

Secure System Configuration Guide

Fiber Service Platform 3000R7

Product Release: 22.2

Document Issue: A

Document Number: 80000073674

 **ADVA**[™]
An Adtran Company

Copyright © 2001-2023 Adtran Networks SE. All rights reserved.

Adtran Holdings, Inc.
901 Explorer Blvd.
Huntsville, AL 35806
USA

Adtran Networks SE, formerly known as ADVA Optical Networking SE (an Adtran company)
Campus Martinsried
Fraunhoferstrasse 9a
82152 Martinsried/Munich
Germany

Terms of Use ("Terms"):

Acceptance of Terms

By using this content, including without limitation any services, portals, webpages, manuals, documentation and any other information provided herein (hereinafter referred to as "Content" and/or "Service"), you assent to the following terms of use. If you do not agree to these terms, please do not use this Content.

If you are using this Content on behalf of your employer/hirer/contractor, you represent and warrant that you are authorized to accept these Terms on your employer's/hirer's/contractor's behalf.

Use of the Content and Service

You agree not to access the Content by any means other than through the interface that is provided by Adtran Networks SE. Adtran Networks SE, formerly known as ADVA Optical Networking SE, includes its affiliates and successors ("Adtran"). You will not use the Service for any purpose that is unlawful or prohibited by these Terms. You may not use the Service in any manner that could damage, disable, overburden, impair, or otherwise result in unauthorized access to or interference with, the proper functioning of any Content, accounts, systems, networks of Adtran or its licensor(s).

If parts of the Content (including without limitation service) require you to open an account, to choose a password and/or a user name, you are entirely responsible for maintaining the confidentiality of your password and account, and for any and all activities that occur under your account. You will maintain and promptly update your account and any information you provide to Adtran to keep it accurate, current and complete.

You will notify Adtran immediately of any unauthorized use of your account or any other breach of security. Adtran will not be liable for any losses you incur as a result of someone else using your password or account, either with or without your knowledge. However, you could be held liable for losses incurred by Adtran due to someone else using your account at any time, without the permission of the account hold.

You may obtain direct access via the Content (including without limitation portal or system) to certain confidential information of Adtran and its suppliers and contractors, including without limitation technical, contractual, product, delivery, pricing, marketing and other valuable information that should reasonably be understood as confidential ("Confidential Information"). You must hold Confidential Information in strict confidence. Title to Confidential Information remains with Adtran or its respective suppliers and contractors.

No Warranties

ALL CONTENT IS PROVIDED ON AN "AS IS AVAILABLE" BASIS WITHOUT ANY WARRANTY OF ANY KIND EITHER EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ADTRAN MAKES NO WARRANTY AS TO THE ACCURACY, COMPLETENESS, OR RELIABILITY OF ANY CONTENT AVAILABLE HEREIN. USE OF THE CONTENT IS AT YOUR SOLE RISK. YOU ARE RESPONSIBLE FOR VERIFYING ANY INFORMATION BEFORE RELYING ON IT AND FOR TAKING ALL NECESSARY PRECAUTIONS TO ENSURE THAT CONTENT IS FREE OF VIRUSES. The content of this document may include technical inaccuracies or typographical errors. Adtran may make changes at any time to the Content (including without limitation portals, systems, products or specifications) without notice and makes no commitment to update Content.

Adtran may provide economic projections and forward-looking statements on this Content (including without limitation on portals or systems) that relate to future facts. Such projections and forward-looking statements are subject to risks which cannot be foreseen and which are beyond the control of Adtran. Adtran is therefore not in a position to make any representation as to the accuracy of economic projections and forward-looking statements or their impact on the financial situation of Adtran or the market in the shares of Adtran.

Limitation of Liability

IN NO EVENT SHALL ADTRAN NETWORKS SE OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THE ACCESS OR USE OF THE CONTENT (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND BASED ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE), EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE SAME APPLIES FOR ANY HARDWARE OR SOFTWARE INCLUDED IN THE CONTENT, UNLESS A SIGNED AGREEMENT WITH ADTRAN NETWORKS SE OR ITS AFFILIATE(S) OR THE APPLICABLE PRODUCT LIABILITY LAW EXPRESSLY STATES OTHERWISE.

Trademarks and Copyright

Documents and information, including text, images, graphics, sound files, animation files, video files and their arrangement made available in the Content (including without limitation the portal or system) are subject to copyright and other intellectual property protection. They may not be copied for commercial use or distribution and may not be modified or reposted to other internet sites.

Unless otherwise indicated, all marks displayed on the Content (including without limitation portals) are subject to the trademark rights of Adtran Networks SE or the respective trademark owner. Adtran Networks SE and the Adtran Networks SE Logo are trademarks or registered trademarks of Adtran Networks SE in Germany and other countries.

Any software that is made available for download from the Content ("Software") is a copyrighted work of Adtran or the respective copyright owner.

The furnishing of this content does not give you any license or rights with respect any content, patents and/or trademarks herein, unless the Content (including without limitation software) is governed by the terms of your

signed agreement with Adtran. Any reproduction or redistribution of the Content (including without limitation Software) not in accordance with the foregoing is expressly prohibited.

Third Party Content

Third-party content is the property of their respective owners and does not imply a partnership between Adtran and any other company. Any references to content that is not from Adtran are provided for convenience only and do not in any manner serve as an endorsement of that content.

Software generally known as "open source software" is licensed pursuant to the applicable license terms, accessible under the following link: <https://advadocs.com/webhelp/4237/Default.htm>. The copyright owners of such software disclaim all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose, and all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits.

