

Audience

System Engineers, Channel Partners, Service Partners, End Users

Course Description

This class is recommended for all administrators of SonicWALL® Aventail E-Class SSL VPN appliances who need to maintain and monitor a SonicWALL Aventail E-Class SSL VPN appliance. Upon completing the course, students are encouraged to take the Certified SonicWALL System Administrator (CSSA) exam.

The Secure Remote Access Administrator Training Course provides instruction on the administration and management of the E-Class SSL VPN appliance to provide secure, anywhere access to applications and resources for employees, business partners and other users. The course covers using the SonicWALL Aventail Management Console (AMC) to provide users with secure access to any application, from corporate laptops or un-managed computers, based on secure authentication and authorization policies and appropriate End Point Control requirements. Students will also learn how to deploy SonicWALL Aventail Secure Desktop for added security, as well as deploy graphical terminal shortcuts for native Web-based access to Windows Terminal Servers and Citrix server farms.

Pre-requisites

It is assumed that the student will have at least a basic understanding of the technologies being used in their environments or the environments of their customers.

- Basic understanding of networking and networking technologies
- Comfort with basic command-line utilities
- Familiarity with SSL, certificates, and certificate authorities
- Basic understanding of directories (LDAP, Microsoft Active Directory, or RADIUS)
- Basic understanding of VPN technology (IPSec and SSL)

Format

Instructor-led training with emphasis on hands-on exercises.

Course Description

3 Day Course: 8:30am-5:00pm



Secure Remote Access Administrator Training v.9

Table of Contents

Section 1: Course Introduction

Section 2: Introduction and Architectural Overview: includes top-level information about SSL VPNs, the different appliance models, and an overview on the SonicWall Aventail Management Console (AMC), WorkPlace, mobility, end point control, certificates, and firewall policies.

Section 3: General and Network Settings: includes creating administrator accounts and roles, managing product licensing, network configurations, DNS settings, gateway routing, and the process of creating and installing SSL certificates and CA certificates.

Section 4: Authentication Servers: includes setting up Active Directory, LDAP, RADIUS, and Public Key Infrastructure authentication servers, as well as defining advanced settings such as Active Directory and LDAP over SSL, password management, NTLM authentication forwarding, and using customized authentication prompts.

Section 5: User Management: includes setting up realms and using chained authentication, creating references to users and groups (including using dynamic groups and nested groups), and defining communities for group organization.

Section 6: Resources and Access Control Rules: includes defining different resource types and creating resources within AMC. In addition, access control rules are covered in detail, including defining different connection types and both basic and advanced access control rule settings.

Section 7: End Point Control: includes an overview of using end point control for data and network protection, using Standard, Quarantine, and Deny zones to classify a user's end point, and creating device profiles to define the attributes of a zone (including device watermarking). Also, data protection agents are covered, including SonicWALL Aventail Cache Control and SonicWALL Aventail Secure Desktop as well as client integrity agents, including a virtual keyboard.

Section 8: WorkPlace Portal: includes using the WorkPlace portal for creating personalized user access to resources, customizing WorkPlace sites and using multiple WorkPlace site certificates, creating and modifying WorkPlace shortcuts including graphical terminal shortcuts and support for Citrix server farms.

Section 9: Access Methods: includes configuring access methods for both managed and non-managed devices, mobile devices, and for access to Web applications, client/server applications, and full network access. Included in this section is using static, dynamic, and secure NAT IP address pools for tunnel clients, configuring auto-updating for Connect Tunnel clients, and post-connection scripting for all tunnel clients.

Section 10: System Administration: includes performing basic maintenance in AMC, such as shutting down and upgrading the appliance, as well as backups and restores through the command-line utilities and the UI. In addition, working with system log files and monitoring tools, and capturing network traffic is covered. A checklist of security best practices is also covered.



Secure Remote Access Administrator Training v.9

Student Assessment

Formative evaluations (knowledge checks and hands-on exercises) are incorporated throughout the course, and the last 2 hours of day three is reserved for an online certification exam. Any participant who successfully completes this course and passes the certification exam will be deemed a Certified SonicWALL System Administrator (CSSA).

The exam is administered in the class by the instructor at the end of the 3-day course. 120 minutes are allotted for 55 questions. A passing score is 75% or higher.

At the end of the exam you are immediately notified of your exam score and if you passed or failed the exam. Upon successfully passing the exam you will be sent an e-mail containing your CSSA certificate. In addition, you can view your certification details, such as the certification expiration date, on MySonicWALL. You can also print your certificate and access the CSSA certification logo for use on your business cards, e-mail signatures, and resume.

Registration

For end-users, log in to training.sonicwall.com for an updated schedule, pricing information, and to purchase a class. SonicWALL partners can access this information on PartnerLink.

For additional information, contact training@sonicwall.com.

Student Quotes

"This is hands-down the most well planned and organized training class I have ever attended. Aventail has succeeded in training where larger companies like Oracle have failed."

"The content of the courseware is great, and the hands-on exercises are perfect for me to refer to when I start making changes to my Aventail appliance."

"Great presentation. Any questions the instructor couldn't answer, he contacted an Aventail engineer and followed up with us. The exercises are very well prepared and covered all uses of the appliance in great detail. This course has helped me understand my company's current VPN setup better as well as given me multiple new ideas on how we can better secure and limit our remote access."

"Information was well presented. Application and PowerPoint slides were thorough and went along with the training guides and corresponded with correct chapters. Every administrative topic was covered. The ability of using VMware was a great idea."

