Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1) and 12.5(2)

First Published: 2020-03-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Change History

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

Change	See	Date
Added more security considerations and recommendations	RDP-TCP Connection Security	July, 2023
New section has been added for important considerations when running vulnerability scans and penetration tests	Vulnerability Scan and Penetration Test Considerations	September, 2022
Document updated to MR Release 12.5(2)	MR related changes in applicable sections.	July, 2022
Added Release number 12.5(2) to the title	Title	
Win2k Windows Hardening Updates	Cisco Unified Contact Center Enterprise Security Hardening for Windows Server Windows Server Hardening	
Initial Release of Document for Release 12.5(1)		

Change	See	Date
OpenJDK updates	Java Upgrades	March, 2021
	Upgrade Tomcat Utility	
Added the Firewall inbound rules that are disabled by default.	Windows Server Firewall	January, 2020
Added information for supported Content Security Policy directives	Other Security Considerations	
Updated Tomcat version	Upgrade Tomcat Utility Upgrade Tomcat	
Updated certificate information	Generate and Copy Third Party CA Signed Certificates	

About This Guide

This document describes security hardening configuration guidelines for Cisco Unified Intelligent Contact Management (Unified ICM) on Windows Server. 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 and Windows Server 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: https://www.cisco.com/cisco/web/psa/default.html.

Related documentation includes the documentation sets for 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 https://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.
- Documentation for Cisco Unified Communications Manager is accessible from: https://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 Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

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

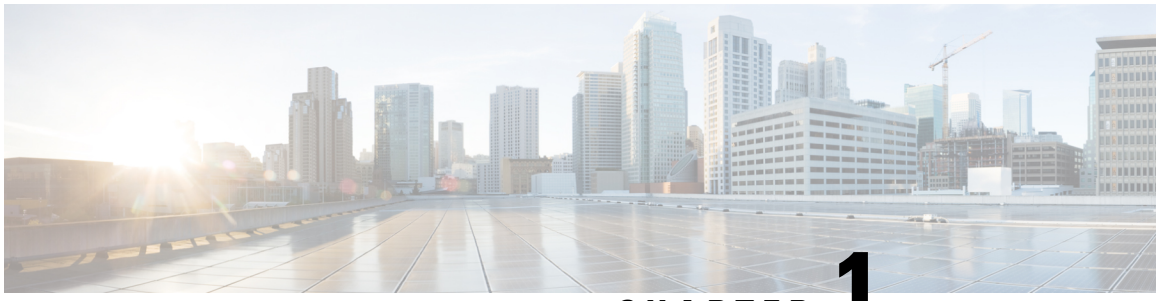
We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Your Security Strategy and Unified CCE

Security Evolves Constantly

The security landscape is ever evolving with threats emerging daily. The new threats bring increasing sophistication and innovative mechanisms with substantial potential impact on your business. A security strategy is a necessity that aids your business to protect the confidentiality, integrity, and the availability of your data and system resources.

This chapter discusses how the security architecture of the contact center enterprise products and the Cisco security process supports your security strategy. It also discusses the Collaboration Security Control Framework (SCF) which encapsulates our vision of a security strategy.

How We Support Your Security Strategy

We support your security strategy with synergies between security processes, technologies and tools, and security policies for compliance in your contact center enterprise solution. These directly derive from:

- Cisco's Product Security Requirements
- Market-based Security and Compliance Requirements
- Mandatory Regulations, Security, and Compliance Requirements
- Collaboration Security Control Framework

Your security adherence should incorporate the goals of the Collaboration Security Control Framework (SCF). The Cisco Secure Development Lifecycle (CSDL) processes aligns our development efforts with the SCF.

Related Topics

Our Secure Development Processes, on page 16

Collaboration Security Control Framework

The Collaboration Security Control Framework provides the design and implementation guidelines for building secure and reliable collaboration infrastructures. These infrastructures are resilient to both well-known and new forms of attacks. The SCF is a combination of a model, methodology, control structure, and control sets to support the assessment of technical risk in an infrastructure architecture. The SCF integrates into an ongoing process of continuous improvement. That process incrementally improves the security posture of the infrastructure architecture. These improvements address current key threats and identify, track, and defend against new and evolving threats.

The SCF defines security actions that help enforce the security policies and improve visibility and control. The SCF revolves around two security ideals, each with three supporting pillars:

- Total Visibility
  - Identify
  - Monitor
  - Correlate
- Complete Control
  - Harden
  - Isolate
  - Enforce

The SCF requires a foundation of architectural resiliency in the contact center enterprise solutions.

Security Architecture Principles

Cisco's Secure Development Lifecycle aligns with and, in some areas, leads the industry in creating highly secure solution architectures. Our Secure Coding Standards design the CSDL principles into every Unified CCE release. These standards work to prevent vulnerabilities from entering the product. They seek to eliminate undefined behaviors that can lead to unexpected program behavior and known exploitable vulnerabilities.

The Security Architecture Principles mandate that you deploy defensive measures against known security vulnerabilities. These measures include the following:

- Trust, but verify
- Securing weak entities and significant entities
- Mandatory platform hardening
- Fail safe and fail securely
- Defend in depth (Each entity verifies inputs.)
- Default is always "Least Privilege" unless approved explicitly

- Segregate privileges (Role separation and duty separation)
- Every entity is tri-party approved before entering the eco system (Ops, Release, and Security)
- Protection of PII data and any sensitive data, both at-rest and in-transmission
- Log all failures and all CRUD (Create, Read, Update, and Delete) actions and protect the logs

Unified CCE Solution Security Architecture

Our security architecture comprises multiple, layered security options and controls. You can deploy these security features to meet your individual security requirements. You can combine these features to achieve a robust security posture against attacks.

The contact center enterprise solutions include some servers that run on a Windows OS and others that run on the Linux-based Cisco Voice OS (VOS). The security architecture leverages the resources of the OS on which a particular server runs.

On a Windows OS, the Unified CCE servers leverage the Windows Firewall, Windows NT LAN Manager version 2 (NTLMv2), Windows Hardening Policies, and Active Directory. These servers include:

- The Router and Logger
- The Peripheral Gateway
- The Administration & Data Server
- Cisco Voice Portal
- Unified Contact Center Management Portal

The Cisco VOS platform is a closed, appliance-based model which runs within a Linux (shell) OS architecture. The servers that run on VOS include:

- Cisco Finesse
- Cisco Unified Intelligence Center
- Virtual Voice Browser
- Unified Communications Manager
- Cisco Unity Connection
- Cisco Identity Service
- Live Data
- Customer Collaboration Platform

This figure shows the core elements of a Unified CCE instance:

Application endpoints, like desktops and phones, involve Computer Telephony Interface (CTI), JTAPI, and any TAPI applications. These endpoints are secured by leveraging TLS and SRTP. The solution also uses a Certificate Trust List (CTL) which you create that establishes signaling authentication between Client and Server.

Network Security Architecture

The contact center enterprise solution offers a flexible network security model. There are many areas on the network where, based on your unique needs and compliance requirements, you can apply security to the solution. These include Firewalls, Access Control Lists (ACLs), private network addressing, Network Address Translation (NAT), setting up a DMZ, SRTP, and Internet Protocol Security (IPsec).

You can secure in-flight data by deploying IPsec. IPsec is an Internet layer 3 framework of open standards that are designed to ensure private, secure communications over Internet Protocol (IP) networks. The use of cryptographic security services and policies provides security. IPsec helps defend against:

- Network-based attacks from untrusted computers that can result in the denial-of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Network security attacks (IP Spoofing, DNS hijacking) against critical servers, other computers, and the network

You can deploy IPsec in two modes in your contact center enterprise solution. LAN or WAN network endpoints support either transport mode or tunnel mode deployments. Contact Center nodes (such as Peripheral Gateways, Routers, and Loggers) support only transport mode IPsec.

You secure voice traffic in your solution by applying encryption directly to the Real-Time Transport Protocol (RTP) which delivers audio and video streaming. RTP streams do not terminate within the core contact center enterprise solution. Adjunct devices, such as Unified CM and voice gateways, supply the media termination within the solution.

Secure Real-Time Transport Protocol (SRTP) is the method that secures the voice and video traffic.

Unified CCE web servers use Microsoft Internet Information Services (IIS) for web server responses and Apache Tomcat for the client authentication. Communication between Web servers and web-based users is trusted and encrypted using HTTPS and Transport Layer Security (TLS) protocols.

The servers that make up the contact center enterprise solution reside in a protected data center. They are not typically exposed to open internet traffic. These servers sit behind a firewall or DMZ. The only exceptions are Microsoft Active Directory Domain Controllers, Customer Collaboration Platform servers, and the Email and Chat web servers which reside inside a DMZ.

This guide focuses primarily on the premises-based deployment of our solutions. Cisco also offers cloud-based contact center applications, such as the Customer Journey Platform. We are thorough in ensuring compliance with international standards requirements for cloud data handling. Cisco has completed Binding Corporate Rules with the EU, the EU-US Privacy Shield, and the APEC agreements for cloud data handling and cross-border transfers. The Cisco Trust Center website provides details of these protections: https://www.cisco.com/c/en/us/about/trust-center.html.

The Goal of Total Visibility

The SCF model defines a structure of security objectives and supporting security actions to organize security controls. The SCF model is based on proven industry practices and security architecture principles. The model

grows from the accumulated practical experience of Cisco engineers in designing, implementing, assessing, and managing service provider, enterprise, and small and medium-sized business (SMB) infrastructures.

Using the SCF model, you gain an insight into the system's activities through total visibility objectives. The SCF mandates that the system knows the following:

- Who accesses the system
- What actions are performed
- Whom to inform about any anomalies, functional deviations, or suspicious activities

Key considerations for the goal of total visibility include the following:

- Identifying and classifying users, traffic, applications, protocols, and usage behavior
- Monitoring and recording activity and patterns
- Collecting and correlating data from multiple sources to identify trends and system-wide events
- Detecting and identifying anomalous traffic and threats

Identify Everything in the System

Contact center enterprise solutions leverage two common methods for user authentication and authorization. Unified CCE leverages NTLMv2 for Server-to-Server authentication. Administrative user accounts use Active Directory (AD) for authentication and authorization to perform tasks that are related to staging, deployment, and operations.

By default, Unified CCE agents authenticate through the Unified CCE configuration SQL database. You can optionally deploy Single Sign-On (SSO) to authenticate agents with a qualified Identity Provider (IdP). The IdP can be internal or external, but must provide SAMLv2 assertions for authentication. In an SSO deployment, the application's configuration database does not store user passwords. After authentication succeeds, Unified CCE supplies OAuth tokens through the Identity Service (IdS) for authorization to protected resources with its Identity Service (IdS).

Identify Your Users

Contact center enterprise solutions recognize these classes of users:

- Administrators
- Agents and supervisors
- API users

Contact center enterprise recognizes two subclasses of administrators: domain administrators and local administrators. AD holds all Administrator identity and authorization. You use domain administrator accounts for setup-related tasks that require Domain Administrative privileges, such as AD staging. You use local administrator accounts for tasks that only require local Administrative privileges in AD. Such tasks include binding to an AD root Organization Unit (OU) instance or accessing diagnostic tools.

Agents are the core users of the contact center enterprise solution. You create and authenticate agent accounts through the configuration database.

Supervisors need extra privileges for tasks such as reskilling agents and running reports. Because of this, you create supervisor accounts in AD.

Contact center enterprise solutions include several APIs for interfacing with third-party tools. All Unified CCE REST API calls are stateless (not session sticky), but are also authenticated calls through HTTPS. You define authorized API users during the initial system deployment.

Identify Your Devices

The Unified CCE solution contains devices that play a central role in user-related data management for authentication and authorization. These devices also provide the capability to perform a lightweight audit through the change control history.

The Unified CCE Administration and Data Server contains a copy of the Unified CCE configuration schema in a SQL database. This information provides a default (non-SSO) method of authenticating contact center agents. It also provides a mapping of privileges for system administrators to allow for least-privileged access control by using Unified CCE's Feature Control Set.

To support Single Sign-On (SSO) for agents and supervisors, the solution deploys Cisco Identity Service (IdS), a VOS-based appliance. The Cisco IdS has a trust relationship with the IdP and is responsible for internal OAuth token management across protected resources, such as Cisco Finesse and Cisco Unified Intelligence Center. If you enable SSO in your contact center, the relevant agent and supervisor authentication data reside in your IdP and not in the Unified CCE database.

The Unified CCE Logger contains a redundant, primary copy of the entire Unified CCE configuration. The Unified CCE Router uses a dynamic key generation method to synchronize and store all configuration transactions and their related history in the Logger database. The Unified CCE tools can leverage these configuration and recovery keys to track and revert changes in the Call Routing Script history and general Unified CCE configuration transactions.

Active Directory plays a central role in managing security policies across our core Windows-based Unified CCE components and in providing authentication for administrative users. User passwords that AD stores reside in the local Security Accounts Manager (SAM) database and are part of the Unicode Pwdattribute hash value. Windows generates this hash value as a product of the LAN Manager and Windows NT hash. Unified CCE accounts that you create for use with Web Setup and Web Administrator authenticate with an AD user account.

Identify Your Services and Applications

Unified CCE servers operate in a trusted Microsoft Active Directory domain. Before installing any Unified CCE components, you must first perform the required AD staging. You create a root OU (Organizational Unit) in the target AD domain where the Unified CCE servers reside. You can place the root OU, "Cisco_ICM," either at the domain root or nested within another OU. Do not nest the root OU more than one layer under the domain root. To create the root OU, you run Unified CCE's Domain Manager. Provide Domain Administrator rights or delegated (full control) rights to a sub-OU where our root OU is nested. Once the Domain Manager creates the root OU, you no longer require Domain Administrator rights for the rest of the installation.

After installing the core software, you run WebSetup to create the AD Service accounts required for the Unified CCE database services. WebSetup is hard-coded to create these accounts within the AD root OU by default. However, once this is complete, you can run our Service Account Manager (SAM) utility to map our DB services to pre-configured AD accounts. If you perform this custom mapping of our service account users, you can delete the default service accounts that Unified CCE WebSetup created.

Unified CCE web servers are configured for secure access (HTTPS). Cisco provides an application, SSL Encryption Utility (SSLUtil.exe), to help configure web servers for use with TLS. This utility simplifies the task of configuring TLS encryption by performing the following functions:

- SSL Configuration
- SSL Certificate Administration

The Cisco Unified Contact Center Security Wizard is a standalone server hardening deployment tool that simplifies your security configuration. You can do the following tasks in the Security Wizard:

- Define Windows Firewall policies
- Apply SQL Hardening
- Perform Network Isolation with IPsec

You may also use OS tools to perform these security tasks, such as, those found in IIS.

We qualify each software release to operate with specific versions of third-party anti-virus software. Ensure that your solution uses a qualified anti-virus software.

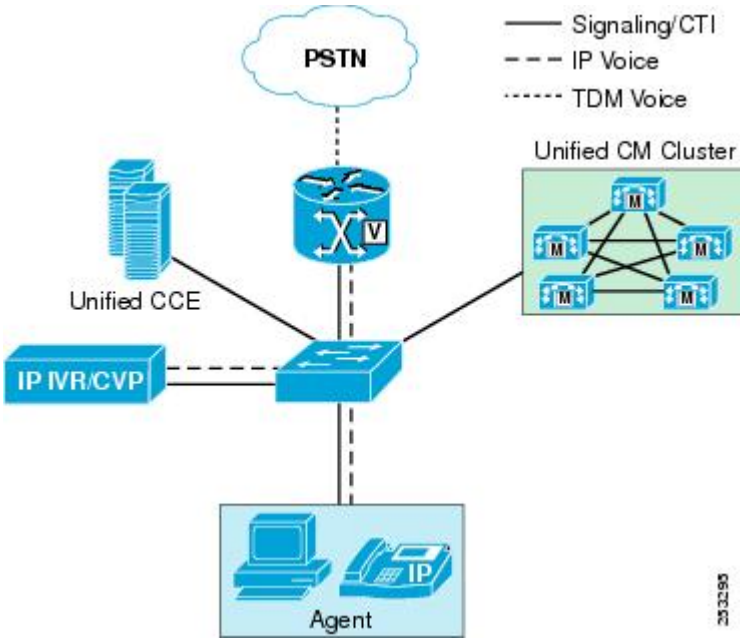
Monitor Everything in the System

Monitoring plays a vital role in effectively managing the operations which must cover all the critical components of the product architecture. Monitoring helps in detecting any security issues for analysis and mitigation as soon as possible based on their severity.

Security issues can come from network attacks, network breakages, application security attacks, and transaction failures which can result in a Denial of Services.