Export Controls

The Content (including without limitation service, Software, or technology derived or obtained from the portals) may be subject to the export control laws and/or the import laws of various country ("Controlled Items"). This includes without limitation the export control laws and regulations of Germany, the European Union, and the United States. You agree to comply strictly with all such laws. In particular, you will not use, distribute, transfer or transmit the Controlled Items (even if incorporated into other products) except in compliance with such laws. You are also responsible for complying with all applicable legal regulations of the country where you are registered, and any foreign countries with respect to the use of the Controlled Items by you, your affiliates, subsidiaries, directors, employees, authorized users and permitted third parties, including end-users. Adtran will support you in obtaining any necessary export or import license for Controlled Items. You agree that none of the Controlled Items will be sold or otherwise transferred to, or made available for use by or for, any entity that is (a) named on the EU, U.S. or other government-issued Sanctioned Party Lists (Denied Party List, Restricted Party, etc.) or (b) engaged, directly or indirectly, in the design, development, production, stockpiling, or use of chemical or biological weapons, nuclear programs (including activities related to nuclear devices, nuclear reactors, and nuclear fuel-cycle activities), missiles and maritime nuclear propulsion projects, except as authorized under applicable laws and regulations.

You agree that, in the event you are notified by Adtran, a third party or a governmental agency about a license requirement for Controlled Items or particular transactions, you will not export or re-export the Controlled Items or pursue the transactions, directly or indirectly, until the required licenses are obtained, and work with Adtran, the third party or the governmental agency to procure the required licenses.

You agree to indemnify and hold harmless Adtran in the event of your non-compliance with any applicable German, EU, and U.S. export control laws and the export controls or import laws of other countries.

Governing Law and Place of Jurisdiction

The Content and any dispute arising out of or in connection with this Content is governed by German Law, without its choice of law provisions and the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded. The District Court of Munich has exclusive jurisdiction for any dispute arising out of or in connection with this Content.

Privacy Statement

All terms related to our privacy information are available at: <https://www.adva.com/en/about-us/legal/privacy-statement>

All terms related to our privacy information for Customer Portal users are available at: <https://advaoptical-communities.force.com/customerportal/CustomerPortalTCs>

Contents


Preface	8
Safety Symbol and Message Conventions	8
Documentation	10
FSP 3000R7 Documentation Suite	10
Accessing Documentation	11
Documentation Feedback	11
Obtaining Technical Assistance	11
Customer Portal	11
Technical Services	12
Call ADVA	12
Introduction	13
Overview	13
Physical Security	14
Network Security	14
Deliverable Verification Procedure	14
Security Maintenance	15
Secure Configuration	16
Updating Software	17
Changing the Password at First Login	18
Enabling Password Restrictions	19
Configuring New User Accounts	19
Configuring Mutual Authentication	22
Disabling Bootloader Access	23
Enabling Remote Authentication	23
Disabling Insecure Protocols	23
Disabling Telnet	24
Disabling FTP	24

Disabling HTTP redirection to HTTPS	24
Disabling TL1	24
Disabling SNMPv1/SNMPv2c	25
Disabling GNMI	25
Configuring a Security Banner	25
Disabling Older Versions of TLS	25
Configuring Remote SysLog	26
Configuring Audit Events	26
Configuring Packet Filtering	26
Configuring Whitelist	27
Configuring DoS Protection	27
Configuring the ICMP Filter	27
Disabling Serial Port Access	28
Regenerating the SSH Host Key	28
Regenerating the SSL Certificate	28
Configuring the PKI Certificate	29
Configuring the NTP Server	30
Disabling Login Presentation	30
Configuring Last Successful Login Display	31
Configuring Last Failed Login Display	31
Configuring Login Failure Delay	31
Disabling Requests for User Privilege Upgrade	31
Configuring TLS Ciphers	32
Configuring SSH Ciphers	32
Checking Open Ports	32
Configuring Control Plane Interfaces	34
Running Self-Test	34
Debugging and Diagnostic Tools	35
SSH and SSL	38
SSH Algorithms	38
Supported Host Key Algorithms	38
Recommended SSH Host Key Algorithms	38
Supported SSH Key Exchange Algorithms	39
Recommended SSH Key Exchange Algorithms	39
Supported SSH Encryption Algorithms	39
Recommended SSH Encryption Algorithms	39
Supported SSH Message Authentication Code Algorithms	40

Recommended SSH Message Authentication Code Algorithms	40
SSL Ciphers	40
Supported SSL Ciphers	40
Recommended SSL Ciphers	41
Root Rights	43





Preface


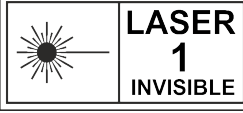






Safety Symbol and Message Conventions	8
Documentation	10
Obtaining Technical Assistance	11





	<p>The pictures or graphics shown in this document are for reference only. They are based on the latest hardware revision available at the time of publication. The equipment you received might look different than pictures or graphics shown in this document.</p>
---	---

Safety Symbol and Message Conventions

You will see these symbols throughout the documentation. All personnel should correctly follow and not ignore any safety instructions.

Icon	Meaning	Description
	Warning	Means danger and alerts you to a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved and be familiar with standard practices for preventing accidents.
	Electric Voltage Warning	Means danger and alerts you to risks caused by electricity that could result in death or serious injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.
	Shock hazard warning. Disconnect all power plugs.	Indicates that all power sources must be disconnected before servicing to avoid shock hazard.
	Laser Radiation Warning	Warns you about the risk of possible laser radiation, which may result in a serious eye injury.

