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
IPsec with Network Isolation Utility
Window Server Firewall Configuration

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

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