English

Fujitsu Server BS2000 SE Series

Security Manual

User Guide

Valid for:
M2000 V6.5A
X2000 V6.5A
HNC V6.5A

Edition December 2023

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to: bs2000services@fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2015

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2015.

Copyright and Trademarks

All hardware and software names used are trademarks of their respective manufacturers.

The Xen® mark is a trademark of Citrix Systems, Inc., which manages the mark on behalf of the Xen open source community. The Xen® mark is registered with the U.S. Patent and Trademark Office, and may also be registered in other countries.

Novell and SUSE are registered brands of Novell, Inc. in the USA and other countries.

Linux is a registered brand of Linus Torvalds.

Windows® is a registered trademark of Microsoft Corporation.

The Linux-based basic software M2000, X2000, and HNC which is installed on the Management Unit, Server Unit x86, and HNC contains Open Source Software. The licenses for this can be found in the LICENSES directory on the relevant installation DVD.

Table of Contents

Security Manual 5
1 Introduction 6
1.1 Objective and concept of this manual 7
1.2 Changes to the predecessor manual 8
1.3 Notational conventions 9
2 Architecture of the SE servers and networks 10
2.1 Hardware 11
2.2 Architecture of SE servers 12
2.3 Networks 14
2.4 Cluster 16
3 Secure access to management functions 17
3.1 Role strategy and user accounts 18
3.1.1 Role strategy and role authorizations 19
3.1.2 User accounts 23
3.1.2.1 Centrally managed accounts (LDAP accounts) 24
3.1.2.2 Authorization for account management 25
3.1.2.3 Further accounts of the base system 26
3.1.2.4 Accounts for add-on packs 27
3.1.3 Authentication 28
3.1.4 Password administration for local accounts 29
3.1.5 Configuring access to an LDAP server 32
3.2 Access to the SE Manager 33
3.2.1 Security settings on the administration PC 34
3.2.2 Communication with encryption 35
3.2.3 Session management 36
3.3 Text-based access (at shell level) 37
3.4 Alternative accesses with Secure Shell 38
3.4.1 Generating the keys 39
3.4.2 Using SSH agents 41
3.4.3 PuTTY with PuTTYgen and Pageant 43
3.4.3.1 Key generator PuTTYgen 44
3.4.3.2 Authentication agent Pageant 45
3.5 Access via the local console 46
3.6 Access to the iRMC of the Management Unit 47
3.7 Protected access to the BIOS and the bootloader 48
4 Secure access to systems 49
4.1 Secure access to BS2000 systems 50

4.1.1 Security in the BS2000 operating system 51
4.1.2 Downloading KVP logging files 52
4.1.3 Alternative access to the BS2000 operating system with PuTTY 53
4.2 Secure access to systems on Application Units 54
4.2.1 Configuration changes 55
4.2.2 Access to the iRMC / Management Board of the Application Unit 56
4.2.3 Integration of Application Unit into the SE Manager 57
4.2.4 Access via the local console 58
5 Remote service (via AIS Connect) 59
5.1 Service account 60
5.2 Logging support operations 61
5.3 Using encryption 62
5.4 Using the "shadow terminal" function 63
5.5 Monitoring the current usage of the service access 64
5.6 Access to external assets 65
6 Configuration and diagnostic data 66
6.1 Configuration data backup 67
6.2 Diagnostic data 68
7 Network security 69
7.1 Network services 70
7.2 IP-based access restriction 72
7.3 Security at Net Unit level 73
7.4 Net-Storage 74
7.5 SNMP 75
8 Security of the base system 76
8.1 Hardening the base system 77
8.2 Software signature 79
8.3 Digital certificates 80
8.3.1 Confirming/importing a certificate in the web browser 81
8.3.2 Using the standard certificate 85
8.3.3 Creating and activating a new self-signed certificate 88
8.3.4 Requesting an SSL certificate 89
8.3.5 Uploading and activating a customer-specific certificate 91
9 Logging actions (audit logging) 93
10 Event logging and alarm management 94
11 Related publications 96

Security Manual

1 Introduction

This user manual describes the security features of the SE server based on its operating and service concept.
For a general description of the SE Server, refer to the "Operation and Administration" manual [2].