Monitor Your Network

You can monitor your contact center enterprise solution with the Unified Communications Manager Real-Time Monitoring Tool (RTMT). RTMT collects diagnostic information and also gathers platform and application configuration data. RTMT provides an administrative interface for collecting health and status information and requests for all devices in its network topology. By configuring RTMT, you can then use other security tools to analyze its data for security issues, like network-based attacks (Slow-TCP attacks, "Slowloris," or packet bombardment such as "ping of death"). This figure shows the solution components that RTMT monitors for their network interactions.



Contact center enterprise solutions capture specific network events. They report abnormalities in network requests. Each component checks for the heartbeat of the other components with which it interfaces. Our solutions can track these network events:

- Host not reachable
- TCP Timeouts
- Excessive Response Delays

Your contact center enterprise solution has built-in capabilities to aid reporting on network abnormalities and to integrate with third-party security intelligence tools:

- Real-time performance monitoring of contact center devices
- Device inventory management and discovery
- Prebuilt and custom Threshold, Syslog, Correlation, and System Rules
- Link status, device status, device performance, device 360
- Event alert generation in the form of email messages, for user-configured thresholds
- Trace collection and viewing in default viewers that exist in RTMT

Your security strategy should include security intelligence tools that can integrate with the contact center enterprise solution and analyze this data. You can find third-party tools to fill this role. Cisco also has its own security intelligence tools:

Cisco AMP

https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Cisco AMP (Advanced Malware Protection) provides global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches. But, you can't rely on prevention alone. AMP also

continuously analyzes the file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Cisco Stealthwatch

https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

Cisco Stealthwatch uses industry-leading machine learning and behavioral modeling to help identify and respond quickly to emerging threats. You can monitor your network to see who is on, and what they are doing using the telemetry from your network infrastructure. This capability helps protect your critical data with smarter network segmentation.

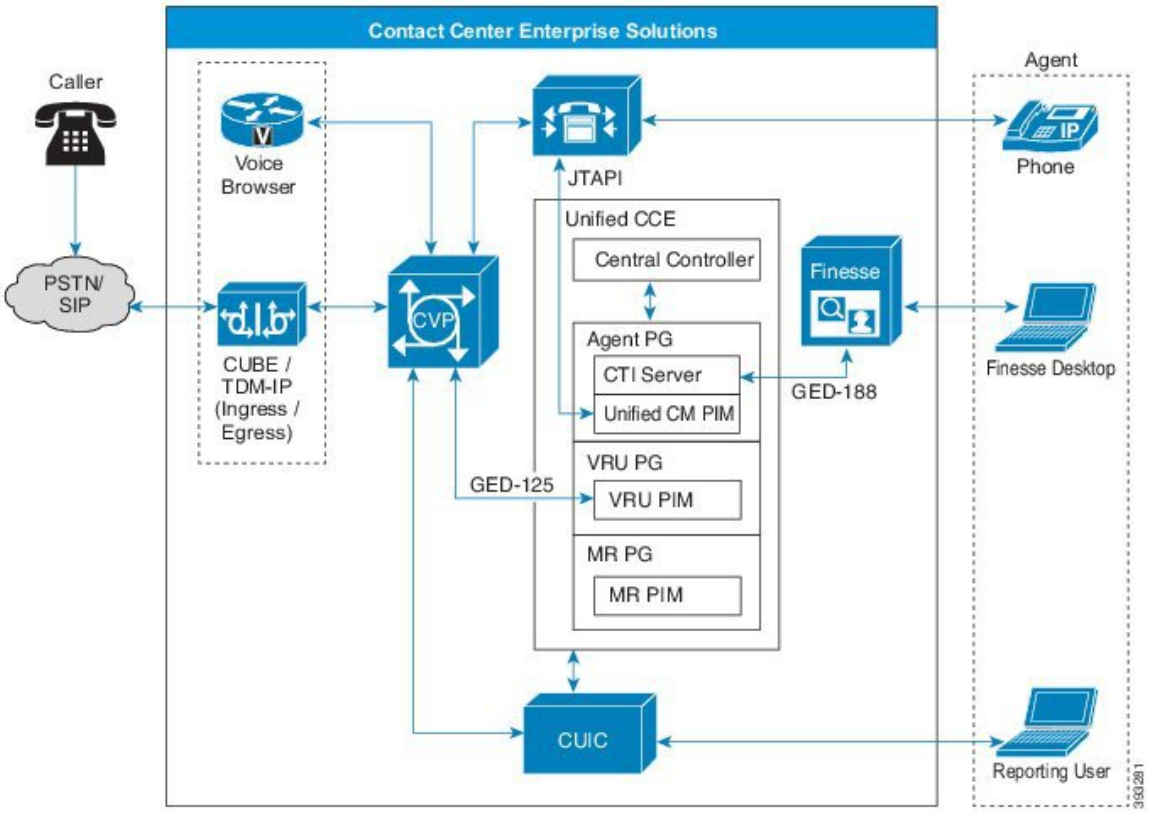
Cisco Prime Assurance

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

Cisco Prime Assurance provides automated accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics for Cisco installations.

Monitor Your Data

The components in contact center enterprise solutions communicate with other components as part of their business transaction orchestration. The components monitor major data transmission for the segments that this figure shows.



Incoming Calls

Unified CCE receives calls in two primary ways. Inbound calls can come through a PSTN or an IP-based SIP trunk that uses VoIP technology to stream media services to a telephony endpoint. In both cases, the physical media traverses between the ingress carrier, voice gateways, and Unified CM media termination endpoints. The physical media stream does not terminate within the core Unified CCE components. But, Unified CCE and Unified CVP provide critical real-time signaling for call treatment and handling.

The contact center enterprise solution includes security features that are designed to actively detect and prevent inbound call attacks that are related to:

- Toll Fraud
- Telephony Denial of Service (TDoS)

Toll fraud is the illicit use of a telephony system to make long-distance (international) calls without any accountability. To prevent toll fraud in a Cisco Collaboration network, you can employ various tools:

- Unified Communications Manager class of service (CoS)
- Voice gateway toll fraud prevention applications
- Voice gateway class of restriction (CoR)
- Cisco Unity Connection restriction rules

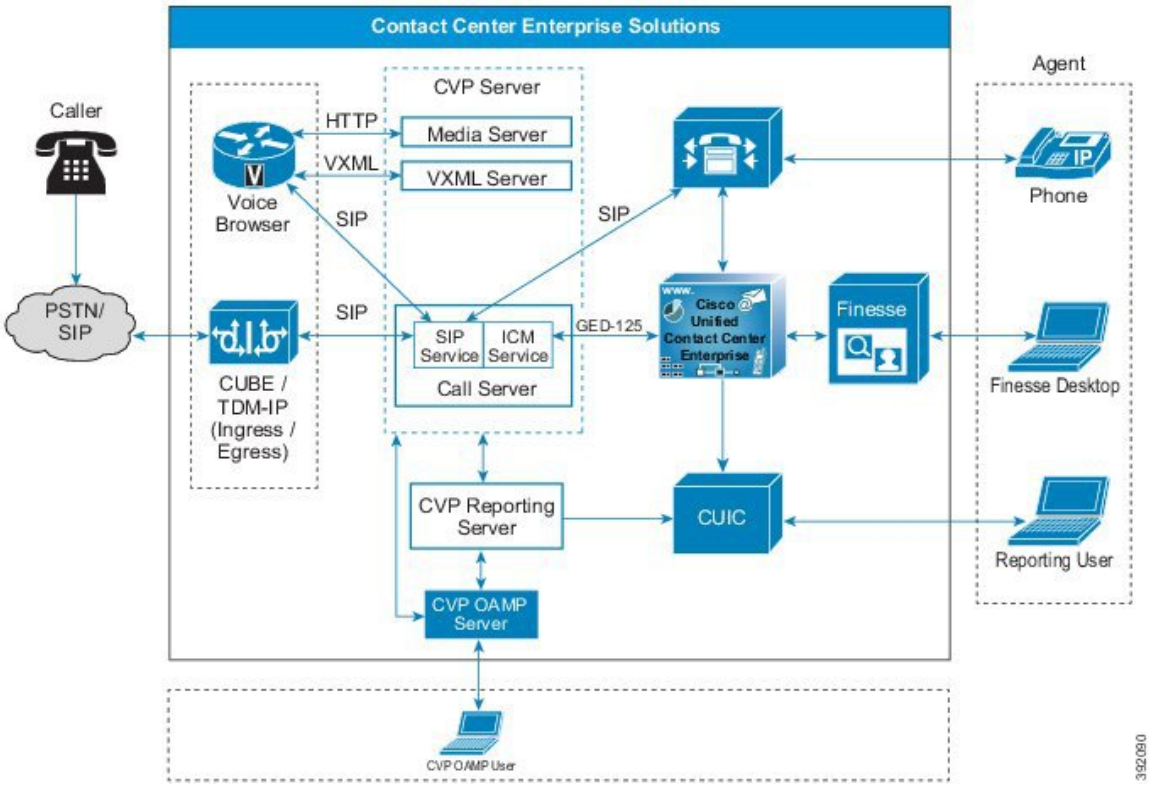
TDoS attacks generally follow the same model as a data network Denial of Service (DoS). Unauthorized users flood the system with too many access requests and prevent legitimate users from accessing the system. Unified CCE comes equipped with a congestion control capability. You can use Congestion Control to monitor the Calls Per Second (CPS) patterns for incoming calls and to alert and protect the contact center from TDoS attacks.

Business Transactions

These are some of the business transactions for which our solution captures data and monitors for diagnostic data and any failure:

- **Routing control**—Messages that enable a Unified CM cluster to request routing instructions
- **Device and call monitoring**—Messages that enable a cluster to notify Unified CCE of state changes
- **Device and call control**—Messages that enable a Unified CM cluster to receive instructions from Unified CCE

Figure 1: Unified CCE Business Transactions (Call Flows between Components)



Record What You Monitor

Most application logging frameworks focus on identifying technical faults as they occur. The Unified CCE solution supplies both platform and process logging capabilities through a combination of a custom Diagnostic Framework API and industry-standard SNMP and Syslog protocols.

Security auditing requires a more tightly integrated method that blends reactive logging with proactive tools and analysis to prevent possible system health-impacting issues from occurring. Our solutions have built-in auditing features capable of the following:

- Cradle-to-grave call reporting
- Detailed agent reporting through Unified Intelligence Center and an open database schema
- Audit trails for blended task routing between agents and customers
- Open database schema support that enables the tracking of administrative changes by leveraging the t_Event and the Recovery tables
- RTMT for automated alerting

Syslog and the central repository service log business transactions and other data transmissions. Unified Intelligence Center provides reporting and analysis capabilities for auditing.

RTMT sends alerts for any configured violations (incidents) as an email message. It also specifically configures system critical violations (incidents) with SNMP Traps. RTMT can report on the following types of events:

- Device Inventory Management
- Voice and Video Endpoint Monitoring
- Diagnostics
- Fault Management
- Real-time performance monitoring of contact center devices
- Events and Alarms along with a root cause analysis
- Contact Center device dashboards—Prebuilt and custom
- Threshold, Syslog, Correlation, and System Rules—Prebuilt and custom
- Multi-tenancy and logged-in agent licensing information

Correlate Everything in the System

Applying context and meaning to information security requires the correlation of recorded events, incidents, and failures from the application logging and auditing. Correlation adds critical information value by evaluating the relationships between various information silos. Unified CCE can correlate real-time and historical events within the solution to increase the value of your security information.

The correlation of events, incidents, and failures helps to identify, understand, and troubleshoot system failures and issues. The correlation is more effective than finding individual root causes in an isolated manner.

Make Use of Alerts and Notifications

Alerts, notifications, and alarms are a system capability that notifies system administrators of an event. The system can take corrective or preventive actions based on these alerts to ensure smooth business operations. The solution enables you to track significant events, such as, account sign-in attempts.

Some of the alert capabilities available in contact center enterprise solutions are:

- The SNMP Event Translator facility converts Windows events, in real time, into an SNMP trap.
- Microsoft SQL server includes events capturing and reporting through its new audit capabilities. See Microsoft documentation for details.

Note Cisco does not support C2 event capturing for audits in Microsoft SQL Server in contact center enterprise solutions due to degradation in transaction performance.

- The alerting mechanism of the event log monitoring system is a crucial part of AD design. This mechanism helps channel an administrator's attention toward any undesirable incidents to ensure AD security is not compromised.

  For more information on AD security monitoring and alerts, see https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise.

- Contact center enterprise solutions allow remote administration of the Unified CCE server with Windows Remote Desktop. The solution logs all security events for such administration activities. The centralized logging features in Windows Remote Desktop enable you to log events with Windows Server Event Log or an SNMP event monitor.

  For more details on how Unified CCE solutions capture system events, refer to the auditing chapter in this guide.

Related Topics

Auditing , on page 89

Correlate Events with Security Incidents

Any business event can become an incident. Your business must also classify some system events as an incident by default. Address corrective and preventive actions for those events in your Operations Run Book or Standard Operational Procedures. Contact center enterprise defines the following business events as incidents which require administrative notifications and corrective actions.

- Host not reachable
- TCP Timeouts
- Excessive Response Delays
- Unknown Link status
- Unknown device status
- Device & call control & monitoring message failures
- Routing control message failures

Our solutions provide alert and notification capabilities for these incidents. They send information of such critical failures to administrators for predefined corrective actions.

For more details, refer to the chapter on auditing in this guide.

Related Topics

Auditing , on page 89

The Goal of Complete Control

The Collaboration Security Control Framework mandates system resiliency through its complete control objective. The SCF provides enough parameters to make the system secure and resilient by default, reducing known security vulnerabilities.

Harden What You Can

Hardening is the process of closing off avenues for potential attacks by changing default settings in hardware and software.

Systems Hardening

All systems come with a set of default resources enabled. The objective of systems hardening is to disable the unused resources on a system and only enable what your business needs require. System hardening applies for operating systems, webservers, application servers, database servers, middleware, firewalls, routers, and the hardware that runs them – irrespective of vendors and manufacturers.

For more information, see the sections on hardening and compliance in this guide.

Contact center enterprise solutions require hardening procedures. Our system hardening procedures and guidelines are based on multiple industry standards, such as, the Center for Internet Security, NIST Security standard SP-800-123, and others. We mandate systems hardening for all product deployments as part of your organizational security policies and practices.

OS Hardening

OS hardening makes an operating system more secure by removing or disabling unwanted services, applications, and ports that the OS includes by default. Hardening properly sets the correct and relevant permissions and privileges on applications, the file system, and network settings. It also deletes unused files and applies the latest patches.

Database Hardening

Database hardening follows the principle of least privilege. It restricts user access by locking down functions that your users do not require and might misuse. Database hardening also includes segregation of privileges and access restrictions to different schemas and tables for the correct and relevant users only. Applying database hardening principles ensures greater security through "Role Separation Privileges" for the Systems Administrator and Database Administrators.

Firewall Hardening

A firewall defines the perimeter-level security for your enterprise or your internal infrastructure. Firewalls are one of the first defense mechanisms for a network or for a host to protect its services and applications.

Following industry-standard firewall hardening principles is critical to your security strategy.

For more information, see the *Cisco Firewall Best Practices Guide* at https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html.

Server Hardening

Server or infrastructure hardening applies the appropriate security to each network component, including Web servers, Application servers, and any other applications or services. Server hardening starts with a security survey to model the threats that may impact your product or site. Identify all aspects of your environment (such as components in the Web tier) that could be insecure. Before deploying the product or service, remove any known weaknesses through configuration changes.

For more information, see the Center for Internet Security site (https://www.cisecurity.org/cis-benchmarks/).

Middleware, Other Software, and Hardware Hardening

SNMP provides a simple architecture with a wealth of information on the health of network devices. However, SNMP offers little security, because it relies on a community string to protect data exchanged between two computers. This community string is in clear text, which effectively voids many security measures. Properly secure SNMP to protect the confidentiality, integrity, and availability of both the network data and the network devices.

For more information, see the following sources:

- The section on fortifying SNMP in *Cisco Guide to Harden Cisco IOS Devices* at https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc54
- *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

AD hardening requires a complete investigation of who has elevated privileges throughout a Microsoft Windows environment. You can then reconfigure these settings to ensure that all users have the appropriate access. This is a multistep, yet straightforward process which covers the following:

- Local users and groups
- AD Users
- AD groups User Rights
- AD Delegation
- Group Policy Delegation
- Password management
- Auditing and monitoring of AD
- Service Accounts

For more information, see the Microsoft TechNet article on securing AD at https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160982(v=msdn.10).

