considerations 53  
SQL Server Users and Authentication 54  
SQL Server 2008 R2 Security Considerations 55  
Automated SQL 2008 R2 Hardening 56  
SQL Server Security Hardening Utility 56  
Utility Location 56  
Harden SQL Server 56  
Roll Back SQL Server Security Hardening 56
No Argument  57
Output Log  57
Manual SQL 2008 R2 Server Hardening  57

CHAPTER 7  
Cisco SSL Encryption Utility  59
SSL Encryption Utility  59
SSL Installation During Setup  59
SSL Encryption Utility in Standalone Mode  60
Enable Transport Layer Security (TLS) 1.0 Protocol  60

CHAPTER 8  
Auditing  63
Auditing  63
View Auditing Policies  63
View Security Log  64
Real-Time Alerts  64
SQL Server Auditing Policies  64
SQL Server C2 Security Auditing  64
Active Directory Auditing Policies  64

CHAPTER 9  
General Antivirus Guidelines  67
Antivirus Guidelines  67
Unified ICM/Unified CCE Maintenance Parameters  69
Logger Considerations  69
Distributor Considerations  69
CallRouter and PG Considerations  69
Other Scheduled Tasks Considerations  69
File Type Exclusion Considerations  69

CHAPTER 10  
Remote Administration  71
Windows Remote Desktop  71
Remote Desktop Protocol  72
RDP-TCP Connection Security  72
Per-User Terminal Services Settings  72
pcAnywhere  73
Restricted Access to Internal Machines 73
Unauthorized Connections to pcAnywhere Host 73
Data Stream Protection During Remote Control Session 75
Unauthorized Changes to Installed Product 76
Identifying Security Risks 76
Event Logging During Remote Control Session 76
VNC 76

CHAPTER 11

Other Security Considerations 77
Other Cisco Call Center Applications 77
   Cisco Unified ICM Router 77
   Peripheral Gateways (PGs) and Agent Login 77
   Cisco CTI Object Server (CTIOS) 78
   CTIOS and Monitor Mode Connection 78
   Cisco Agent Desktop 78
   Endpoint Security 78
      Agent Desktops 78
      Unified IP Phone Device Authentication 79
      Media Encryption (SRTP) Considerations 80
      IP Phone Hardening 80
   Java Upgrades 80
   Microsoft Security Updates 81
   Microsoft Service Pack Policy 81
   Microsoft Internet Information Server (IIS) 82
   Active Directory Deployment 82
      AD Site Topology 82
      Organizational Units 82
         Application-Created OUs 82
         AD Administrator-Created OUs 83
   Network Access Protection 85
      Network Policy Server 85
      Unified CCE Servers and NAP 85
   WMI Service Hardening 85
      WMI Namespace-Level Security 86
More WMI Security Considerations  86
SNMP Hardening  86
Toll Fraud Prevention  87
Third-Party Security Providers  88
Third-Party Management Agents  88
Preface

- Change History, on page ix
- About This Guide, on page ix
- Audience, on page x
- Organization of This Guide, on page x
- Related Documents, on page xi
- Obtaining Documentation and Submitting a Service Request, on page xi
- Field Alerts and Field Notices, on page xii
- Documentation Feedback, on page xii
- Conventions, on page xii

Change History

This table lists and links to changes made to this guide and gives the dates those changes were made. Earliest changes appear in the bottom rows.

<table>
<thead>
<tr>
<th>Change</th>
<th>Link</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added information about updating Java.</td>
<td>Java Upgrades, on page 80</td>
<td>May 26, 2015</td>
</tr>
<tr>
<td>Removed information on Microsoft Baseline Security Analyzer.</td>
<td></td>
<td>Initial release of document for 10.5(1)</td>
</tr>
<tr>
<td>Reorganized guide.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Access Protection supports Windows 8.1 (Professional and Enterprise)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

About This Guide

This document describes security hardening configuration guidelines for Cisco Unified Intelligent Contact Management (Unified ICM) on Windows Server 2008 R2. The term “Unified ICM” includes: Unified Contact Center Enterprise/Hosted (Unified CCE/CCH), and Cisco Unified Intelligent Contact Management Enterprise/Hosted. Optional Unified ICM applications that apply to these server configurations are also addressed here, except for the following:
• Cisco Unified Web Interaction Manager (Unified WIM)
• Media Blender (when not coresident with a Peripheral Gateway [PG]; if coresident with a PG then these guidelines are applicable)
• Dynamic Content Adapter
• Cisco Unified E-Mail Interaction Manager (Unified EIM)

References throughout this document to “Unified ICM/Cisco Unified Contact Center Enterprise (Unified CCE)” assume these configurations. Do not use with security hardening on any accompanying applications in the customer’s particular solution, whether provided by a Cisco partner or Cisco, such as PSO applications, with security hardening. Consider special testing and qualification to ensure that security configurations do not hinder the operation of those applications.

The configurations presented in this document represent the parameters that Cisco uses internally to develop and test the applications. Other than the base Operating System and application installations, any deviation from this set cannot be guaranteed to provide a compatible operating environment. You cannot always uniformly implement the configurations in this document. Your implementation can modify or limit the application of these guidelines to meet certain corporate policies, specific IT utilities (for example, backup accounts), or other external guidelines.

---

**Note**

Operating System Security Hardening is not supported.

---

**Audience**

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

The target reader of this document is an experienced administrator familiar with SQL Server 2008 R2 and Windows Server 2008 R2 installations. The reader is also fully familiar with the applications in the Unified ICM/Unified CCE solution, as well as with the installation and administration of these systems. The intent of these guidelines is to additionally provide a consolidated view of securing the various third-party applications on which the Cisco contact center applications depend.

---

**Organization of This Guide**

This document is organized into the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Support</td>
<td>A brief overview of the encryption methods used in Unified ICM/Unified CCE.</td>
</tr>
<tr>
<td>IPsec and NAT Support</td>
<td>Security considerations for deploying IPsec and Network Address Translation (NAT) in a Unified ICM/Unified CCE environment.</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Security Wizard</td>
<td>Details on how to use the Security Wizard to configure various security features.</td>
</tr>
</tbody>
</table>
# Related Documents

Documentation for Cisco Unified ICM/Contact Center Enterprise, as well as related documentation, is accessible from Cisco.com at: [http://www.cisco.com/cisco/web/psa/default.html](http://www.cisco.com/cisco/web/psa/default.html).

Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, and Cisco Unified Intelligence Center. The following list provides more information:

- For documentation for the Cisco Unified Contact Center products, go to [http://www.cisco.com/cisco/web/psa/default.html](http://www.cisco.com/cisco/web/psa/default.html), and select **Voice and Unified Communications > Customer Collaboration > Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**. Then, select the product or option that you are interested in.

- For troubleshooting tips for these Cisco Unified Contact Center products, go to [http://docwiki.cisco.com/wiki/Category:Troubleshooting](http://docwiki.cisco.com/wiki/Category:Troubleshooting), then select the product or option you are interested in.

- Documentation for Cisco Unified Communications Manager is accessible from: [http://www.cisco.com/cisco/web/psa/default.html](http://www.cisco.com/cisco/web/psa/default.html).

# Obtaining Documentation and Submitting a Service Request

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

### Field Alerts and Field Notices

Cisco can modify its products or determine key processes to be important. These changes are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Sign in [www.cisco.com](http://www.cisco.com) and then access the tool at [https://www.cisco.com/cisco/support/notifications.html](https://www.cisco.com/cisco/support/notifications.html).

### Documentation Feedback

To provide comments about this document, send an email message to the following address: [contactcenterproducts_docfeedback@cisco.com](mailto:contactcenterproducts_docfeedback@cisco.com).

We appreciate your comments.

### Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.  
• A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*)  
• A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade 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> |
<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| < >        | 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. |
Encryption Support

- User and Agent Passwords, on page 1
- Call Variables and Extended Call Variables, on page 1
- Internet Script Editor, on page 1
- CTI OS C++/COM Toolkit, on page 2
- Cisco Contact Center SNMP Management Service, on page 2
- Additional Encryption, on page 3

User and Agent Passwords

Unified ICM and Unified CCE systems are highly distributed applications composed of many node and server applications. The system stores application user and contact center agent passwords in the Logger and the Distributor databases as an MD5 Message-Digest Algorithm hash. When passed from one server node to another, such as from a PG to a Router, the system passes the passwords as MD5 hashes.

Call Variables and Extended Call Variables

To protect data sent in call variables or expanded call context (ECC) variables, Unified ICM relies on IPsec and the deployment of IPsec policies between servers running Windows Server 2008 R2.

In a contact center enterprise environment, the establishment of an IPsec channel between the Cisco Unified Communications Manager (Unified CM) and the Peripheral Gateway is also supported. Use SHA-1 as your integrity algorithm and 3DES as your encryption algorithm. For the Internet Key Exchange (IKE) security algorithm, use at least a minimum of Diffie-Hellman Group 2 for a 1024-bit key, or 2048-bit key if processing power allows it.

Internet Script Editor

Unified CCE supports, as a default on Windows Server 2008 R2, the encryption of traffic for users accessing the Internet Script Editor and Web Setup applications. The traffic encryption protects all user sign-ins and optionally session traffic done from a remote machine from snooping. The applications that implement the Transport Layer Security (TLS) v1.0 protocol using the Open SSL libraries are HTTP-based.

The Internet Script Editor web application is deployed and enabled for 128-bit SSL encryption in IIS 7 as a default. All supervisor sign-ins, user sign-ins, and data exchanged is protected across the network.
For more information about enabling certain Cipher Suites in IIS, see the article KB 245030.

**Related Topics**
- Cisco SSL Encryption Utility, on page 59

## CTI OS C++/COM Toolkit

The CTI OS (C++/COM toolkit) and agent desktops implement TLS v1.0 protocol using the OpenSSL libraries to protect data exchanged between 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: SHA2

---

**Important**

When you enable CTI OS Security, agent capacity decreases by 25%.


## Cisco Contact Center SNMP Management Service

Unified ICM and Unified CCE include a Simple Network Management Protocol (SNMP v3) agent to support authentication and encryption (privacy) provided by *SNMP Research International*. Our implementation exposes the configuration of the communication with a management station to be authenticated using the SHA-1 digest algorithms. For all SNMP messages to be encrypted, our implementation uses one of the following protocols:

- 3DES
- AES-192
- AES-256

Additional Encryption

In addition to the encryption in the contact center applications, Cisco supports the deployment of the solution across sites running Cisco IOS IPsec in Tunnel Mode with HMAC-SHA1 Authentication (ESP-SHA-HMAC) and 3DES Encryption (ESP-3DES).

Related Topics

- IPsec and NAT Support, on page 5
CHAPTER 2

IPsec and NAT Support

- About IPsec, on page 5
- Support for IPsec in Tunnel Mode, on page 6
- Support for IPsec in Transport Mode, on page 6
- IPsec Connection to Unified Communications Manager, on page 9
- IPsec Activity, on page 9
- NAT Support, on page 11
- NAT and CTI OS, on page 11
- IPsec and NAT Transparency, on page 11
- Other IPsec References, on page 11

About IPsec

Internet Protocol security (IPsec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, by using cryptographic security services.