The description of the security features of the SE server mainly refers to the level of the basic operating system M2000 at the externally accessible Management Unit (MU). The HNC and Server Unit (SU) type units are sealed off from the outside and are therefore not described in detail. Where appropriate, differences that must be observed for Application Units (AU) are discussed.

The most important general security features are mentioned below. The base systems of the SE Server units (M2000, HNC and X2000) based on SUSE Linux Enterprise Server (SLES) 15 can be described as secure and hardened for the following reasons:

- Only signed software components which are absolutely essential for operation are installed.
- Nonprivileged accounts are used for users of all roles (e.g. Administrator or BS2000 operator). These are equipped with clearly defined (and restricted) functions and access rights as part of a differentiated role strategy. No access to the system is possible outside this role strategy. Rights cannot be escalated; access to the `root` account is locked.
- The role and user strategies enable personalized accounts to be configured and passwords and password attributes to be managed.
- The data traffic between the administration PC and Management Unit, HNC and Server Unit x86 is encrypted.
- All ports which are not used are closed.
  Services are started only when they are actually used.
- The configuration of the base systems is based on the recommendations of the Center for Internet Security (CIS, http://www.cisecurity.org). Deviations from these recommendations result only from the functions required for operation. These deviations do not, however, lead to security holes.

> ¡ In the few cases in which administration measures affect the security of the system, information and instructions on correct handling are provided under the heading **Security-relevant actions**.

Security-relevant aspects of BS2000 or other operating systems and applications which are operated using the systems are not examined.

1.1 Objective and concept of this manual

The manual contains the security-relevant information for the SE server. The systems Management Unit, HNC, Server Unit x86 and Application Units on the SE server are examined individually.

The Application Units have a special position. Compared to the Management Unit, HNC and Server Unit, in the Application Units the user plays a greater role in administration and monitoring. The information in this manual therefore applies generally only for the Management Unit, HNC and Server Unit x86. When information also applies for Application Units, this is stated specifically.

The Management Unit, HNC and Server Unit x86 are systems that have been specially configured and hardened by Fujitsu.
By contrast, the operating system which is optionally preinstalled on an Application Unit contains no special security provisions. Here the user bears sole responsibility for configuring a secure system.

On the other hand the Management Unit, HNC and Server Unit x86 differ in their functionality, which means that some of the information in this manual is only applicable for some of these systems. In this case the systems concerned are named at the start of the section (in the heading or in the introductory sentence).

The various chapters of the manual deal with the topics which are relevant to security.

The operation and administration of the SE server are described in detail in the “Operation and Administration” manual [2] and in the context-sensitive online help of the SE Manager. There you will also find further information on operating the functions dealt with in this Security Manual.

Information on security in BS2000 is provided in the “Introduction to System Administration” manual [8] and the manuals for the software product SECOS [9 and 10].

Readme file

When a Readme file exists for a product version, you will find it online on the manual server at https://bs2manuals.ts.fujitsu.com. This file contains brief information on the product version in English or German.

Additional product information in the Release Notice

Current information, version and hardware dependencies and instructions for installing and using a product version are contained in the associated Release Notice. These Release Notices also are available online at https://bs2manuals.ts.fujitsu.com.

Target groups of this manual

This manual is intended for administrators and security officers (e.g. with the role Security administrator) of an SE server. Knowledge is required of the BS2000, Linux and, where appropriate, Windows operating systems. Basic knowledge of how to operate graphical interfaces is also an advantage.

1.2 Changes to the predecessor manual

This manual describes the functionality of the SE Manager with the use of the basic software M2000/X2000/HNC V6.5A.

Functional extensions

The functional extensions when using the basic software M2000/X2000/HNC V6.5A are fully described in the user guide „Administration and Operation“ [2]. Under security aspects, especially the following new features are relevant:

- Introduction of a new RBAC-based role concept with basic roles and user-defined roles based on these roles
- Introduction of a new authorization assignment aimed at BS2000 systems for BS2000 operators, with independent authorizations for console and dialog
- Introduction of the Security Monitor (SecMon), which regularly checks the security settings and defaults and generates appropriate events if necessary
- Extension of the Resource Monitor (ResMon), which regularly checks the currently available resources
- Support of multi-factor authentication (MFA) for login at the SE Manager
- Replacement of security fixes and hot fixes by updates

