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 has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2003–2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface ix

Change History ix

About This Guide ix

Audience x

Related Documents x

Communications, Services, and Additional Information x

Field Alerts and Field Notices xi

Documentation Feedback xi

Conventions xi

CHAPTER 1

Encryption Support 1

User and Agent Passwords 1

Call Variables and Extended Call Variables 2

Internet Script Editor 2

CTIOS C++/COM Toolkit 2

Cisco Contact Center SNMP Management Service 3

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

IPsec Connection to Unified Communications Manager 9
Contents

CHAPTER 3 Cisco Unified Contact Center Security Wizard 13
  About Unified Contact Center Security Wizard 13
  Configuration and Restrictions 13
  Run Wizard 14
  Windows Firewall Configuration 14
  Network Isolation Configuration Panels 15
  SQL Hardening 18

CHAPTER 4 IPsec with Network Isolation Utility 19
  IPsec 19
  Manual Deployment or Network Isolation Utility 19
  Cisco Network Isolation Utility 20
  Network Isolation Utility Information 20
    IPsec Terminology 20
    Network Isolation Utility Process 21
  Traffic Encryption and Network Isolation Policies 22
  Network Isolation Feature Deployment 22
    Important Deployment Tips 22
    Sample Deployment 23
    Device Two-Way Communication 25
    Boundary Devices and Unified CCE 26
  Caveats 27
  Batch Deployment 29
  Network Isolation Utility Command-Line Syntax 29
Contents

CHAPTER 8
Cisco SSL Encryption Utility 55
   SSL Encryption Utility 55
      SSL Installation During Setup 55
   SSL Encryption Utility in Standalone Mode 56
      Transport Layer Security (TLS) Requirement 56

CHAPTER 9
Auditing 57
   Auditing 57
      View Auditing Policies 57
   View Security Log 58
   Real-Time Alerts 58
      SQL Server Auditing Policies 58
         SQL Server C2 Security Auditing 58
   Active Directory Auditing Policies 58

CHAPTER 10
General Antivirus Guidelines 61
   Antivirus Guidelines 61
      Unified ICM/Unified CCE Maintenance Parameters 63
         Logger Considerations 63
         Distributor Considerations 63
         CallRouter and PG Considerations 63
         Other Scheduled Tasks Considerations 63
   File Type Exclusion Considerations 63

CHAPTER 11
Remote Administration 65
   Windows Remote Desktop 65
      Remote Desktop Protocol 66
      RDP-TCP Connection Security 66
      Per-User Terminal Services Settings 66
   pcAnywhere 67
      Restricted Access to Internal Machines 67
      Unauthorized Connections to pcAnywhere Host 67
CHAPTER 12

Other Security Considerations 71

Other Cisco Call Center Applications 71
Cisco Unified ICM Router 71
Peripheral Gateways (PGs) and Agent Login 71
Cisco CTI Object Server (CTIOS) 72
CTIOS and Monitor Mode Connection 72
Cisco Agent Desktop 72
Endpoint Security 72
Agent Desktops 72
Unified IP Phone Device Authentication 72
Media Encryption (SRTP) Considerations 73
IP Phone Hardening 73
Java Upgrades 73
Upgrade Tomcat Utility 74
Upgrade Tomcat 74
Revert Tomcat 75
Microsoft Security Updates 75
Microsoft Service Pack Policy 76
Microsoft Internet Information Server (IIS) 76
Active Directory Deployment 76
AD Site Topology 77
Organizational Units 77
Application-Created OUs 77
AD Administrator-Created OUs 77
Network Access Protection 78
Network Policy Server 78
Unified CCE Servers and NAP 78
WMI Service Hardening 78
WMI Namespace-Level Security  78
More WMI Security Considerations  79
SNMP Hardening  79
Toll Fraud Prevention  80
Third-Party Security Providers  81
Third-Party Management Agents  81

APPENDIX A

UCCE Security Compliance  83
Unified CCE Security Hardening for Windows Server  83
Preface

• Change History, on page ix
• About This Guide, on page ix
• Audience, on page x
• Related Documents, on page x
• Communications, Services, and Additional Information, on page x
• Field Alerts and Field Notices, on page xi
• Documentation Feedback, on page xi
• Conventions, on page xi

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cumulative minor defect fixes</td>
<td></td>
<td>April, 2019</td>
</tr>
<tr>
<td>New Upgrade Tomcat Utility section added.</td>
<td>Upgrade Tomcat Utility, on page 74</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 2012 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:

• Enterprise Chat and Email
• Dynamic Content Adapter
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.

**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 2014 and Windows Server 2012 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.

**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).

**Communications, Services, and Additional Information**

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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 and then access the tool at 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.

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. |
<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>italic font</td>
<td>Italic font is used to indicate the following:&lt;br&gt;• To introduce a new term. Example: A <em>skill group</em> is a collection of agents who share similar skills.&lt;br&gt;• A syntax value that the user must replace. Example: IF <em>(condition, true-value, false-value)</em>&lt;br&gt;• A book title. Example: See the <em>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</em>.</td>
</tr>
<tr>
<td>window font</td>
<td>Window font, such as Courier, is used for the following:&lt;br&gt;• Text as it appears in code or that the window displays. Example:&lt;br&gt;  &lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets are used to indicate the following:&lt;br&gt;• For arguments where the context does not allow italic, such as ASCII output.&lt;br&gt;• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>
Encryption Support

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

User and Agent Passwords

When Single Sign-On (SSO) is enabled, it hands off the Agent and Supervisor authentications to a third party Identity Provider (IDP). In such a case, the Agent and Supervisor passwords are not stored in the Unified CCE database.