Related Topics

SQL Server Hardening, on page 67
Windows Security Hardening, on page 115

Isolate What You Can

The focus of isolation is to add extra controls that limit the scope of attacks and vulnerabilities. Isolation minimizes their impact on users, services, and systems. By creating logical and physical security zones, you can prevent access between the functional blocks in the infrastructure. This method limits the scope of a security breech exploitation.

Systems and Architecture Isolation

Contact center enterprise solutions follow a defense-in-depth approach. This approach functionally segments all major components and segments the firewalls for a tiered, functional security management.

User Segmentation

Contact center enterprise classifies its users as administrators, supervisors, and agents. Each role has specific allocated tasks. Agents and administrators are separated through their sign-in capabilities, any applied location restrictions, and other functional restrictions to agents. Supervisors and administrators can sign in from any terminal or application to monitor and manage the systems.

Application Isolation

Contact center enterprise isolates applications based on their functional role. Firewall segmentation secures the applications and enables the applications so that only relevant components can connect to them.

The system administrators use NAT-enabled sign-in credentials to manage these individual components remotely with SSH terminals or secure remote screen sharing protocols on Windows. Such isolation minimizes the risk of an attack spawning further to other system functions.

Enforce What You Can

The SCF's main focus is on enhancing visibility and control. The success of your security policies ultimately depends on the degree that they enhance visibility and control. Smart enterprises take a measured approach to policy enforcement, using a combination of policy awareness, discreet monitoring, and enforcement, which includes:

- Identifying and communicating risk—What's the problem?
- Creating an accepted policy and guidance infrastructure—What do we expect accountable parties to do?
- Developing processes to monitor the conformance with a policy—How do we know that we are successful?
- Preparing response capabilities for when the controls fail—If there is a breach, who does what to mitigate it?

Effective governance is directly connected to the consequences of inaction. Policies set expectations and assign accountability. They comply with legal, regulatory, and technical security requirements, spelling out what they do and don't permit. The policies define how management governs and provide direction to their security strategy and architecture.

Cisco enforces its internal security policies and procedures, such as CSDL, on the contact center enterprise products by default from its development to its deployment and operations.

Our Secure Development Processes

Cisco's Security and Trust Engineering group advocates and accelerates trustworthy processes, policies, and technology across Cisco's products and solutions through the following:

- Cisco Secure Development Lifecycle (CSDL)
- Cisco Security Engagement Managers
- Cisco Security Advocate Program
- Cisco Advanced Security Initiatives Group (ASIG)

These processes, groups, and specialists evaluate Cisco products and services to identify security vulnerabilities and weaknesses. Together they produce mitigation and improvement plans and perform security analysis on Cisco products and services on continuous improvement cycles. They also define secure development requirements and tools to support CSDL.

CSDL ensures a consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software. CSDL conforms to guidelines of ISO 27034, "Information Technology – Security Techniques – Application Security". Enforcement and mandatory implementation of

CSDL is part of Cisco's ISO compliance process. Since 2013, Cisco has used ISO/IEC 27034–1 as a baseline to evaluate CSDL. All current mandatory application-security-related policies, standards, and procedures along with their supporting people, processes, and tools meet or exceed the guidance in ISO/IEC 27034–1 as published in 2011.

For more information, see the section on CSDL at https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html.

Cisco's internal security policies ensure that we harden our release staging environments and FCS sandbox environments identically to production deployment security standards and procedures.

Cisco enforces auto-hardening scripts and hardened images of its software stack such as web servers, application servers, database servers, middleware software, and operating systems. This hardening helps speed up deployment and avoids chances of a human error in hardening systems.

Our internal deployments for release testing and FCS testing must clear all the security scanning tools that are deployed within the development cycle.

Our Deployment and Operations Security Processes

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information for Cisco products and networks.

Cisco PSIRT works 24 hours a day, 7 days a week with Cisco customers, Cisco engineering and support, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks.

PSIRT announcements are available on *Cisco Security Advisories & Alerts* at https://tools.cisco.com/security/center/publicationListing.x.

Our Compliance, Data Security, and Privacy Processes

Cisco internal security processes mandate that security compliance is part of our product and services design. Contact center enterprise solutions follow these processes.

Our internal security and compliance processes are rigorous. Since our offerings contain third-party software components, our solution iterates through technical, legal, and supply-chain security verification processes to ensure security is not compromised. These processes are integral to our product development lifecycle and act as an entry criteria for release.

However, our built-in security covers only part of a comprehensive security strategy. Add your own procedures to ensure compliance with the applicable security, business, and local security requirements while designing your solution's security strategy.

Security Standards, Practices, and Compliance

We define *Product Security Requirements* for our products as a release criterion. We compile these requirements from internal and external sources, based on known risks, customer expectations, and industry practices. Each industry and region has its own unique requirements.

We strive to build products that aid you in complying with these security and privacy requirements. We prioritize those requirements that are common across multiple regions and organizations. Our security

requirements for contact center enterprise solutions reflect the requirements of the standards for the applicable industries:

- The General Data Protection Regulation (EU Regulation 2016/679) PII Data Protection (European Union Personally Identifiable Information)
- The United States Sarbanes-Oxley Act
- The United States Health Insurance Portability and Accountability Act (HIPPA)
- ISO27001
- Common Criteria for Information Technology Security Evaluation
- United States government certifications and standards:
  - National Institute of Standards and Technology (NIST) SP 800 Series
  - Federal Information Security Management Act (FISMA)
- Other market-demand-based security and compliance requirements:
  - SysAdmin, Audit, Network, Security (SANS) Top 20
  - Open Web Application Security Project (OWASP) Top 10
  - Payment Card Industry Data Security Standard (PCI DSS)

Because standards and requirements often overlap, we produce common compliance sheets to help you verify that our products meet your requirements. For an example of these compliance sheets, see the *Simplified Crosswalk—HIPAA, PCI, and SOX* at https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/HIPAA/default/HIP_AppD.html.

Data Security and Privacy

Data security and privacy is of the utmost priority in your contact center. Contact center enterprise products enforce data classification standards and policies to secure the identified sensitive data, including Personally Identifiable Information (PII), within your contact center solution.

Organizations generally choose to not store PII or credit card data on any local system unless necessary. The Unified CCE solution uses Extended Call Context (ECC) variables for PII data within the call script applications. Unified CCE does not write these variables to the historical database or otherwise stored.

If an audio recording is part of your Customer Care policy, do not record credit card information. Many organizations choose to have the agent pause the recording when the credit card information is spoken. Others look to a more automated method using desktop analytics or an integration with third-party applications that provide an automatic pause and resume functionality. If the path to the data source traverses “open, public networks,” like the Internet, ensure that you encrypt the data while in transit.

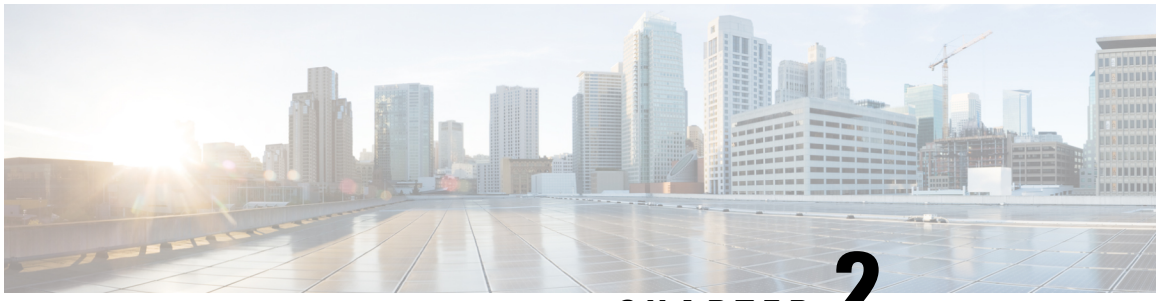
Security for PII and Other Sensitive Data

Contact center enterprise products use Cisco’s internal definition of sensitive personal information. We base that definition on multiple security requirements.

Contact center enterprise products internally use secure channels to communicate sensitive information such as user-ids, passwords, session information, and PII. When connecting to any third-party application services, connecting over secure protocols for data communications is mandatory.

PII includes the following:

- Contact information (name, email, phone, postal)
- Forms of identification (SSN, Driver's License, Passport, Fingerprints)
- Demographic info (age, gender)
- Occupational Info (Job title, Company name, Industry, Employee email, phone, pager)
- Health care info (Plans, providers, history, insurance, genetic info)
- Financial info (Bank, credit, and debit card account numbers, purchase history, credit records)
- Online activity (IP Address, cookies, flash cookies, sign-in credentials.)
- Data that permits access to a customer's account (Password, Personal Identification Number)
- Telecommunications and traffic data (Call details records, internet traffic, invoicing, call histories)
- Customer's real-time location
- Credit card numbers and bank account information
- Government-issued identifiers such as Social Security Number and Driver's License
- Data that could be used to discriminate (such as, race, ethnic origin, religions or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle, physical or mental health)
- Data that could be used to facilitate identity theft (such as mother's maiden name)



CHAPTER 2

Encryption Support

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

Call context variables in Unified CCE may contain sensitive data depending on how it is configured and scripted in your system Peripheral. Variables between 1 to10 are stored in the Termination Call Detail records, and the Expanded Call Context (ECC) variables are stored in the Termination Call Variable and Router Call Variable records on the Historical Data Server (HDS), if the **Persistent** check box is checked.

These variables are neither encrypted in the memory nor when they are stored in the database. Therefore, be cautious about the data you store in these variables. These variables are typically used for diagnostics and custom reporting only.

Unified CCE has strategies for encrypting the variables during transport and encrypting the drive where they are stored.

For more information, see About IPsec, on page 25 and Manage Secured PII in Transit, on page 77.

Internet Script Editor

Note If you use Unified Contact Center Management Portal (Unified CCMP) or Unified Contact Center Domain Manager (Unified CCDM), you cannot use Transport Layer Security (TLS) v1.0 for Internet Script Editor.

The Internet Script Editor web application uses the TLS v1.2 protocol only which provides encryption using a cipher that the endpoints negotiate. 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

Unified CCE Certificate Management Utilities, on page 73

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-256 digest algorithms. For all SNMP message encryption, our implementation uses one of the following protocols:

- AES-192
- AES-256

For more information, see the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

TLS Encryption Support

External interfaces such as data center interfaces and external components such as Cisco Finesse, Customer Collaboration Platform, CVP, and Application Gateways support encryption using TLS.

Supported Ciphers

The following AES ciphers are used for encryption:

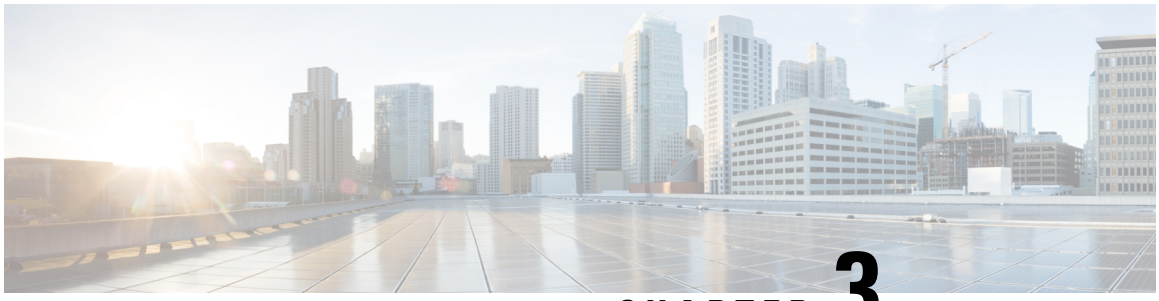
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES128-SHA
- AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA256