1.3 Notational conventions

The following **notational conventions** are used in this manual:

i	This symbol indicates important information and tips which you should bear in mind, in particular the section **Security-relevant actions**.
!	This symbol and the word **CAUTION!** precede warning information, which in interests of system and operating security you should always observe this information.
>	The action which you must perform is indicated by this symbol.
italics	Texts from the SE Manager
`monospace`	System inputs and outputs
<abc>	Variables which are replaced by values.
Key symbols	Keys are displayed as they appear on the keyboard. When uppercase letters need to be entered, the Shift key is specified, e.g. SHIFT - A for A. If two keys need to be pressed at the same time, this is indicated by a hyphen between the key symbols.
[number]	The titles of related publications in the text are abbreviated. The complete title of each publication which is referred to by a number is listed in the Related Publications chapter after the associated number.

Names and abbreviations

In this manual, abbreviations are used to describe the SE server models and their components. These are explained in the introduction to the Basic Operating Manual [3] in the section "Models, Names, Abbreviations".

2 Architecture of the SE servers and networks

The description is divided into the following sections:

- Hardware
- Architecture of SE servers
- Networks
- Cluster

2.1 Hardware

A server of the Fujitsu Server BS2000 SE series (SE server for short) can consist of the following components:

- Management Unit (MU) with SE Manager
  The operation of the SE server with a single Management Unit is called a "single-MU configuration". The Management Unit can be redundant in design. An SE server configuration with more than one Management Unit (MU redundancy on the SE server or Management Cluster with two SE servers) is called "multi-MU configuration".
  MU redundancy ensures that the components of the SE server can still be operated if one MU fails. In particular this means that the SKP functionality is then still available for operating an SU /390.
- Server Unit (SU)
  An SU enables operation of BS2000 (Native BS2000 or VM2000). The SE servers SE710 and SE730 are each equipped with an SU /390. The SE servers SE310, SE320 and SE330 each contain an SU x86.
- Application Unit (AU)
  Multiple AUs can be operated on the SE server. An AU enables operation of applications under Linux, Windows or hypervisor-based systems.
- Net Unit (NU)
  The Net Unit offers maximum performance and security for internal communication in an SE server and for a connection to customer networks (IP networks). For an SU /390, an HNC is an additional component of the Net Unit.
  In the case of SE /390 the Net Unit is always redundant in design. In the case of SE x86 redundancy of the Net Unit is optional.
  The Net Unit is supplied preconfigured, is autonomous with respect to SE server management, and can easily be connected to the customer network.
- Rack console and KVM switch
- Peripherals (storage)
- Optional hardware components:
  Disk storage systems (for SU x86, AU), tape library systems (for SU x86), FC switches

