Training Catalogue

Product Training

Partner Training

Inhaltsverzeichnis

Training Courses

To enable you to use our security solutions professionally, we offer a training program for all genua products. The mode of operation is covered in detail, and all questions concerning installation and ongoing maintenance are handled.

To assure the best learning effect, the maximum number of participants is limited to twelve, eight or 6 participants, depending on the course. The training takes place in our well-equipped training rooms in Kirchheim near Munich, Germany. genua can be easily reached by car and public transportation. Several hotels and restaurants are in the vicinity of our office.

Current training dates are published on our homepage:

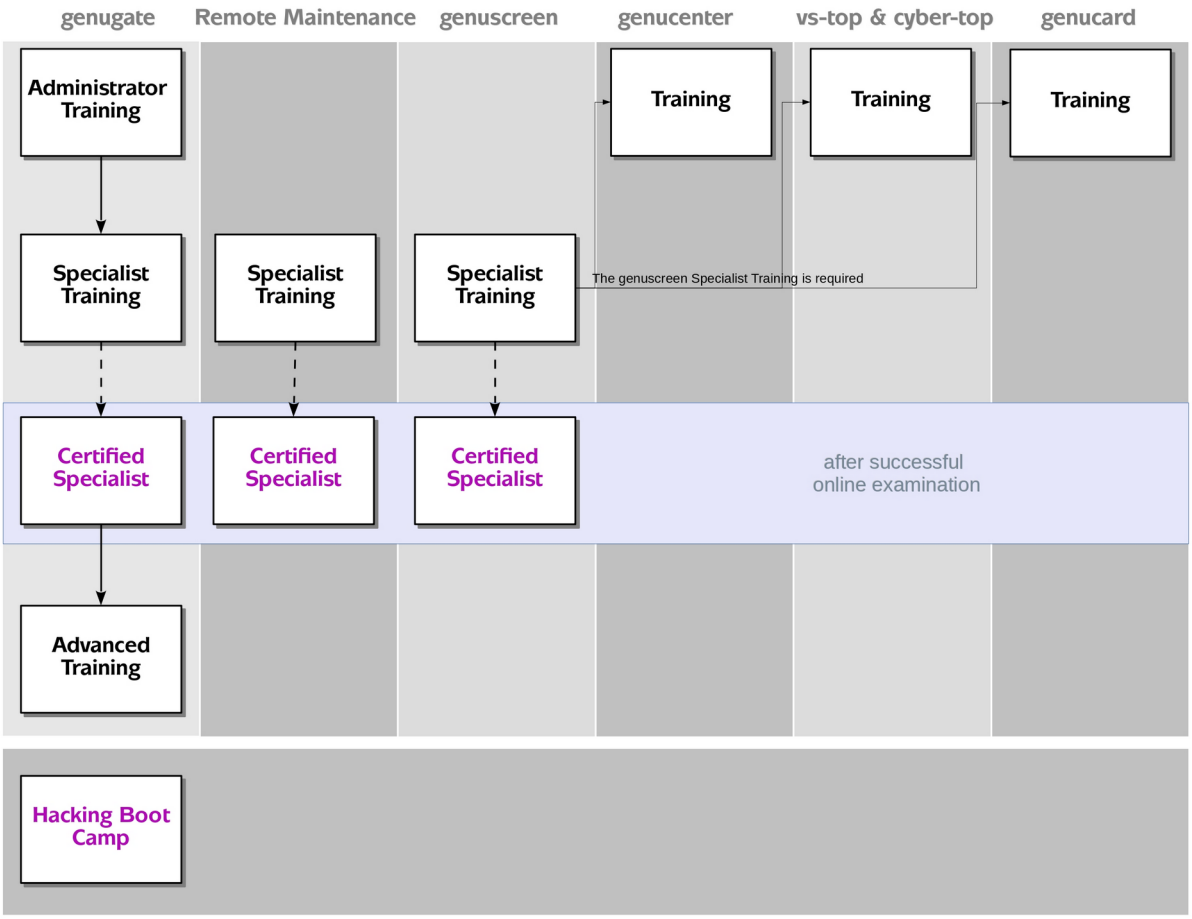
https://www.genua.de/loesungen/trainings-bootcamp/alle-termine.html

You can register for a course directly on our website, use the fax enclosed reply form, or contact your genua partner.

The following pages provide an overview of training content, and the terms and conditions.

We are looking forward to see you at the genua training facilities!