Icon	Meaning	Description
	Laser Radiation Warning – Hazard Level 3B	Warns you about the risk of possible laser radiation if the system is not used as designed or altered in any way.
	Laser Radiation Warning — Class 1 Laser	Warns you that the equipment contains Class 1 lasers, which are safe under all normal use conditions. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.
	Laser Radiation Warning – Class 1M Laser	Warns you that the equipment contains Class 1M lasers, which are safe for all conditions of use except when the beam is passed through magnifying optics. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.
	Laser Radiation Warning – Hazard Level 1M	Warns you that the equipment contains Class 1M lasers, which are safe for all conditions of use except when the beam is passed through magnifying optics. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.
	Caution	Alerts you to a potentially hazardous situation or condition that may result in minor or moderate injury.
	Lifting Hazard Caution	Indicates a potentially hazardous situation or condition that may result in a personal injury or damage to equipment due to the weight of an object.
	Skin Burn Caution	Indicates the risk of possible skin burns. When working with system components, be aware of proper handling procedures.
	Electrostatic Caution	Indicates the possibility of equipment damage due to electrostatic discharge (ESD). If the ESD-prevention instructions are ignored or not followed correctly, damage can occur.

Icon	Meaning	Description
	Notice	Indicates the risk of equipment damage, malfunction, process interruption, or negative impacts on surroundings.
	Documentation	Advises of the importance of carefully reading all instructions before proceeding or provides links to additional information to read. Failure to do so may result in personal injury or damage to equipment.
	Waste Disposal Alert	Points out the importance of properly disposing of waste electrical or electronic equipment and its components. Disregard of the instruction can threaten the environment.
	Note	Indicates supplemental information or helpful recommendations.

Documentation

FSP 3000R7 Documentation Suite	10
Accessing Documentation	11
Documentation Feedback	11

FSP 3000R7 Documentation Suite

- FSP 3000R7 Hardware Description
- FSP 3000R7 High-Density Subshelf Guide
- FSP 3000R7 Installation and Commissioning Manual
- FSP 3000R7 Maintenance and Troubleshooting Manual
- FSP 3000R7 Management Data Guide
- FSP 3000R7 Module and System Specification
- FSP 3000R7 NETCONF User Guide
- FSP 3000R7 Network Element Director
- FSP 3000R7 Provisioning and Operations Manual
- FSP 3000R7 Safety Guide
- FSP 3000R7 Secure System Configuration Guide

- FSP 3000R7 TL1 Commands and Syntax Guide
- FSP 3000R7 TL1 Maintenance and Troubleshooting Manual
- FSP 3000R7 TL1 Module Parameters Guide

Accessing Documentation

Documentation Portal	https://docs.adtran.com/
-----------------------------	---

Documentation Feedback

We want our documentation to be as helpful as possible. Feedback is always welcome.

Email	admin@advadocs.com
--------------	--

Obtaining Technical Assistance

Product Maintenance Agreements and other customer assistance agreements are available for ADVA products through your ADVA distribution channel. Our service options include:

- 24 x 7 telephone support
- Web-based support tools
- On-site support
- Technical training, both on-site and at ADVA facilities in Germany and the USA
- Expedited repair service
- Extended hardware warranty service

Customer Portal

You can use the customer portal to:

- Access company information and resources at any time.
- Find information specific to your requirements, such as networking solutions, services, and programs.
- Resolve technical issues by using online support services.
- Download and test software packages.
- Order ADVA training materials.

Access	https://www.adva.com/en/customer-portal
Questions	customer-portal-admin@adva.com

Technical Services

Technical services are available to customers who need technical assistance with an ADVA product that is under warranty or covered by a maintenance contract.

Online	https://www.adva.com/en/about-us/contact
Email	support@adva.com

Call ADVA

Europe, Middle East and Africa
Martinsried/Munich, Germany
+49 (0)89 89 06 65 0

North America
Norcross, GA, USA
+1 678 728 8600

Chapter 1

Introduction

Secure System Configuration Guide is valid as long as the customers configure products according to the secure configuration guidance. All the security test cases (positive and negative) have to be executed on a product provisioned according to the secure configuration guidance.

If the product is not provisioned according to the Secure System Configuration Guide then it may be unnecessarily exposed to the security vulnerabilities. The provider of the products may revoke the warranty, because they cannot be responsible then for the threats concerning the security issues, and other elements that can break or destroy the products, or related systems.

This section contains these topics:

Overview	13
Physical Security	14
Network Security	14
Deliverable Verification Procedure	14
Security Maintenance	15

Overview

Before you use the FSP 3000R7, configure it according to the FSP 3000R7 Secure System Configuration Guide.

To protect FSP 3000R7, an administrator uses a private key, or credentials, to access the platform. You must protect this private key on any other platform where these credentials reside. The only general-purpose computing capabilities available on the FSP 3000R7, such as compilers or user applications, are those services necessary to operate, administer, and support the FSP 3000R7. Other security and assurance measures within the operational environment most likely provide traffic protection.

The scope of protection by the FSP3000R7 is to safeguard data that originates from the shelf or that the device itself will use, including administrative and audit data. The network environment provides physical security that is appropriate to the integrity of the FSP 3000R7 and its data.

Physical Security

ADVA FSP3000 shelf is designed for use and deployment in a typical data center or telecommunication equipment office. The facility should incorporate appropriate controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software acquisition controls, and contingency planning.

It is assumed that the facility's security controls restrict the equipment and time that an attacker can have at the module's location.