When SSO is not enabled, the Agent and Supervisor passwords are stored in the configuration database with an MD5 hash. Unified CCE has mechanisms to protect data in transit, and options for protecting data at rest.

Administrator and Configuration user login uses credentials that are stored in Active Directory. These passwords are not stored in the Unified CCE database. The exception is System Inventory, which allows centralized configuration and management of Unified CCE services from a central location via CCE Administration web page. System Inventory requires credentials to manage and get diagnostic information from other sub-systems in the Unified CCE Solution. These passwords are stored with AES 256-bit encryption in the AW database.

CCE Admin web page users are authenticated using the Active Directory credentials.

CUIC reporting users can either use SSO or AD credentials to log on depending on whether SSO is enabled or not. If SSO is not enabled, then Supervisor reporting users use Active Directory authentication to gain access to reporting, and not the local MD5 password stored in the configuration database.

Note

Unified CCE cannot read, set, or change user passwords in Active Directory. It is possible and likely that the Supervisor reporting users may use a password (their AD password) to login to CUIC that is different from their agent password set by the configuration administrator.
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 2012 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 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 https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings.

Related Topics
   Cisco SSL Encryption Utility, on page 55

CTI OS C++/COM Toolkit

The CTI OS (C++/COM toolkit) and agent desktops implement TLS v1.2 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.

Note

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 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 19

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 installed.

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


• Cisco Unified CCE 11.0
**Supported Communication Paths**

Unified ICM Release supports deploying IPsec in a Window Server 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**

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

Each IPsec policy consists of one or more IPsec rules. Each IPsec rule consists of 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)
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-Hellman groups 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 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 2012 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

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

- Automated SQL Server Hardening, on page 49
- IPsec with Network Isolation Utility, on page 19
- Windows Server Firewall Configuration, on page 37

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 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 19
- Windows Server Firewall Configuration, on page 37

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.

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

Warning

- 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 37

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 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 19

## SQL Hardening

You can use the SQL Hardening wizard to:

• Apply the SQL Server security hardening.
• Upgrade from a previously applied hardening.
• Roll back previously applied hardening.

In the SQL Hardening Security Action panel, you can:

• Apply or Upgrade SQL Server Security Hardening
• Roll back Previously Applied SQL Server Security Hardening

**Note**

The Rollback is disabled if there is no prior history of SQL Server security hardening or if the hardening was already rolled back.

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

**Related Topics**

*Automated SQL Server Hardening*, on page 49
CHAPTER 4

IPsec with Network Isolation Utility

- IPsec, on page 19
- Manual Deployment or Network Isolation Utility, on page 19
- Cisco Network Isolation Utility, on page 20
- Network Isolation Utility Information, on page 20
- Traffic Encryption and Network Isolation Policies, on page 22
- Network Isolation Feature Deployment, on page 22
- Caveats, on page 27
- Batch Deployment, on page 29
- Network Isolation Utility Command-Line Syntax, on page 29
- Troubleshoot Network Isolation IPsec Policy, on page 34

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 with Network Isolation Utility, on page 19
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, 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 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.

For fuller descriptions of Microsoft Windows IPsec terminology, see

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)
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 22
Sample Deployment, on page 23
Device Two-Way Communication, on page 25
Boundary Devices and Unified CCE, on page 26

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.

**Related Topics**

- Caveats, on page 27

### 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 3: Example Unified Contact Center System](image)

   Figure 3: 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>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>
<tr>
<td>Administration Server, Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS)</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>Internet Script Editor Clients/Webskilling</td>
</tr>
<tr>
<td></td>
<td>Third-Party Clients/SOL 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:
### Boundary Device

<table>
<thead>
<tr>
<th>Domain Controllers: such as those for RTR, LGR, Administration &amp; Data Server or HDS, and PGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Boundary Device: Domain Controller IP Address</td>
</tr>
<tr>
<td>• Traffic Direction: Outbound</td>
</tr>
<tr>
<td>• Protocol: Any</td>
</tr>
<tr>
<td>• Port: Not Applicable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS, WINS, Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote Access or Remote Management software: such as that for every Trusted Device (VNC, pcAnywhere, Remote Desktop Connection, SNMP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Boundary Device: Any host</td>
</tr>
<tr>
<td>• Traffic Direction: Inbound</td>
</tr>
<tr>
<td>• Protocol: TCP</td>
</tr>
<tr>
<td>• Port: 5900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unified Communications Manager Cluster for PGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Boundary Device: A specific IP Address (or Subnet)</td>
</tr>
<tr>
<td>• Traffic Direction: Outbound</td>
</tr>
<tr>
<td>• Protocol: TCP</td>
</tr>
<tr>
<td>• Port: All ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agent Desktops</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Finesse Server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Boundary Device: A Subnet</td>
</tr>
<tr>
<td>• Traffic Direction: Inbound</td>
</tr>
<tr>
<td>• Protocol: TCP</td>
</tr>
<tr>
<td>• Port: 42028</td>
</tr>
</tbody>
</table>

### 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.
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.

Important

- 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:

<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
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>Creates a new policy or enables an existing one from the stored policy XML file. Optionally enables encryption of the network traffic data. Creates a new policy in Windows IPsec policy store and adds all Boundary Devices listed in the XML file. If the XML file does not exist, then it creates a new XML file. The /encrypt option overrides the value set in the XML file.</td>
</tr>
</tbody>
</table>
### Network Isolation Utility Command-Line Syntax