1 Overview


genugate
Remote Maintenance
genuscreen
genucenter
vs-top & cyber-top
genucard
Administrator Training
Specialist Training
Specialist Training
Specialist Training
Training
Training
Training
The genuscreen Specialist Training is required
Certified Specialist
Certified Specialist
Certified Specialist
after successful online examination
Advanced Training
Hacking Boot Camp

2 Product Training

2.1 genugate Administratior Training

The high resistance firewall genugate ensures maximum security at interfaces based on the two-tier firewall system. The genugate system has also been accepted by the Federal German Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and certified as meeting the strict EAL 4+ level Common Criteria (CC) requirements. In addition, genugate has been classified as “Highly Resistant” due to its extremely high resistance against direct attacks – the security it provides corresponds with the requirements of the EAL 7 level. genugate is the only firewall in the world that offers such a high level of security.

In this course, setup and functionality of genugate are presented. The numerous possibilities for configuration and run time system supervision are reviewed in detail.

Contents:

- genugate layout and functions
- System administration of the application level gateway
- System administration of the packet filter
- genugate user administration
- Connection concept
- Statistics and log files
- WWW
- Mail

Participants:	Administrators, data protection officers and other employees who install, configure and manage genugate systems
Necessary prior knowledge:	Good knowledge of UNIX, TCP-IP and the administration of complex network environments
Duration:	2 days, 9 am to 5 pm
Number of participants:	8

2.2 genugate Specialist Training

The high resistance firewall genugate ensures maximum security at interfaces based on the two-tier firewall system. The genugate system has also been accepted by the Federal German Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and certified as meeting the strict EAL 4+ level Common Criteria (CC) requirements. In addition, genugate has been classified as “Highly Resistant” due to its extremely high resistance against direct attacks – the security it provides corresponds with the requirements of the EAL 7 level. genugate is the only firewall in the world that offers such a high level of security.

In the specialist course, the genugate options HA and VPN in the DMZ, as well as of complex firewall installations are presented. The course is complemented by practical exercises and strategies for troubleshooting a running system.

Contents:

- Installation
- Troubleshooting
- Installation and management of an HA system (OSPF)
- Installation and management of an HA system (CARP)
- Working with an HA system
- VPN in the DMZ
- Disaster Recovery
- IPv6

Participants:	Administrators, data protection officers and other employees who install, configure and manage genugate systems
Required training:	genugate administrator training
Duration:	3 days, 9 am to 5 pm
Number of participants:	8

After the course, we offer an online examination. After completing the test successfully, you will receive the certificate *Certified genugate Specialist*.

2.3 genugate Release Training

We are constantly updating and developing our IT security solutions. Refresher courses on new product features and their best use are available on a regular basis. All updates and new features are demonstrated in a hands-on seminar that also is the best preparation for our online exam. Customers and partners may join us to test their knowledge and receive a product certificate.

Participants:	Administrators who already use the genugate system, and want to learn about the newest version features and renew certification
Required training:	genugate administrator training
Duration:	1 day, 9 am to 5 pm
Number of participants:	8

2.4 genugate Advanced Training

The high resistance firewall genugate ensures maximum security at interfaces based on the two-tier firewall system. The genugate has also been accepted by the Federal German Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and certified as meeting the strict EAL 4+ level Common Criteria (CC) requirements. In addition, the genugate has been classified as “Highly Resistant” due to its extremely high resistance against direct attack – the security it provides corresponds with the requirements of the EAL 7 level. The genugate is the only firewall in the world that offers such a high level of security.

This course presents installation, configuration, and administration of the high resistance firewall genugate in extensive operational environments. Core topics are the SSH relay, the DNS concept, and SNMPv3.

Contents:

- SSH relay
- Protocol conformity filter PCF
- DNS concept with unbound and NSD
- Link Aggregation
- SNMPv3
- Radius and LDAP
- Nagios and Zabbix
- Logging and system monitoring
- IPv6

Participants:	Administrators, data protection officers and other employees who install, configure and manage genugate systems in complex environments
Necessary prior knowledge:	genugate administrator training
Duration:	2 days, 9 am to 5 pm
Number of participants:	8

2.5 Remote Maintenance Specialist Training

The genubox security platform offers intelligent remote services at any location. The appliance initializes encrypted VPN tunnels over the Internet to the managed servers for the exchange of data, and offers an integrated application platform. This platform supports the implementation of custom applications that can be executed remotely to monitor, remote control and maintain machinery such as robotic automation systems, printing machines or diesel engines of ships.

Setup and operation of the genubox are presented clearly and concretely. Installation, management via the server, and updates are explained step-by-step. Interesting examples are an important part of this course.