You can deploy IPsec in many different ways. This chapter explains what IPsec is and how to secure selected communication paths using IPsec. The "IPsec with Network Isolation Utility" chapter explains a more restricted, but automated, application of IPsec to secure the entire traffic to and from the server. The Network Isolation Utility also saves you work in applying IPsec. Even if you use this utility to apply IPsec, read this chapter to understand the IPsec deployment options. You can then use the one that is the most beneficial for your environment.


Implementing IPsec in a contact center environment means finding a balance between ease of deployment, usability, and protecting sensitive information from unauthorized access.

Finding the proper balance requires the following:
- Assessing the risk and determining the appropriate level of security for your organization.
- Identifying sensitive 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.

How you use or deploy the application influences the security considerations. For example, the required security differs between a single main site deployment and a deployment across multiple sites which might not communicate across trusted networks. The security framework in Windows Server 2008 R2 is designed to fulfill stringent security requirements. However, software alone is less effective without careful planning and assessment, effective security guidelines, enforcement, auditing, and sensible security policy design and assignment.

When you enable IPsec, expect the following impacts on scalability:

• The maximum supported operational capacities for peripheral gateways in a CCE deployment decrease by 25%. This capacity reduction applies to agents, VRU ports, SIP Dialer ports, and call rate.
• The maximum call rate (calls per second) that the CCE deployment supports decreases by 25%.

Related Topics
IPsec with Network Isolation Utility, on page 25

Support for IPsec in Tunnel Mode

Due to increased security concerns in data and voice network deployments, Unified ICM and Unified CCE support IPsec between Central Controller sites and remote peripheral (PG) sites. This secure network implementation implies a distributed model where the WAN connection is secured with IPsec tunnels. The configuration of Cisco IOS IPsec in Tunnel Mode means that only the Cisco IP Routers (IPsec peers) between the two sites are part of the secure channel establishment. All data traffic is encrypted across the WAN link, but unencrypted on the local area networks. Tunnel Mode ensures traffic flow confidentiality between IPsec peers, which 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)

Commonly, QoS networks classify and apply QoS features based on packet header information before traffic is tunnel encapsulated and encrypted.

Support for IPsec in Transport Mode

System Requirements

For IPsec Support in Transport Mode, you need to have Microsoft Windows Server 2012 R2 installed.

Following are the system requirements for IPsec Support in Transport Mode:

• Cisco Unified CCE 10.0+
• Microsoft Windows Server 2008 R2
Supported Communication Paths

Unified ICM Release supports deploying IPsec in a Windows Server 2008 R2 operating environment to secure server-to-server communication. The support is limited to the following list of nodes, which exchange customer-sensitive data:

1. The connection between the NAM Router and the CICM Router
2. The public connections between the redundant Unified ICM Router/Logger pairs
3. The private connections between the redundant Unified ICM Router/Logger pairs
4. All connections between the Unified ICM Router and the Unified ICM Peripheral Gateway (PG)
5. All connections between the redundant Unified ICM Router/Logger pairs and the Administrator & Data Server (Primary/Secondary) with Historical Data Server (HDS)
6. All connections between the redundant Unified ICM Router/Logger pairs and the Administration Server, Real-time and Historical Data Server, and Detail Data Server (Primary/Secondary)
7. The public and private connections between the redundant Unified ICM PG pair
8. The connections between the redundant Unified ICM PG pair and the Unified Communications Manager in a Unified CCE deployment

For all these server communication paths, consider a High security level as a general basis for planning an IPsec deployment.

IPsec Policy Configuration

Each IPsec policy consists of one or more IPsec rules. Each IPsec rule consists of the following:
- 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. With this method, you create an IPsec policy first and then you add and configure rules. Add filter lists (specifying traffic types) and filter actions (specifying how the traffic is treated) during rule creation.

An IPsec Security Policy must be created for each communication path and on each end (on every server). Provide the following 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)
     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
• X.509 certificates can also be used in a production environment depending on customer preference. With Unified ICM requiring Active Directory in all deployment models, relying on Kerberos as the authentication method does not require any extra security credential management. For PG to Unified CM connections, use a pre-shared key (PSK).
• For enhanced security, do not use PSK authentication because it is a relatively weak authentication method. In addition, PSKs are stored in plain text. Only use PSKs for testing. For more information, see the Microsoft Technet articles on pre-shared key authentication.

   • Integrity algorithm: SHA1
   • Encryption algorithm: 3DES
   • Diffie-Hellman group: Medium (DH Group 2, 1024-bit key)
**Note**

- For enhanced security, use a Diffie-Hellman key of at least 2048-bit strength to mitigate the threat from LogJam vulnerability attacks (CVE - CVE-2015-4000). For more information, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000. Strong Diffie-Hellmangroups combined with longer key lengths increase the computational difficulty of determining a secret key. For more information, see the Microsoft Technet articles on key exchange methods.

- Using longer key lengths results in more CPU processing overhead.

---

### IPsec Connection to Unified Communications Manager

On Unified CCE systems where the Unified Communications Manager is not in the same domain as the Unified ICM system, you cannot use Kerberos for authentication. For such systems, use X.509 certificates.

### IPsec Activity

#### IPsec Monitor

You can use IP Security Monitor (ipsecmon) to monitor IPsec on a Windows Server 2008 R2 operating system. For details about the IPsec Monitor, see the Microsoft Technet article.

### Enable IPsec Logging

If your policies do not work correctly, you can enable the logging of the IPsec security association process. This log 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 enable IPsec logging.

**Procedure**

**Step 1** Choose **Start > Run**.

**Step 2** Type **Regedit32** and click **OK** to get into the Registry Editor.

**Step 3** Double-click **HKEY_LOCAL_MACHINE**.

**Step 4** Navigate to **System\CurrentControlSet\Services\PolicyAgent**.

**Step 5** Double-click **Policy Agent**.

**Step 6** Right-click in the right pane and choose **Edit > Add Key**.

**Step 7** Enter **Oakley** as the key name (case sensitive).

**Step 8** Double-click **Oakley**.

**Step 9** Right-click in the left pane and choose **New > DWORD Value**.
Step 10 Enter the value name `EnableLogging` (case sensitive).
Step 11 Double-click the value and set the DWORD to 1.
Step 12 Click OK.
Step 13 Go to a command prompt and type `net stop policyagent & net start policyagent`.
Step 14 Find the log in `%windir%\debug\Oakley.log`.

### Network Monitoring

The Network Monitor component (netmon) that ships with Windows Server 2008 R2 can capture frames that are sent to or from the computer on which Network Monitor is installed. For more information, see Microsoft documentation at [https://support.microsoft.com/kb/933741](https://support.microsoft.com/kb/933741).

### System Monitoring

The built-in Performance console (perfmon) enables you to monitor network activity along with the other system performance data. 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. Be sure to 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`
NAT Support

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.

You can deploy IP Phones in a Unified CCE environment across NAT. You can locate remote Peripheral (PG) servers on a NAT network remote from the Central Controller servers (Routers and Loggers). NAT support qualification 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.


NAT and CTI OS

Unified CCE does not support CTI OS Silent Monitor with NAT for the following reasons:

- 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 Unified Communications Manager.

- The CTI toolkit Supervisor Desktop provides the CTI toolkit Agent Desktop an IP address to which it forwards sniffed VoIP packets. That IP address is an address on the data center address space.

IPsec and NAT Transparency

The IPsec NAT Transparency feature introduces support for IPsec traffic to travel through NAT or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPsec. VPN devices automatically detect NAT Traversal (NAT-T). There are no configuration steps for a router running Cisco IOS Software Release 12.2(13)T and later. If both VPN devices are NAT-T capable, then NAT-T is autodetected and autonegotiated.

Other IPsec References

Cisco Unified Contact Center Security Wizard

• About Unified Contact Center Security Wizard, on page 13
• Configuration and Restrictions, on page 13
• Run Wizard, on page 14
• Example of Security Wizard Usage, on page 14
• Windows Firewall Configuration, on page 17
• Network Isolation Configuration Panels, on page 18
• Example of SQL Hardening Panels, on page 21

About Unified Contact Center Security Wizard

The Cisco Unified Contact Center Security Wizard is a security deployment tool for Unified ICM/CCE that simplifies security configuration through its step-by-step wizard-based approach.

The Security Wizard enables you to run the following Unified ICM/CCE security command-line utilities:

• Windows Firewall Utility
• Network Isolation Utility
• SQL Hardening Utility

Related Topics

IPsec with Network Isolation Utility, on page 25
Windows Server Firewall Configuration, on page 43
Automated SQL 2008 R2 Hardening, on page 56

Configuration and Restrictions

The following are Security Wizard restrictions:

• The Security Wizard does not interfere with applications that run on the network. Run the Security Wizard only during the application maintenance window because it can potentially disrupt connectivity when you set up the network security.

• The Security Wizard works on a Windows Server 2008 R2 platform.
• The Firewall Configuration Utility and the Network Isolation Utility must be configured after Unified ICM is installed on the network.

• The Security Wizard requires that the command-line utilities are on the system to configure security. The Wizard detects if a utility is not installed and notifies the user.

• The Security Wizard can execute on all Unified ICM or Unified CCE servers, but does not execute on a Domain Controller.

Related Topics
IPsec with Network Isolation Utility, on page 25
Windows Server Firewall Configuration, on page 43

Run Wizard

The ICM-CCE-CCH Installer installs the Security Wizard places and places it in the “%SYSTEMDRIVE%\CiscoUtils\UCCSecurityWizard” directory. 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 CCE Tools > Security Wizard.

Note
Before you use the wizard, read the chapters in this guide about each of the utilities included in the wizard to understand what the utilities do.

The Security Wizard presents you with a menu list of the security utilities (the Security Hardening, the Windows Firewall, Network Isolation Utility, and SQL Utility). You run each utility, one at a time.

You can go back and forth on any menu selection to understand what each one contains. However, after you click the Next button for any particular feature, either complete configuration or click Cancel to go back to the Welcome page. The Security Wizard is self-explanatory; each utility has an introductory panel, configurations, a confirmation panel, and a status panel.

What to do next
When you select a value different from the default that could cause a problem, the wizard displays a warning.

In the rare event that the back-end utility script dies, a temporary text file created in the UCCSecurityWizard folder is not deleted. This text file contains command-line output, which you can use this file to debug the issue.

Example of Security Wizard Usage

The following image shows the Security Wizard introductory panel.
Figure 1: Security Wizard Welcome Page

Cisco Unified Contact Center Security Wizard

The 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.

Figure 2: Windows Firewall Wizard Introduction Panel

Windows Firewall Wizard

This wizard configures the stateful firewall built in Windows Server 2012 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.

You must be an administrator on this server to successfully configure this feature.
Figure 3: Network Isolation Configuration Panel

This wizard configures Windows Server 2012 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. You must be an administrator on this server to successfully configure this feature.