<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADD BOUNDARY</strong></td>
<td>cscript ICMNetworkIsolation.vbe /addBoundary DNS</td>
<td>WINS</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cscript ICMNetworkIsolation.vbe /addBoundary DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This example adds the DNS server to the Boundary Device list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cscript ICMNetworkIsolation.vbe /addAnyHostBoundary &lt;Outbound</td>
<td>Inbound&gt; &lt;TCP</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cscript ICMNetworkIsolation.vbe /addAnyHostBoundary Inbound TCP 5900</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This example allows VNC access from all machines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cscript ICMNetworkIsolation.vbe /addIPAddrBoundary &lt;IP address&gt; &lt;Outbound</td>
<td>Inbound&gt; &lt;TCP</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cscript ICMNetworkIsolation.vbe /addIPAddrBoundary 10.86.121.160 Outbound Any</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This example allows all outbound traffic to a device with the specified IP address.</td>
<td></td>
</tr>
<tr>
<td>Argument Name</td>
<td>Syntax and Example</td>
<td>Function</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
|               | 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. |
<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
</table>
| REMOVE BOUNDARY | cscript ICMNetworkIsolation.vbe /removeBoundry DNS|WINS|DHCP|GATEWAY  
For example:  
cscript ICMNetworkIsolation.vbe /removeBoundry 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. |
<table>
<thead>
<tr>
<th>Argument Name</th>
<th>Syntax and Example</th>
<th>Function</th>
</tr>
</thead>
</table>
|               | 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. |
| 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\CiscoICMIPsecConfig.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.
CHAPTER 5

Windows Server Firewall Configuration

- Windows Server Firewall, on page 37
- Cisco Firewall Configuration Utility Prerequisites, on page 38
- Run Cisco Firewall Configuration Utility, on page 38
- Verify New Windows Firewall Settings, on page 39
- Windows Server Firewall Communication with Active Directory, on page 39
- CiscoICMfwConfig_exc.xml File, on page 43
- Windows Firewall Troubleshooting, on page 43

Windows Server Firewall

Windows Server 2012 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.


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 2012 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

---

**Cisco Firewall Configuration Utility Prerequisites**

Install the following software before using the Firewall configuration utility:

1. Windows Server 2012 R2
2. Unified ICM/CCE components

---

**Note**

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

---

**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, run `cscript %SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig.vbe`, or, on Windows Server 2012 R2, run `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat`.

**Step 3**

**Step 4**  
When you first run the script, the script runs `configfirewall.bat`. The script then asks you to rerun the application using the same command. Rerun the script if instructed to do so.

**Step 5**  
Click OK.

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

**Step 6**  
Reboot the server.

**Related Topics**

Windows Firewall Configuration, on page 14

## 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.

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.

**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`
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 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>138</td>
<td>UDP</td>
<td></td>
<td>NetBIOS NetLogon and Browsing</td>
</tr>
<tr>
<td>139</td>
<td>UDP</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>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>3269</td>
<td></td>
<td>LDAP</td>
<td>LDAP GC SSL</td>
</tr>
<tr>
<td>42</td>
<td></td>
<td>Wins</td>
<td>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>UDP</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:

```
<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.

You can 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.

Note 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 via Control Panel.

To undo the firewall settings:
Procedure

Step 1  Stop all application services.
Step 2  Open a command window by choosing Start > Run and entering CMD in the dialog window.
Step 3  Click OK.
Step 4  Enter the following command cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig.
Step 5  Enter UndoConfigFirewall.bat for Windows Server.
Step 6  Reboot the server.
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.
4. Set a strong password for the sa account before installing ICM.
6. Enable SQL Server Agent Service and set to Automatic for database maintenance in Unified ICM.

Note

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. Disable the SQL guest account.
8. Restrict sysadmin membership to your Unified ICM administrators.
9. Block TCP port 1433 and UDP port 1434 at the network firewall, unless the Administration & Data Server is not in the same security zone as the Logger.
10. Provide protection with good housekeeping:
   1. Delete or archive these setup files after installation if they are present:
      • 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, delete the following files if they are present:
      • setup.iss in `%Windir%`
      • sqlsp.log in Windows Temp

11. Change the recovery actions of the Microsoft SQL Server service to restart after a failure.

12. Remove all sample databases.


**Related Topics**

- SQL Server Users and Authentication, on page 48
- Virtual Accounts, on page 51

---

**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 [https://msdn.microsoft.com/en-us/library/ms188670.aspx](https://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 3: Password and Account Settings**

<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>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------</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>

Mixed mode authentication is enforced through SQL Server automated hardening.

During automated SQL Server hardening, if the sa password is found as blank, a randomly generated strong password is generated so as to secure the sa account.

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

**SQL Server Security Considerations**

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

---

### Note

#### Automated SQL Server Hardening

The SQL Server Security Automated Hardening utility performs the following:

- Enforces Mixed Mode Authentication.
- Ensures that the Named Pipe (np) is listed before TCP/IP (tcp) in the SQL Server Client Network Protocol Order.
- Disables SQLWriter and SQLBrowser 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.
You can optionally apply the SQL Server Security Hardening as part of Unified CCE installation and upgrade or via the Security Wizard tool. The utility is internally managed by running the Windows PowerShell script ICMSQLSecurity.ps1. You can also apply the hardening by directly running the PowerShell script.

**Utility Location**

The utility is located at:

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

**HARDEN Command**

At the Windows PowerShell command line, enter:

```plaintext
Powershell .\ICMSQLSecurity.ps1 HARDEN
```

---

**Note**

The current SQL Server configuration is backed up to

```plaintext
<ICMInstallDrive>:\CiscoUtils\SQLSecurity\icmsqlsecuritybkp.xml
```

before the utility applies the SQL Server hardening.

---

**ROLLBACK Command**

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:

```plaintext
Powershell .\ICMSQLSecurity.ps1 ROLLBACK
```

---

**Note**

The following settings are required for Unified CCE to function properly. They are not reverted to their original state when automated rollback is performed:

1. Named Pipe (np) listed before TCP/IP(tcp) in the SQL Server Client Network Protocol Order.

---

**Help for Commands**

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

**Output Log**

All output logs are saved in the file:

```plaintext
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity\Logs\ICMSQLSecurity.log
```
Manual SQL Server Hardening

By default, SQL Server 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 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.

Virtual Accounts

Virtual Accounts are preferred over Network or Local Services account for SQL Services because of the former's higher level of security. Virtual accounts run with the lowest privileges. The CCE installer adds the Perform Volume Maintenance Tasks privilege to the SQL account. This privilege is needed to perform database-related operations, such as creating and expanding the database.

If your corporate policy does not allow the use of this privilege, you can remove it. However, performing database-related operations such as creating and expanding the database takes more time (depending on the size of your database).
Windows Hardening

- Windows Server Hardening, on page 53

Windows Server Hardening

Unified CCE installer has a customized security policy in the form of Group Policy Object (GPO) backup. You can apply this policy into a separate Organization Unit (OU), that contains Unified CCE servers. The policy ensures the proper functioning of the Unified CCE application, and with improved security. Clearly identify the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and ensure that it is documented in accordance with your corporate policy.

Create this OU either at the same level as the Computers container or at the Cisco ICM Root OU. If you are unfamiliar with Active Directory, engage your Domain Administrator to assist you with Group Policy deployments.

Note

You can only apply Unified CCE GPO backup to the member server OU that is created under Windows Server Domain Controller.

Figure 7: Group Policy Deployments

After the security policy is applied at the OU level, any differing policies must be blocked from being inherited at the Unified ICM/Unified CCE Servers OU. Keep in mind that you can override blocking inheritance, a configuration option at the OU object level, when you select the Enforced/No Override option at a higher...
hierarchy level. The application of group policies must follow a thought-out design that starts with the most common denominator, and those policies must be restrictive only at the appropriate level in the hierarchy.

**Related Topics**

AD Administrator-Created OUs, on page 77

## Applying Unified CCE Security Policies to Unified CCE Server

You can apply the customized Unified CCE security polices to the Unified CCE servers, by following these steps:

1. Create a Member Server OU in the domain, and at the same level as the *Computers* container or the Cisco ICM Root OU.

2. Move all the Unified CCE Windows 2012 R2 Servers to the newly created OU.

3. Extract the Unified CCE security Group Policy Object (GPO) backup zip file that is located in `%SYSTEMDRIVE%\CiscoUtils\SecurityTemplates\UCCE_GPO.zip`.

4. Using the Group Policy Management Console (GPMC) tool, link the GPO backup to the newly created OU so that the Unified CCE group policies are pushed to all the Unified CCE Servers under that OU.

---

**Note**

The Group Policy Object (GPO) backup zip file is also located in the `ICM-CCE-CCHInstaller\SecurityTemplates` folder in the installation media (DVD).

See Appendix A for the list of security policies that are supported by Unified CCE for hardening the Unified CCE servers.
Chapter 8

Cisco SSL Encryption Utility

- SSL Encryption Utility, on page 55

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.

Note

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

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 for Unified CCE web applications installed on Windows Server. You can configure Internet Script Editor for SSL.

SSL Installation During Setup

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

Note

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.

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.

### Transport Layer Security (TLS) Requirement


---

**Note**

For backward compatibility with the earlier versions of clients, you can downgrade the Unified CCE Windows systems to earlier versions of TLS by following Microsoft procedures.

If you apply security hardening without configuring support for TLS, your 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.
Auditing

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

Note

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** 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>
Active Directory Auditing Policies
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 Unified CCE Solution Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.


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 *Unified CCE Solution Compatibility Matrix* 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 multtiered 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 65
- pcAnywhere, on page 67
- VNC, on page 70

Windows Remote Desktop

Remote Desktop permits users to remotely execute applications on Windows Server from a range of devices over virtually any network connection. You can run Remote Desktop in either Application Server or Remote Administration modes. Unified ICM/Unified CCE only supports Remote Administration mode.

*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 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**

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