It is assumed that all personnel that have administrator access to the FSP3000 operating system refrain from applying digital forensic techniques to recover deleted data from TOE file systems on solid state memories that have wear-leveling features.

Network Security

Nobody from the Internet should have access to a sub-network with hardware. It is recommended to put FSP 3000R7 behind a firewall and/or a L3 demarcation device to restrict inbound and outbound traffic.

Deliverable Verification Procedure

FSP 3000R7 software must be downloaded from the ADVA customer portal. The secure communication protocol of HTTPS encrypts all communication between the server and client to protect customer portal communication. The certificate of the HTTPS connection should be checked and the closed lock symbol should be visible in the address line of the browser. Product-specific libraries store all related software. As a customer, you may have your own dedicated library that contains information specific to your network and configuration. This library is visible only to you. The checksum that each software item publishes protects the confidentiality and integrity of the software. The checksum is SHA-256.

To verify the integrity of ADVA FSP3000R7 software:

1. Log in to the customer portal.
2. Download the software.

3. Calculate the checksum of the downloaded item on your local system.

If the checksum(s) match: No evidence of modification to the software, no communication errors.

If the checksum(s) don't match: Evidence of modification to the software, communication errors.

Security Maintenance

It is recommended to upgrade hardware and software to ensure efficiency and security.

Chapter 2

Secure Configuration

This section describes steps for improving the security of a network element. It contains these topics:

Updating Software	17
Changing the Password at First Login	18
Enabling Password Restrictions	19
Configuring New User Accounts	19
Configuring Mutual Authentication	22
Disabling Bootloader Access	23
Enabling Remote Authentication	23
Disabling Insecure Protocols	23
Configuring a Security Banner	25
Disabling Older Versions of TLS	25
Configuring Remote SysLog	26
Configuring Audit Events	26
Configuring Packet Filtering	26
Configuring Whitelist	27
Configuring DoS Protection	27
Configuring the ICMP Filter	27
Disabling Serial Port Access	28
Regenerating the SSH Host Key	28
Regenerating the SSL Certificate	28
Configuring the PKI Certificate	29
Configuring the NTP Server	30
Disabling Login Presentation	30
Configuring Last Successful Login Display	31
Configuring Last Failed Login Display	31
Configuring Login Failure Delay	31

Disabling Requests for User Privilege Upgrade	31
Configuring TLS Ciphers	32
Configuring SSH Ciphers	32
Checking Open Ports	32
Configuring Control Plane Interfaces	34
Running Self-Test	34



Due to a bug in the HSTS implementation of Firefox, it is recommended to use Chrome. Normally the webserver should send an HSTS header, that this web page wants to be retrieved always via HTTPS. The browser (e.g. Firefox) remembers this wish the next time the user types an HTTP address, the browser will automatically use HTTPS instead. Firefox stores the pages with HSTS in a file SiteSecurityServiceState.txt. When the file has a size of 1024 entries, Firefox falls back to the old behavior and allows HTTP connections without any warning.

Network Element Director supports HTTP Strict Transport Security (HSTS). This feature is enabled by default. You cannot disable this setting.

Updating Software

You must log in with ADMIN privileges. Complete these steps to securely update your software.

1. Download the ZIP file, which contains all release files, including software and FW packs, from the ADVA Customer Portal.
2. Verify the ZIP file SHA-256 and compare it to the second source, for example, the Customer Portal Web Service.
3. On the NE, enable the Secure SW Install (SW-SECURE-UPDATE).
4. Install the software on the customer file server by using this OpenSSL command. An example of CON file: F7022011.CON:

openssl command:

```
$ openssl cms -md sha256 -sign -binary -in F7022011.CON -outform DER -
out F7022011.SIG -signer client_cert.crt -inkey client_key.pem -keyopt
rsa_padding_mode:pss -keyopt rsa_pss_saltlen:32 -nosmimecap
```

input:

F7022011.CON – Example of a CON file

client_key.pem – Private key used to sign the CON file

`client_cert.crt` – The certificate that corresponds to `client_key.pem`. This certificate will be included in the SIG file.

output:


`F7022011.SIG` – the signature file. The name must be the same as CON fil, but with an SIG extension name instead of CON. The customer file server will then have one additional file: `F7022011.SIG`.

In PKI view, import a Certificate Authorities (CAs) certificate or certificates, which is described in a separate document. You can import the certificate manually or use the SCEP protocol that you use to sign `client_cert.crt`. In the PKI view, mark those Certificate Authority certificates as trusted. You can now perform a secure upgrade.

Changing the Password at First Login

When you log in with ADMIN privileges, you must first change the default password. After you connect to the NE, a prompt asks you to provide your current password, your new password, and then re-type the new password. In a browser window, complete these steps.


1. In the address bar, type your node IP address and press Enter.
2. In the **Username** field, enter your user name.
3. In the **Password** field, enter your password.
4. Click **Login**.
5. In the **Password Change** window, complete these fields:
 - a. **Current Password**: enter your current password.
 - b. **New Password**: enter your new password.
 - c. **New Password**: re-enter your new password.
 - d. Click **Change**.

	<p>Your new password must:</p> <ul style="list-style-type: none"> • Have a minimum of fifteen characters. • Contain at least two lowercase alphabetic characters. • Contain at least two uppercase alphabetic characters. • Contain at least two numeric characters. • Contain at least two of these special characters: !, @, #, \$, %, ^, (,), -, +, , ~, {, }, [,], ~, ,,
---	--

Enabling Password Restrictions

To enable password restrictions, first enable Enhanced Security mode and change the ADMIN password.