Cipher Suite Management

You can add or remove the supported ciphers from the following registries for the server and client respectively:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL
Configuration\ServerCiphers
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL
Configuration\ClientCiphers
```



CHAPTER 3

IPsec and NAT Support

About IPsec

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

For more information, see https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

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 negligible impacts on performance with no impact on call processing rates. :

Related Topics

IPsec with Network Isolation Utility

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:

- AES 128
- AES 256

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.

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.
- If you intend to customize the IPsec policy, you can modify the IPsec setting and customize it. For more information, see the Microsoft Documentation on Configure Data Protection (Quick Mode) Setting.

6. Key Exchange Security Method - IKE Security Algorithms (Defaults)
   - Integrity algorithm: SHA1
   - Encryption algorithm: 3DES
   - Diffie-Hellman group: Medium (DH Group 2, 1024-bit key)

Note

- For enhanced security, 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 **`Regedt32`** 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`.

Message Analyzer

Message Analyzer enables you to capture, display, and analyze protocol messaging traffic; and to trace and assess system events and other messages from Windows components.

For more information on Message Analyzer, see Microsoft Documentation.

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 usual 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 usual 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.

For more detailed resources on how to configure NAT, see https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml.

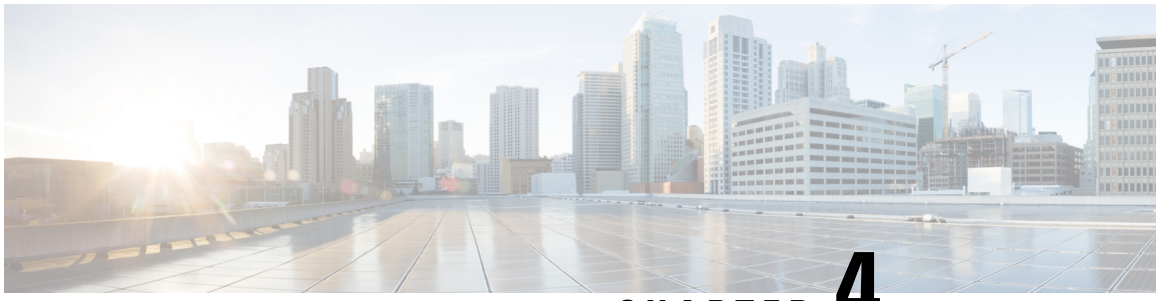
For more details on how to deploy IP Phones across NAT, see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf.

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). If both VPN devices are NAT-T capable, then NAT-T is autodetected and autonegotiated.

Other IPsec References

- IPsec Architecture: https://technet.microsoft.com/en-us/library/bb726946.aspx
- See Microsoft documentation for details on Windows Server.
- Windows Firewall and IPsec: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security



CHAPTER 4

Unified Contact Center Security Wizard

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 69
IPsec with Network Isolation Utility , on page 39
Window Server Firewall Configuration, on page 57

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 runs on all Unified ICM or Unified CCE servers, but does not run on a Domain Controller.

Related Topics

IPsec with Network Isolation Utility

Window Server Firewall Configuration, on page 57

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.

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

- Disable the Windows firewall.

Note You cannot disable the firewall using the security wizard when the Windows server hardening is applied. See Windows Server Hardening. This is because when the hardening is applied, if you try to disable the firewall, it will be re-enabled.

- 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 run *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.

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.

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

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.

Note The SQL hardening wizard can be used on SQL Server 2019 only after applying the mandatory 12.6(1) ES for Windows and SQL Server 2019 support.

In the SQL Hardening Security Action panel, you can:

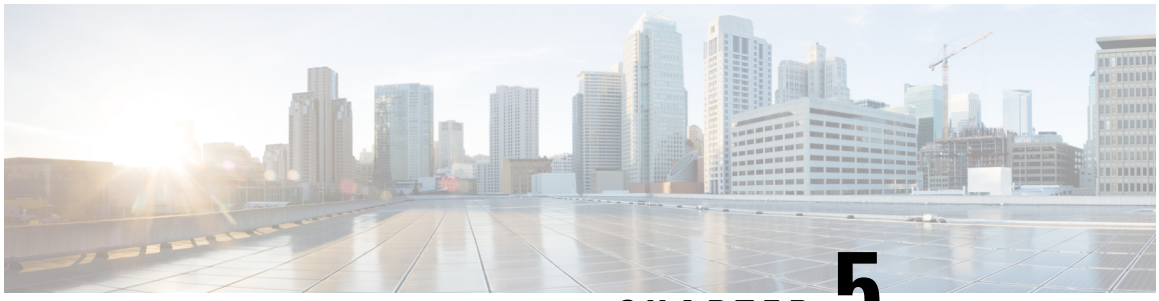
- Apply or Upgrade SQL Server Security Hardening
- Roll back Previously Applied SQL Server Security Hardening

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 69



CHAPTER 5

IPsec with Network Isolation Utility

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.

For more information, see https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

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

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

https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

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:
   a. **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.

   b. **Boundary Devices Rule**

      This rule involves the following items:

      - **Boundary Devices Filter List:** (empty by default)

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

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

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

5. The Network Isolation Utility logs all commands and actions in a log file at: `<SystemDrive>:\CiscoUtils\NetworkIsolation\Logs\CiscoICMNetworkIsolation.log`.

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

Traffic Encryption and Network Isolation Policies

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

Note

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

Related Topics

About IPsec, on page 25
IPsec and NAT Support, on page 25

Network Isolation Feature Deployment

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

Related Topics

Boundary Devices and Unified CCE, on page 46
Device Two-Way Communication, on page 45
Important Deployment Tips, on page 42
Sample Deployment, on page 43

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

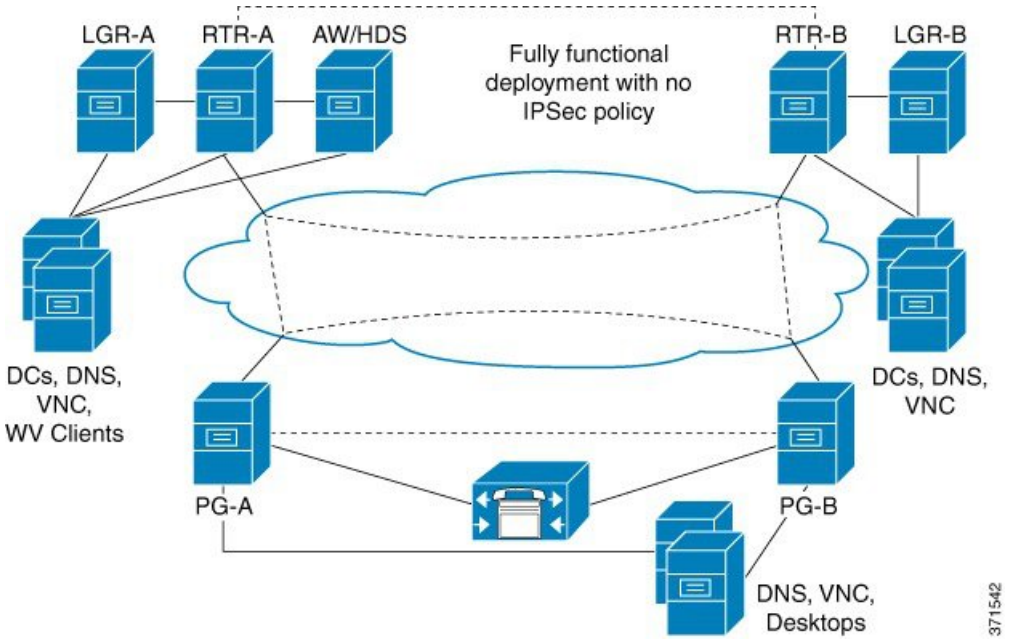
Caveats, on page 47

Sample Deployment

The following is one sample deployment.

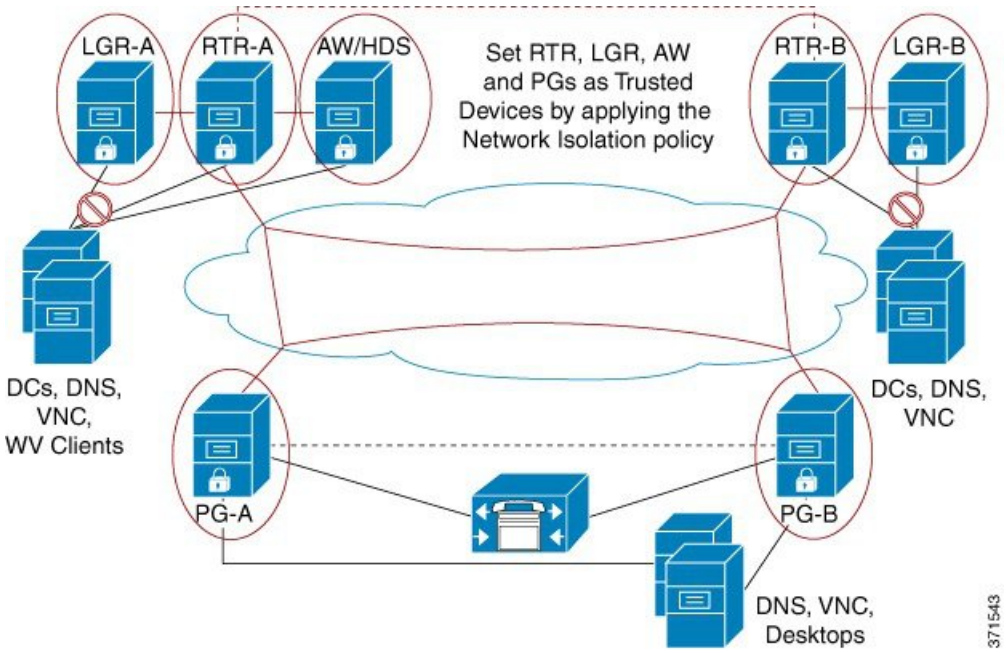
1. Start with a fully functional Unified ICM or Unified CCE system that has no IPsec policy deployment.

Figure 2: Example Unified Contact Center System



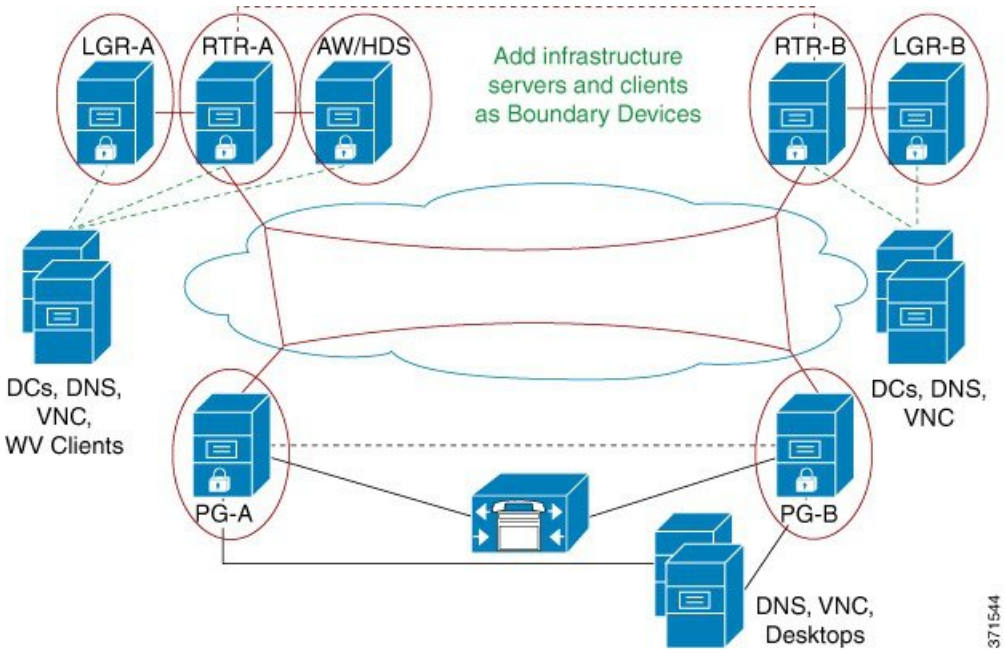
2. Set the CallRouter, the Logger, the Administration & Data Server, and the PGs as Trusted Devices by running the Network Isolation Utility on each of them.

Figure 3: Example: Add Trusted Devices



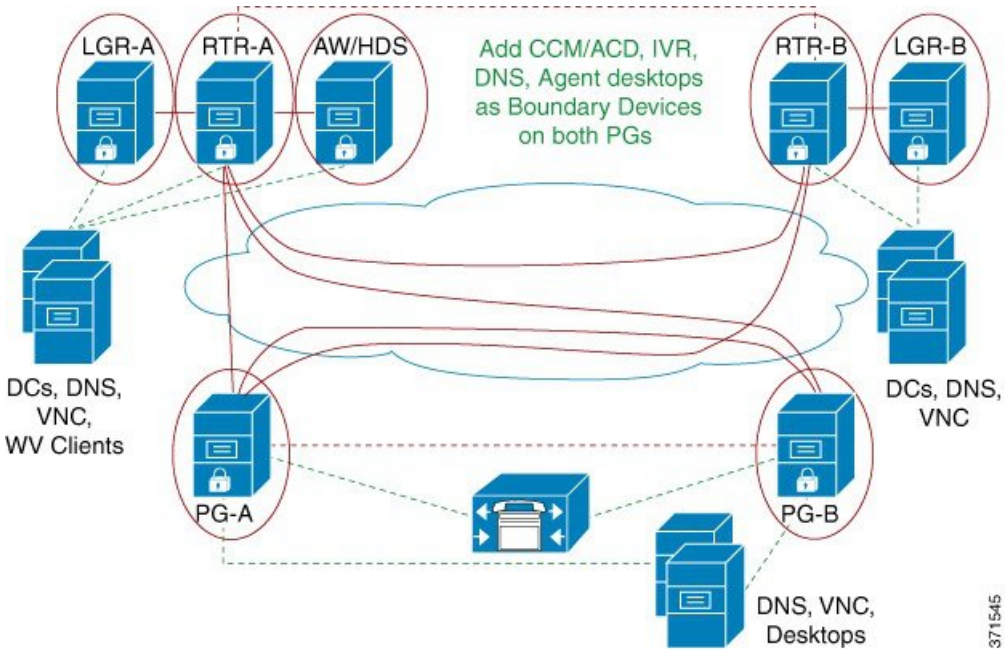
3. Add the infrastructure servers and clients as Boundary Devices.

Figure 4: Example: Add Boundary Devices



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

Figure 5: Example: Add Boundary Devices on 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.

Unified CCE component	Target Devices
CallRouter	CallRouter (on the other side in a redundant system)
	Logger
	Administration & Data Server/Historical Database Server
	NAM Router
	Peripheral Gateway (on both sides in a redundant system)
	Application Gateway
	Database Server
	Network Gateway

Unified CCE component	Target Devices
Logger	Historical Database Server/Administration & Data Server
	CallRouter
	Campaign Manager
	Dialer
Peripheral Gateway	Multichannel/Multimedia Server
	CallRouter (on both sides in a redundant system)
	Peripheral Gateway (on the other side in a redundant system)
	Unified Communications Manager
	Administration & Data Server legacy PIMS/switches
Administration & Data Server/Historical Database Server	Multichannel/Multimedia Server
	Router
	Logger
	Custom Application Server
	CON API Clients
	Internet Script Editor Clients/Webskilling
	Third-Party Clients/SQL party
Administration Server, Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS)	Multichannel/Multimedia Server
	Router
	Logger
	Custom Application Server
	Internet Script Editor Clients/Webskilling
	Third-Party Clients/SOL party

Boundary Devices and Unified CCE

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

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

Caveats

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

Caveats include the following:

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

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

- Adding a new device as a Boundary Device requires a change to the policy on all Trusted Devices that need access to this new device without IPsec.
- A change in the Preshared Key must be invoked on all Trusted Devices.
- If you enable encryption on only one Trusted Device, that device cannot communicate with the other Trusted Devices because its network traffic is encrypted. Enable encryption on all or none of the Trusted Devices.
- Do not use the Windows IPsec policy MMC plug-in to change the IPsec policy. The Network Isolation Utility maintains its own copy of the policy. Whenever the Network Isolation Utility executes, the utility reverts to its last saved configuration, ignoring any changes made outside the utility (or the Security Wizard).
- The Network Isolation Utility does not interfere with applications that run on the network. However, run the utility only during the application maintenance window because the utility can disrupt connectivity when you set up the network security.
- If your network is behind a firewall, then configure the firewall to:
  - Allow IP protocol number 50, which is the ESP (Encapsulating Security Protocol).
  - Allow UDP source and destination traffic on port 500 for the IKE protocol.
- If you are using the NAT protocol, configure the firewall to forward traffic on UDP source and destination port 4500 for UDP-ESP encapsulation.
- Any changes made to the application port usage, such as a web server port, must also be reflected in the policy.
- Deploy the Network Isolation Policy after the Unified ICM or the Unified Contact Center application is configured and confirmed to be working.
- For an inventory of the ports used across the contact center suite of applications, see the following documentation:
  - *Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html
  - at https://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

  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.

Note Use the Security Wizard for initial policy creation or modification. You can use the command line for batch deployment.

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

C:\CiscoUtils\NetworkIsolation>

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

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

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

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

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

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

In the syntax:

- angle brackets < >= required

- square brackets [ ] = optional
- pipe or bar | = any one of the items between the bars

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

Table 1: Network Isolation Utility Command Syntax for Each Argument

Argument Name	Syntax and Example	Function
HELP	cscript ICMNetworkIsolation.vbe /?	Displays the syntax for the command.
ENABLE POLICY	cscript ICMNetworkIsolation.vbe /enablePolicy <36+ characters PreSharedKey in double quotes> [/encrypt] **Note** The only nonsupported character for use in the PresharedKey is double quotes because that character marks the beginning and end of the key. You can enter any other character within the key. For example: `cscript ICMNetworkIsolation.vbe /enablePolicy "myspecialpresharedkey123456789mnbvcx"`	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.
Note The add, remove, and delete arguments make a backup of the XML file and name it xml.lastconfig before carrying out their function.		

Argument Name	Syntax and Example	Function
ADD BOUNDARY	cscript ICMNetworkIsolation.vbe /addBoundary DNS|WINS|DHCP|GATEWAY For example: `cscript ICMNetworkIsolation.vbe /addBoundary DNS` This example adds the DNS server to the Boundary Device list.	Adds to the Boundary Device list the type of device specified. The type can be specified as DNS, WINS, DHCP, or GATEWAY. The utility recognizes DNS, WINS, DHCP, and GATEWAY as the Domain Name System (DNS) device, the Windows Internet Name Service (WINS) device, the Dynamic Host Configuration Protocol (DHCP) device, and the default Gateway (GATEWAY) device respectively. The Windows operating system dynamically detects a change in IP address for each of the preceding types of devices and dynamically updates the Boundary filter list accordingly.
	cscript ICMNetworkIsolation.vbe /addAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber> For example: `cscript ICMNetworkIsolation.vbe /addAnyHostBoundary Inbound TCP 5900` This example allows VNC access from all machines.	Adds to the Boundary Device list any device that matches the following criteria: • One of the specified traffic directions (outbound or inbound). • One of the specified protocols, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). • The specified port.