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.
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.

pcAnywhere now requires a password for all host sessions. This security feature prevents users from inadvertently launching an unprotected host session.

pcAnywhere lets dial-up users specify a call-back number for remote control sessions. In a normal pcAnywhere session, the remote connects to the host, and the session begins. When callback is enabled, the remote calls the host, but then the host drops the connection and calls back the remote at the specified phone number.

### Table 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 (lock computer)</td>
<td>no</td>
<td>Yes</td>
<td></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>
**Data Stream Protection During Remote Control Session**

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

pcAnywhere offers three levels of encryption:

- pcAnywhere encryption
- Symmetric encryption
- Public key encryption

**Table 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>pcAnywhere 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, 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.
Other Security Considerations

- Other Cisco Call Center Applications, on page 71
- Java Upgrades, on page 73
- Upgrade Tomcat Utility, on page 74
- Microsoft Security Updates, on page 75
- Microsoft Service Pack Policy, on page 76
- Microsoft Internet Information Server (IIS), on page 76
- Active Directory Deployment, on page 76
- Network Access Protection, on page 78
- WMI Service Hardening, on page 78
- SNMP Hardening, on page 79
- Toll Fraud Prevention, on page 80
- Third-Party Security Providers, on page 81
- Third-Party Management Agents, on page 81

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 *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise*:

- 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 *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise* for more information.

### Cisco Agent Desktop

Check the [Cisco Agent Desktop documentation](#) for information about required privileges and other topics that have an impact on security.

### Endpoint Security

#### Agent Desktops

Cisco Finesse supports HTTPS (TLS 1.2 only) for the Administration Console and agent and supervisor clients.

#### 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 — SIP messages authenticated using HMAC-SHA-1
- Signaling Privacy — 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

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 32-bit Java 8 minor version.

• Modify the Windows JAVA_HOME path variable to point to the new Java Runtime Environment (JRE) location if it has changed.
Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 7.0 build releases. (That is, only version 7.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 7.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 7.0.62 to 7.0.65. You cannot use this tool for major or minor version upgrades.

- Revert a Tomcat upgrade.

  If upgrading Tomcat causes a problem, use the utility to revert to the previous release.

  Note: If you use the utility to upgrade Tomcat multiple times, you can revert to only one version back of Tomcat. For example, if you upgrade Tomcat from 7.0.62 to 7.0.63, and then to 7.0.75, the utility reverts Tomcat to 7.0.63.

Before using the tool:


- Download the utility (UpgradeTomcatTool-<version>.jar) and copy it onto the Unified CCE component VMs.

  Download link: https://software.cisco.com/download/release.html?mdfid=284360381&flowid=46270&softwareid=284416107&release=11.6(1)&relind=AVAILABLE&relifecycle=&reltype=latest

- Delete or back up large log files in these directories to reduce upgrade time:
  
  c:\icm\tomcat\logs
  
  c:\icm\debug.txt

Upgrade Tomcat

For detailed information on the results from each step, see the ..\UpgradeTomcatResults\UpgradeTomcat.log file.

  Note: Stop Unified CCE services on the VM before using the Tomcat Utility.

Procedure

Step 1

  From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.
Step 2  Enter this command to run the tool: `java -jar UpgradeTomcatTool-<version>.jar -upgrade`  
For example:  
```
java -jar UpgradeTomcatTool-11.5.1.jar -upgrade
```
Step 3  When prompted, enter the full pathname of the new Tomcat installer.  
For example:  
```
c:\tomcatInstaller\apache-tomcat-<version>.exe
```
Step 4  When prompted, enter `yes` to continue with the upgrade.  
Step 5  Repeat these steps for all unified CCE component VMs.

---

**Revert Tomcat**

For detailed information on the results from each step, see the `../UpgradeTomcatResults/UpgradeTomcat.log` file.

**Note**  
Stop Unified CCE services on the VM before using the Tomcat Utility.

**Procedure**

Step 1  From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.  
Step 2  Enter this command to run the tool: `java -jar UpgradeTomcatTool-<version>.jar -revert`  
For example:  
```
java -jar UpgradeTomcatTool-<version>.jar -revert
```
Step 3  When prompted, enter `yes` to continue with the reversion.  
Step 4  Repeat these steps for all unified CCE component VMs.

---

**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 or cumulative updates released by Microsoft for Windows, IIS, and SQL. Apply critical security patches or cumulative updates 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:


---

**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.

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.

Related Topics

Windows Server Hardening, on page 53
Network Access Protection

Network Access Protection (NAP) is a platform and solution introduced in Windows Server. 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.


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

Step 1  Launch the %SYSTEMROOT%\System32\Wmimgmt.msc MMC control.
Step 2  Right-click the WMI Control icon and select Properties.
Step 3  Select the Security properties page.
Step 4  Select the Root folder and click the Security button.
Step 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.

SNMP Hardening

Refer to the SNMP Guide for Cisco Unified ICM/Contact Center Enterprise for details on installation, setting the community names, usernames, 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:

