© 2017 Casa Systems, Inc.

All rights reserved. Licensed software products are owned by Casa Systems or its suppliers and are protected by United States copyright laws and international treaty provisions.

The information regarding the product in this manual is subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of the product.

In no event shall Casa or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Casa or its suppliers have been advised of the possibility of such damages.
Table of Contents

1 Syllabus ................................................................................................................................. 1-4
  1.1 Audience .......................................................................................................................... 1-4
  1.2 Topics ............................................................................................................................... 1-4
1 Syllabus

This online course will provide the participant an opportunity to learn Casa Cable Modem Termination System (CMTS) C100 and C40G hardware and software. This course is designed with an emphasis on verifying configurations, diagnostics and troubleshooting.

1.1 Audience

Who should participate?

This course is most appropriate for technical professionals who are not typically implementing configurations but rather are in support of the Axyom Security Gateway such as NOC and support engineers who need to understand how to verify, diagnose and troubleshoot the Casa CMTS after production deployments.

1.2 Topics

- Identify the SeGW’s role at the edge of the Provider’s network
- Discuss SeGW features with the functionality each feature provides
- Specify how the SeGW supports local redundancy
- Specify the definitions of the SeGW’s named interfaces
- Identify the components of the SeGW Configuration Hierarchy
  - Distinguish between multi-use and unique-use Individual Elements
  - Specify the four most important parts of a Crypto Template
  - Identify the two parts of a Crypto Map
  - Specify the components of a Security Policy
  - Identify the two parts of a Security Gateway Service
- Identify the Key Performance Indicators (KPIs) the SeGW supports
- Verify critical configurations with the CLI commands