2.2 Architecture of SE servers

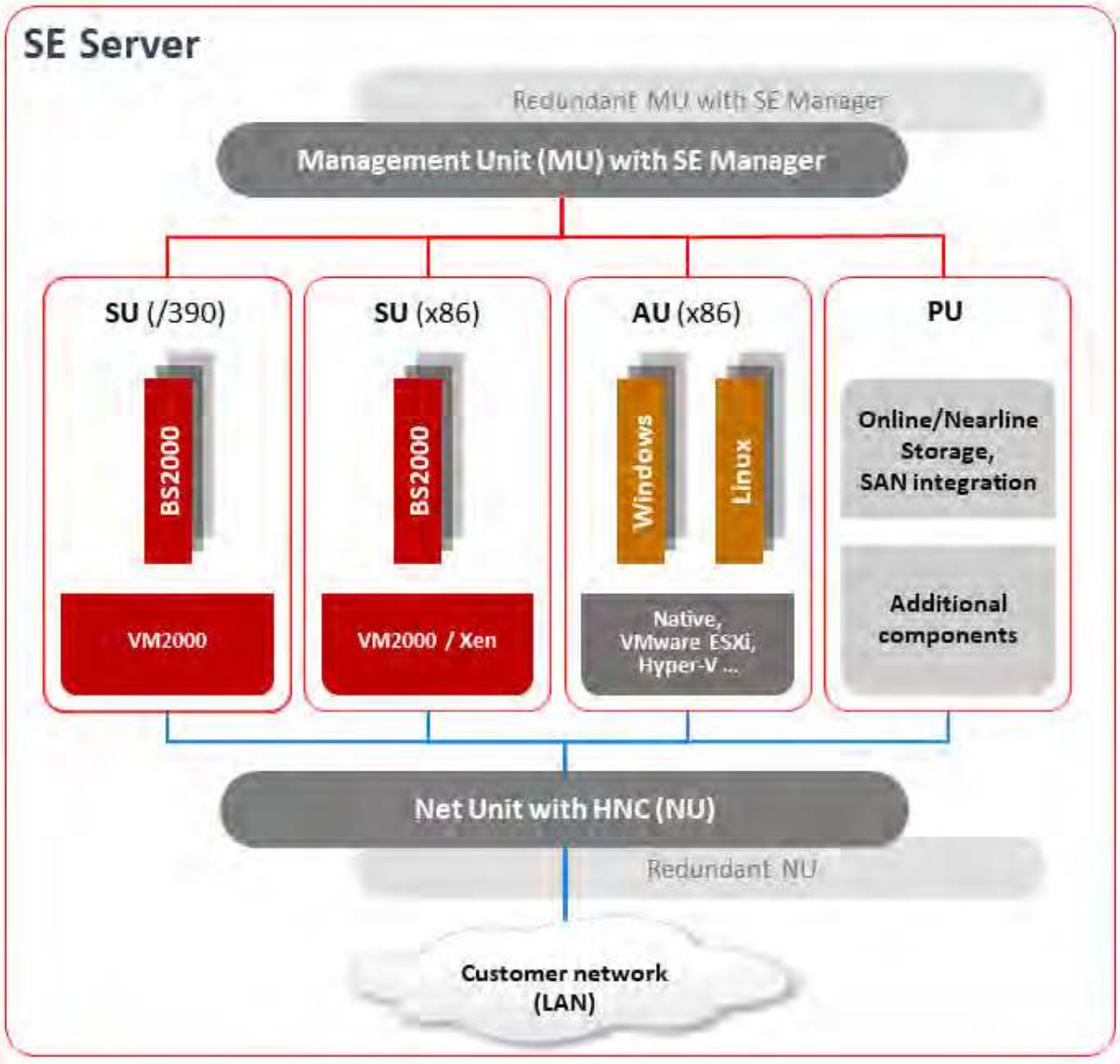


Figure 1: Architecture of SE servers

The SE Manager of each MU enables you to operate and manage all components of the SE server centrally. The SE Manager offers a user-friendly, web-based user interface for this purpose.

The Net Unit offers maximum performance and security for internal communication in an SE server and for a connection to customer networks (IP networks).

Security-relevant actions

The following settings and measures, which are relevant to security, must only be implemented on one MU of the SE server configuration:

- You can configure user accounts and assign individual authorizations for operator accounts. See section "Role strategy and user accounts".
- You can configure multi-factor authentication (MFA) for individual accounts to log in to the SE Manager. See section "Authentication".
- To use centrally managed accounts (LDAP accounts), you have to set up and configure an LDAP access, see section "Configuring access to an LDAP server"

The following settings and measures, which are relevant to security, must be implemented on each MU of the SE server configuration:

- You must define the configuration of the IP addresses and networks in the same way for each MU, see chapter "Network security".
- You must define the security settings for service access on each MU, see section "Using the "shadow terminal" function" and section "Access to external assets".
- At each MU where you call the SE Manager, you must confirm or import the certificate of this MU, see section "Digital certificates".

2.3 Networks

The Net Unit implements the connection of the units to the networks of the SE server and to customer networks. In addition, private networks are available for internal communication in the SE server.

The following logical networks are supported:

- Public management networks
  - Management Admin Network Public (MANPU)
  - Management Optional Admin Network Public (MONPU): the additive administration network can be configured when required (e.g. when AIS Connect is not to be operated via MANPU).
- Management Network Private
  - Management Control Network Private (MCNPR) for SE server communication
  - Management Optional Network Private (MONPR): when required, up to 8 additive networks MONPR<n> (where <n>= 01..08) can be configured for SE server communication.
  - Management Control Network Local (MCNLO) for the local SE server communication
  - Management SVP Network Private (MSNPR) enables SVP communication to the SU /390 on SE710/SE730.
- Data Network Public
  - Data Network Public (DANPU): when required, up to 8 additive networks DANPU<n> (where <n>= 01..08) can be configured for connecting applications to the public customer network.
- Data Network Private
  - Data Network Private (DANPR): when required, up to 99 networks DANPR<n> (where <n>= 01..99) can be configured for internal private customer networks for SE servers.