```
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.

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 prefailure alerts. Unified CCE servers only support 32-bit extension agents.

Related Topics

General Antivirus Guidelines, on page 61
UCCE Security Compliance

• Unified CCE Security Hardening for Windows Server, on page 83

Unified CCE Security Hardening for Windows Server

This topic contains the security baseline for hardening Windows Servers running Unified CCE.

This baseline is essentially a collection of Microsoft group policy settings which are determined by using the Microsoft Security Compliance Manager 4.0 tool.

In addition to the GPO settings provided in the table, disable the following settings:

• NetBIOS

• SMBv1

For more details about these configurations, see the Microsoft Windows Server documentation.

The baseline includes only those settings whose severity qualifies as Critical and Important. The settings with Optional and None severity qualification are not included in the baseline.

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Default Value</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security: LAN Manager authentication level</td>
<td>Send NTLMv2 response only</td>
<td>Send NTLMv2 response only. Refuse LM &amp; NTLM</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Audit NTLM authentication in this domain</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Incoming NTLM traffic</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Interactive logon: Require smart card</td>
<td>Disabled</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network security: Allow Local System NULL session fallback</td>
<td>Not defined</td>
<td>Disabled</td>
</tr>
<tr>
<td>Microsoft network client: Send unencrypted password to third-party SMB servers</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network security: Allow Local System to use computer identity for NTLM</td>
<td>Not defined</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network security: Do not store LAN Manager hash value on next password change</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network Security: Allow PKU2U authentication requests to this computer to use online identities</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network security: Minimum session security for NTLM SSP based (including secure RPC servers)</td>
<td>No minimum</td>
<td>Require NTLMv2 session security, Require 128-bit encryption</td>
</tr>
<tr>
<td>Microsoft network server: Server SPN target name validation level</td>
<td>Off</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Interactive logon: Smart card removal behavior</td>
<td>No Action</td>
<td>Lock Workstation</td>
</tr>
<tr>
<td>Network security: Minimum session security for NTLM SSP based (including secure RPC clients)</td>
<td>No minimum</td>
<td>Require NTLMv2 session security, Require 128-bit encryption</td>
</tr>
<tr>
<td>Interactive logon: Number of previous logons to cache (in case domain controller is not available)</td>
<td>10 logons</td>
<td>4 logon(s)</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: NTLM authentication in this domain</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network access: Let Everyone permissions apply to anonymous users</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Add server exceptions in this domain</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network Security: Restrict NTLM: Audit Incoming NTLM Traffic</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network access: Do not allow anonymous enumeration of SAM accounts and shares</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network access: Do not allow anonymous enumeration of SAM accounts</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Shutdown: Clear virtual memory pagefile</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network access: Remotely accessible registry paths</td>
<td>System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\ServerApplicationsSoftware\Microsoft\WindowsNT\CurrentVersion</td>
<td>System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\ServerApplicationsSoftware\Microsoft\WindowsNT\CurrentVersion</td>
</tr>
<tr>
<td>Network access: Shares that can be accessed anonymously</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Turn off the &quot;Publish to Web&quot; task for files and folders</td>
<td>Not configured</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Shutdown: Allow system to be shut down without having to log on</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>System objects: Require case insensitivity for non-Windows subsystems</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network access: Sharing and security model for local accounts</td>
<td>Classic - local users authenticate as themselves</td>
<td>Classic - local users authenticate as themselves</td>
</tr>
<tr>
<td>Interactive logon: Do not require CTRL+ALT+DEL</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Devices: Allowed to format and eject removable media</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Turn off the Windows Messenger Customer Experience Improvement Program</td>
<td>Not configured</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Turn off Search Companion content file updates</td>
<td>Not configured</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Network access: Allow anonymous SID/Name translation</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network access: Remotely accessible registry paths and sub-paths</td>
<td>System\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP ServerSoftware\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\WindowsNT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndexSystem\CurrentControlSet\Control\Terminal ServerSystem\CurrentControlSet\Control\Terminal Server\UserConfigSystem\CurrentControlSet\Control\Terminal Server\DefaultUserConfigurationSoftware\Microsoft\Windows NT\CurrentVersion\PerflibSystem\CurrentControlSet\Services\SysmonLog</td>
<td>System\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP ServerSoftware\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\WindowsNT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndexSystem\CurrentControlSet\Control\Terminal ServerSystem\CurrentControlSet\Control\Terminal Server\UserConfigSystem\CurrentControlSet\Control\Terminal Server\DefaultUserConfigurationSoftware\Microsoft\Windows NT\CurrentVersion\PerflibSystem\CurrentControlSet\Services\SysmonLog</td>
</tr>
<tr>
<td>Recovery console: Allow automatic administrative logon</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Turn off Autoplay</td>
<td>Not configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Turn off Windows Update device driver searching</td>
<td>Disabled</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Network access: Restrict anonymous access to Named Pipes and Shares</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Recovery console: Allow floppy copy and access to all drives and all folders</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Network access: Named Pipes that can be accessed anonymously</td>
<td>None</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit Policy: System: IPsec Driver</td>
<td>No auditing</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: System: Security System Extension</td>
<td>No auditing</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Account Management: Security Group Management</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</td>
<td>Not defined</td>
<td>Enabled</td>
</tr>
<tr>
<td>Audit Policy: Account Management: Other Account Management Events</td>
<td>No auditing</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: System: Security State Change</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Detailed Tracking: Process Creation</td>
<td>No auditing</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Policy: System: Other System Events</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Logon-Logoff: Account Lockout</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Policy: Policy Change: Audit Policy Change</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Audit: Audit the access of global system objects</td>
<td>Disabled</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit Policy: Logon-Logoff: Special Logon</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Policy: Account Management: User Account Management</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Account Logon: Credential Validation</td>
<td>No auditing</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Logon-Logoff: Logon</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Account Management: Computer Account Management</td>
<td>No auditing</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Policy: Privilege Use: Sensitive Privilege Use</td>
<td>No auditing</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Policy: Logon-Logoff: Logoff</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Policy: Policy Change: Authentication Policy Change</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>Audit: Audit the use of Backup and Restore privilege</td>
<td>Disabled</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit Policy: System: System Integrity</td>
<td>Success and Failure</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Turn off toast notifications on the lock screen</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Microsoft network server: Amount of idle time required before suspending session</td>
<td>15 minutes</td>
<td>15 minute(s)</td>
</tr>
<tr>
<td>Interactive logon: Message text for users attempting to log on</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Interactive logon: Machine inactivity limit</td>
<td>Not defined</td>
<td>900 seconds</td>
</tr>
<tr>
<td>Microsoft network server: Disconnect clients when logon hours expire</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Interactive logon: Message title for users attempting to log on</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network security: Force logoff when logon hours expire</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Sign-in last interactive user automatically after a system-initiated restart</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td>Interactive logon: Display user information when the session is locked</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Interactive logon: Do not display last user name</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Interactive logon: Machine account lockout threshold</td>
<td>Not defined</td>
<td>10 invalid logon attempts</td>
</tr>
<tr>
<td>Allow Remote Shell Access</td>
<td>Not configured</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Devices: Prevent users from installing printer drivers</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Create global objects</td>
<td>Administrators, Service, Local Service, Network Service</td>
<td>Administrators, Service, Local Service, Network Service</td>