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.

Note: A previously configured Network Isolation policy was found. You may modify it using this wizard. For security reasons, you will need to re-enter the PreShared Key again.

Figure 4: SQL Hardening Configuration Panel

This wizard hardens SQL Server 2014 by applying the SQL Server 2014 Security Hardening template designed for the Cisco Unified Contact Center application. This wizard can be used either to apply the SQL Server 2014 security hardening, to upgrade from a previously applied hardening, or to rollback previously applied hardening. Refer to Security Best Practices Guide for ICM for details on the SQL Server 2014 Automated Security Hardening. You must be an administrator on the Windows server as well as have SQL sysadmin role on SQL server to successfully configure this feature.
The Security Wizard requires that the command-line utilities are on the system to configure security. The Wizard detects if a utility is not installed and notifies the user.

The Security Wizard can execute on all Unified ICM or Unified CCE servers, but does not execute on a Domain Controller.

Windows Firewall Configuration

In the Security Wizard Firewall Configuration panel, you can:

- Configure a Windows firewall for your Unified ICM or Unified CCE system.
- Undo firewall configuration settings that were previously applied.
- Restore to Windows Default.

⚠️ Warning

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

- Disable the Windows firewall.
- Edit the Unified ICM Firewall Exceptions XML file. Clicking the Edit ICM Firewall Exceptions XML button opens that XML file in Notepad. Save the file and close it before continuing with the wizard.

The Window Firewall Configuration Utility:

- Must be executed after the Unified ICM application is installed.
- Automatically detects Unified ICM components installed and configures the Windows Firewall accordingly.
• Can add custom exceptions such as an exception for VNC.
• Is installed by default on all Unified ICM and Unified CCE servers.

Related Topics
  Windows Server Firewall Configuration, on page 43

Network Isolation Configuration Panels

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

The Security Wizard interface has the following advantages:

• The configuration panels change dynamically with your input.
• You can browse the current policy.
• You can see the current Network Isolation configuration and edit it if necessary.
• You can add multiple Boundary Devices through a single Security Wizard panel. To add multiple Boundary Devices in the CLI, create a separate command for each device that you want to add.

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

The configuration panels display the last configuration saved in the XML Network Isolation configuration file (not the Windows IPsec policy store), if it is available. The following image shows the configuration panel for Trusted Devices.
The Trusted Devices panel:

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

---

**Note**

To enable or modify a device as Trusted, enter a Preshared Key of 36 characters or more. The length of the typed-in key updates as you enter it to help you enter the correct length.

---

**Note**

You can permanently delete the Network Isolation Utility policy at the command line only.

Use the same Preshared Key on all Trusted Devices or else network connectivity between the Trusted Devices fails.

The following image shows the Network Isolation Boundary Devices panel.
In the Boundary Devices panel:

- The panel dynamically modifies based on the selection made in the previous panel:
  - If you disabled the policy in the previous panel, then the elements in this panel are disabled.
  - If you selected the browse option in the previous panel, 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, 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

Related Topics
IPsec with Network Isolation Utility, on page 25

Example of SQL Hardening Panels

The following image shows the introductory panel for the SQL Hardening utility.

You can use the SQL Hardening wizard to:
• Apply the SQL Server 2008 R2 security hardening.
• Upgrade from a previously applied hardening.
• Roll back previously applied hardening.

For more information on SQL Server hardening, see the section Automated SQL 2008 R2 Hardening.

Figure 8: Security Action Panel

The following image shows the SQL Hardening Security Action panel.

In the SQL Hardening Security Action panel, you can:
• Apply or Upgrade SQL Server 2008 R2 Security Hardening
• Roll back Previously Applied SQL Server 2008 R2 Security Hardening
The Rollback is disabled if there is no prior history of SQL Server 2008 R2 security hardening or if the hardening was already rolled back.

**Note**

The following image shows the SQL Hardening Confirmation panel. You can still change any configuration selections, but after you click **Finish**, you can no longer change your selections.

![SQL Hardening Confirmation Panel](image)

**Figure 9: SQL Hardening Confirmation Panel**

The following image shows the SQL Hardening status panel.

![SQL Hardening Status Panel](image)

**Figure 10: SQL Hardening Status Panel**
The status bar at the top of the panel tells you when the configuration is complete.
Example of SQL Hardening Panels
IPsec

Internet Protocol Security (IPsec) is a security standard developed jointly by Microsoft, Cisco, and many other Internet Engineering Task Force (IETF) contributors. It provides integrity (authentication) and encryption between any two nodes, which could be endpoints or gateways. IPsec is application independent because it works at layer 3 of the network. IPsec is useful for large and distributed applications like Unified ICM because it provides security between the application nodes independent of the application.


Manual Deployment or Network Isolation Utility

The Network Isolation Utility automates much of the work to secure a Unified ICM/Unified CCE environment using IPsec. The Network Isolation utility deploys a preconfigured IPsec policy that secures the entire network traffic to or from the Unified ICM/Unified CCE servers. Network connectivity is restricted to only those servers that share the same policy or are explicitly listed as exceptions.

If you wish to secure network traffic only between selected communication paths, do not use the Network Isolation Utility.

Related Topics

IPsec and NAT Support, on page 5
Cisco Network Isolation Utility

The Cisco Network Isolation Utility uses the Windows IPsec feature to isolate Unified ICM devices from the rest of the network. Examples of Unified ICM devices include the router, the logger, and the peripheral gateway device. The utility creates a Network Isolation IPsec policy, which sets Unified ICM devices as Trusted, and then 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 Unified CM, default gateway devices, CTI OS desktops, serviceability devices, and remote-access computers.

Each Trusted Device has its own list of Boundary Devices. Separate IP addresses or subnets or ports define the Boundary Devices.

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)

Network Isolation Utility Information

The following sections discuss the Network Isolation Utility design and how it works.

IPsec Terminology

The following list contains definitions of basic IPsec terminology:

**Policy**

An IPsec policy is a collection of one or more rules that determine IPsec behavior. In Windows Server 2008 R2, 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 filter list is 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.


Network Isolation Utility Process

Run the Network Isolation Utility separately on each Trusted Device. Do not run the utility on Boundary Devices.

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

After you deploy the Network Isolation IPsec policy on a device, that device is set as Trusted. Traffic flows freely between it and any other Trusted Device without any additional configuration.

When you run the Network Isolation Utility, it does the following:

1. Removes any IPsec policies that are already on that computer. This removal avoids conflicts so the new policy matches on all Unified 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:

   1. Trusted Devices Rule

      This rule involves the following items:

      • **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.

   2. Boundary Devices Rule

      This rule involves the following items:

      • **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. The Network Isolation Utility 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 store the policy state and the Boundary Device list. It does not store the preshared key.

5. The Network Isolation Utility 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.

**Traffic Encryption and Network Isolation Policies**

The Network Isolation policy allows only those computers that have the same preshared key to interact. With Network Isolation, an outside hacker cannot access a trusted computer. But, without encryption enabled, a hacker can still see the traffic coming and going from that computer. Therefore, consider encrypting that traffic.

---

**Note**

- You cannot encrypt traffic to one Trusted Device alone. Encrypt traffic on either all Trusted Devices or none. If only one computer has encrypted traffic, then none of the other Trusted Devices understand it.
- Use encryption offload NICs when IPsec is enabled with encryption so that the encryption software does not affect performance.

---

**Related Topics**

- [IPsec and NAT Support](#), on page 5

---

**Network Isolation Feature Deployment**

The following sections discuss issues to be aware of when designing your deployment plan.

**Related Topics**

- [Important Deployment Tips](#), on page 28
- [Sample Deployment](#), on page 29
- [Device Two-Way Communication](#), on page 31
- [Boundary Devices and Unified CCE](#), on page 33

---

**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. The network isolation feature is applied on one device at a time. This feature instantly limits communication with other devices after it is applied. So, carefully plan how to deploy this feature before using
it or you could accidentally stop your network from working. Write a deployment plan before you implement the Network Isolation feature. Deploy this feature therefore only during a maintenance window and review the caveats before writing your deployment plan.

### Sample Deployment

The following is one sample deployment.

1. Start with a fully functional Unified ICM or Unified CCE system that has no IPsec policy deployment.

   **Figure 11: Example Unified Contact Center System**

2. Set the CallRouter, the Logger, the Administration & Data Server, and the PGs as Trusted Devices by running the Network Isolation Utility on each of them.
3. Add the infrastructure servers and clients as Boundary Devices.

4. Add Unified Communications Manager or ACD server, the DNS, and the agent desktops as Boundary Devices on both PGs.
When you are finished, all Unified Contact Center Trusted Devices communicate only with each other and their respective Boundary Devices (the domain controller, the DNS, the Unified Communications Manager, and so on). Any network attack from outside cannot reach the Trusted Devices, unless it is routed through the Boundary Devices.

**Device Two-Way Communication**

This table lists the two-way communications requirements in a Unified CCE deployment. You can set the target devices as either Trusted or Boundary Devices.

<table>
<thead>
<tr>
<th>Unified CCE component</th>
<th>Target Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallRouter</td>
<td>CallRouter (on the other side in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Logger</td>
</tr>
<tr>
<td></td>
<td>Administration &amp; Data Server/Historical Database Server</td>
</tr>
<tr>
<td></td>
<td>NAM Router</td>
</tr>
<tr>
<td></td>
<td>Peripheral Gateway (on both sides in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Application Gateway</td>
</tr>
<tr>
<td></td>
<td>Database Server</td>
</tr>
<tr>
<td></td>
<td>Network Gateway</td>
</tr>
<tr>
<td>Unified CCE component</td>
<td>Target Devices</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logger</td>
<td>Historical Database Server/Administration &amp; Data Server</td>
</tr>
<tr>
<td></td>
<td>CallRouter</td>
</tr>
<tr>
<td></td>
<td>Campaign Manager</td>
</tr>
<tr>
<td></td>
<td>Dialer</td>
</tr>
<tr>
<td>Peripheral Gateway</td>
<td>Multichannel/Multimedia Server</td>
</tr>
<tr>
<td></td>
<td>CallRouter (on both sides in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Peripheral Gateway (on the other side in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>Administration &amp; Data Server legacy PIMS/switches</td>
</tr>
<tr>
<td>CTI OS Server and CTI OS Clients</td>
<td>CTI OS Server (on the other side in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Peripheral Gateway</td>
</tr>
<tr>
<td></td>
<td>CTI OS Agent desktops</td>
</tr>
<tr>
<td></td>
<td>Cisco Agent Desktop</td>
</tr>
<tr>
<td></td>
<td>All CTI Clients</td>
</tr>
<tr>
<td>Silent Monitor Server</td>
<td>CTI OS Server (on the other side in a redundant system)</td>
</tr>
<tr>
<td></td>
<td>Peripheral Gateway</td>
</tr>
<tr>
<td></td>
<td>CTI OS Agent desktops</td>
</tr>
<tr>
<td></td>
<td>Cisco Agent Desktop</td>
</tr>
<tr>
<td></td>
<td>All CTI Clients</td>
</tr>
<tr>
<td>Administration &amp; Data Server/Historical Database Server</td>
<td>Multichannel/Multimedia Server</td>
</tr>
<tr>
<td></td>
<td>Router</td>
</tr>
<tr>
<td></td>
<td>Logger</td>
</tr>
<tr>
<td></td>
<td>Custom Application Server</td>
</tr>
<tr>
<td></td>
<td>CON API Clients</td>
</tr>
<tr>
<td></td>
<td>Internet Script Editor Clients/Webskilling</td>
</tr>
<tr>
<td></td>
<td>Third-Party Clients/SQL party</td>
</tr>
</tbody>
</table>
### Boundary Devices and Unified CCE