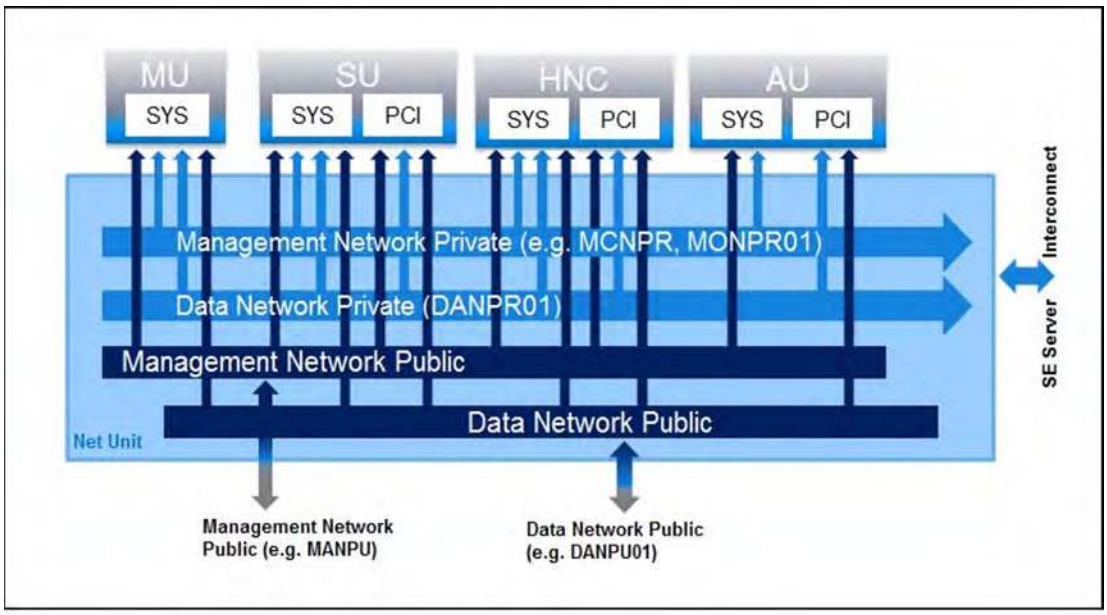


Figure 2: Block diagram of the Net Unit

The use of different networks means that components of one network cannot influence the other network, in other words the networks are protected from each other.

Furthermore, by means of ACL services (TCP/UDP ports) of the DANPU<xx>, MANPU, MONPU, DANPR<xx> and MONPR<xx> networks can be restricted in the Net Unit configuration (see section "Security at Net Unit level").

The base operating systems of the HNC and SU x86 can only be reached over the internal networks and are thus protected from the customer networks.

> **Exception**: This does not apply if Net-Storage with connection to MANPU or DANPU is configured on HNC or SU x86!
> With a suitable firewall setting on HNC or SU x86, you can ensure that only the port required for communication (via NFS v3 or v4) with the Net-Storage is accessible.

In addition to the connections of the units to the switches of the Net Unit (for use by the guest systems), direct cabling from the units to the customer network can also be used.

2.4 Cluster

Two types of clusters are possible in an SE server configuration.

Management Cluster

If two or more SE servers are combined into one management entity, it is called a "Management Cluster" (or "SE Cluster").

A Management Cluster is configured by Customer Support based on the customer's wishes and is used to operate und administrate all SE servers of the SE Cluster together.

A Net Unit connection between the SE servers involved (ISL-E) and one or two external CRD disks for managing the global data are required to establish a Management Cluster.

Regarding administration and operation, all MUs of the Management Cluster are equally ranking. This means you can centrally administer and operate all objects of the whole SE server configuration from one MU.

The SE servers can be operated as long as one MU functions. However, an MU of the local SE server is required for the SVP operation of an SU /390 and its correct HW display.

SU Cluster

Two Server Units of the same type (SU /390 or SU x86) can be combined into a logical unit, a so-called "SU Cluster".