</tr>
<tr>
<td>Access this computer from the network</td>
<td>Everyone, Administrators, Users, Backup Operators</td>
<td>Administrators, Authenticated Users</td>
</tr>
<tr>
<td>Domain controller: Allow server operators to schedule tasks</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Modify an object label</td>
<td>None</td>
<td>No One</td>
</tr>
<tr>
<td>Generate security audits</td>
<td>Local Service, Network Service</td>
<td>Local Service, Network Service</td>
</tr>
<tr>
<td>Increase scheduling priority</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Force shutdown from a remote system</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allow log on through Remote Desktop Services</td>
<td>Administrators, Remote Desktop Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Change the system time</td>
<td>Local Service, Administrators</td>
<td>Local Service, Administrators</td>
</tr>
<tr>
<td>Add workstations to domain</td>
<td>Not defined (Authenticated Users for domain controllers)</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Profile single process</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Deny log on as a batch job</td>
<td>No one</td>
<td>Guests</td>
</tr>
<tr>
<td>Act as part of the operating system</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>Change the time zone</td>
<td>Local Service, Administrators</td>
<td>Local Service, Administrators</td>
</tr>
<tr>
<td>Synchronize directory service data</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Lock pages in memory</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>Access Credential Manager as a trusted caller</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>Create a token object</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>Debug programs</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Deny log on as a service</td>
<td>No one</td>
<td>Guests</td>
</tr>
<tr>
<td>Deny access to this computer from the network</td>
<td>Guests</td>
<td>Guests, NT AUTHORITY\Local account and member of Administrators group</td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>Administrators, Backup Operators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Shut down the system</td>
<td>Administrators, Backup Operators, Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Deny log on locally</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>Replace a process level token</td>
<td>Local Service, Network Service</td>
<td>Local Service, Network Service</td>
</tr>
<tr>
<td>Modify firmware environment values</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allow log on locally</td>
<td>Guest, Administrators, Users, Backup Operators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Restore files and directories</td>
<td>Administrators, Backup Operators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Profile system performance</td>
<td>Administrators, NT Service\WdiServiceHost</td>
<td>Administrators, NT Service\WdiServiceHost</td>
</tr>
<tr>
<td>Log on as a batch job</td>
<td>Administrators, Backup Operators</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Perform volume maintenance tasks</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>Impersonate a client after authentication</td>
<td>Administrators, Service, Local Service, Network Service</td>
<td>Administrators, Service, Local Service, Network Service</td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Take ownership of files or other objects</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>Local Service, Network Service, Administrators</td>
<td>Administrators, Local Service, Network Service</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>No one</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Create symbolic links</td>
<td>Administrators</td>
<td>Administrators</td>
</tr>
<tr>
<td>Create permanent shared objects</td>
<td>No one</td>
<td>No One</td>
</tr>
<tr>
<td>System cryptography: Force strong key protection for user keys stored on the computer</td>
<td>Disabled</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Domain member: Require strong (Windows 2000 or later) session key</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Allow unicast response</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Apply local firewall rules</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Inbound connections</td>
<td>Block</td>
<td>Enabled</td>
</tr>
<tr>
<td>Windows Firewall: Private: Firewall state</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Windows Firewall: Private: Apply local connection security rules</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Private: Allow unicast response</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Windows Firewall: Public: Apply local firewall rules</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Public: Apply local connection security rules</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Firewall: Public: Firewall state</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Windows Firewall: Private: Outbound connections</td>
<td>Allow</td>
<td>Allow (default)</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Outbound connections</td>
<td>Allow</td>
<td>Allow (default)</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Firewall state</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Windows Firewall: Public: Allow unicast response</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Windows Firewall: Public: Inbound connections</td>
<td>Block</td>
<td>Enabled</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Apply local connection security rules</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Private: Display a notification</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Domain: Display a notification</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Windows Firewall: Public: Display a notification</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Firewall: Public: Outbound connections</td>
<td>Allow</td>
<td>Allow (default)</td>
</tr>
<tr>
<td>Windows Firewall: Private: Inbound connections</td>
<td>Block</td>
<td>Enabled</td>
</tr>
<tr>
<td>Windows Firewall: Private: Apply local firewall rules</td>
<td>Yes</td>
<td>Yes (default)</td>
</tr>
<tr>
<td>Default Protections for Internet Explorer</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Password protect the screen saver</td>
<td>Not Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Local Policy</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Admin Approval Mode for the Built-in Administrator account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Protections for Software</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Only elevate UIAccess applications that are installed in secure locations</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Default Protections for Popular Software</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Apply UAC restrictions to local accounts on network logons</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode</td>
<td>Prompt for consent for non-Windows binaries</td>
<td>Prompt for consent on the secure desktop</td>
</tr>
<tr>
<td>User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Local Policy</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Virtualize file and registry write failures to per-user locations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Account Control: Switch to the secure desktop when prompting for elevation</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Run all administrators in Admin Approval Mode</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>WDigest Authentication</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>User Account Control: Behavior of the elevation prompt for standard users</td>
<td>Prompt for credentials</td>
<td>Automatically deny elevation requests</td>
</tr>
<tr>
<td>System ASLR</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>System DEP</td>
<td>Enabled: Application Opt-Out</td>
<td>Enabled</td>
</tr>
<tr>
<td>System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable screen saver</td>
<td>Not Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Force specific screen saver</td>
<td>Not Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Increase a process working set</td>
<td>Users</td>
<td>Not Defined</td>
</tr>
<tr>
<td>User Account Control: Detect application installations and prompt for elevation</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>System SEHOP</td>
<td>Enabled: Application Opt-Out</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network Security: Configure encryption types allowed for Kerberos</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Set client connection encryption level</td>
<td>Not configured</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Microsoft network client: Digitally sign communications (if server agrees)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Domain controller: LDAP server signing requirements</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network security: LDAP client signing requirements</td>
<td>Negotiate signing</td>
<td>Negotiate signing</td>
</tr>
<tr>
<td>Microsoft network client: Digitally sign communications (always)</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (always)</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Setting Name</td>
<td>Default Value</td>
<td>Compliance</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Domain member: Digitally sign secure channel data (when possible)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Domain member: Digitally encrypt or sign secure channel data (always)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (if client agrees)</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Domain member: Digitally encrypt secure channel data (when possible)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Specify the maximum log file size (KB)</td>
<td>20480 KB</td>
<td>Enabled</td>
</tr>
<tr>
<td>Specify the maximum log file size (KB)</td>
<td>20480 KB</td>
<td>Enabled</td>
</tr>
<tr>
<td>Specify the maximum log file size (KB)</td>
<td>20480 KB</td>
<td>Enabled</td>
</tr>
<tr>
<td>Audit: Shut down system immediately if unable to log security audits</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Accounts: Limit local account use of blank passwords to console logon only</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Domain controller: Refuse machine account password changes</td>
<td>Not defined</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Domain member: Disable machine account password changes</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Domain member: Maximum machine account password age</td>
<td>30 days</td>
<td>30 day(s)</td>
</tr>
<tr>
<td>Network access: Do not allow storage of passwords and credentials for network authentication</td>
<td>Disabled</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>
The following table lists the IIS settings with their corresponding default and possible values.