	cscript ICMNetworkIsolation.vbe /addIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: `cscript ICMNetworkIsolation.vbe /addIPAddrBoundary 10.86.121.160 Outbound Any` This example allows all outbound traffic to a device with the specified IP address.	Adds to the Boundary Device list the IP address of a device that has the following configuration: • (required) The specified IP address. • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (required): Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or any protocol. • (optional) any port or a specified port if the selected protocol is TCP or UDP.

Argument Name	Syntax and Example	Function
	cscript ICMNetworkIsolation.vbe /addSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber]	Adds to the Boundary Device list the subnet that has the following configuration: • (required) The starting IP address of the following specified range. • (required) The specified subnet mask (a range of logical addresses within an address space). • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or any protocol. • (optional) any port or a specified port if TCP or UDP is selected as the protocol.

Argument Name	Syntax and Example	Function
REMOVE BOUNDARY	cscript ICMNetworkIsolation.vbe /removeBoundary DNS|WINS|DHCP|GATEWAY For example: `cscript ICMNetworkIsolation.vbe /removeBoundary GATEWAY`	Removes from the Boundary Device list the type of device specified. The type can be specified as DNS, WINS, DHCP, or GATEWAY. The utility recognizes DNS, WINS, DHCP, and GATEWAY as the Domain Name System (DNS) device, the Windows Internet Name Service (WINS) device, the Dynamic Host Configuration Protocol (DHCP) device, and the default Gateway (GATEWAY) device respectively. Windows dynamically detects a change in IP address for each of the preceding types of devices and dynamically updates the Boundary filter list accordingly.
	cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber> For example: `cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary Inbound TCP 5900`	Removes from the Boundary Device list any host device at the specified IP address that matches the following criteria: • One of the specified traffic directions (outbound or inbound). • One of the specified protocols (TCP or UDP). • The specified port number for internet traffic.
	cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: `cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary 10.86.121.160 Outbound Any`	Removes from the Boundary Device list the device at the specified IP address that has the following configuration: • (required) The specified IP address. (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (TCP, UDP, ICMP, or any protocol). • (optional) any port or a specified port if TCP or UDP is the specified protocol.

Argument Name	Syntax and Example	Function
	cscript ICMNetworkIsolation.vbe /removeSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] For example: `cscript ICMNetworkIsolation.vbe /removeSubnetBoundary 10.86.0.0.255.255.0.0 Inbound Any`	Removes from the Boundary Device list all the devices at the specified IP address that have the following configuration: • (required) The starting IP address of the following specified range. • (required) The specified subnet mask. • (required) One of the specified traffic directions (outbound or inbound). • (required) One of the specified protocols (TCP, UDP, ICMP, or any protocol). • (optional) 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.

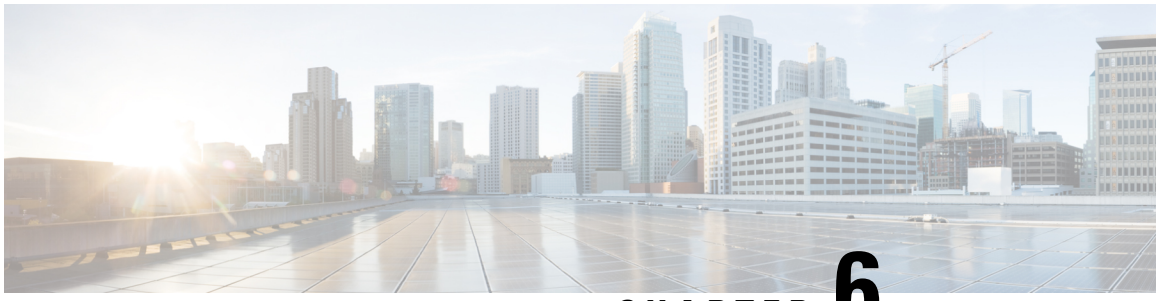
Step 2 Check whether an IP address or port specified in the Boundary Device list was modified after the policy was deployed.

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 6

Window Server Firewall Configuration

Windows Server 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.

For more information, see Microsoft documentation for details.

When you enable Windows Firewall on the servers, open all ports that the CCE solution components require.

Cisco provides a utility to automatically allow all traffic from Unified CCE applications on Windows Server. The utility can open ports for common third-party applications, that the contact center enterprise solution uses. The script reads the list of ports in the file `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml` and uses the directive to modify the firewall settings.

The utility allows all traffic from the applications, it adds 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 allows 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 and Services that are enabled by default:

- 80/TCP and 443/TCP - HTTP and HTTPS (when the system installs IIS or TomCat [for Web Setup])
- Microsoft Remote Desktop
- File and Print Sharing Exception - see https://docs.microsoft.com/en-us/windows-server/storage/file-server/best-practices-analyzer/smb-open-file-sharing-ports.

Firewall inbound rules that are disabled by default:

- Core Networking for IPv6
- Core Networking - IPHTTPS for TCP
- Core Networking - Teredo for UDP
- Network Discovery for Private Profile
- Windows Remote Management - HTTP for domain, private, and public profiles

Service disabled by default:

- File Server Remote Management

Optional ports that you can open:

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

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

For a complete list of port usage, see *Port Utilization Guide for Cisco Unified Contact Center Solutions*, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Cisco Firewall Configuration Utility Prerequisites

Install the following software before using the Firewall configuration utility:

1. For information on operating system, see the Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
2. Unified ICM/CCE components

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

Run Cisco Firewall Configuration Utility

You can run the Cisco Firewall Configuration Utility either from the command line or from the Unified Contact Center Security Wizard.

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

Use the Cisco Firewall Configuration Utility on each server running a Unified ICM component. To use the utility, follow these steps:

Procedure

Step 1 Stop all application services.

Step 2 From a command prompt, run `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat`.

Step 3 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 4 Click **OK**.

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

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

Step 5 Reboot the server.

Related Topics

Windows Firewall Configuration, on page 34

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** > **Windows Administrative Tools** and select **Windows Firewall with Advanced Security** when using Windows Server. Alternatively, choose **Start** > **Control Panel** > **System and Security** > **Windows Firewall**.

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

For more information about restricting File Replication Service (FRS) traffic to a specific static port, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

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

For more information about restricting Active Directory replication traffic to a specific port, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

Procedure

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

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

Step 3 Add the following registry values:

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

Configure Remote Procedure Call (RPC) Port Allocation

For more information about configuring RPC port allocation, see https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows.

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

Server Port	Protocol	Protocol	Service
135	TCP	RPC	RPC Connector Helper (machines connect to determine which high port to use)
137	TCP	UDP	NetBIOS Name

Server Port	Protocol	Protocol	Service
138		UDP	NetBIOS NetLogon and Browsing
139			NetBIOS Session
123		UDP	NTP
389	TCP		LDAP
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
42			Wins Replication
53	TCP	UDP	DNS
88	TCP	UDP	Kerberos
445	TCP	UDP	SMB over IP (Microsoft-DS)
10000	TCP		RPC NTFRS
10001	TCP		RPC NTDS
10002 to 10200	TCP		RPC - Dynamic High Open Ports
NA	ICMP		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.

Test Connectivity

To test connectivity and show the FRS configuration in Active Directory, use the Ntfrsult 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 download Portqry utility and to learn more about it, see https://support.microsoft.com/en-in/help/310099/description-of-the-portqry-exe-command-line-utility.

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.

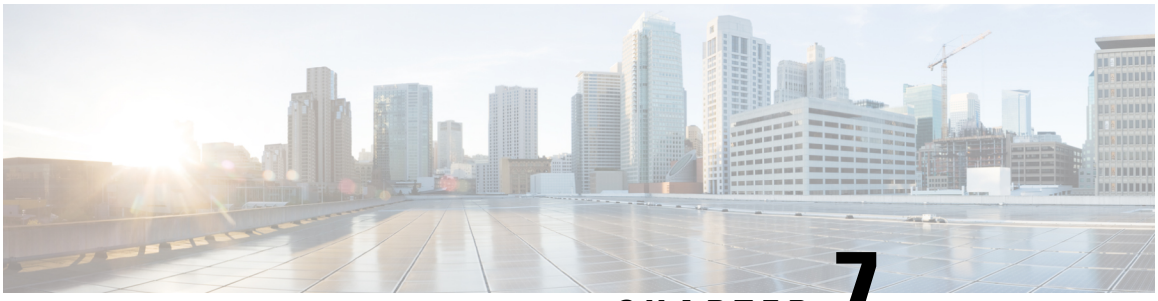
Step 2 Open a command window by choosing **Start** > **Run** and entering `CMD` in the dialog window.

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.



CHAPTER 7

SQL Server Hardening

SQL Server Hardening Considerations

Top SQL Hardening Considerations

Top SQL Hardening considerations:

1. Do not install SQL Server on an Active Directory Domain Controller.
2. Install the latest updates for SQL Server from Microsoft.
3. Set a strong password for the sa account before installing ICM.
4. Always install SQL Server service to run using a least privilege account. Never install SQL Server to run using the built-in Local System account. Instead, use the Virtual account.

   See the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html for more information.
5. Enable SQL Server Agent Service and set to Automatic for database maintenance in Unified ICM.

Note Installing the latest updates for SQL Server from Microsoft might require you to disable the SQL Server Agent service. So before performing the cumulative update installation, reset this service to *disabled*. When the installation is complete, stop the service and set it back to *enabled*.

6. Disable the SQL guest account.
7. Restrict sysadmin membership to your Unified ICM administrators.
8. Block TCP port 1433 (default) and UDP port 1434 at the network firewall, unless the Administration & Data Server is not in the same security zone as the Logger.
9. Change the recovery actions of the Microsoft SQL Server service to restart after a failure.

10. Remove all sample databases.
11. Enable auditing for failed sign-ins.

The following table lists the settings and the corresponding default and supported values for SQL hardening.

Setting Name	Default Value	Supported Value
Scan for Startup Procedures	Disabled |0|	0 or 1 supported. Unified CCE does not require it to be enabled; however, enabling it would not create any problem.
Ad Hoc Distributed Queries	Disabled |0|	0 or 1 supported. 0 is more secure.

Related Topics

SQL Server Users and Authentication, on page 68
Virtual Accounts, on page 71

SQL Server Users and Authentication

When creating a user for the SQL server account, create Windows accounts with the least possible privileges for running SQL server services. Create the accounts during the installation of SQL server.

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, don’t 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

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

During automated SQL server hardening, if the sa password is found blank, a strong password is generated at random 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.

UCCE supports renaming or removal of default built-in MS SQL sa account. If the sa account is used to integrate with UCCE solution components like Finesse, CUIC or any other third-party integrations, the login credentials have to be reconfigured with the renamed sa account.

Note Renaming or removing the sa account has no correlation with SQL Server hardening that happens during installation or upgrade.

SQL Server Security Considerations

Microsoft SQL server provides granular access control and runs with lower privileges by default. In addition to the security provided by SQL server, CCE provides utility to harden the SQL server further. Details are available in the following sections.

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.

Note Run the Security Wizard tool or Windows PowerShell script as an administrator.

Utility Location

The utility is located at:

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

HARDEN Command

At the Windows PowerShell command line, enter:

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

Note The current SQL Server configuration is backed up to `<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:

```
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.
2. Mixed mode authentication.

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:

```
%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.

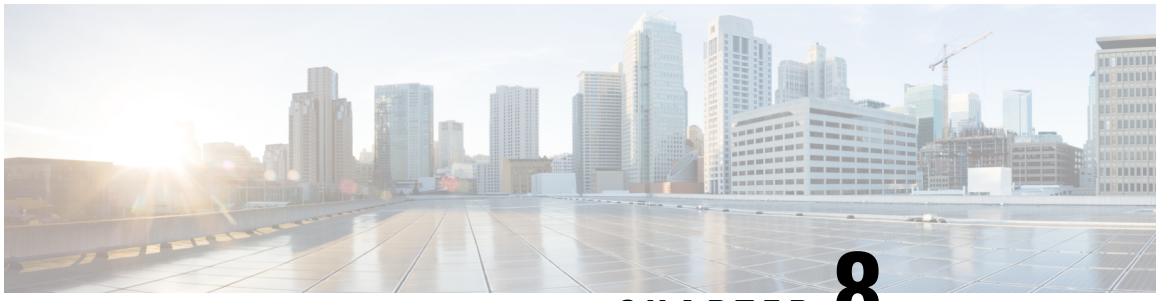
Note The SQL Server Security Hardening utility checks for the availability and order of these endpoints.

- 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).



CHAPTER 8

Certificate Management for Secured Connections

Certificates

Certificates are used to create secure communication between clients and servers. Users can purchase certificates from a certificate authority (CA-signed certificates) or they can use self-signed certificates.

Self-Signed Certificates

Self-signed certificates (as the name implies) are signed by the same entity whose identity they certify, as opposed to being signed by a certificate authority. Self-signed certificates are not considered to be as secure as CA certificates, but they are used by default in many applications.

Unified CCE Certificate Management Utilities

The following certificate management utilities can be used to secure machine-to-machine communication (for example, communication between the Cisco Finesse server and the CTI server), and manage interactions between web applications:

- Cisco SSL Encryption Utility used for web applications (Unified CCE Administration, WebSetup, and ISE).
- CiscoCertUtil used for creating and installing self-signed certificates and CA-signed certificates for use in machine-to-machine communications.
- Diagnostic Framework Cert Utility used for Diagnostic Portico applications.

Note The Unified CCE Certificate Monitoring service monitors the self-signed and CA-signed certificates and keys that are used for certificate management. The service alerts the system administrator about the validity and expiry of these certificates. For more information, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

SSL Encryption Utility

Note Although this utility currently has its original name, the SSL Encryption Utility now configures web applications for use with TLS.

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 TLS.

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 perform. 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

TLS Installation During Setup

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

Note You must restart the SSL Configuration Utility if you use IIS manager to modify TLS settings while the utility is open.

The SSL Configuration Utility can be used to create self-signed certificates, to install the certificates in IIS, and to remove certificates from IIS. When invoked as part of setup, the SSL Configuration Utility sets TLS port in IIS to 443 if it is found to be blank.

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

During setup, the utility generates a self-signed certificate, imports it into the Local Machine Store, and installs it on the web server. Virtual directories are enabled and configured for TLS with 256-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 use the IIS Services Manager to make certificate management changes.

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 you select an instance, the utility displays the installed web applications and their SSL settings. 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 TLS port in IIS to 443 if it is found to be blank.

CiscoCertUtil Utility

The CiscoCertUtil utility helps you manage certificates on any Contact Center Enterprise machine for machine-to-machine secure communication across components. Examples of machine-to-machine secure communications are Finesse to CTI Server (CG), Dialer to CG, MRPG to ECE, and VRU PG to CVP, and so on.

The TLS-enabled components use this utility to set up certificates, and the Contact Center Enterprise setup uses this utility to generate and install certificates.

The CiscoCertUtil utility is supported on servers running Windows Server. It performs the following functions:

- Generates selfsigned certificates.
- Generates certificate signing requests (CSR).
- Installs remote certificates to the local machine certificate store under the Personal/ROOT/CA folder.
- Deletes certificates from the local machine certificate store under the Personal/ROOT/CA folder.
- Generates selfsigned certificates in the PEM format, which is an X509 extension.
- Generates the corresponding key with the filename *host.key*.
- Does not validate any certificate.
- Does not create any log file pertaining to the operations that it performs. If there are errors, the error log appears on the console.

Note Use the CiscoCertUtil utility to install or delete selfsigned certificates only.

How to use CiscoCertUtil Utility:

CiscoCertUtil *[/generateCert]|[/generateCSR]|[/generateCert /f]|[/remove <cert_name>]|[/install <cert_file>]| [/list]|[/help]|* commands.

Where:

1. */list* displays a list of certificates that are present in the local machine store under personal (LOCAL_MACHINE/MY), root (LOCAL_MACHINE/ROOT) and ca (LOCAL_MACHINE/CA) store.
2. */generateCert* generates a selfsigned RSA certificate with the filename *host.pem* and a key with the filename *host.key*. The selfsigned certificate is copied to `<install_drive>:\icm\ssl\certs` folder. If the key exists, the same key is used to generate the selfsigned certificate *host.pem*. An RSA key length of 2048 bits is used.

   The */generateCert* command does not overwrite *host.key* and *host.pem*. To overwrite the existing self-signed certificate, use the */generateCert /f* command. This command overwrites *host.key* and *host.pem* if already available in the system.

Note During CCE installation, a selfsigned certificate is already generated. You need to use the */generateCert* command only if you have to generate a new certificate. For example, you may need to generate a certificate in situations when the key of the certificate is compromised or the selfsigned certificate has expired.

3. */generateCSR* The command generates a CSR with the filename *host.csr* and a key with the filename *host.key*, which is a private key. The *host.csr* file is then sent to Certification Authority to obtain the digital identity certificate. If the key exists, the same key is used to generate *host.csr*.

Note When you generate a certificate signing request (CSR), you will be prompted to key in the Organization Unit (OU). Based on the RFC5280 standard and baseline requirement, the Organization Unit is not required. You can leave this field blank so that the Certificate Authorities will not include the field in the certificate.

Use the **openssl req -in <csr_file> -noout -text** command to validate the presence of the Organization Unit field.

4. */remove* <*certificate_name*> removes the certificate <*cert_name*> from the local machine certificate store under the Personal folder. If the command fails to run, an error message appears. To display the list of certificates that are present, use the */list* command.
5. */install* <*cert_file*> <*optional_cert_store – my/root/ca*> installs the certificate that is mentioned as <*cert_file*> into the local machine certificate store under the Personal (my) or Trusted root (root) or Intermediate Certificate Authorities (CA) folder based on the option provided. If no option is provided, the certificate will be installed in the Personal folder. If the command fails to run, an error message appears.

   An example of this command:

   ```
   CiscoCertUtil /install c:\icm\ssl\certs\host.pem.
   ```

6. */help* displays the usage of the commands.

Note If the *remove* command fails, use the *list* command to verify whether the certificate you attempted to remove is present in the local machine certificate store.

Manage Secured PII in Transit

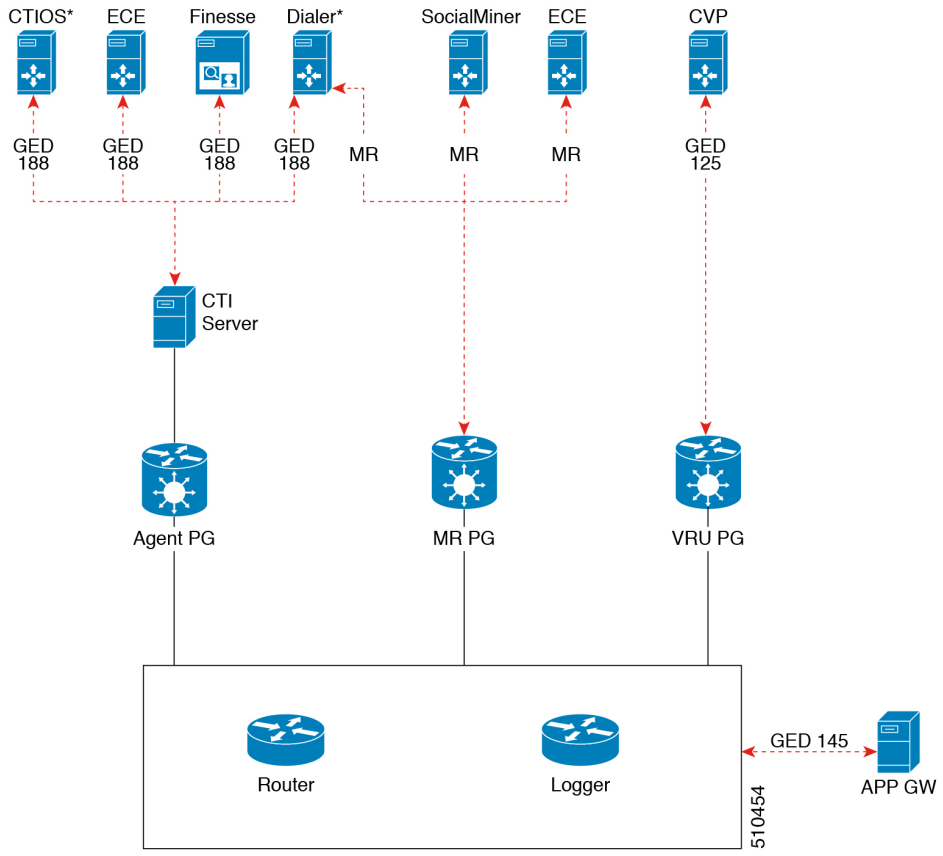
The Contact Center Enterprise solution handles customer sensitive Personally Identifiable Information (PII) that include credit card information, PIN, and other sensitive details. Such sensitive information is sent across the system in ECC variables and can be exploited.

The transport channels such as GED 188, GED 125, GED 145, and MR carry PII and are susceptible to exploitation. It is therefore necessary to secure the transport channels that carry PII and protect them from any threats.

Securing PII is also necessary to adhere to the regulatory security compliance. The CCE solution uses the TLS protocol to enable security of the transport channels that carry PII.

Note The communication channels between the Central Controller and PG are not secure. For end-to-end solution security, use the IPSec Network Isolation Zone.

Figure 6: Secured Connection Example



The following table lists the use cases for secured connections, the corresponding server-to-client matrix, and the protocol used:

Use Case	Server	Supported Client	Protocol
Secured self-service communications: To secure self-service communications, enable secured connection in CVP and VRU PG.	CVP	VRU PG	GED 125
Secured outbound calls: To secure outbound calls, enable secured connection in the CTI server, Dialer, and Media Routing PG.	CTI Server	Dialer	GED 188
	Dialer	MR PG	Media Routing Protocol
Secured agent desktop communications: To secure the communications with Cisco Finesse Server and CTI OS, enable mixed-mode connection in the CTI server. Next, enable secured connection in the Cisco Finesse Server or in CTI OS, as applicable.	CTI Server	Cisco Finesse	GED 188
		CTI OS	
Secured third-party integration: To secure third-party integration with CCE, enable secured connection in the application gateway servers and clients.	Application Gateway Servers	Application Gateway Clients	GED 145

Use Case	Server	Supported Client	Protocol
Secured multi-channel communications: To secure multi-channel communications, enable secured connection between: • ECE (Services Server) and MR PG (Client) • Customer Collaboration Platform (CCP) and MR PG (Client) • • CTI server and ECE (Client)	ECE	MR PG	Media Routing Protocol
	Customer Collaboration Platform		
	CTI Server	ECE	GED 188

To establish secured connection between a server and a client, you need to create mutual authentication by using one of the following security certificates:

- Self-signed Certificate
- Third-party CA Signed Certificate

Locations for Certificates and Keys

Store the certificates, intermediate and trusted certificates, and keys at the following directories in the respective machines:

The steps to generate and install certificates are provided in following section.

Manage Certificates

Managing Certificates for Unified CCE Component

All certificates are managed using Cisco tools. For more details, see Unified CCE Certificate Management Utilities, on page 73

Installing the Server Certificate on the Client Machine

Procedure

Step 1 On the server machine, generate a certificate by using the command: *<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*. This command generates a certificate in the PEM format and copies it in this path `C:\icm\ssl\certs`.

If a valid self-signed certificate is already available, skip to step 2. For more information, see the */generateCert* section in CiscoCertUtil Utility, on page 75.

Step 2 Navigate to the path `c:\icm\ssl\certs`.

Step 3 Copy **host.pem** to a temporary location on the client machine.

Step 4 On the client machine, install this certificate file on the trusted certificate store, by using the command:*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*. If the certificate file already exists in the trusted certificate store of the client machine, remove this existing certificate file before installing a new one.

Step 5 To confirm that you installed the certificate file successfully, run the *CiscoCertUtil /list* command. Then, check if the server host name is listed under `LOCAL_MACHINE/ROOT`.

Installing the Client Certificate on the Server

Procedure

Step 1 On the client system, generate a certificate by using the command: *<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*. This command generates a certificate in the PEM format and copies it in this path `C:\icm\ssl\certs`.

If a valid self-signed certificate is already available, skip to step 2. For more information, see the */generateCert* section in CiscoCertUtil Utility, on page 75.

Step 2 Navigate to `c:\icm\ssl\certs`.

Step 3 Copy **host.pem** to a temporary location on the server.

Step 4 On the server, install this certificate file on the trusted certificate store, by using the command:*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*. If the certificate file already exists in the trusted certificate store of the server, remove this existing certificate file before installing a new one.

Step 5 To confirm that you have installed the certificate file successfully, run the *CiscoCertUtil /list* command. Then, check if the client host name is listed under `LOCAL_MACHINE/ROOT`.

What to do next

Restart the corresponding services after installing the certificates.

Managing Certificates for Finesse

Refer to the following steps for security certificate management for Finesse server.

Exporting a Certificate from Finesse Server

Use this procedure to export security certificates from the Finesse server.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration console on Finesse server.

Use the FQDN path of the Finesse server (`http://FQDN of Finesse server:8443/cmplatform`) to sign in.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Click **Find**.

Step 4 Perform one of the following steps based on whether the Tomcat certificate is listed or not:

- If the Tomcat certificate is not listed:
  - Click **Generate New**.
  - Reboot the VOS server when the certificate generation is complete.
  - Restart this procedure.
- If the Tomcat certificate is listed:
  - Click the certificate to select it. Click **Download .pem file** and save the file to your desktop.
  - Ensure that the certificate you select includes the hostname for the server.

What to do next

Perform these steps for all the Finesse server nodes.

Importing a Certificate to Finesse Server

Use this procedure to import security certificates to the Finesse server.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on Finesse server.

Use the FQDN path of the Finesse server (`http://FQDN of Finesse server:8443/cmplatform`) to sign in.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Click Upload Certificate.

Step 4 Select **Certificate Name** > **tomcat-trust**.

Step 5 Click **Browse**.

Browse to the location of the CTI Server certificate with the `.pem` file extension.

Step 6 Select the file and click **Upload File**.

What to do next

Repeat steps 3 to 6 for the remaining unloaded certificates.

After you upload all the certificates, restart the `Finesse Tomcat` application.

Generate and Copy CA Certificates of Unified CCE Components

If you are using Certificate Authority (CA) certificates for mutual authentication of CCE machines, do the following:

1. Generate CSR using `CiscoCertUtil`.

   This command generates a host.csr file and sends the CSR to a trusted Certificate Authority for sign-off. To generate a new CSR, see CiscoCertUtil Utility, on page 75.

2. Obtain the CA-signed application certificate, Root CA certificate, and Intermediate Authority certificate.
3. Copy the CA-signed application certificate file into the appropriate folder (`<install_drive>:\icm\ssl\certs` as applicable.
4. Restart the services
5. Install the CA-signed application certificate using the command `CiscoCertUtil / install <cert file > <optional cert store>`. Certificate store can be my, root or ca with default being my when not specified. You can also manually install the CA Certificate to Windows trust store, if not already installed or present. You can verify if certificate is installed properly using windows `certlm.msc` utility in personal, Trusted Root or Intermediate Certificate Authorities based on option specified in install command. Default is Personal if no option is provided.

Certificate Management for Customer Collaboration Platform

Control Customer Collaboration Platform Application Access

By default, access to Customer Collaboration Platform administration user interface is restricted. Administrator can provide access by allowing clients IP addresses and revoke by removing the client's IP from the allowed list. For any modification to the allowed list to take effect, Cisco Tomcat must be restarted.

Note IP address range and subnet masks are not supported.

utils whitelist admin_ui list

This command displays all the allowed IP addresses. This list is used to authorize the source of the incoming requests.

Syntax

utils whitelist admin_ui list

Example

```
admin: utils whitelist admin_ui list

Admin UI whitelist is:
```

```
10.232.20.31
10.232.20.32
10.232.20.33
10.232.20.34
```

utils whitelist admin_ui add

This command adds the provided IP address to the allowed list of addresses.

Syntax

utils whitelist admin_ui add

Example

```
admin:utils whitelist admin_ui add 10.232.20.33

Successfully added IP: 10.232.20.33 to the whitelist

Restart Cisco Tomcat for the changes to take effect
```

utils whitelist admin_ui delete

This command deletes the provided IP address from the allowed list.

Syntax

utils whitelist admin_ui delete

Example

```
admin:utils whitelist admin_ui delete 10.232.20.34

Successfully deleted IP: 10.232.20.34 from the whitelist

Restart Cisco Tomcat for the changes to take effect
```

Obtaining a CA-Signed Certificate

Each time you sign-in, the browser validates the certificate presented by the server. If the certificate is not signed by a trusted root Certificate Authority (CA), the browser will typically not allow the connection until the user explicitly allows it. In order to avoid this, you must obtain a root certificate signed by a CA and install it onto Customer Collaboration Platform. Also, you must upload the certificate onto the VOS components.

After You Upload the Certificates

For the uploaded certificates to take effect, do the following:

1. Restart the XMPP Service. (SSH to Customer Collaboration Platform and enter the command *utils service restart CCP XMPP Server* as an administrator in the Commad Line Interface).
2. Restart the Cisco Tomcat service. (SSH to Customer Collaboration Platform and enter the command *utils service restart Cisco Tomcat* as an administrator in the Command Line Interface).

Obtaining a Self-Signed Certificate

Browsers handle self-signed certificates in different ways. The sections below describe how to handle self-signed certificates on the browsers supported for Customer Collaboration Platform.

Internet Explorer and Self-Signed Certificates

When using an IE browser on a Windows machine, make sure your DNS server is properly configured and you can resolve the fully qualified Customer Collaboration Platform hostname to the Customer Collaboration Platform address. Use a signed certificate from a trusted certificate authority (like Verisign).

If you use a self-signed certificate (which is what is installed with Customer Collaboration Platform), follow these steps to avoid getting certificate warnings each time you sign in.

- In your Start menu, right click on IE and select "Run as Administrator".
- Enter the URL for your Customer Collaboration Platform server in the address bar.
- When prompted by the security warning, click on **Continue to this website (not recommended)**.
- Your address bar turns red and you see a certificate error next to the address bar. Select the certificate error.
- Select **View certificates** at the bottom of the popup. This opens a certificate dialog.
- On the General tab, select **Install Certificate...**.
- The certificate export wizard launches. Click **Next**.
- When prompted for where to store the certificates, select **Place all certificates in the following store**, then click **Browse** and select **Trusted Root Certification Authorities**.
- Click **Ok**, then click **Next** and **Finish** to complete the certificate import wizard.
- Click **Yes** when prompted about importing the certificate.
- Close and restart your browser to access Customer Collaboration Platform.

Firefox and Self-Signed Certificates

Due to changes in the Firefox security model, there are additional self-signed certificates that must be accepted to use the Customer Collaboration Platform web application on Firefox.

When accessing a Customer Collaboration Platform server using a newly installed Firefox browser (any version), Firefox attempts to connect to the main port that Customer Collaboration Platform uses first (port 443). If it cannot connect, it prompts the user to accept the self-signed certificate.

Note If pop ups are blocked, you are given instructions on how to manually launch the certificate page. Also, if the certificate window is closed before the certificate is accepted, the page will automatically re-launch.

- If prompted, click **I Understand the Risks**, then click **Add Exception**.
- Click **Confirm Security Exception**.

Next, Firefox attempts to connect to port 7443 (the secure XMPP port). With Firefox, a second self-signed certificate must now be accepted to use this port. Customer Collaboration Platform displays a "Checking Connectivity..." screen during this process

If the"Checking Connectivity..." screen persists after a few seconds, click **Continue** to proceed to the Firefox certificate acceptance screen (as above).

Click **I Understand the Risks**, then **Add Exception**, and **Confirm Security Exception** again.

Users need only go through this process the first time they use a new Firefox browser and self-signed certificates. After the certificates are in place, users may not see the "Checking Connectivity..." screen (or it will appear briefly and proceed to the Customer Collaboration Platform sign on screen).

Google Chrome and Self-Signed Certificates

When accessing a Customer Collaboration Platform server using Google Chrome Browser, it attempts to establish a Private secure connection using port 7443.

- After keying in the Server IP address in Chrome, the browser displays a connection warning stating **"Your Connection is not private**." To proceed with a secure connection, click **Advanced**.
- Click **Proceed to <Server IP Address>.** Next, Chrome attempts to connect to port 7443 (the secure XMPP port).
- The browser displays **"Checking connectivity**." Click **Continue** to proceed. This opens another Chrome tab, where you are prompted with another connection warning.
- Click **Advanced.**
- Upon clicking **"Proceed to <Server IP Address>",** the Customer Collaboration Platform log on page is displayed.

Note Users need to go through this process only the first time they use a new Chrome browser and self-signed certificates.

Transport Layer Security (TLS) Requirement

Contact center enterprise solutions use Transport Layer Security (TLS). Refer to your browser's documentation for details on how to configure support for TLS. See the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for the supported TLS versions.

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.

Upgrading to 12.5(1a)

A new 12.5(1a) base installer is available with OpenJDK JRE as the supporting Java run time for all the CCE applications. Its predecessor, the 12.5(1) installer, employs Oracle JRE.

Note To verify the base installer version, go to **Control Panel** > **Programs** > **Programs and Features** > **Cisco Unified ICM/CCE <version>**.

Any installation using the 12.5(1) installer can continue to use Oracle JRE and receive Java security updates and fixes from the Oracle website. However, if you have to apply an ES on 12.5(1), you must install CCE 12.5(1) ES55 as described in Migrating CCE 12.5(1) Oracle JRE to OpenJDK, on page 87 and then install the Java updates from the OpenLogic website.

Run the following checks if you are considering installing an ES after upgrading to 12.5(1a):

- The following ESs are included in ES 55 and need not be installed if ES 55 is installed: ES4, ES5, ES7, ES12, ES21, ES22, ES25, ES30, ES33, ES39, ES43, ES50, and ES51.
- The following ESs are not included in ES 55 and can be installed after installing ES 55: ES2, ES9, ES11, ES13, ES16, ES17, ES18, ES19, ES20, ES24, ES26, ES27, ES28, ES31, ES32, ES34, ES35, ES37, ES38, ES40, ES42, ES44, ES45, ES46, ES47, ES49.
- ES 55 must be installed before you apply any patch greater than ES 55.

For more details, see the *Cisco Unified Contact Center Enterprise Engineering Specials (ES) Information* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/ucce_b_unified-contact-center-enterprise-engineering/ucce_b_unified-contact-center-enterprise-engineering_chapter_0110.html.

After installing ES 55 patch and switching to Open JDK, you may upgrade the current Open JDK 1.8 version to a later version by one of the following ways:

- Manual Upgrade of Open JDK, on page 88
- Upgrade Open JDK Using the Open JDK Upgrade Tool, on page 87

These procedures also ensure that the certificates are imported to the OpenJDK Java KeyStore path.

Migrating CCE 12.5(1) Oracle JRE to OpenJDK

Follow these steps to install UCCE 12.5(1) ES 55 to migrate the 12.5(1) CCE core components such as Routers, Roggers, and PG servers to OpenJDK JRE.

Before you begin

Do not uninstall any of the ESs installed before ES 55.

Procedure

Step 1 Run the following commands to export the certificates of all the components from the Oracle Java KeyStore.