1. Select **Node > Security > Access**.
2. In the **Password Management** area, **Security Mode** field, select **Enhanced**.
3. In the **Security Mode** window, click **Apply**. The system automatically logs you out.
4. Log in to the node again.
5. Enter the current password.
6. In the **Password Change** window, **New Password** field, enter the new password. The system automatically logs you out.
7. Log in to the node again.
8. Enter the new password.

	<p>Enter a new password that:</p> <ul style="list-style-type: none">• Has a minimum of fifteen characters.• Contains at least two lowercase alphabetic characters — a to z.• Contains at least two uppercase alphabetic characters — A to Z.• Contains at least two numeric characters — 0 to 9.• Contains at least two of these special characters: !, @, #, \$, %, ^, (,), -, +, , ~, {, }, [,], ~, .
--	--

Configuring New User Accounts

We recommend that you follow the principle of least privilege. This security principle authorizes access to a person or entity at the lowest privilege level necessary to perform authorized tasks. Create unique local accounts with complex passwords. Remove unnecessary accounts.

To properly create a new user account, specify these parameters:

- password length, mixed case, special characters, digits
- password hash type
- timeouts
- password age
- login fail count
- SNMP security level

- SNMP auth protocol
- SNMP privacy type
- privilege level (operator/monitor and so forth)

Recommended settings:

Parameter	Value
Password	minimum of 15 characters: mixed case, special characters, digits
Authentication Protocol	SHA-512
TL1 Timeout Period [min]	maximum 15
Login Fail Count	maximum 3
Max Password Age [day]	maximum 60
Min Password Age [day]	minimum 1
Password Expire Warning [day]	7
SNMP level	authPriv
Privacy Key Type	User Specified

1. Select **Node > Users > Manage**.
2. Click **Add** to open the **Add Account** window.

In the **Add Account** window, continue with these steps:

1. Enter **Username**.
2. Select **User Privilege** as follows:

User Type	Description
admin	Has the highest privileges on the NCU, including read-write access to every part of the system.
provision	Has read-write access to all settings related to shelves, modules, plugs, optics, and some system-wide settings. Additionally a user with provision privileges can update the software and firmware. The provision-level user has similar access rights as an admin, but no access to security settings or user management settings.
operator	Has limited write access to the system limited to operational settings such as switch loopbacks and force lasers.

User Type	Description
monitor	Only has read access rights and can change only his or her own password.
crypto	Has monitor capabilities with some exceptions. The main task of a crypto user is to configure security-related settings on encryption modules. This user can change the Crypto-Officer password and the authentication password, set bypass mode, and allow a firmware update.
snmponly	Has the same access rights as admin users, but can only connect to the NE through SNMP.

Complete these fields.

3. **Password**, type the new user's password, which must meet these criteria:

- Contains at least two lowercase alphabetic characters — a to z.
- Contains at least two uppercase alphabetic characters — A to Z.
- Contains at least two numeric characters — 0 to 9.
- Is a minimum of 15 characters long.
- Contains at least two of these special characters:
!, @, #, \$, %, ^, (,), -, +, |, ~, {, }, [,], -, .

4. **Retype Password**, retype the new user password.

5. **TL1 Timeout**, select **Yes**.

6. **TL1 Timeout Period [min]**, set the value to **15**.



If this account has admin privileges, in the Sudo Access field specify whether the new account will have sudo access. We recommend that you allow sudo access only to trusted admin users.

7. **Login Fail Count**, set the value to **3**.

8. **Max Password Age [day]**, set the value to **42**.

9. **Min Password Age [day]**, set the value to **7**.

10. **Password Expire Warning [day]**, set the value to **7**.

11. **SNMP > Access**, select **authPriv**.

SNMP version	Level	Authentication	Encryption
v1	noAuthNoPriv	Community String	No
v2c	noAuthNoPriv	Community String	No
v3	noAuthNoPriv	Username	No

v3	authNoPriv	MD5/SHA/SHA-256/SHA-512	No
v3	authPriv	MD5/SHA/SHA-256/SHA-512	Yes (AES-128)

Continue with these steps to complete these fields:

1. **Authentication Protocol**, select **SHA-512**.
2. **Privacy Key Type**, select **User Specified**.

Privacy Key Type	Description
User Specified	Configure a new privacy key for the SNMPv3 user.
User Password	Use the user's existing password as the key for the SNMPv3 user.

3. **Privacy Key**, enter a new user SNMP privacy key that meets the password criteria.
4. **Retype Privacy Key**, retype the privacy key.
5. Click **Add**.

Configuring Mutual Authentication

To configure mutual authentication:

- Add and authenticate certificate authorities.
 - Set the Certificate Authority certificates trust setting to trusted.
 - Import and install the required certificate files on your local computer.
1. Select **Node > Security Applications > HTTPS**.
 2. In the **Client Authentication** area:
 - a. In the **Client Authentication** field, select **Enable**.
 - b. Select the relevant **Client Authority**.
 - c. Click **Apply**.



Ensure that you configure the proper certificate in your browser before you enable mutual authentication, or you can lose connectivity to the NE.

Disabling Bootloader Access

1. Select **Node > Security > Access**.
2. In the **Access Management** area, the **NCU Boot Loader Access** field, select **Disable**.
3. Click **Apply**.



If you disable bootloader access, you will increase security but lose the possibility to restore a lost password.

Enabling Remote Authentication

If you want to enable remote authentication, please make sure that the authentication, authorization and accounting (AAA) solution you use is free of vulnerabilities. Ensure that used solution will not use legacy authentication and authorization methods. If you want to use remote authentication, it is recommended to use CHAP protocol. ADVA is not responsible for vulnerabilities in third-party applications.