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Default Value</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive logon: Prompt user to change password before expiration</td>
<td>14 days</td>
<td>14 day(s)</td>
</tr>
<tr>
<td>Allow indexing of encrypted files</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td>Accounts: Rename administrator account</td>
<td>Administrator</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Do not display network selection UI</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Microsoft accounts to be optional</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Accounts: Administrator account status</td>
<td>Enabled</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Accounts: Guest account status</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Accounts: Rename guest account</td>
<td>Guest</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Prevent enabling lock screen slide show</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Prevent enabling lock screen camera</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>IRC Ports</td>
<td>Not Defined</td>
<td>Disabled</td>
</tr>
<tr>
<td>Outgoing Email Port 25</td>
<td>Not Defined</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advanced Audit Policy Configuration</td>
<td>Success</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit Directory Service Access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Other Windows Hardening Considerations**

The following table lists the IIS settings with their corresponding default and possible values.
### Setting Name | Default Value | Supported Values
---|---|---
ASP.NET Application Custom Error | RemoteOnly | • **On**: The system displays custom errors to both remote systems and the local host.  
• **Off**: The system displays ASP.NET errors to both remote systems and the local host.  
• **RemoteOnly**: The system displays custom errors to the remote systems and ASP.NET errors to the local host.  

**Note**: You can use any of these options available without impacting the system functionality.  

<table>
<thead>
<tr>
<th>HTTPOnlyCookie</th>
<th>Off</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowUnlisted</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

**requestFiltering**  
File extensions blocked using `false` as the value for the `allowed` attribute:

- .asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinf, .licx, .resx, .resources, .mdb, .vsproj, .java, .jsl, .ldd, .ssdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules  
- .asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinf, .licx, .resx, .resources, .mdb, .vsproj, .java, .jsl, .ldb, .ssdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules

**Note**: Certain extensions, such as .exe, .htm and .dll, cannot be filtered in IIS.
INDEX

A
auditing 57
  viewing auditing policies 57

B
batch deployment 29

C
Cisco firewall configuration utility 38, 39, 43
  prerequisites 38
  troubleshooting 43
  verifying 39
Cisco network isolation utility 20, 21
  process 21
  working 20
Cisco SSL encryption utility 55, 56
  encrypting in standalone mode 56
  installing during setup 55
cti os c++/com toolkit 2

I
IPSec 9
  logging 9
  monitoring IPSec activity 9

N
network monitoring 10

P
per-user terminal services settings 66
  preventing 67, 70
  unauthorized changes to the installed product 70
  unauthorized connections to a pcAnywhere host 67

R
Remote desktop 66

S
security log 58
security wizard 14
  using 14
SQL server 2014 49
  automated hardening 49
  security hardening utility 49
SQL server hardening 47
  top hardening 47
support for IPSec 6
  in transport mode 6
  system monitoring 10

W
WMI service hardening 78