```
cd %JAVA_HOME%\bin
```

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -export
-storepass <store password> -alias <alias of the cert> -file <filepath>.cer
```

Step 2 Follow the instruction in the Readme file to install the UCCE 12.5(1) ES 55 patch.

ES 55 installs the 1.8 (update 272) version of the 32-bit OpenLogic Java and ensures that all the services run on this Java environment.

Step 3 Modify the JAVA_Home environmental variable to the OpenJDK path used in Step 2.

Step 4 Run the following commands to import the certificates in the new path:

```
cd %CCE_JAVA_HOME%\bin
```

```
keytool -keystore "C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\lib\security\cacerts"
 -import -storepass <store password> -alias <alias of the cert> -file <filepath>.cer
```

Upgrade Open JDK Using the Open JDK Upgrade Tool

Follow these steps to upgrade your Open JDK to the latest version using the Open JDK Upgrade tool.

Procedure

Step 1 Download the latest 1.8 version patch from the OpenLogic site at https://www.openlogic.com/openjdk-downloads and copy it to the server.

Step 2 Copy the downloaded file into the Unified CCE component VMs.

Example:

```
C:\UpgradeOpenJDK
```

Step 3 Run the following commands to export all the certificates from the existing Oracle Java KeyStore.

```
cd %CCE_JAVA_HOME%\bin
```

```
 keytool -keystore "C:\Program Files
(x86)\OpenJDK\jre-8.0.272.10-hotspot\lib\security\cacerts" -export -storepass <store password>
 -alias <alias of the cert> -file <filepath>.cer
```

Step 4 Download the OpenJdkUpgradeTool utility from the following location to a local folder:

https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(1)

Step 5 Run openJDKUtility.exe from the unzipped folder and follow the instructions in the ReadMe file.

Step 6 From the **Control Panel**, search for "Environmental Variables." From the search results, select **Edit the System Environmental Variables**.

In the **System Properties** dialog box that opens, under the **Advanced** tab, click **Environmental Variables**.

In the **Environmental Variables** dialog box that opens, under **System variables**, ensure that the JAVA_Home variable is set to the OpenJDK path used in Step 4.

Step 7 Run the following commands to import the certificates to the new path.

```
cd %CCE_JAVA_HOME%\bin
```

```
keytool -keystore "C:\Program Files (x86)\OpenJDK\<jre-8.0.292.10-hotspot or new
version>\lib\security\cacerts" -import -storepass <store password> -alias <alias of the
cert> -file <filepath>.cer
```

Manual Upgrade of Open JDK

Follow these steps to manually upgrade your Open JDK to the latest version.

Procedure

Step 1 Download the latest 1.8 version patch from the OpenLogic site at https://www.openlogic.com/openjdk-downloads and copy it to the server.

Step 2 Run the following commands to export all the certificates from the existing Oracle Java KeyStore.

```
cd %CCE_Java_HOME%\bin
```

```
 keytool -keystore "C:\Program Files
(x86)\OpenJDK\jre-8.0.272.10-hotspot\lib\security\cacerts" -export -storepass <store password>
 -alias <alias of the cert> -file <filepath>.cer
```

Step 3 Follow the instructions in OpenLogic Java readme file to install the Java patch downloaded in step 1.

Step 4 From the **Control Panel**, search for "Environmental Variables." From the search results, select **Edit the System Environmental Variables**.

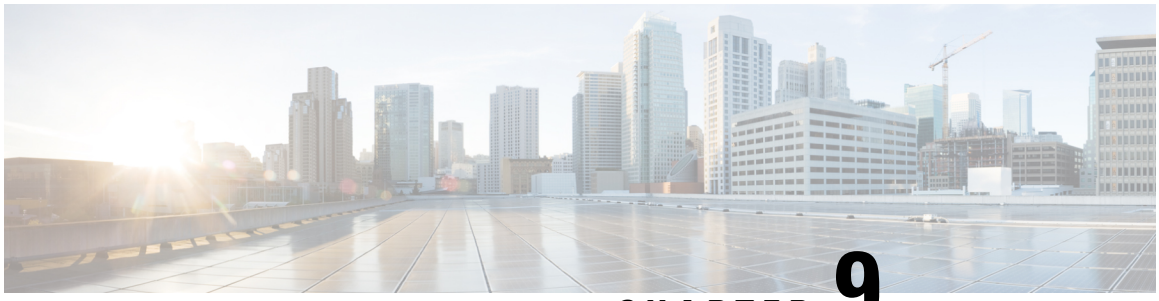
In the **System Properties** dialog box that opens, under the **Advanced** tab, click **Environmental Variables**.

In the **Environmental Variables** dialog box that opens, under **System variables**, ensure that the JAVA_Home variable is set to the OpenJDK path used in Step 4.

Step 5 Run the following commands to import the certificates to the new path.

```
cd %CCE_Java_HOME%\bin
```

```
keytool -keystore "C:\Program Files (x86)\OpenJDK\<jre-8.0.292.10-hotspot or new
version>\lib\security\cacerts" -import -storepass <store password> -alias <alias of the
cert> -file <filepath>.cer
```



CHAPTER 9

Auditing

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

For general SQL Server auditing policies, see the Microsoft documentation .

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

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

Configuration Auditing

Unified CCE captures a history of all system configuration changes in the Config_Msg_Log table. However, the information that is captured in the Config_Msg_Log table is encrypted. To display the table in a meaningful format, use the dumpcfg utility, which is a database administration tool. You can use the information that is retrieved for auditing purposes.

To run the utility, on the command prompt use the following command:

dumpcfg *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]*|.

Where:

1. *database* is the case-sensitive name of the logger database.
2. *@server* is the hostname of the AW or logger database.
3. *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|* are the time range for which the information is required.

   RecoveryKey is a value that the software uses internally to track virtual time.

The *dumpcfg* command displays the following output details:

- **LogOperation**: Indicates the type of the configuration operation. For example, *Add* and *Update*.
- **TableName**: Represents the name of the table that the configuration operation had impacted.
- **DateTime** Indicates the date and time of the configuration operation.
- **ConfigMessage**: Lists all the configuration messages for a configuration operation.

For example, if you add a skill group and then run the following command:

For example, if you add a skill group and then run the command:**dumpcfg ucce_sideA@uccergr100a /bd 09/27/2018**

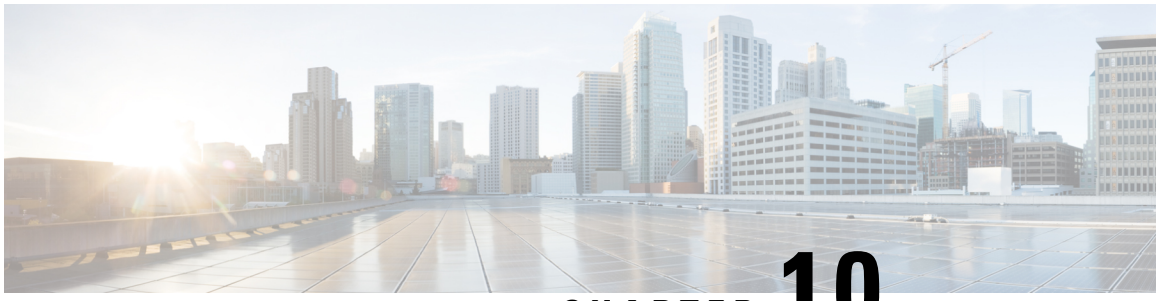
The output displays the following details:

LogOperation - **Add**.

TableNames -skill_target and t_skill_group.

DateTime - the exact timestamp when the skill group was added.

ConfigMessage - the field names impacted, such as **Peripheral Name**, **Enterprise Name**, and so on.



CHAPTER 10

General Antivirus Guidelines

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 *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

For more information about the Cisco Guidelines on third-party software product, see the *Cisco Customer Contact Software Policy for Use of Third-Party Software Bulletin* at https://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-ip-interactive-voice-response-ivr/prod_bulletin09186a0080207fb9.html.

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

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

The following list highlights some general guidelines:

- Ensure that your corporate Antivirus strategy includes specific provisions for any server that is positioned outside the corporate firewall or subject to frequent connections to the public Internet.

- Refer to the *Contact Center Enterprise 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.
- 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 multitiered 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.
- 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.
- 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

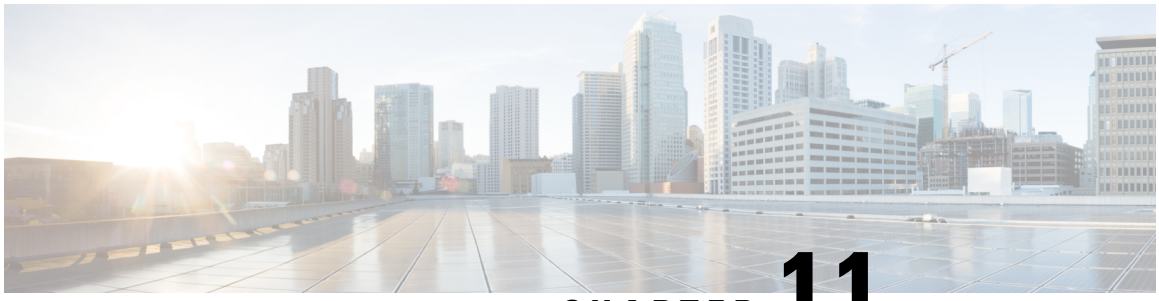
Several binary files that are written to during the operation of Unified ICM processes have little risk of virus infection.

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
- *.repl
- *.localrepl

Note If you are using Outbound High Availability replication, the **repl** directory, which is at `/icm/<cust>/la` or `lb/repl` should be excluded from antivirus scanning.

Note Exclude the *c:\icm* folder from all antivirus scans.



CHAPTER 11

Remote Administration

Windows Remote Desktop

Remote Desktop permits users to remotely run 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 original 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 protect your RDP-TCP connection, use the Microsoft 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 that a session can remain active to one or two days.
- Limit the time that 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 enabling Network Level Authentication (NLA) on the RDP server using one of the following ways:
    - On your remote server, navigate to **Settings > Remote Desktop Settings** and select the **Require devices to use Network Level Authentication to connect (Recommended)** checkbox.
    - In the Group Policy editor, navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security** and enable the **Require user authentication for remote connections by using Network Level Authentication** policy.
- Consider setting high encryption levels to protect against unauthorized monitoring of the communications. In the Group Policy Editor, navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security**. Click the **Set client connection encryption level** policy, select the **Enabled** option, and then set **Encryption Level** to **High Level**.

Note To prevent man-in-the-middle attacks against your remote Server Message Block (SMB) server, we recommend that you enforce message signing in the host configuration. To do so, set the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature** registry key value to **1**. Alternatively, in the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** and enable the following policies:

- Microsoft network client: Digitally sign communications (always)
- Microsoft network client: Digitally sign communications (if server agrees)
- Microsoft network server: Digitally sign communications (always)
- Microsoft network server: Digitally sign communications (if client agrees)

Per-User Terminal Services Settings

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

Procedure

Step 1 Using Active Directory Users and Computers, right-click a user and then select **Properties**.

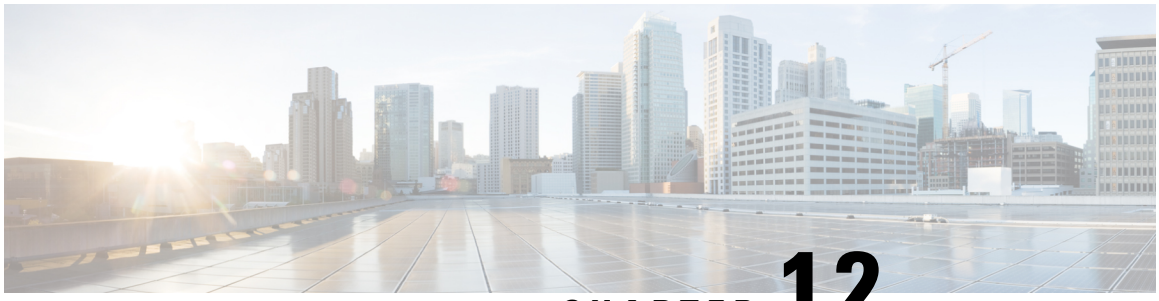
Step 2 On the Terminal Services Profile tab, set a user's right to sign in to terminal server by checking the **Allow logon to terminal server** check box. Optionally, create a profile and set a path to a terminal services home directory.

Step 3 On the Sessions tab, set session active and idle time outs.

Step 4 On the Remote Control tab, set whether administrators can remotely view and control a remote session and whether a user's permission is required.

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.



CHAPTER 12

Other Security Considerations

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’s 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:** The default is 15. Number of minutes before the AccountLockoutThreshold count goes back to zero. This is applicable if the account doesn't get locked out, but you have unsuccessful login attempts less than the value mentioned in AccountLockoutThreshold.

- **AccountLockoutThreshold:** The default is 3. This is the number of unsuccessful login attempts after which the account is locked out.

Note These settings are applicable only on Desktop solutions other than Cisco Finesse, such as CTI OS with a System Peripheral Gateway.

Finesse blocks access to user accounts, if agents or supervisors try to sign in to the desktop five times consecutively with a wrong password. The lockout period is five minutes. For more information about these settings, see the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

When Single Sign-On (SSO) is enabled for an agent, the account lockout mechanism is managed by the associated identity provider.

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 contact center enterprise solution, you can implement device authentication for the Cisco Unified IP Phones. Contact center enterprise solutions support 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

Before enabling SRTP in your deployment, consider the following points:

- To use secure media on the agent leg, ensure that the installed IP phones are compatible with SRTP.
- The Virtualized Voice Browser supports SRTP for the VRU leg.
- The IOS VXML Gateway does 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

With the IP phone device configuration in Unified CM, you can disable certain phone features to harden the phones. For example, you can disable the phone's PC port or restrict a PC from accessing the voice VLAN. Changing some of these settings can disable the monitoring and recording features of the contact center enterprise solution. The settings are defined as follows:

- **PC Voice VLAN Access**—Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access prevents the attached PC from sending and receiving data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the phone. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled (the default).

- **Span to PC Port**—Indicates whether the phone forwards packets transmitted and received on the Phone Port to the PC Port. To use this feature, enable PC Voice VLAN access. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled.

Disable the following setting to prevent man-in-the-middle (MITM) attacks. Some third-party monitoring and recording applications use this mechanism for capturing voice streams.

- **Gratuitous ARP**—Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

  This setting is Disabled.

Vulnerability Scan and Penetration Test Considerations

Keep in mind the following considerations when you are performing the vulnerability scans and penetration test in your deployment:

- Cisco recommends that you perform the vulnerability scan and penetration test during off-peak times and maintenance windows on the production system.
- When you install patches for Maintenance Releases (MRs) or Engineering Specials (ES) for Unified ICM and Unified CVP, older versions of files that are included in the patch are backed up. You need these older versions of the files to be restored if you choose to uninstall the MR or ES patches for any reason. These older versions that are backed-up are not used by the software running on your computer and they do not pose any security threat. If you receive any software vulnerability notification on these backed-up folders or files, treat them as False Positive and define rules to suppress them. Details on the backup folders and file locations are available in the rollback files (Rollback_ICM_*.txt and Rollback_CVP_*.txt) inside each of the patch information folder:

- For Unified ICM—The following are the backup folders and file locations:
  - PatchInfo_ICM_* within <install_drive>\icm
  - PatchInfo_ICM_* within <install_drive>\icm\AdminClient\lib\setup.war
- For Unified CVP—Patchinfo_CVP_* within <install_drive>\Cisco\CVP

Note You can delete the files in the backup folders. However, ensure to take a backup of these files if you need to roll back.

Java Upgrades

In 12.5(1), after the initial release, CCE transitioned from Oracle to OpenJDK for the Java runtime environment. Newer installs and upgrades with 12.5(1a) base installer run with OpenJDK JRE while the older installs and upgrades with 12.5(1) base run with Oracle JRE. Existing 12.5(1) deployments will transition to OpenJDK with 12.5(1) ES55, which in turn is a mandatory prerequisite for receiving further maintenance patches on CCE.

During installations and upgrades, Unified CCE installs the required base Java version.

Before updating the Java Runtime Environment (JRE):

- Execute the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.

Important Use JAVA_HOME if you are employing Oracle JRE.

- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

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.

  For the most current Java support information, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

  You can download and install the Oracle Java updates from the Oracle website and the OpenJDK Java updates from the OpenLogic website.
- Modify the Windows CCE_JAVA_HOME[1] environment variable to point to the new OpenJDK Java Runtime Environment (JRE) location if it has changed.

[1] If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

After updating the OpenJDK Java Runtime Environment (JRE):

- Execute the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.