Disabling Insecure Protocols

These protocols are considered secure:

- SNMPv3
- TL1 Encrypted Mode
- NETCONF
- SSH
- HTTPS

Other protocols are considered insecure and it is recommended to disable them.



You should only enable the protocols that are being used.

This section contains these topics:

Disabling Telnet	24
Disabling FTP	24
Disabling HTTP redirection to HTTPS	24

Disabling TL1	24
Disabling SNMPv1/SNMPv2c	25
Disabling GNMI	25

Disabling Telnet

Telnet is disabled by default and it is not recommended to use it. If you enable it by accident, disable it using these steps:

1. Select **Security > Access**.
2. In the **Access Management** area, in the **Telnet Interface** field, select **Disable**.
3. Click **Apply**.

Disabling FTP

FTP is disabled by default and it is not recommended to use it. If you enable it by accident, disable it using these steps:

1. Select **Security > Access**.
2. In the **Access Management** area, in the **FTP Client** field, select **Disable**.
3. Verify that the **FTP Server** field is set to **Disable**.
4. Click **Apply**.

Disabling HTTP redirection to HTTPS

This option is disabled by default and it is not recommended to use it. If you enable it by accident, disable it using these steps:

1. Select **Node > Security > Access**.
2. In the **Access Management** area, in **HTTP Redirect to HTTPS** field, select **Disable**.
3. Click **Apply**.

Disabling TL1

It is recommended not to use TL1. If you want to use TL1, use the encrypted mode.

1. Select **Node > General > Controls**.
2. In the **Interfaces** area, set the **TL1 Interface** to **Disable**.
3. Click **Apply**.

Disabling SNMPv1/SNMPv2c

1. Select **Node > General > Controls**.
2. In the **Interfaces** area, **SNMPv1** field, select **Disable**.
3. In the **Interfaces** area, **SNMPv2c** field, select **Disable**.
4. Click **Apply**.

Disabling GNMI

This option is disabled by default and it is not recommended to use it. If you enable it by accident, disable it using these steps:

1. Select **Node > General > Controls**.
2. In the **Interfaces** area, **GNMI Interface** field, select **Disable**.
3. Click **Apply**.

Configuring a Security Banner

1. Select **Node > Security > Access**.
2. In the **Warning Message** area, **Access Warning Message** field, enter the warning message.
3. Set **Access Warning** to **Enable**.
4. Click **Apply**.



For example, you can use Access Warning Message like this:

WARNING TO UNAUTHORIZED USERS: This system is for authorized users only. Disconnect immediately if you are not an authorized user!

Disabling Older Versions of TLS

1. Select **Node > Security Applications > SSL/TLS**.
2. In the **Transport Layer Security (TLS) Authentication** area, in the **TLS Support** field, select **1.2** and **1.3**.
3. Click **Apply**.

Configuring Remote SysLog

1. Select **Node > General > Controls**.
2. In the **Remote Event Recipients (SysLog)** area, click **Add**.
3. In the **Add Remote Event Recipients (SysLog)** window, **IPv4/v6 Address** field, enter the applicable IP address.
4. Click **Add**.

To add a port user label to the SysLog information:

1. In the **Remote Event Recipients (SysLog)** area, **Message Extension** field, select **Add User Label** and click **Apply**.



To ensure accountability, assign a specific person or persons to review the logs and identify any violations. Setting auditing to enabled is not adequate to ensure accountability.

Configuring Audit Events

1. Select **Node > Security > Access**.
2. In the **Log** area, **Audit Logs** field, select **Enable**.
3. Click **Apply**.



You must deploy the remote collector. If you enable audit logs, the volume of log-data will increase significantly. Before you enable audit logs, consider your network bandwidth and log collector capacities.

Configuring Packet Filtering

1. Select **Node > Security > Access**.
2. In the **Access Management** area, verify that the **Packet Filter** field is set to **Enable**.
3. Click **Apply**.

Configuring Whitelist

1. Select **Node > Security > Packet**.
2. In the **Node Management Approved IP Addresses** area, click **Add**.
3. In the **Add Approved IP Address** window, **IP Operation** field, select **IPv4** or **IPv6**.
4. If operation is IPv4:
 - a. Enter the **IP Mask**.
 - b. Set the **Admin State** to **In Service**.
 - c. Enter the **IP Address**.If operation is IPv6:
 - a. Set the **Admin State** to **In Service**.
 - b. Enter the **IPv6 Address**.
 - c. Enter the **IPv6 Prefix Length**.
5. Click **Add**.
6. In the **Node Management IP Address Filters** area, set the system to accept packets only to the System IP address.
7. In the **Node Management IP Address Filters** area, **Approved IP Filter** field, select **Enable**.
8. Click **Apply**.

Configuring DoS Protection

1. Select **Node > Security > Packet**.
2. In the **Controls** area, the **Denial of Service Guard** field, verify that **Enable** is set.
3. Click **Add**.



Configuring the ICMP Filter

1. Select **Node > Security > Packet**.
2. In the **Internet Control Message Protocol (ICMP)** area:
 - a. In the **ICMP Filter** field, select **Enable**.
 - b. In the **Drop Echo Requests** field, select **Enable**.
 - c. In the **Drop Source-Quench** field, select **Enable**.
 - d. In the **Drop Redirects** field, select **Enable**.
 - e. In the **Drop Timestamp Requests** field, select **Enable**.

- f. In the **Drop Addr. Mask Requests** field, select **Enable**.
3. Click **Apply**.