Contents:

- Installation
- genubox layout and functions
- System administration using genucenter or the standalone GUI
- Firewall and VPN configuration
- Configuration of a remote maintenance solution via genucenter (rendezvous)
- Modules

Participants:	Administrators who install, configure and manage the genubox in complex environments, or design their use
Necessary prior knowledge:	Good knowledge of UNIX, TCP-IP, and the administration of complex network environments
Duration:	2,5 days, 1 pm to 5 pm and 9 am to 5pm
Number of participants:	8

After the course, we offer an online examination. After completing the test successfully, you will receive the certificate *Certified Remote Maintenance Specialist*.

2.6 genuscreen & genucrypt Specialist Training

With the stateful packet filter genuscreen you can guard your network securely from the outside world, and in addition protect particularly sensitive systems within corporate networks. Typically, this powerful firewall will be added as a bridging firewall to existing networks and implement security zones: All incoming traffic will be analyzed, and only explicitly permitted connections will be transmitted.

The VPN appliance genucrypt enables confidential communication over public networks. The appliance encrypts the data, and establishes secure connections known as VPN (Virtual Private Networks) tunnels. This method also securely transfers highly sensitive information between distributed locations, with powerful encryption techniques guaranteeing confidentiality.

Product layout and functions are presented in this course. You will install, configure and administer the appliance. We will demonstrate how to administer multiple machines comfortably with the Central Management Station genucenter.

Contents:

- genuscreen installation
- Layout and functions of genuscreen/genucrypt
- System administration using the standalone GUI
- Firewall and VPN configuration
- Configuration of L2TP connections
- SNMPv3
- HA operation
- Installation and configuration of genuscreen plus
- genucenter overview

Participants:	Administrators and other employees who install, configure and manage genuscreen/crypt systems in complex environments or plan their use
Necessary prior knowledge:	Good knowledge of UNIX, TCP-IP, and the administration of complex network environments
Duration:	1.5 days, 9 am to 5 pm and 9 am to 2 pm
Number of participants:	8

After the course, we offer an online examination. After completing the test successfully you will receive a certificate *Certified genuscreen Specialist.*

2.7 genucenter Training

genua security solutions can be configured, administrated and continuously monitored via the integrated genucenter Central Management Station GUI. Using this overview, it is easy to keep an eye on your IT security and make sure all systems are up-to-date and running flawlessly. Modifications and updates can be simultaneously transferred to any number of systems using the convenient group functionality. Thus, policies can be consistently implemented in the entire network. New additions to your IT security environment are easily integrated by the Central Management Station, and immediately set up with an established configuration.

To acquaint you with the new features of genucenter 4.2, we offer one-day genucenter training courses. Product layout and functions are presented. You will install, configure and administer the appliance. In addition to the new GUI, we also demonstrate the new genucenter high availability concept.

Contents:

- genucenter layout and functions
- New GUI
- Use of filters
- VPN definitions
- Disaster recovery with genucenter
- High availability with genuscreen

Participants:	Administrators and other employees who install, configure and manage genuscreen/ crypt systems in complex environments or plan their use
Required training:	genuscreen & genucrypt specialist training
Duration:	1,5 days, 2 pm to 5 pm and 9 am to 5 pm
Number of participants:	8

2.8 genucard Training

A “restricted” VPN solution as certified by the BSI can be implemented in a setup with the mobile security device genucard, the firewall & VPN appliance genuscreen and the central management station genucenter.

Transmitted data will be protected by strong encryption algorithms. In this course, the administration of genucards and genuscreens using genucenter and smartcards is presented.

Contents:

genucenter layout and functions

- New GUI
- Use of filters
- VPN definitions
- Disaster recovery with genucenter
- High availability with genuscreen
- VS-NfD (“confidential/restricted”) conformity
- Introduction to smartcards

genucard

- Basics
- Installation and configuration
- Test setups
- Using smartcards

Participants:	Administrators and other employees who install, configure and manage VPN installations in complex environments or plan their use.
Required equipment:	Own laptop (Linux or Windows 7 (2x USB, 1x Ethernet) for connecting the genucard (No Apple MAC, please)
Required training:	genuscreen and genucrypt specialist or genubox specialist training
Duration:	3,5 days, 2 pm to 5 pm and 9 am to 5 pm
Number of participants:	6

2.9 vs-top & cyber-top Training

The Security Laptop can be installed and operated with a setup consisting of the Security Laptop, the genuscreen Firewall & VPN Appliance, and the Central Management Station genucenter.

Transmitted data will be protected by strong encryption algorithms During this course you will learn how to securely install and operate the Security Laptop via genucenter (with practical exercises).

