



## Preface

---

This guide describes the Cisco Guard (Guard), how it functions, and how to perform administration tasks.

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

This preface contains the following sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

## Audience

The *Cisco Guard Configuration Guide* is intended primarily for the following audiences:

- Network administrators
- Engineers
- Operators
- Network security professionals

This guide assumes a thorough knowledge of networking and networking security.

# How to Use This Guide

This guide is organized as follows:

Chapter	Description
<a href="#">Chapter 1, “Product Overview”</a>	Describes the Cisco Guard (Guard) and outlines the Guard operation states and components.
<a href="#">Chapter 2, “Initializing the Guard”</a>	Describes the initial procedures required to connect and configure the Guard. The chapter outlines the Guard CLI environment and authentication methods.
<a href="#">Chapter 3, “Configuring the Guard”</a>	Describes how to configure Guard services and access control.
<a href="#">Chapter 4, “Configuring Traffic Diversion”</a>	Describes the zone traffic diversion process and how to configure diversions.
<a href="#">Chapter 5, “Configuring Zones”</a>	Describes how to create and manage zones.
<a href="#">Chapter 6, “Configuring Zone Filters”</a>	Describes the zone filters and how to configure them.
<a href="#">Chapter 7, “Configuring Policy Templates and Policies”</a>	Describes the zone policies and policy templates and how to configure them.
<a href="#">Chapter 8, “Learning the Zone Traffic Characteristics”</a>	Describes the learning process and how to use the learning process to construct and tune the policies that the Guard uses for zone protection.
<a href="#">Chapter 9, “Protecting Zones”</a>	Describes how to configure and activate zone protection.
<a href="#">Chapter 10, “Using Interactive Protect Mode”</a>	Describes the Interactive protect mode and the recommendations, the user decision options, and the policy interactive status.
<a href="#">Chapter 11, “Using Attack Reports”</a>	Describes the attack reports, the report structure, and viewing options.
<a href="#">Chapter 12, “Using Guard Diagnostic Tools”</a>	Describes the Guard diagnostic tools.
<a href="#">Chapter 13, “Performing Maintenance Tasks”</a>	Describes how to perform tasks that are required for Guard maintenance.
<a href="#">Chapter 14, “Analyzing Guard Mitigation”</a>	Describes how to analyze the zone traffic patterns and identify configuration problems. The chapter provides a short explanation on how to identify the type of attack and recommended actions that you can take according to the analysis.
<a href="#">Appendix A, “Understanding Zone Traffic Diversion”</a>	Provides additional information relating to the traffic diversion procedure including sample code lines.
<a href="#">Appendix B, “Troubleshooting Diversion”</a>	Provides information about the traffic diversion troubleshooting procedure with sample screens.

# Symbols and Conventions

This guide uses the following conventions:

Style or Symbol	Description
<b>boldface</b> font	Boldface text indicates commands and keywords that you must enter exactly as shown.
<i>Italics</i> font	Italic font indicates arguments arguments for which you supply the values.
Screen font	Screen font indicates the screen display, such as a prompt, and information that the Guard displays on the screen. Do not enter screen font as part of the command.
[x]	Square brackets indicate an optional element (keyword or argument).
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
[x {y   z}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to select one. If you do, you have some required choices.

This guide uses the zone name *scannet* and the prompt *user@GUARD-conf-zone-scannet#* in examples.

This guide uses the following symbols and conventions to identify different types of information:



## Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



## Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



## Tip

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.



## Timesaver

Means the described action saves time. You can save time by performing the action described in the paragraph.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>