This table lists the Boundary Devices That are typically required in a Unified CCE deployment:

<table>
<thead>
<tr>
<th>Boundary Device</th>
<th>Configuration Example</th>
</tr>
</thead>
</table>
| Domain Controllers: such as those for RTR, LGR, Administration & Data Server or HDS, and PGs | • Boundary Device: Domain Controller IP Address  
• Traffic Direction: Outbound  
• Protocol: Any  
• Port: Not Applicable |
| DNS, WINS, Default Gateway | — |
| Remote Access or Remote Management software: such as that for every Trusted Device (VNC, pcAnywhere, Remote Desktop Connection, SNMP) | VNC:  
• Boundary Device: Any host  
• Traffic Direction: Inbound  
• Protocol: TCP  
• Port: 5900 |
| Unified Communications Manager Cluster for PGs | • Boundary Device: A specific IP Address (or Subnet)  
• Traffic Direction: Outbound  
• Protocol: TCP  
• Port: All ports |
**Boundary Device** | **Configuration Example**
--- | ---
Agent Desktops | *CTI OS Server:*
• Boundary Device: A Subnet
• Traffic Direction: Inbound
• Protocol: TCP
• Port: 42028

**Caveats**

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

Caveats include the following:

- **Important** Enabling the policy remotely blocks remote access unless a provision is made in the Boundary Device list for remote access. Add a Boundary Device for remote access before enabling the policy remotely.

- **Important** Add all domain controllers as Boundary Devices or your domain login fails. If domain login fails, your Unified ICM services also fail to start or you can see delayed login times. This list of domain controllers includes all domains in which Unified ICM is installed. The list also includes all domains in which Web Setup tool, configuration users, and supervisors exist.

- Adding a new device as a Boundary Device requires a change to the policy on all Trusted Devices that 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, that device cannot communicate with the other Trusted Devices because its network traffic is encrypted. Enable encryption on all or none of the Trusted Devices.

- Do not use the Windows IPsec policy MMC plug-in to change the IPsec policy. The Network Isolation Utility maintains its own copy of the policy. Whenever the Network Isolation Utility executes, the utility reverts to its last saved configuration, ignoring any changes made outside the utility (or the Security Wizard).

- The Network Isolation Utility does not interfere with applications that run on the network. However, run the utility only during the application maintenance window because the utility can disrupt connectivity when you set up the network security.

- If your network is behind a firewall, then 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 protocol.

• If you are using the NAT protocol, 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.

• Deploy the Network Isolation Policy after the Unified ICM or the Unified Contact Center application is configured and confirmed to be working.

• For an inventory of the ports used across the contact center suite of applications, see the following documentation:

To aid in firewall configuration, these guides list the protocols and ports used for agent desktop-to-server communication, application administration, and reporting. They also provide a listing of the ports used for intra-server communication.

### Batch Deployment

You can use the following XML file to help speed up deployment when a common set of Boundary Devices must be added to all Trusted Devices:

```xml
<system drive>\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML
```

This XML file contains the list of Boundary Devices and policy state for one Trusted Device. You can use this file to replicate the policy on other Trusted Devices.

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

### Network Isolation Utility Command-Line Syntax

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

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
- pipe or bar `|` = any one of the items between the bars

The following table lists the command syntax for all uses of the command.
### Table 1: Network Isolation Utility Command Syntax for Each Argument

<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HELP</td>
<td>cscript ICMNetworkIsolation.vbe /?</td>
<td>Displays the syntax for the command.</td>
</tr>
<tr>
<td>ENABLE POLICY</td>
<td>cscript ICMNetworkIsolation.vbe /enablePolicy&lt;36+ characters PreSharedKey in double quotes&gt; [/encrypt]</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  
The only nonsupported character for use in the PreSharedKey is double quotes because that character marks the beginning and end of the key. You can enter any other character within the key.  

For example:  
cscript ICMNetworkIsolation.vbe /enablePolicy “myspecialpresharedkey123456789mbvcx”  

**Note**  
The add, remove, and delete arguments make a backup of the XML file and name it xml.lastconfig before carrying out their function.
<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
</table>
| 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  
This example allows all outbound traffic to a device with the specified IP address. | 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), Internet Control Message Protocol (ICMP), or any protocol.  
• (optional) any port or a specified port if the selected protocol is TCP or UDP. |
### Argument Name | Syntax and Example | Function
--- | --- | ---
 | cscript ICMNetworkIsolation.vbe /addSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] | 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.

For example:
cscript ICMNetworkIsolation.vbe /addSubnetBoundary 10.86.0.0.255.255.0.0 Inbound TCP 42028
This example allows a CTI OS Server to listen for agent desktops on the 10.86.x.x network.
<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
</table>
| 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.  
Windows 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>  
For example:  
cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary Inbound TCP 5900 | Removes from the Boundary Device list any host device at the specified IP address that matches the following criteria:  
• 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. |
### Argument Name | Syntax and Example | Function
--- | --- | ---
 | cscript ICMNetworkIsolation.vbe /removeSubnetBoundary <Starting IP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] | 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) a port or a specified port.
 | cscript ICMNetworkIsolation.vbe /removeSubnetBoundary 10.86.0.0.255.255.0.0 Inbound Any | For example: |  
DISABLE POLICY | cscript ICMNetworkIsolation.vbe /disablePolicy | Disables the Unified 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 have a network connectivity problem and you do not know the cause, disable the policy 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 Unified ICM Network Isolation Security policy from the Windows IPsec policy store and renames the XML file to CiscoICMIPsecConfig.xml.lastconfig.

### Troubleshoot Network Isolation IPsec Policy

Use the following steps to troubleshoot the Network Isolation IPsec policy:

**Procedure**

**Step 1**  
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 important that the policy is deployed after the Unified ICM application is configured and tested.

**Step 2**  
Check whether an IP address or port specified in the Boundary Device list was modified after the policy was deployed.
Step 3 Check whether a communication path is set as Trusted and Boundary. An overlap of both causes communication to fail.

Step 4 Confirm by looking in the `<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMPsecConfig.XML` file whether the required Boundary Devices are listed as Boundary Devices. Use the Security Wizard to check the Boundary Devices.

Step 5 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 always overwrites the IPsec policy store with the configuration stored in the XML file.

Step 6 Check for any listed caveats.
Windows Server Firewall Configuration

• Windows Server Firewall, on page 43
• Cisco Firewall Configuration Utility Prerequisites, on page 44
• Run Cisco Firewall Configuration Utility, on page 44
• Verify New Windows Firewall Settings, on page 45
• Windows Server Firewall Communication with Active Directory, on page 46
• CiscoICMfwConfig_exc.xml File, on page 49
• Windows Firewall Troubleshooting, on page 50

Windows Server Firewall

Windows Server 2008 R2 includes Windows Firewall. Windows Firewall is a stateful host firewall that drops all unsolicited incoming traffic. This behavior of Windows Firewall provides some protection from malicious users and programs that use unsolicited incoming traffic to attack computers.


Note

Windows Firewall is disabled by default on systems that have been upgraded to SP1. Systems that have a new installation of Windows Server 2008 R2 have Windows Firewall enabled by default.

When you enable Windows Firewall on your servers, open all ports that the Unified ICM/Unified CCE components require.

Cisco provides a utility to automatically allow all traffic from Unified ICM/Unified CCE applications on a Windows Server 2008 R2. Also, the utility can open ports for common third-party applications used in the Unified ICM/Unified CCE 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.

The utility allows all traffic from Unified ICM/Unified CCE 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 *port number* to the list of excepted traffic. Edit the `CiscoICMfwConfig_exc.xml` file to enable these ports.

Ports/Services enabled by default:

- 80/TCP and 443/TCP - HTTP/HTTPS (when IIS or TomCat [for Web Setup] is installed)
- Microsoft Remote Desktop

Optional ports you can open:

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

---

**Note**

You can edit the XML file to add port based exceptions outside of this list.

---

**Cisco Firewall Configuration Utility Prerequisites**

Install the following software before using the Firewall configuration utility:

1. Windows Server 2008 R2 SP1 or higher
2. Unified ICM/CCE components

---

**Note**

If you install any more components after configuring the Windows Firewall, reconfigure the Windows Firewall. This process involves removing the previous configuration and rerunning the Windows Firewall configuration utility.

---

**Run 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.

---

**Warning**

If you attempt to run this utility from a remote session, such as VNC, you can be “locked out” after the firewall starts. If possible, perform any firewall-related work at the computer because network connectivity can be severed for some remote applications.
Use the Cisco Firewall Configuration Utility on each server running a Unified ICM component. To use the utility, follow these steps:

**Procedure**

**Step 1** Stop all application services.

**Step 2** From a command prompt, on Windows Server 2008, run `cscript %SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig.vbe`, or, on Windows Server 2008 R2, run `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat`.

**Step 3** When you first run the script, the script runs `register.bat` for Windows Server 2008 or `configfirewall.bat` for Windows Server 2008 R2. The script then asks you to rerun the application using the same command. Rerun the script if instructed to do so.

**Note** When using a Windows Server 2008 system, the script might not recognize that you previously ran the script. If the script does not recognize that you previously ran the script, manually run the `register.bat` file from the command line.

After you run the script, a confirmation dialog box appears.

**Step 4** Click **OK**.

The script verifies that the Windows Firewall service is installed, then starts this service if it is not running. The script then updates the firewall with the ports and services specified in the file `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`.

**Step 5** Reboot the server.

**Related Topics**

[Windows Firewall Configuration](#), on page 17

---

**Verify New Windows Firewall Settings**

You can verify that the Unified ICM components and ports were added to the Windows Firewall exception list by following these steps:

**Procedure**

**Step 1** Choose **Start > Settings > Control Panel > Windows Firewall** or select **Administrative Tools > Windows Firewall with Advanced Security** when using Windows Server 2008 R2.

The Windows Firewall dialog box appears.

**Step 2** Click the **Exceptions** tab. Then click the **Inbound and Outbound Rules** tab of the Windows Firewall dialog box for Windows Server 2008 R2.