Contents:

genucenter Basics:

- Menu structure
- Creating new appliances (genuscreen, Security Laptop)
- VPN basics
- Packet filter rules
- Connection and access profiles
- Friendly Net Detection (FND)
- VS-NfD (“confidential/restricted”) conformity
- Introduction to smart cards

Security Laptop:

- Differences between vs-top and cyber-top
- HW architecture and L4 basics
- Installation of the laptop and setting up the compartments
- FND
- franzi – framebuffer display
- vroni – control for the firewall and VPN compartment
- Troubleshooting

Participants:	Administrators and technicians responsible for the installation and operation of Security Laptops who provide end-user support or who are planning to use the Security Laptops
Required training:	genuscreen and genucrypt Specialist or Remote Maintenance Specialist Training
Duration:	3,5 days, 2 pm to 5 pm and 9am to 5pm
Number of participants:	6

3 Hacking Bootcamp

In the *Hacking Bootcamp*, network administrators learn about the methods of hackers, and the most important issues in securing a system. The techniques demonstrated of course may not be used to attack or spy on others. Therefore every participant must sign a corresponding declaration of commitment included with your order confirmation.

Contents:

Acquiring Information: Methods how to acquire information for use in a subsequent attack.

Sniffing methods: How to trace and analyze the data stream of a network by simple means.

Cracking passwords: Many passwords can be easily cracked – see for yourself!

Scanning: Use different programs to search for open resources in our test network for use in an attack. Several types of scanning are explained.

Exploits: Specific attacks, such as exploiting buffer overflows, denial-of-service attacks, using manipulated Web sites or taking over connections.

Rootkits: Programs frequently installed by attackers in successfully hijacked systems. Learn what rootkits contain, what they exactly do, how to install, and how to identify them.

WaveLAN: The design of wireless networks, WEP encryption and associated problems is presented. Furthermore, the special denial-of-service attack concerning the 802.11 protocol is discussed in detail.

Participants:	Firewall administrators and all interested in techniques and methods to attack systems
Necessary prior knowledge:	Good knowledge of UNIX and TCP/IP
Required equipment:	Own laptop
Duration:	3 days, 9 am to 5 pm
Number of participants:	12

4 Training für genua Partners

4.1 genua Product Fundamental Training (GPFT)

This course to certify as a *Certified genua Partner* addresses employees and technical staff in sales and distribution. We at genua believe that sales staff should have basic technical knowledge, and that technical staff should know about important sales-oriented aspects.

Contents:

Sales:

- Introduction to the genua product family and services in the consulting environment
- talking points
- license and export regulations

Project planning and tender planning:

- Evaluation of the desired security level
- typical examples of network structures
- preparation of offers to tender
- approaches to complex solutions

Participants:	Sales and technical staff in charge of genua products.
Necessary prior knowledge:	Basic knowledge of UNIX and TCP/IP
Duration:	1 day, 9 am to 5 pm
Number of participants:	12

5 Application

Training:	
Date:	

Hereby I accept the conditions for participation in the genua GmbH training course selected above. I understand that enrollment in the course is legally binding.

Please enter in upper case and print clearly:

Name			
Company			
Adress			
Zip code and City			
Phone			
Location, Date		Signature	

GL-WP-0520-09-D

Contact:

genua GmbH, Domagkstrsse 7, 85551 Kirchheim near Munich, Germany
phone +49 89 991950-303, fax +49 89 991950-999, training@genua.de,
www.genua.de

6 Terms

The following terms and conditions apply to genua training courses for end customers and sales partners:

1. The number of participants is limited for each course. Available seats are assigned in the order of written registration. To register, please contact genua or your genua sales partner two weeks before the course at the latest. Your registration will either be con firmed, or in case of overbooking you will be noti fied.
2. In case the minimum number of registrations is not reached, genua reserves the right to cancel a course up to seven days beforehand without incurring any liabilities. Registered participants may cancel up to two weeks beforehand and receive a full refund. A later cancellation will incuradministrative charges of 50% of the course fee.
3. The course fee covers: the course itself, all necessary infrastructure, training materials, lunch and beverages.
4. genua reserves the right to modify technical course content to a reasonable extent without advance notice.
5. Smoking is not permitted on genua premises. However, smoking is possible during breaks outside of the building.
6. With the training goals in mind, genua asks all participants to be punctual and attend the course in its entirety. Participants receive written con firmation of attendance on completion of the course. This con firmation will not be issued in case of participation of less than 50% of the course duration. In case of a partner training course, the partner certi ficate will only be issued if at least 90% of the course duration was attended.
7. Course fees are due two weeks in advance.

As of July 2015

Terms and Conditions for genua GmbH Training