An SU Cluster is configured by Customer Support based on the customer's wishes and provides the Live Migration (LM) function for the BS2000 systems of the two Server Units.

For further information on cluster types and the Live Migration function, see the "Operation and Administration" manual [2]. For further information on using clusters, see the "Cluster Solutions for SE Servers" whitepaper [7].

3 Secure access to management functions

The description is divided into the following sections:

- Role strategy and user accounts
  - Role strategy and role authorizations
  - User accounts
    - Centrally managed accounts (LDAP accounts)
    - Authorization for account management
    - Further accounts of the base system
    - Accounts for add-on packs
  - Authentication
  - Password administration for local accounts
  - Configuring access to an LDAP server
- Access to the SE Manager
  - Security settings on the administration PC
  - Communication with encryption
  - Session management
- Text-based access (at shell level)
- Alternative accesses with Secure Shell
  - Generating the keys
  - Using SSH agents
  - PuTTY with PuTTYgen and Pageant
    - Key generator PuTTYgen
    - Authentication agent Pageant
- Access via the local console
- Access to the iRMC of the Management Unit
- Protected access to the BIOS and the bootloader

3.1 Role strategy and user accounts

Accounts and authorizations work globally, i.e. cross-MU. In a multi-MU configuration, each action has to be performed once and on one MU only.

In the case of a Management Cluster, each role or account is valid for the whole cluster.

3.1.1 Role strategy and role authorizations

One major part of the security strategy is the role strategy which incorporates the following features:

- The roles are graduated: Only the necessary interfaces and functions are available to each role.
- Each user account is permanently assigned to a role.
- No rights escalation is possible, i.e. no access (or transition) is possible to interfaces and functions other than those envisaged. In particular, no access is possible to the `root` account of the base operating system.
- Roles
  For users, the basic roles mentioned below are defined. In addition, user-defined roles can be configured by combining basic roles. With the exception of the Administrator and Service roles, the remaining roles have restricted rights tailored to their respective areas of responsibility. In addition to the SEM functionality described below, each basic role also has access to some further SEM windows like the main windows Dashboard and Certificates and may administrate its own password, download the CA certificate of the MU and access the event logging.
  - Administrator
    The Administrator role is higher ranking than the other roles (except the Service role). It entitles to all functions of the SE Manager as well as for shell access and execution of all functions of the recommended CLI. It cannot be combined with other roles in a user-defined role.
  - BS2000 administrator
    A BS2000 administrator has the authorization for functions of the SE Manager which are necessary to operate BS2000 systems. In addition, they also have some administrator authorizations: switching the units SU, MU and HNC on/off, performing a CSR backup, creating diagnostic data, accessing the shadow terminal, read access to the hardware inventory, and configuration of scheduled power on/off of the units SU, MU and HNC. Furthermore a BS2000 administrator may execute the commands bs2Console, bs2Dialog and svpConsole via PuTTY on a remote unit.
  - BS2000 operator
    A BS2000 operator has the authorization for functions of the SE Manager which are necessary to operate BS2000 systems. An administrator or security administrator can also configure specific authorizations individually for a BS2000 operator account. Furthermore a BS2000 operator may execute the commands bs2Console, bs2Dialog and svpConsole via PuTTY on a remote unit.
  - AU administrator
    An AU administrator has the authorization for functions of the SE Manager which are necessary to operate the systems on AUs. In addition, they also have some administrator authorizations: switching the AUs on/off, read access to the hardware inventory, and configuration of scheduled power on/off of the AUs.
  - Read-only administrator
    A Read-only administrator has the right to view all windows of the SE Manager, however modifying actions are not allowed.
  - Security administrator
    A Security administrator has full authorization for the windows and functions of the SE Manager under the categories Authorizations and Logging.
  - Hardware administrator
    A Hardware administrator has full authorization for the windows and functions of the SE Manager under the categories Hardware -> Units, Hardware -> HW inventory, Hardware -> Energy and Service -> Units.