**Step 3** Scroll through the list of excepted applications. Several Unified ICM executables now appear on the list and any ports or services defined in the configuration file.
Windows Server Firewall Communication with Active Directory

Open the ports that the domain controllers (DCs) use for communication by LDAP and other protocols to ensure that Active Directory can communicate through your firewall.

Consult the Microsoft Knowledge Base article KB179442 for important information about configuring firewall for Domains and Trusts.

To establish secure communications between DCs and Unified ICM Services, 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)

Domain Controller Port Configuration

Define the following port definitions on all DCs within the demilitarized zone (DMZ) that can replicate to external DCs. Define the ports on all DCs in the domain.

Restrict FRS Traffic to Specific Static Port

Be sure to consult the Microsoft Knowledge Base (KB) KB319553 for more information about restricting File Replication Service (FRS) traffic to a specific static port.

Procedure

Step 1
Start Registry Editor (regedit.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 Specific Port

Be sure to consult the Microsoft Knowledge Base article KB224196 for more information about restricting Active Directory replication traffic to a specific port.
Procedure

Step 1 Start Registry Editor (regedit.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

Consult the Microsoft Knowledge Base article KB154596 for more information about configuring RPC port allocation.

Procedure

Step 1 Start Registry Editor (regedit.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 Firewall Ports

Consult the Microsoft Knowledge Base article KB179442 for a detailed description of the ports that are used to configure a firewall for domains and trusts.

Table 2: Windows Server 2008 R2 Firewall Ports

<table>
<thead>
<tr>
<th>Server Port</th>
<th>Protocol</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
<td>TCP</td>
<td>RPC</td>
<td>RPC Connector Helper (machines connect to determine which high port to use)</td>
</tr>
<tr>
<td>137</td>
<td>TCP</td>
<td>UDP</td>
<td>NetBIOS Name</td>
</tr>
<tr>
<td>Server Port</td>
<td>Protocol</td>
<td>Protocol</td>
<td>Service</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>138</td>
<td>UDP</td>
<td></td>
<td>NetBIOS NetLogon and Browsing</td>
</tr>
<tr>
<td>139</td>
<td></td>
<td></td>
<td>NetBIOS Session</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td></td>
<td>NTP</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td></td>
<td>LDAP</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>UDP</td>
<td>LDAP SSL</td>
</tr>
<tr>
<td>3268</td>
<td></td>
<td></td>
<td>LDAP GC</td>
</tr>
<tr>
<td>3269</td>
<td></td>
<td></td>
<td>LDAP GC SSL</td>
</tr>
<tr>
<td>42</td>
<td></td>
<td></td>
<td>Wins Replication</td>
</tr>
<tr>
<td>53</td>
<td>TCP</td>
<td>UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>88</td>
<td>TCP</td>
<td>UDP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>UDP</td>
<td>SMB over IP (Microsoft-DS)</td>
</tr>
<tr>
<td>10000</td>
<td>TCP</td>
<td></td>
<td>RPC NTFRS</td>
</tr>
<tr>
<td>10001</td>
<td>TCP</td>
<td></td>
<td>RPC NTDS</td>
</tr>
<tr>
<td>10002 to 10200</td>
<td>TCP</td>
<td></td>
<td>RPC - Dynamic High Open Ports</td>
</tr>
<tr>
<td>NA</td>
<td>ICMP</td>
<td></td>
<td>A layer 3 protocol suite in the TCP/IP suite. This is used in pings and traces. You can block echo replies by closing port 7.</td>
</tr>
</tbody>
</table>

### Test Connectivity

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

**Procedure**

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.

### Validate Connectivity

To validate connectivity between the domain controllers, use the Portqry tool.
To obtain the Portqry tool, see the following Microsoft website: https://www.microsoft.com/en-us/download/details.aspx?id=17148.

**Procedure**

**Step 1** Download the PortQryV2.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 that the ports are open.

Consult the Microsoft Knowledge Base article KB832919 for more information about PortQry features and functionality.

### 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. This modification ensures that the firewall works properly in the Unified ICM/Unified CCE environment.

The file consists of three main parts:

- **Services**: The services that are allowed access through the firewall.
- **Ports**: The ports for the firewall to open.
  
  This setting 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 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 more services or ports to the CiscoICMfwConfig_exc.xml file and rerun the script to reconfigure Windows Firewall. For example, to allow your *Jaguar* server connections from port 9000 (CORBA), add a line in the `<Ports>` section to open port 9000 on the Windows Firewall:

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

**Note**

This change is only needed if remote Jaguar administration is required. Usually, this change is not needed.

On Windows Server 2008 R2, you could use **Windows Firewall with Advanced Security** to add or deny the ports or applications.
The file lists some commonly used ports as XML comments. You can quickly enable one of these ports by moving the port out of the comments to a place before the </Ports> tag.

Windows Firewall Troubleshooting

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

Windows Firewall General Troubleshooting Notes

Some general troubleshooting notes for Windows Firewall:

1. When you run the CiscoICMfwConfig application for the first time, run the application twice to successfully register of FirewallLib.dll. Sometimes, especially on a slower system, you need a delay for the registration to complete.

2. If the registration fails, the .NET framework might not be installed correctly. Verify that the following path and files exist:

   %windir%\Microsoft.NET\Framework\v2.0.50727\regasm.exe
   %windir%\Microsoft.NET\Framework\v1.1.4322\gacutil.exe

3. Change %SYSTEMDRIVE%\CiscoUtils\FirewallConfig\Register.bat as necessary to meet the environment.

Windows Firewall Interferes with Router Private Interface Communication

Problem 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.

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

Solution Configure static routes on both Side-A and Side-B routers for the private addresses (high and nonhigh).

Windows Firewall Shows Dropped Packets Without Unified CCE Failures

Problem The Windows Firewall Log shows dropped packets but the Unified ICM and Unified CCE applications do not exhibit any application failures.

Possible Cause The Windows Firewall logs traffic for the host when the traffic is not allowed or when no allowed application listens to that port.

Solution 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 and connect on what ports.

Undo Firewall Settings

You can use the firewall configuration utility to undo the last application of the firewall settings. You need the CiscoICMfwConfig_undo.xml file.
The undo file is written only if the configuration is completed successfully. If this file does not exist, manual cleanup is necessary using the Windows Firewall Control Panel Applet.

To undo the firewall settings:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Stop all application services.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Open a command window by choosing <strong>Start &gt; Run</strong> and entering <strong>CMD</strong> in the dialog window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the following command: <code>cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig</code>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter <code>UndoConfigFirewall.bat</code> for Windows Server 2008 R2.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Reboot the server.</td>
</tr>
</tbody>
</table>
SQL Server Hardening Considerations

Top SQL Hardening Considerations:

1. Do not install SQL Server on an Active Directory Domain Controller.
2. In a multitier environment, run web logic and business logic on separate computers.
3. Install the latest applicable SQL Server service pack and security updates. Refer to the Unified CCE Compatibility Matrix for the compatible service pack for your product.
4. Set a strong password for the sa account before installing ICM.
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. Instead, use the Network Services account.


6. Enable SQL Server Agent Service and set to Automatic for database maintenance in Unified ICM.

   Applying SQL Server security updates or hotfixes can require that you disable the SQL Server Agent service. Reset this service to “disabled” before performing the update. When the update has completed, stop the service and set it back to “enabled”.

7. 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 runs under (for example, <domain>\SQLServiceAcct>). From the Local Policy editor, temporarily grant “logon locally” privileges to this account to enable EFS then remove this right after signing out.
Only enable EFS if data theft is a concern; there is a performance impact.

Warning
To copy and send the data to other parties, back up the database to a different, unencrypted directory to ensure that the receiving party can read the backup. You can do this backup from the SQL Server Enterprise Manager.

Note
8. Disable the SQL guest account.
9. Restrict sysadmin membership to your Unified ICM administrators.
10. Block TCP port 1433 and UDP port 1434 at the firewall, unless the Administration & Data Server is not in the same security zone as the Logger.
11. Provide protection with good housekeeping:
   1. Run the KillPwd utility to remove password data from setup files. Detailed instructions on how to run this utility can be found in the Microsoft article KB 263968.
   2. Delete or archive these setup files after installation:
      • sqlstp.log
      • sqlsp.log
      • setup.iss

      The files are in `<systemdrive>:\Program Files\Microsoft SQL Server\MSSQL\Install for a default installation` or `<systemdrive>:\Program Files\Microsoft SQL Server\ MSSQL$<Instance Name>\Install for named instances`.

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

12. Change the recovery actions of the Microsoft SQL Server service to restart after a failure.
13. Remove all sample databases.
14. Enable auditing for failed logins.

Related Topics
   SQL Server Users and Authentication, on page 54

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. Create the accounts during the installation of SQL Server.
During installation, SQL Server Database Engine is set to either Windows Authentication mode or SQL Server and Windows Authentication mode. If Windows Authentication mode is selected during installation, the sa login is disabled. If you later change authentication mode to SQL Server and Windows Authentication mode, the sa login remains disabled. To enable the sa login, use the ALTER LOGIN statement. For more details, see http://msdn.microsoft.com/en-us/library/ms188670.aspx.

The local user or the domain user account that is created for the SQL Server service account follows the Windows or domain password policy respectively. Apply a strict password policy on this account. However, do not set the password to expire. If the password expires, the SQL Server service ceases to function and the Administration & Data Server fails.

Site requirements can govern the password and account settings. Consider minimum settings like the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce Password History</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>12 characters</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum Password Age</td>
<td>1 day</td>
</tr>
<tr>
<td>Account Lockout Duration</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Account Lockout Threshold</td>
<td>3 invalid logon attempts</td>
</tr>
<tr>
<td>Reset Account Lockout Counter After</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

**Note**

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

Mixed mode authentication is enforced through SQL Server 2008 R2 automated hardening.

During web setup, if the sa password is blank, a randomly generated strong password is generated and used to secure the sa account.

**Important**

This randomly generated sa password is displayed only once during the install. Make note of the password because it is not presented again.

You can reset the sa account password after installation by logging on to the SQL Server using a Windows Local Administrator account.

**SQL Server 2008 R2 Security Considerations**

Microsoft SQL Server 2008 R2 is far more secure by design, default, and deployment than prior versions. Microsoft SQL Server 2008 R2 provides a much more granular access control and a new utility to manage
attack surface, and runs with lower privileges. When implementing Microsoft SQL Server 2008 R2 security features, the database administrator must follow the guidelines in the following section.

Automated SQL 2008 R2 Hardening

The SQL Server Security Automated Hardening utility performs the following:

- Enforces Mixed Mode Authentication.
- Verifies that the Named Pipe (np) is listed before TCP/IP (tcp) in the SQL Server Client Network Protocol Order.
- Disables SQLWriter, SQLBrowser, MSSQLServerADHelper100 Services.
- Forces SQL server user 'sa' password if found blank.

SQL Server Security Hardening Utility

The SQL Server Security Hardening utility allows you to harden or roll back the SQL Server security on Logger and Administration & Data Server/HDS components. The Harden option disables unwanted services and features. If the latest version of the security settings is 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 before 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.