Disabling Serial Port Access

1. Select **Configure > Shelf 1**.
2. Select **Slot A NCU-II/NCU-3**.
3. In the **Serial Port** area, click the relevant port.
4. In the **Configure Details** window, **Admin State** field, select **Disable**.
5. Click **Apply & Exit**.

	The serial port shouldn't be connected to the Serial Device Server.
	If you disable serial port, you may lose some debugging functions in case of losing the IP address.

Regenerating the SSH Host Key

1. Select **Node > Security Applications > SSH > Host Keys**.
2. Select the **RSA/RSA2** SSH Key Encryption.
3. In the **Generate and Activate SSH Host Key** window, **SSH Host Key Generate** field, select **4096**.
4. Click **Generate and Activate**.


	SSH Host key length should be at least 3072 bits.
---	---


Regenerating the SSL Certificate

1. Select **Node > Security Applications > HTTPS**.
2. In the **Certificate Generation** window, **Renew Mode**, select **Manual**.
3. Click **Apply**.

4. Set the **Key Length** to **4096**.
5. Set the **SSL Valid Period** to **2**,
6. Set the SSL Certificate IP fields.
7. Click **Apply & Generate Certificate**.

Configuring the PKI Certificate

	Please confirm that any non-blank URL points to a trustworthy server.
---	---

	Please make sure that the PKI solution you use is free of vulnerabilities.
---	--

ADVA is not responsible for vulnerabilities in third-party applications.

1. Select **Node > Security > Certificate Authorities**.
2. In the **Certificate Authorities (CA)** area, click **Add**.
3. In the **Certificate Authorities** window:
 - a. Select a **CA Identifier**.
 - b. In the **SCEP Configuration** area, enter the **SCEP URL** for a trusted CA.
 - c. In the **SCEP Advanced Configuration** area, enter the **SCEP Query Message**.

	Some servers require the NTLM authentication. In that case, in the SCEP Authentication area, enter Domain , User Name and Password , and click Apply .
---	---

4. In the **Certificate Authorities (CA)** area:
 - a. Select the **PKI Server Identifier**.
 - b. Click **Update**.
 - c. Click **Apply**.
5. In the **Certificates** area:
 - a. Select the **Identifier**.
 - b. In the **Configure Details** window, set the **Trust Settings** to **Trusted**.
6. In the **Keys** area, click **Add**.
7. In the **Cryptographic Keys** window:

- a. Select the **Identifier** and select the proper **Key Profile**.
 - b. In the **Key And Certificate Renewal** area, select the proper **Certificate Authority**.
 - c. In the **Certificate Request Configuration** area, enter the information following your network plan.
 - d. Click **Add**.
8. In the **Certificates** area, select the **Identifier**.
 9. In the **Configure Details** window, the **Certificate Activation** area, click **Activate**.
 10. Click **Apply**.

Configuring the NTP Server

1. Select **Node > General > Date & Time**.
2. In the **Network Time Protocol (NTP) Keys** area, click **Add**.
3. In the **Add NTP Key** window, set the **NTP Key Id** and **NTP Digest Algorithm**.
4. In the **NTP Key** field, enter the NTP server key. These parameters must be exactly the same as on the NTP Server.
5. Click **Add**.
6. In the **Network Time Protocol (NTP) Servers** area, click **Add**.
7. In the **Add NTP Server** window:
 - a. Enter the **IPv4/v6 Address**.
 - b. Select the **IP Subnet**.
 - c. Set the **Admin State** to **In Service**.
 - d. Set the **NTP Authentication** to **Private Key** and select a proper **NTP Key Id**.
 - e. Click **Add**.
8. In the **Date & Time** area, set the **NTP Operation** to **Client**.
9. Click **Apply**.

Disabling Login Presentation

1. Select **Node > Security > Access**.
2. In the **Access Management** area, **Login Presentation** field, select **Prompt**.
3. Click **Apply**.

Configuring Last Successful Login Display

1. Select **Node > Security > Access**.
2. In the **Password Management** area, **Show Last Success Login** field, select **Enable**.
3. Click **Apply**.

Configuring Last Failed Login Display

1. Select **Node > Security > Access**.
2. In the **Password Management** area, **Show Last Failed Login** field, select **Enable**.
3. Click **Apply**.

Configuring Login Failure Delay

1. Select **Node > Security > Access**.
2. In the **Password Management** area, in the **Login Failure Delay [s]** field, enter **5**.
3. Click **Apply**.




After each failed login, user's account is temporarily locked.

Disabling Requests for User Privilege Upgrade

1. Select **Node > Security > Access**.
2. In the **Access Management** area, the **User Privilege Upgrade** field, select **Disable**.
3. Click **Apply**.


Configuring TLS Ciphers

1. Select **Node** > **Security Applications** > **SSL/TLS**.
2. In the **TLS Ciphers** area, **TLS Ciphers Profile** field, select **Default**.
3. Click **Apply**.

	The default value allows only BSI recommended ciphers.
---	--

Configuring SSH Ciphers

1. Select **Node** > **Security Applications** > **SSH**.
2. In the **SSH Ciphers** area, the **SSH Ciphers Profile** field, select **Default**.
3. Click **Apply**.