Important Use JAVA_HOME if you are employing Oracle JRE.

- Import the certificates for all the components that you previously exported from the truststore before you updated the JRE.

  The command to import certificates is *keytool -import -keystore <JRE path>\lib\security\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

Change Java certificate store password

The default password for Java trust-store (%CCE_JAVA_HOME%/jre/lib/security) and CCE trust-store (<install_dir>:\icm\ssl\) is *changeit*. As a good security practice, it is recommended to change the default password.

Follow these steps to change the store password:

Procedure

Step 1 Open the command prompt and change to the installation directory.

Step 2 Run the following command:

For Java trust-store:

```
keytool -storepasswd -keystore (%CCE_JAVA_HOME%/jre/lib/security/cacerts
```

For CCE trust-store:

```
keytool -storepasswd -keystore <install_dir>:\icm\ssl\cacerts
```

Step 3 At the **Enter keystore password** prompt, type the current password and press Enter.

Step 4 At the **New keystore password** prompt, type your new password and press Enter.

Step 5 At the **Re-enter new keystore password** prompt, type your new password again and press Enter.

The new password is saved to `cacerts`.

Upgrade OpenJDKUtility

The Cisco Upgrade OpenJDKUtility:

- Upgrades OpenJDK JRE to latest release.

- Supports upgrade for both MSI and Zip file formats.
- Automatically sets the CCE_JAVA_HOME environment variable to updated version so that Unified CCE applications can employ the latest OpenJDK version as the Java runtime.

Before using the tool:

- Download the OpenJDK installer (JRE package) from the OpenLogic OpenJDK website: https://www.openlogic.com/openjdk. (Both msi and zip formats are supported).
- Copy the downloaded file into the Unified CCE component VMs. *For Example* **C:\UpgradeOpenJDKTool**.
- Download the utility from https://software.cisco.com/download/home/284360381/type/284416107/release/12.5(1) and unzip **OpenJdkUpgradeTool.zip** to any local folder. For example: Download and Unzip under **C:\UpgradeOpenJDKTool**.
- Run **openJDKUtility.exe** from unziped folder For all the supported commands and for more details, refer to the *Readme.html* (which is available as part of the *OpenJdkUpgradeTool.zip*).

  Once the installation is successful, **CCE_JAVA_HOME** is updated and does not trigger the system reboot.

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 9.0 build releases. (That is, only version 9.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 9.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 9.0.21 to 9.0.22. You cannot use this tool for major or minor version upgrades.

  Revert a Tomcat upgrade.

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 9.0.21 to 9.0.22, and then to 9.0.24, the utility reverts Tomcat to 9.0.22.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-9/. Copy the installer onto the Unified CCE component VMs. For Example C:\UpgradeTomcatTool.
- Download the utility zip file, extract it, and run the batch file to upgrade Tomcat.

  Download link: https://software.cisco.com/download/home/284360381/type/284416107/release/12.5(1) If you are in CCE Release 12.5(2), download tomcat utility 12.5(2). Follow steps mentioned in Tomcat Utility 12.5(2) for upgrade or revert options in 12.5(2)

- Delete or back up large log files in these directories to reduce upgrade time:

  <ICM install directory>:\icm\tomcat\logs
  <ICM install directory>:\icm\debug.txt

Related Topics

Tomcat Utility 12.5.2

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: **tomcatutility.bat -upgrade**.

Step 3 When prompted, enter the full pathname of the new Tomcat installer.

For example:

```
c:\tomcatInstaller\apache-tomcat-<version>.exe
c:\tomcatInstaller\apache-tomcat-9.0.21.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: **tomcatutility.bat -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 and Software Updates

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

Assess all security and software update 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 and software update patches. Follow the Microsoft guidelines about when and how you apply these updates.

Note Assess the security exposure of the critical security patches or cumulative updates that are released by Microsoft for Windows Operating System , IIS, and SQL. Apply critical security patches or cumulative updates as you deem necessary for your site.

Refer to *Cisco Customer Contact Software Policy for Third-Party Software/Security Updates* at https://www.cisco.com/c/en/us/products/contact-center/unified-contact-center-enterprise/bulletin-listing.html

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

This section describes the Active Directory Deployment topology. For more detailed Active Directory (AD) deployment guidance, consult the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

While you can deploy your solution in a dedicated Windows Active Directory domain, it is not a requirement. Instead, you can use Organizational Units to deploy security principles. This closer integration with AD and the power of security delegation means that your corporate AD directories can house application servers (for domain membership), user and service accounts, and groups.

Global Catalog Requirements

Contact center enterprise solutions use the Global Catalog for Active Directory. All domains in the AD Forest in which the Unified CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookups, and group lookups.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.

Active Directory Site Topology

In a geographically distributed contact center enterprise solution, you locate redundant domain controllers at each of the sites. You establish a Global Catalog at each site to properly configure Inter-Site Replication Connections. Contact center enterprise solutions communicate with the Active Directory servers that are in their site. This requires an adequately implemented site topology in accordance with Microsoft guidelines.

Organizational Units

Application-Created OUs

When you install the solution software, the AD Domain in which the VMs are members must be in Native Mode. The installation adds several OU objects, containers, users, and groups for the solution. You need delegated control over the Organizational Unit in AD to install those objects. You can locate the OU anywhere in the domain hierarchy. The AD Administrator determines how deeply nested the contact center enterprise solution OU hierarchy is created and populated.

Note 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.

The contact center enterprise installation integrates with a Domain Manager tool. You can use the tool standalone for preinstalling the OU hierarchies and objects required by the software. You can also use it 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.

Active Directory 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.

Related Topics

Windows Server Hardening

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.

For more information about platform requirements for NAP client, see the Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

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 SNMP service. A more secure agent infrastructure replaces the Microsoft 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 usually 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.

Supported Content Security Policy Directives

Content-Security-Policy Directives

Content-Security-Policy (CSP) directives allow you to reduce the risk of XSS attacks by allowing web applications to define the locations from where resources are loaded.

CSP directives are provided in headers to prevent browsers from loading data, from locations other than those specified in the CSP directives.

Supported Content-Security-Policy Directives for Websetup and Diagnostic Portico

CSP directive-name	Description	directive-value
`base-uri`	This directive restricts the URLs which can be used in the <base> element. If this value is absent, then any URI is allowed. If this directive is absent, the user agent will use the value in the <base> element.	'self '
`frame-ancestors`	This directive defines the valid sources for embedding the resource using `<frame> <iframe> <object> <embed><applet>`.	'self '
`default-src`	The `default-src` is the default policy used while loading content such as JavaScript, Images, CSS, Fonts, AJAX requests, Frames, and HTML5 Media.	For **Diagnostic Portico**—'self ', 'unsafe-inline' and 'unsafe-eval' For **Websetup**—'self '

For more information about the browsers that support the Content Policy Headers for Websetup and Diagnostic Portico, see http://3.%20https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP#Browser_compatibility.

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 run 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 93

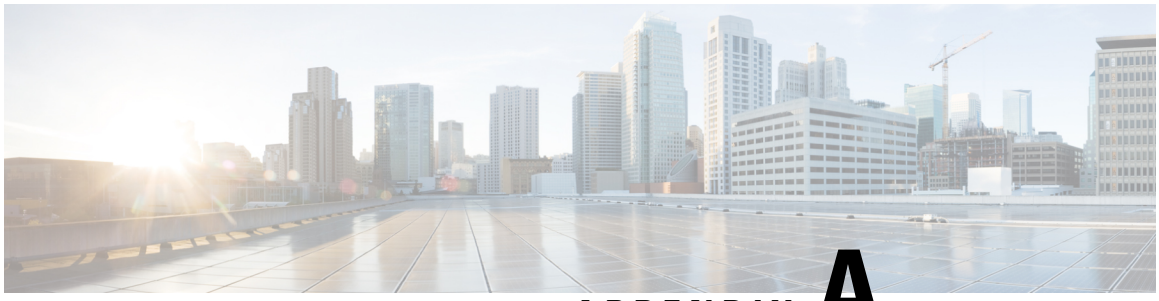
Self-Encrypting Drives

With Unified CCE, you can deploy self-encrypting drives (SED) that have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The encrypting and decrypting of data does not impact overall system performance.

A media encryption key on the disk controls the encryption and decryption of data. A security key also known as the Key-Encryption-Key or Authentication passphrase is used to encrypt the media encryption key. The security key can be provided locally by the user or remotely by using the KMIP server. If you lock the drive, no security key is required to retrieve the data.

For more information on SEDs, see the ***Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide*** https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html.

The drives to be deployed must match the specifications for hard drives mentioned in the Virtualization Wiki. For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.



APPENDIX A

Windows Security Hardening

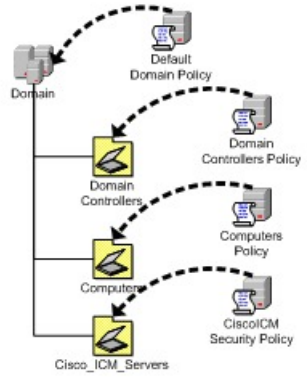
Windows Server Hardening

As a best practice, we recommend using the Microsoft security baseline and CIS benchmarks for secure configuration of ICM servers. Use the latest Microsoft security baseline and Level 1 CIS benchmark profile to lower the attack surface without impacting the functionality and performance.

Apply the security policy in the form of Group Policy Object (GPO) into a separate Organizational Unit(OU) that contains ICM servers. Name the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and ensure to name these servers in accordance with your corporate policy.

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

Figure 7: Group Policy Deployments



After applying the security policy at the OU level, block any differing policies from being inherited at the Unified ICM/Unified Contact Center Enterprise Servers OU. You can override a 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 thought-out design that starts with the most common denominator. These group policies must be restrictive at the appropriate level in the hierarchy.

Cisco Unified Contact Center Enterprise Security Hardening for Windows Server

This section outlines the security baseline that is needed for hardening Windows Servers running ICM servers. This security baseline is essentially a collection of Microsoft group policy settings based on the Microsoft security baseline and Level 1 CIS benchmark profile.

To apply the security baseline in the domain controller, perform the following steps:

1. Download the security hardening templates applicable for the respective Windows version from the Microsoft and CIS benchmark URL. You can download these security hardening templates from https://www.microsoft.com/en-us/download/details.aspx?id=55319 and https://workbench.cisecurity.org/files?q=&tags=3.
2. Install the latest Administrative Templates (ADMX) for the Windows Server. These templates can be downloaded from the Microsoft website at https://www.microsoft.com/en-us/download/details.aspx?id=103667. You can install the `.msi installer` on any Windows node as per your IT policy. The windows server can be ICM or non ICM or Domain Controller.
3. Navigate to the installed location of administrative templates. Copy the below-mentioned template files to the domain controller SYSVOL folder.
   - Copy the *.admx files from the PolicyDefinitions folder to `\<Domain>\SYSVOL<Domain>\Policies\PolicyDefinitions`
   - Copy the *.adml files from the PolicyDefinitions<applicable-language> folder to `\<Domain>\SYSVOL<Domain>\Policies\PolicyDefinitions\en-US`

Note The domain controller automatically copies the admx and adml files to all the domain-joined machines.

Select the applicable language code (en-US) based on your deployment setting.

Create the PolicyDefinitions folder if it does not exist.

4. Create a Group Policy Object in the domain controller using the **Group Policy Management** console and import respective policy using the Import Setting Wizard in the console as per below details. This can be done directly on the ICM nodes based on the IT policy.
   - The downloaded Microsoft baseline (see Step-1) has Group Policy Object (GPO) for Windows Client, Windows Server, Common GPO for both Client and Server, Domain Controller, and Internet Explorer. We recommend you to import the GPO specific to Windows Server, Internet Explorer, and Common GPO for both Client and Server.
   - The downloaded CIS baseline (see Step-1) has GPO for Domain Controller, Microsoft, and User. We recommend importing only the MS-L1 and User-L1 GPO.
5. Create the custom GPO in the Domain Controller to override the policies outlined in the **Security Baseline Policy Exception for ICM**, and import the custom exception GPO using import setting wizard in the console. You can manually override the policies directly on the ICM nodes based on the IT policy.

6. Ensure that the exception policy imported (see Step-5) has higher priority such that the exception policy is applied after the Microsoft and CIS policies are applied.

Note Step 6 is applicable only on domain controllers.

7. Create the OU **Cisco_ICM_Servers** (or a similar identifiable name) under the domain. Map all the ICM machines to this OU. You can perform this step at any point, even before performing Step-1.
8. Link the created GPO (see Step-4 and Step-5) to the OU created (see Step-7).
9. Restart the ICM servers in the organizational unit or run the **gpupdate** command on the respective target ICM nodes to apply the security baseline.

Security Baseline Policy Exception for ICM

The following CIS baseline policies impact the ICM functionality.

The recommended values (outlined in the table below) are to be used for the exception policies to override the recommended values of CIS.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	CIS	Administrators, NT Service/MSSQLServer	The ICM database engine runs as service **MSSQLSERVER**. The **NT SERVICE/MSSQLSERVER** login is used by the service to connect to the database engine. This policy impacts on this connectivity. Hence, include the **NT SERVICE/MSSQLSERVER** setting in addition to the **Administrators** setting.
Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	CIS	Yes	This setting has an impact on operations of duplex CCE systems. For example, it impacts the private interface between the duplex router process.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	CIS	Disabled	This policy impacts the CCE functionality. For example, patch install is impacted. Applications such as snmp, msgagent etc., are blocked. You can enable this only after configuring the appropriate rules under the setting **Configure Attack Surface Reduction rules: Set the state for each ASR rule**. These include adding trusted/known applications with path in the exception list. The list of impacted application differs, so the recommendation is to set the value to **`Disabled`**.
Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days'	CIS	Disabled	Automatic updates interrupt the functionality during automatic restarts.
Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	CIS	Disabled	Automatic updates interrupt the functionality during automatic restarts.
Ensure 'Configure Automatic Updates' is set to 'Enabled'	CIS	Disabled	Automatic updates interrupts the functionality during automatic restarts.
Ensure 'No auto restart with logged-in users for scheduled automatic updates installations' is set to 'Disabled'	CIS	Enabled	Automatic updates interrupt the functionality during automatic restarts.

The following policies are optional. You can enable these policies as per the IT policy after considering the remarks column carefully.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Allow log on locally' is set to 'Administrators'	CIS	BUILTIN\Users, BUILTIN\Administrators	After you apply the policy, the Domain only accounts cannot log in to the machine and perform operations. We recommend you to add **`BUILTIN\Users`** and **`BUILTIN\Administrators`**. You can enable this policy based on the IT policy and operational requirements.
Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only)	CIS	Guests	This policy may have operational impacts specifically for day 0/1 activities. We recommend setting the value to **Guests**. You can override this policy based on the IT policy and operational requirements.
Ensure 'Deny log on through Remote Desktop Services is set to 'Guests, Local account' (MS only)	CIS	Guests	This policy may have operational impacts specifically for day 0/1 activities. We recommend you setting the value to **Guests**. You can override this policy based on the IT policy and operational requirements.
'Prevent ignoring certificate errors' to be set as 'Enabled'	Microsoft	Disabled	CCE web applications such as Websetup cannot be accessed using Internet Explorer. Accessing these web applications with other supported browsers like Mozilla Firefox and Google Chrome will not be impacted due to this policy. We recommend setting the value to **`Disabled`**.
'Turn on Enhanced Protected Mode' to be set as 'Enabled'	Microsoft	Disabled	CCE web applications such as Websetup cannot be accessed using Internet Explorer. Accessing these web applications with other supported browsers like Mozilla Firefox and Google Chrome will not be impacted due to this policy. We recommend setting the value to **`Disabled`**.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only)	CIS	Enabled	This policy has operational impacts. For example, if a member server goes out of domain for any reason, with this policy in place ,we need to use unrecommended safe mode login to add back the member server to the domain. Other operations will have similar impact too.

Enable the following policies after you install the ICM server. Refer to the Remarks column for the deviations observed.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	CIS	Administrators, Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.
Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	CIS	Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.
Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	CIS	Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.

Note The CIS benchmark versions **1.2.1 for Windows Server 2019, version 1.3.0 for Windows Server 2016, Microsoft baseline Windows Server 2019 version 1809, and Microsoft baseline Windows Server 2016 version 1607** are validated. Before applying the higher version of CIS and Microsoft benchmark, analyze the additional policies introduced in the new version for the impact on ICM functionality and performance. We recommend the GPOs must be tailored according to your organization's need. We recommend rolling out the GPOs to a small group of systems, preferably in a lab environment before rolling out into production.

In addition to the GPO settings, disable the following settings in Windows Server:

- NetBIOS
- SMBv1

Windows Security Hardening