Utility Location

The utility is located at:

%SYSTEMDRIVE%\CiscoUtils\SQLSecurity

Harden SQL Server

On the command line enter:

Perl ICMSQLSecurity.pl HARDEN

Note

The current SQL Server configuration is backed up to

<ICMInstallDrive>:\CiscoUtils\SQLSecurity\ICMSQLSEcurity.bkp before the utility applies the SQL Server hardening.

Roll Back SQL Server Security Hardening

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

To roll back to the previous SQL Server configuration, enter the following command:

Perl ICMSQLSecurity.pl ROLLBACK
The following security hardening settings are not removed when:

1. SQL Server security mode is currently set to Windows Only Authentication.
2. SQL Server user “sa” is set to random password.
3. SQLVSSWriter, SQLBrowser, and MSSQLServerADHelper100 services are disabled.

You can roll back these settings manually using SQL Server Management Studio tool.

**No Argument**

If you use no argument with the command line, the help appears.

**Output Log**

All output logs are saved in the file:

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

**Manual SQL 2008 R2 Server Hardening**

By default, SQL Server 2008 R2 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 endpoints. Unified ICM requires only Named Pipes and TCP/IP endpoints.

**Procedure**

- Enable both Named Pipes and TCP/IP endpoints during SQL Server 2008 R2 setup. Make sure that the Named Pipes endpoint has a higher order of priority than TCP/IP.

**Note**

The SQL Server Security Hardening utility checks for the availability and order of these endpoints.

- Disable access to all unrequired endpoints. For instance, deny connect permission to VIA endpoint for all users/groups who have access to the database.
SSL Encryption Utility

Unified CCE web servers are configured for secure access (HTTPS). Cisco provides SSL Encryption Utility (SSLUtil.exe) to help you configure web servers for use with SSL.

The SSL Encryption Utility is only supported on servers running Windows Server 2008 R2.

Operating system facilities such as IIS can also accomplish the operations performed by the SSL encryption utility; however the Cisco utility simplifies the process.

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

The SSL Encryption Utility generates log messages pertaining to the operations that it performs. When it runs as part of setup, log messages are written to the setup log file. When the utility is in standalone mode, the log messages appear in the SSL Utility Window and the <SystemDrive>\temp\SSLUtil.log file.

The SSL Encryption Utility performs the following major functions:

- SSL Configuration
- SSL Certificate Administration

SSL is available only for Unified ICM web applications installed on Windows Server 2008 R2. The contact center web applications that you can configure for SSL are:

SSL Installation During Setup

By default, setup enables SSL for Unified CCE Internet Script Editor application.

If you use IIS manager to modify SSL settings while the SSL Configuration Utility is open, the SSL Configuration Utility does not reflect those changes until you restart the utility.
The SSL Configuration Utility also facilitates creation of self-signed certificates and installation of the created certificate in IIS. You can also remove a certificate 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.

Unified CCE does not support the import of third-party certificates on Windows-based components.

To use SSL for Internet Script Editor, accept the default settings during installation and the supported servers use SSL.

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 has an existing server certificate installed, a log entry is added and no changes take effect. Use the utility in standalone mode or directly use the IIS Services Manager to do any certificate management changes.

---

**SSL Encryption Utility in Standalone Mode**

In standalone mode, the SSL Configuration Utility displays the list of Unified ICM instances installed on the local machine. When Unified 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.

The SSL Configuration Utility also facilitates the creation of self-signed certificates and the installation of the created certificate in IIS. You can also remove a certificate 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.

**Enable Transport Layer Security (TLS) 1.0 Protocol**

The ICM security template enables FIPS-compliant strong encryption, which requires the TLS 1.0 protocol enabled instead of SSL 2.0 or SSL 3.0.

Use the following steps to enable the TLS 1.0 protocol:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch Internet Explorer.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Tools menu, select Internet Options.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Scroll to Security and check the Use TLS 1.0 check box.</td>
</tr>
</tbody>
</table>

See the Microsoft Knowledge Base (KB) [KB 811833](#) for more information about security settings.
If you apply security hardening and Internet Explorer is not configured to support the TLS 1.0 protocol, the web browser cannot connect to the web server. An error message indicates that the page is either unavailable or that the website is experiencing technical difficulties.
Enable Transport Layer Security (TLS) 1.0 Protocol
Auditing

You can set auditing policies to track significant events, such as account logon attempts. Always set Local policies.

Domain auditing policies always overwrite local auditing policies. Make the two sets of policies identical where possible.

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

View Auditing Policies

Procedure

Step 1 Choose 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.

---

**View Security Log**

After setting auditing policies, view the security log once a week. Look for unusual activity such as Logon failures or Logon successes with unusual accounts.

To view the Security Log:

**Procedure**

Choose Start > Programs > Administrative Tools > Event Viewer.

---

**Real-Time Alerts**

Windows provides the SNMP Event Translator facility. This facility 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.

For more information about configuring the translation of events to traps, see the Microsoft TechNet articles on the [Evntcmd](#).

Refer to the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* guide for information about configuring SNMP trap destinations.

---

**SQL Server Auditing Policies**


---

**SQL Server C2 Security Auditing**

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

Cisco does not support C2 auditing for SQL Server in the Unified ICM/Unified CCE environment.

---

**Active Directory Auditing Policies**

Routinely audit Active Directory account management and logins. Also monitor audit logs for unusual activity.

The following table contains the hardened and default DC Audit policies.
Table 4: Active Directory Audit Policy Settings

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

Antivirus Guidelines

Antivirus applications have numerous configuration options that allow granular control of what data is scanned, and how the data is scanned on a server.

With any antivirus 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 are for installing an antivirus application within a particular environment. Refer to your particular antivirus product documentation for more detailed configuration information.

You can use third-party antivirus software products that adhere to the guidelines in this chapter. For a list of antivirus software products that are tested by Cisco, see the Compatibility Matrix for Unified CCE at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.


Only use approved Anti-Virus (AV) software products with Unified ICM/Unified CCE.

---

**Warning**

Often, the default AV configuration settings increase CPU load and memory and disk usage, adversely affecting software performance. Cisco tests specific configurations to maximize product performance. It is critical that you use the following guidelines for using AV software with Unified ICM/Unified CCE.

Viruses are unpredictable and Cisco cannot assume responsibility for the consequences of virus attacks on mission-critical applications. Take particular care for systems that use Microsoft Internet Information Server (IIS).

The following list highlights some general guidelines:
• Ensure that your corporate Antivirus strategy includes specific provisions for any server that is positioned outside the corporate firewall or subject to frequent connections to the public Internet.

• Refer to the *Compatibility Matrix for Unified CCE* for the application and version that is qualified and approved for your release of Unified ICM/Unified CCE.

• Update AV software, and definition files regularly, following your organization's policies.

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

  Avoid scanning of any files that are accessed from remote drives (such as network mappings or UNC connections). Where possible, ensure that each of these remote machines has its own antivirus software installed, thus keeping all scanning local. With a multithreaded antivirus strategy, scanning across the network and adding to the network load is not required.

• Schedule full scans of systems by AV software **only** during scheduled maintenance windows, and when the AV scan cannot interrupt other Unified 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.

• Heuristics scanning has higher overhead over traditional antivirus 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 approach is the default setting for most antivirus applications. Implementing on-access scanning on file reads yields a higher impact on system resources than necessary in a high-performance application environment.

• On-demand and real-time scanning of all files gives optimum protection. However, this configuration has the overhead of scanning files that cannot support malicious code (for example, ASCII text files). Exclude files or directories of files, in all scanning modes, that you know present no risk to the system.

• Schedule regular disk scans only during low-usage times and at times when application activity is lowest.

• Disable the email scanner if the server does not use email.

  Also, set the AV software to block IRC ports and block port 25 to block any outgoing email.

• If your AV software has spyware detection and removal, then enable this feature. Clean infected files, or delete them (if these files cannot be cleaned).

• 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 is to clean the file, the second to delete or quarantine the file.

• If it is available in your AV software, enable buffer overflow protection.

• Set your AV software to start on system startup.
Unified ICM/Unified CCE Maintenance Parameters

A few parameters control the application activity at specific times. Before you schedule AV software activity on Unified ICM/Unified CCE Servers, ensure that Antivirus software configuration settings do not schedule “Daily Scans,” “Automatic DAT Updates,” and “Automatic Product Upgrades” during critical times.

Logger Considerations

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 Considerations

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

CallRouter and PG Considerations

On the CallRouter 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, because Unified ICM processes increase during those times.

Other Scheduled Tasks Considerations

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

File Type Exclusion Considerations

Several binary files that are written to during the operation of Unified ICM processes 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
Remote Administration

- Windows Remote Desktop, on page 71
- pcAnywhere, on page 73
- VNC, on page 76

Windows Remote Desktop

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

Remote Desktop can be used for remote administration of ICM-CCE-CCH server. The mstsc command connects to the local console session.

Using the Remote Desktop Console session, you can:
- Run Configuration Tools
- Run Script Editor

**Note** Remote Desktop is not supported for software installation or upgrade.

**Note** Administration Clients and Administration Workstations can support remote desktop access. But, only one user can access a client or workstation at a time. Unified CCE does not support simultaneous access by several users on the same client or workstation.
Remote Desktop Protocol

Communication between the server and the client uses native Remote Desktop Protocol (RDP) encryption. By default, encryption based on the maximum key strength supported by the client protects all data.

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

Windows Server 2008 R2 Terminal Services enable you to shadow a console session. Terminal Services can replace the need for pcAnywhere or VNC. To launch from the Windows Command Prompt, enter:

Remote Desktop Connection: mstsc /v:<server[:port]>

RDP-TCP Connection Security

To provide protection on the RDP-TCP connection, use Microsoft's Remote Desktop Services Manager to set the connection properties appropriately:

• Limit the number of active client sessions to one.
• End disconnected sessions in five minutes or less.
• Limit the time a session can remain active to one or two days.
• Limit the time a session can remain idle to 30 minutes.
• Select appropriate permissions for users and groups. Give Full Control only to administrators and the system. Give User Access to ordinary users. Give Guest Access to all restricted users.
• Consider restricting reconnections of a disconnected session to the client computer from which the user originally connected.
• Consider setting high encryption levels to protect against unauthorized monitoring of the communications.

Per-User Terminal Services Settings

Use the following procedure to set up per-user terminal services settings for each user.

Procedure

| Step 1 | Using Active Directory Users and Computers, right-click a user and then select Properties. |
| Step 2 | On the Terminal Services Profile tab, set a user's right to sign in to terminal server by checking the Allow logon to terminal server check box. Optionally, create a profile and set a path to a terminal services home directory. |
| Step 3 | On the Sessions tab, set session active and idle time outs. |
| Step 4 | On the Remote Control tab, set whether administrators can remotely view and control a remote session and whether a user's permission is required. |
pcAnywhere

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

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.

For more information about pcAnywhere, see the Symantec web site.

---

**Note**
This discussion applies to all approved versions of pcAnywhere. Refer to the Compatibility Matrix for the versions qualified and approved for your release of ICM.

