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.