	The default value allows the use of only the German Federal Office for Information Security (BSI) recommended ciphers.
---	--

Checking Open Ports

Open ports can be checked via nmap tool:

```
# nmap -sT -sU -p- <SUT>
```


Application/Service	Protocol	Port Number
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
Web Server	TCP	80, 443
Web Redirector	TCP	80, 443
NETCONF	TCP	830
TL1	TCP	2024, 2025, 8778

TL1 (Human Mode)	TCP	2024, 8778
TL1 (NMS Mode)	TCP	2025, 8778
TL1 (Encrypted Mode)	TCP	6252, 6253, 8778
TL1 (Human Encrypted Mode)	TCP	6252, 8778
PCEP	TCP	4189
GNMI	TCP	50051
DHCP Server	UDP	67
DHCP Client	UDP	68
NTP	UDP	123
SNMP Agent	UDP	161

If you disable any of the above applications/services (or the TCP/UDP ports not mentioned above), the NE will:

- for TCP:
 - reject any incoming TCP SYN packets, for example reply with a TCP Reject packet.
 - drop, i.e. silently discard any TCP packets with a flag set other than SYN.
- for UDP:
 - reject any incoming UDP packets, i.e. reply with an ICMP "Destination protocol unreachable" message (Type 3, Code 2).

If other applications, not mentioned above, will need to open a listening socket, for instance for internal communication, shall do so only on interfaces that are not visible to the external DCN (e.g. the loopback interface, backplane.4, etc.). Examples are the cpcli (127.0.0.1:7000), DRBD (backplane.6:7789..7797), etc.

	<p>NTP opens a listening port (UDP 123) for all modes: client, server, and relay.</p> <p>UDP port 162 is used as an outgoing port to send SNMP traps. As such it is not a listening port and will not show up in port-scans and hence should not be in this table.</p> <p>The Path Computation Engine Protocol typically opens a listening socket on the System IP address, for instance any packet with destination port TCP 4189 received via any of the external interfaces is accepted; as such this constitutes an open port also.</p>
---	---

Configuring Control Plane Interfaces

1. Select **Node > General > Controls**.
2. In the **Control Network** area, the **Control Plane** field, select **Disable**.
3. Click **Apply**.

Running Self-Test

1. Select **Node > General > Controls**.
2. In the **Functionality** area, the **Selftest Fail Control** field, select **Non-Operational**.
3. Click **Apply**.



You can run a self-test only on NCU-3.

Chapter 3

Debugging and Diagnostic Tools

This section contains a list of available debugging tools:

- gdb
- gdb-add-index
- gdbreplay
- gdbserver
- gcore
- anacron
- audisp-remote
- auditctl
- auditd
- ausearch
- aureport
- audisp-syslog
- badblocks
- bashbug
- blkid
- blkdiscard
- blkzone
- bootlogd
- bzip2recover
- capttest
- chacl
- catchsegv

- chcpu
- debugfs
- devlink
- dump-remind
- e2freefrag
- e2image
- e2initrd_helper
- e2scrub
- e2scrub_all
- e2undo
- e4crypt
- e4defrag
- findfs
- filefrag
- findmnt
- fsck.minix
- fstrim
- fsfreeze
- fstab-decode
- genl
- getpcaps
- getfacl
- getfattr
- ipmaddr
- iptunnel
- lstat
- logsave
- lsblk
- lslocks
- nameif
- mii-tool
- mkfs.minix
- mklost+found
- mountpoint
- partx
- pcretest
- pppdump

- pppstats
- pprof-symbolize
- pslog
- pzst
- rarp
- radvdump
- resize2fs
- restore-tar
- red
- rmt
- routel
- routef
- rpcinfo
- run
- runuser
- rtmon
- rtacct
- rtpr
- savelog
- scriptreplay
- setfattr
- sfdisk
- sln
- smartctl
- sulogin
- tcpdchk
- try-from
- tracepath
- tracepath6
- uuidd
- uuiddparse

Chapter 4

SSH and SSL

This section contains these topics:

SSH Algorithms	38
SSL Ciphers	40

SSH Algorithms

This section contains a list of supported and recommended ssh algorithms:

Supported Host Key Algorithms

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512
- ssh-ed25519
- ssh-rsa

Recommended SSH Host Key Algorithms

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512

Supported SSH Key Exchange Algorithms

- curve25519-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group15-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512

Recommended SSH Key Exchange Algorithms

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512

Supported SSH Encryption Algorithms

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com
- AEAD_AES_256_GCM

Recommended SSH Encryption Algorithms

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes256-gcm@openssh.com

Supported SSH Message Authentication Code Algorithms

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com

Recommended SSH Message Authentication Code Algorithms

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com

SSL Ciphers

This section contains a list of supported and recommended ssl ciphers:

Supported SSL Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_CCM_8
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CCM
- TLS_RSA_WITH_AES_128_CCM_8
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CCM
- TLS_RSA_WITH_AES_256_CCM_8
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Recommended SSL Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

Chapter 5

Root Rights

After upgrading to the R22.1.1, all existing admin-account users get a sudo option enabled. Admin-account users with a sudo option enabled can create and edit all other admin accounts. Admin-account users with a sudo option disabled can only create and edit other admin accounts with disabled sudo option. The system always enforces that at least one admin account has a sudo option enabled. The account overview indicates each admin account with a sudo option enabled.

Admin-account users with a sudo option enabled are allowed to use the sudo tool to execute commands with the root rights. Admin-account users with a sudo option enabled can use sudo that requires the password of the current user to elevate privileges. The root account is disabled, login is not possible. You should only use sudo privilege escalation in special cases. It is recommended to be done by dedicated personnel who understands the system. Number of sudo allowed admins should be limited to a necessary minimum.

We trust you have received the usual lecture from the local System Administrator.

It usually boils down to these three things:

1. Respect the privacy of others.
2. Think before you type.
3. With great power comes great responsibility.