---

**Note**
Administration Clients and Administration Workstations can support remote desktop access. But, only one user can access a client or workstation at a time. Unified CCE does not support simultaneous access by several users on the same client or workstation.

---

**Restricted Access to Internal Machines**

An important security technique is to restrict connections from outside your organization. pcAnywhere provides these ways to accomplish that 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 created remote objects. This security code must be present on both ends to make a connection.

---

**Unauthorized Connections to 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 several security features to help you achieve this objective.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Mandatory passwords</td>
<td>pcAnywhere now requires a password for all host sessions. This security feature prevents users from inadvertently launching an unprotected host session.</td>
</tr>
<tr>
<td>Callback security (for dial-up connections)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 5: General pcAnywhere Security Settings**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict connections after an end of session</td>
<td>no</td>
<td>(optional)</td>
<td>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.</td>
</tr>
<tr>
<td>Wait for anyone</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>and secure by</td>
<td>no</td>
<td>Yes</td>
<td>(lock computer)</td>
</tr>
</tbody>
</table>

**Table 6: Security Options - Connection Options**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt to confirm connection</td>
<td>no</td>
<td>(optional)</td>
<td>This feature prompts the host user to acknowledge the remote caller and permit or reject the connection. By enabling this feature, users know when someone is connecting to their host computer. This feature depends on the remote administration policy of whether users must be physically present at the remotely accessed server.</td>
</tr>
</tbody>
</table>

**Table 7: Security Options - Login Options**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make password case sensitive</td>
<td>no</td>
<td>yes</td>
<td>Lets you use a combination of uppercase and lowercase letters in a password. This setting applies to pcAnywhere Authentication only.</td>
</tr>
</tbody>
</table>
PC Anywhere lets host users limit the number of times a remote user can attempt to login during a single session to protect against hacker attacks.

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 8: Security Options - Session Options

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit login attempts per call</td>
<td>3</td>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>Limit time to complete login</td>
<td>3</td>
<td>1</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Data Stream Protection During Remote Control Session

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

PC Anywhere offers three levels of encryption:
- PC Anywhere encryption
- Symmetric encryption
- Public key encryption

### Table 9: Encryption Configuration

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>&lt;none&gt;</td>
<td>Symmetric</td>
<td>Lists the following encryption options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>None</strong>: Sends data without encrypting it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>PC Anywhere encoding</strong>: Scrambles the data using a mathematical algorithm so a third party cannot easily interpret the data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Symmetric</strong>: Encrypts and decrypts data using a cryptographic key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Public key</strong>: 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.</td>
</tr>
</tbody>
</table>
Unauthorized Changes to Installed Product

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

Identifying Security Risks

The Symantec Remote Access Perimeter Scanner (RAPS) lets administrators scan their network and telephone lines to identify unprotected remote access hosts and address 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.

Event Logging During 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 Server 2008 R2), or an SNMP monitor.

VNC

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

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default</th>
<th>Change to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny lower encryption level</td>
<td>no</td>
<td>Yes</td>
<td>Refuses a connection with a computer that uses a lower level of encryption than the one you selected.</td>
</tr>
<tr>
<td>Encrypt user ID and password only</td>
<td>no</td>
<td>no</td>
<td>Encrypts only the remote user's identity during the authorization process. This option is less secure than encrypting an entire session.</td>
</tr>
</tbody>
</table>
Other Security Considerations

- Other Cisco Call Center Applications, on page 77
- Java Upgrades, on page 80
- Microsoft Security Updates, on page 81
- Microsoft Service Pack Policy, on page 81
- Microsoft Internet Information Server (IIS), on page 82
- Active Directory Deployment, on page 82
- Network Access Protection, on page 85
- WMI Service Hardening, on page 85
- SNMP Hardening, on page 86
- Toll Fraud Prevention, on page 87
- Third-Party Security Providers, on page 88
- Third-Party Management Agents, on page 88

Other Cisco Call Center Applications

The following sections discuss security considerations for other Cisco Call Center applications.

Cisco Unified ICM Router

The file `dbagent.acl` is an internal, background file. Do not edit this file. However, this file must have the READ permission set, so that the file can allow users to connect to the router's real-time feed.

Peripheral Gateways (PGs) and Agent Login

There is a rate limit of Unified CCE agent login attempts with incorrect password. By default, the agent account is disabled for 15 minutes after three incorrect password attempts, counted over a period of 15 minutes.

You can change this default by using 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`

The registry keys include the following:

- **AccountLockoutDuration**: Default. After the account is locked out because of unsuccessful login attempts, this value is the number of minutes the account remains locked out.
• **AccountLockoutResetCountDuration**: Default 15. Number of minutes before the AccountLockoutThreshold count goes back to zero. This value is applicable when the account does not get locked out, but you have unsuccessful login attempts that are less than AccountLockoutThreshold.

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

**Cisco CTI Object Server (CTI OS)**

In the *Cisco CTI Object Server (CTI OS)* System Manager Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted:

• Desktop Users: The section “Desktop User Accounts” contains instructions for configuring privileges for desktop users.

**CTI OS and Monitor Mode Connection**

There is a rate limit on Monitor Mode connection. When TLS is enabled and a password is required, Monitor Mode is disabled for 15 minutes after three incorrect password attempts (configurable). Counter resets on a valid login. Refer to the *Cisco CTI Object Server (CTI OS)* System Manager Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for more information.

**Cisco Agent Desktop**

Check the [Cisco Agent Desktop documentation](https://www.cisco.com/c/en/us/products/unified-collaboration/ciscoagt/agent-desktop/index.html) for information about required privileges and other topics that have an impact on security.

**Endpoint Security**

**Agent Desktops**

The CTI OS (C++/COM toolkit) and CAD agent desktop servers both support TLS encryption to the server. This encryption protects agent sign-in and CTI data from snooping. A mutual authentication mechanism enables the CTI OS Server and client to agree on a cipher suite for authentication, key exchange, and stream encryption. The cipher suite used is as follows:

- Protocol: SSLv3
- Key exchange: DH
- Authentication: RSA
- Encryption: AES (128)
- Message digest algorithm: SHA1

The following figure shows the encryption implementation's use of X.509 certificates on the agent desktops and on the servers. The implementation supports the integration with a Public Key Infrastructure (PKI) for the most secure deployment. By default, the application installs and relies on a self-signed certificate authority (CA) to sign client and server requests. However, Cisco supports integration with a third-party CA. This
mechanism is the preferred method because of the increased security provided by a corporate-managed CA or external authority such as VeriSign.

**Figure 15: Secure Agent Desktops (Certificate-Based Mutual Authentication)**

The following figure shows the Certificate Authority enrollment procedure to generate certificates used by the agent and the servers. The agent desktop certificate enrollment process is manual. The process requires the creation of certificate signing requests (CSRs) at each endpoint. The CSRs are then transferred to the certificate authority responsible for signing and generating the certificates.

**Figure 16: Certificate Authority Enrollment Procedure**

Cisco Finesse supports HTTPS for the Administration Console and Agent and Supervisor Desktops. HTTPS is not supported for Agent and Supervisor Desktops in large deployments (over 1000 agents).

**Unified IP Phone Device Authentication**

When designing a Unified CCE solution based on Unified Communications Manager, customers may choose to implement device authentication for the Cisco Unified IP Phones. Unified CCE supports Unified Communications Manager’s Authenticated Device Security Mode, which ensures the following:

- Device Identity — Mutual authentication using X.509 certificates
- Signaling Integrity — SCCP/SIP messages authenticated using HMAC-SHA-1
- Signaling Privacy — SCCP/SIP message content encrypted using AES-128-CBC
Media Encryption (SRTP) Considerations

Certain IP phones support Secure Real-Time Transport Protocol (SRTP). Before enabling SRTP in your deployment, consider the following points:

- The Unified CVP VXML Browser does not support SRTP.
- Deployments that use span-based silent monitoring do not support SRTP.
- Mobile Agents cannot use SRTP.
- The Cisco Outbound Option Dialers do not support SRTP. While calls are connected to the Dialer, the calls cannot use SRTP. But, calls can negotiate SRTP once the call is no longer connected to the Dialer.

IP Phone Hardening

The IP phone device configuration in Unified CM provides the ability to disable a number of phone features to harden the phones, such as disabling the phone's PC port or restricting a PC from accessing the voice VLAN. Changing some of these settings can disable the monitoring/recording feature of the Unified CCE solution. The settings are defined as follows:

- PC Voice VLAN Access
  - Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Disabling this feature will disable desktop-based monitoring and recording.
  - Setting: Enabled (default)

- Span to PC Port
  - Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. To use this feature, PC Voice VLAN access must be enabled. Disabling this feature will disable desktop-based monitoring and recording.
  - Setting: Enabled

Disable the following setting to prevent man-in-the-middle (MITM) attacks unless the third-party monitoring and/or recording application deployed uses this mechanism for capturing voice streams. The CTI OS Silent Monitoring feature and CAD Silent Monitoring and Recording do not depend on Gratuitous ARP.

- Gratuitous ARP
  - Indicates whether the phone will learn MAC addresses from Gratuitous ARP responses.
  - Setting: Disabled

Java Upgrades

During installations and upgrades, Unified CCE installs the base required Java version. Oracle can release Java updates with important security fixes after you install your contact center. You can apply Java updates to your contact center as follows:

- You can apply Java updates for the latest Java 6 minor version.
• You may need to modify the Windows JAVA_HOME path variable to point to the new Java Runtime Environment (JRE) location if it has changed.

Release 10.5(2) applies JRE 1.6.087.

Microsoft Security Updates

Automatically applying security and software update patches from third-party vendors has some risk. Subtle changes in functionality or extra layers of code can alter the overall performance of Cisco Contact Center products.

Assess all security patches released by Microsoft and install those patches deemed appropriate for your environment. Do not automatically enable Microsoft Windows Update. The update schedule can conflict with other Unified ICM/Unified CCE activity. Consider using Microsoft Software Update Service or similar patch management products to selectively apply Critical and Important security patches. Follow the Microsoft guidelines about when and how you apply these updates.

Assess the security exposure of the critical security patches released by Microsoft for Windows, IIS, and SQL. Apply critical security patches as you deem necessary for your site.


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 on the Compatibility Matrix web page for each product.

Microsoft Software Update Services (SUS) or Windows Server Update Services are alternatives to the default Windows Update website. You can configure the Microsoft Windows Automatic Update Client to poll a server that runs one of these alternatives to retrieve updates.

This approach enables you to selectively approve updates and determine when they get deployed on production servers.

To use Automatic Updates with a server that runs Software Update Services, see the Software Update Services Deployment white paper. See the following Microsoft website: http://www.microsoft.com/windowsserversystem/updateservices/techinfo/previous/susdeployment.mspx.
Microsoft Internet Information Server (IIS)

Internet Script Editor requires Internet Information Server (IIS). Disable the service on any other node except for the Distributor. There are some exceptions for the multimedia configuration of the solution. In that case, follow the product documentation and system requirements.

Active Directory Deployment


While Unified ICM and Unified CCE systems may still be deployed in a dedicated Windows Active Directory domain, it is not a requirement. What makes this possible is the capability of the software security principals to be installed in Organizational Units. This closer integration with AD and the power of security delegation means that corporate AD directories can be used to house application servers (for domain membership), user and service accounts, and groups.

AD Site Topology

In a geographically distributed deployment of Unified ICM or Unified CCE, redundant domain controllers must be located at each of the sites, and properly configured Inter-Site Replication Connections must be established with a Global Catalog at each site. The Unified CCE application is designed to communicate with the AD servers that are in their site, but this requires an adequately implemented site topology in accordance with Microsoft guidelines.

Organizational Units

Application-Created OUs

The installation of Unified ICM or Unified CCE software requires that the AD Domain in which the VMs are members must be in Native Mode. The installation will add a number of OU objects, containers, users, and groups that are necessary for the operation of the software. Adding these objects can be done only in an Organizational Unit in AD over which the user running the install program has been delegated control. The OU can be located anywhere in the domain hierarchy, and the AD Administrator determines how deeply nested the Unified ICM/Unified CCE OU hierarchy is created and populated.

Note

Local Server Accounts and groups are not created on the application servers. All created groups are Domain Local Security Groups, and all user accounts are domain accounts. The Service Logon domain account is added to the Local Administrators' group of the application servers.

Unified ICM and Unified CCE software installation is integrated with a Domain Manager tool that can be used standalone for pre-installing the OU hierarchies and objects required by the software, or can be used
when the Setup program is invoked to create the same objects in AD. The AD/OU creation can be done on the domain in which the running VM is a member or on a trusted domain.

Do not confuse the creation of AD objects with Group Policy Objects (GPO). The Automated Security Hardening, which is provided and follows the standard Microsoft Security Template format, is not added to AD as part of the software installation through the configuration of a GPO. The security policy provided by this customized template (for Unified ICM/Unified CCE applications) is applied locally when a user chooses to apply hardening, or it can be pushed down through a GPO through manual AD configuration using the provided policy file, `CiscoICM_Security_Template.inf`.

**AD Administrator-Created OUs**

An administrator can create certain AD objects. A prime example is the OU container for Unified CCE Servers. This OU container is manually added to contain the VMs that are members of a given domain. You move these VMs to this OU once they are joined to the domain. This segregation controls who can or cannot administer the servers (delegation of control). Most importantly, the segregation controls the AD Domain Security Policies that the application servers in the OU can or cannot inherit.

As noted before, Unified ICM/Unified CCE servers ship with a customized security policy. You can apply this policy at this server OU level through a Group Policy Object (GPO). Block any differing policies from being inherited at the Unified ICM/Unified CCE Servers' OU. Remember that someone can override blocking inheritance, a configuration option at the OU object level, by selecting the Enforced/No Override option at a higher hierarchy level. The application of group policies must follow a well-planned design. Start with the most common denominator, and restrict those policies only at the appropriate level in the hierarchy. For a more in-depth explanation on how to deploy group policies properly, see the pages in the *Microsoft Security Compliance Manager* site at [http://technet.microsoft.com/en-us/library/cc677002.aspx](http://technet.microsoft.com/en-us/library/cc677002.aspx).
The following notes apply to the preceding figure:

- The application setup creates the Cisco_ICM organizational unit object hierarchies.
- The AD administrators create Unified ICM Servers and Unified CCE Servers organizational unit objects to separately apply custom Cisco Unified ICM Security Policies through a GPO if necessary.
- Flexible Single Master Operation servers must be distributed across Domain Controllers in the appropriate sites according to Microsoft guidelines.
Network Access Protection

Network Access Protection (NAP) is a platform and solution introduced in Windows Server 2008 R2. NAP helps to maintain the network's overall integrity by controlling access to network resources based on a client computer's compliance with system health policies.

The NAP server validates client health using the system health policies.

The NAP server is supported on Windows Server 2008 R2.

The NAP client is supported on the following operating systems:

- Windows Server 2008 R2
- Windows 7

Network Policy Server

Do not use a Unified CCE server for any other purpose than for Unified CCE approved software. Do not run the Network Policy Server on any Unified CCE VM.

Unified CCE Servers and NAP

You can use NAP in a few different ways. The following are some deployment options a user can consider using with Unified CCE:

- Unified CCE servers using a limited access environment—NOT SUPPORTED

  Warning
  In this model, the Unified CCE servers are inaccessible if they fall out of compliance. This inaccessibility would cause the entire call center to go down until machines become compliant again.

- Unified CCE server uses monitoring-only environment—This mode is useful to track the health status of the Unified CCE servers.

- Unified CCE servers that are exempt from health validation—In this mode, the Unified CCE servers work in a NAP environment but do not become inaccessible from the network. A Unified CCE server's state of health does not affect communications to and from the other Unified CCE servers.

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:

Procedure

1. Launch the %SYSTEMROOT%\System32\Wmimgmt.msc MMC control.
2. Right-click the WMI Control icon and select Properties.
4. Select the Root folder and click the Security button.
5. Remove EVERYONE from the selection list then click the OK button.

Only give ALL rights to <machine>\Administrators.

More WMI Security Considerations

The WMI services are set to **Manual** startup by default. Third-Party Management agents use these services to capture system data. Do not disable WMI services unless required.

Perform DCOM security configuration in a manner that is consistent with your scripting environment. Refer to the WMI security documentation for more details on using DCOM security. For information on securing a remote WMI connection, see the Microsoft Developer Network article: [http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx](http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx).

SNMP Hardening

Refer to the **SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted** for details on installation, setting the community names, user names, and trap destinations.

Although the Microsoft Management and Monitoring Tools subcomponents are necessary for SNMP manageability, the Web Setup tool disables the Microsoft native SNMP service. A more secure agent infrastructure replaces the native Microsoft native SNMP service. Do not re-enable the Microsoft SNMP service. It can cause conflicts with the Cisco-installed SNMP agents.

Explicitly disable the Microsoft SNMP trap service. Do not run management software for collecting SNMP traps on contact center servers. This restriction makes the Microsoft SNMP trap service unnecessary.

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 contact center hosts located on internal networks behind corporate firewalls, enable SNMP manageability by applying the following configuration and hardening:

1. Create SNMP v1/v2c community strings or SNMP v3 usernames using a combination of upper, and lowercase characters. DO NOT use the common “public” and “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 username. 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 usernames on manageable devices to accept SNMP requests only from those hosts running SNMP management applications. (This configuration is done through the SNMP agent configuration tool when defining community strings and usernames.)

5. Enable sending of SNMP traps for authentication failures. These traps alert you to potential attackers trying to “guess” community strings and usernames.

SNMP manageability is installed on contact center servers and is executing by default. However, for security reasons, SNMP access is denied until the previous configuration steps have been completed.

For greater security, you can configure IPsec filters and an IPsec policy for SNMP traffic between an SNMP management station and SNMP agents. Follow the Microsoft advice on how to configure the filters and policy. For more information on IPsec policy for SNMP traffic, see the Microsoft TechNet articles.

**Toll Fraud Prevention**

Toll fraud is a serious issue in the Telecommunications Industry. The fraudulent use of telecommunications technology can be expensive for a company, so the Telecom Administrator must take the necessary precautions to prevent fraud. For Unified CCE environments, resources are available at Cisco.com on how to lock down Unified CM systems and to mitigate against toll fraud.

In Unified ICM, the primary concern is in using dynamic labels in the label node of a Unified ICM script. If the dynamic label is constructed from information entered by a caller (such as with Run External Script), then constructing labels of the following form is possible:

- 9....
- 9011....
- And similar patterns

These labels can send the call to outside lines or even to international numbers. Some dial plans configured in the routing client can allow such numbers to go through. If the customer does not want such labels used, then the Unified ICM script must check for valid labels before using them.

A simple example is an ICM script that prompts the caller with “If you know your party's extension, enter it now,”. The script then uses the digits entered blindly in a dynamic label node. This script might transfer the call anywhere. If you do not want this behavior, then either the Unified ICM routing script or the routing client’s dial plan must check for and disallow invalid numbers.

An example of a Unified ICM script check is an “If” node that uses an expression such as:

```python
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 case is only an example. Each customer must decide what is and what is not allowed based on their own environment.

Unified ICM does not normally transfer calls to arbitrary phone numbers. Numbers have to be explicitly configured as legal destinations. Alternatively, the logic in the Unified ICM routing script can transfer the call to a phone number from a script variable. You can write scripts so that a caller enters a series of digits and the script treats it as a destination phone number, asking the routing client to transfer the call to that number. Add logic to such a script to make sure the requested destination phone number is reasonable.
Third-Party Security Providers

Cisco has qualified Unified ICM software with the Operating System implementations of NTLM, Kerberos V, and IPsec security protocols.

Note

NTLMv1 is required on the Administration Server and Real-Time Data Server (AW) for integration of Cisco Finesse, Release 10.5. NTLMv2 is allowed with later versions of Cisco Finesse with Unified CCE, Release 10.5(x). Select the LAN Manager authentication level accordingly.

Cisco does not support other third-party security provider implementations.

Third-Party Management Agents

In their server operating system installations, some vendors include agents to provide convenient server management and monitoring.

Such agents can be valuable, but also impact performance. Cisco does not support their use on mission-critical Unified ICM/CCE servers.

Warning

Configure agents in accordance to the antivirus policies described in this document. Do not execute Polling or intrusive scans during peak hours, but rather schedule these activities for maintenance windows.

Note

Install SNMP services as instructed by these third-party management applications to take full advantage of the management capabilities provided with your servers. Without SNMP, enterprise management applications do not receive hardware pre-failure alerts. Unified CCE servers only support 32-bit extension agents.

Related Topics

General Antivirus Guidelines, on page 67
INDEX

A
antivirus guidelines 67
auditing 63
viewing auditing policies 63

B
batch deployment 35

C
Cisco firewall configuration utility 44, 45, 50
prerequisites 44
troubleshooting 50
verifying 45
Cisco network isolation utility 26, 27
process 27
working 26
Cisco SSL encryption utility 59, 60
encrypting in standalone mode 60
installing during setup 59
cti os c++/com toolkit 2

E
encryption support 1

I
IPSec 5
IPSec 9
logging 9
monitoring IPSec activity 9

N
NAT 5
network monitoring 10

P
per-user terminal services settings 72
preventing 73, 76
unauthorized changes to the installed product 76
unauthorized connections to a pcAnywhere host 73

R
remote administration 71
Remote desktop 72

S
security hardening utility 57
manual hardening 57
security log 64
security wizard 14
using 14
SQL server 2008 R2 55, 56
automated hardening 56
security considerations 55
security hardening utility 56
SQL server hardening 53
top hardening 53
support for IPSec 6
in transport mode 6
system monitoring 10

W
windows server firewall configuration 43
WMI service hardening 85