- Storage administrator
  A Storage administrator has full authorization for the windows and functions of the SE Manager under the categories Devices -> … -> IORSF files | Disks | Tape devices, Hardware -> Units -> … -> FC interfaces | Multipath disks | CRD disks and Hardware -> Storage (without STORMAN!).
- Power operator
  A Power operator has authorization for the main window Units under the category Hardware and the functions for powering units on and off.
- IP network administrator
  An IP network administrator has full authorization for the windows and functions of the SE Manager under the categories Hardware -> Units -> … -> IP interfaces, Hardware -> Management -> … -> IP configuration | Routing & DNS and Hardware -> IP networks.
- FC network administrator
  An FC network administrator has full authorization for the windows and functions of the SE Manager under the categories Hardware -> FC networks and Devices -> BS2000 paths.
- Shadow terminal operator
  A Shadow terminal operator has authorization for access to the main window Service -> Units -> <MU> -> Remote Service, wherefrom a shadow terminal can be opened.

- Add-on-specific roles
  - OPENSM2
    - OPENSM2 administrator
      An OPENSM2 administrator has authorization for access to the add-on OPENSM2 and to its administration on all Management Units.
    - OPENSM2 information
      A user with role OPENSM2 information has authorization for access to the add-on OPENSM2. The administration of the add-on is not allowed.
  - OPENUTM
    - OPENUTM administrator
      An OPENUTM administrator has authorization for access to the add-on OPENUTM and to its administration on all Management Units (Master and Administration Write privileges).
    - OPENUTM operator
      An OPENUTM operator has authorization for access to the add-on OPENUTM including administration (Administration Write privilege).
    - OPENUTM information
      A user with role OPENUTM information has authorization for read access to the add-on OPENUTM (Administration Read privilege).
  - ROBAR
    - ROBAR administrator
      A ROBAR administrator has authorization for access to the add-on ROBAR and to its administration on all Management Units.
    - ROBAR operator
      A ROBAR operator has authorization for access to the add-on ROBAR. The administration of the add-on is not allowed.
  - STORMAN
    - STORMAN administrator
      A STORMAN administrator has authorization for access to the add-on STORMAN and to its administration on all Management Units.
    - STORMAN information
      A user with role STORMAN information has authorization for access to the add-on STORMAN. The administration of the add-on is not allowed.
- Service
  The Service role is reserved exclusively for Customer Support.

Overviews of the role-specific tasks and functions are also provided in the “Operation and Administration” manual [2] and in the online help.

When special basic roles are mentioned below, such as BS2000 administrator or Security administrator, this also refers to those user-defined roles which contain these basic roles.

- Individual rights for BS2000 operators

  An administrator or security administrator can grant and deny rights for certain functions of the SE Manager to a BS2000 operator account.

  - Console access to particular BS2000 systems
  - Dialog access to particular BS2000 systems
  - SVP SU /390

  Security-relevant actions

  An administrator or security administrator can release or lock the following functions of the SE Manager for operating (see main menu *Authorizations -> Users -> Operator rights*):

  - Access to the SVP (SE Server with SU /390 only)
  - Access to a BS2000 console on a particular BS2000 system
  - Access to the BS2000 dialog on a particular BS2000 system

3.1.2 User accounts

(User) Accounts are assigned unambiguously to the roles and usages.

The accounts have the following role-specific features:

Administration

- There is the predefined, undeletable local administrator account `admin`.
- Any number of additional administrator accounts can be created.
  These accounts can be deleted again.
- In terms of their functional scope, all administrator accounts are equal.

BS2000 operating

- Any number of BS2000 operator accounts can be created.
  These accounts can be deleted again.
- In terms of their functional scope, all newly configured BS2000 operator accounts are initially equal ranking. The functional scope can be enhanced individually by assigning individual rights.

Accounts with other roles

- Any number of accounts with one of the other base roles resp. with a user-defined role can be created.
  These accounts can be deleted again.
- In terms of their functional scope, all accounts with the same role are equal ranking.

Service

- There is a predefined, undeletable and unchangeable account `service` which is reserved for Customer Support.
  See also section "Further accounts of the base system".

3.1.2.1 Centrally managed accounts (LDAP accounts)

In addition to local accounts, an administrator or security administrator can also permit LDAP accounts for the various roles. These accounts are managed centrally on an LDAP server (in particular also the passwords).

In order to use LDAP accounts, the access to an LDAP server must be configured. In the Management Cluster, access to the LDAP server can be configured specifically for one SE server. See section "Configuring access to an LDAP server". When this requirement is satisfied, the administrator, when creating an account, can release an LDAP account by means of the account type for the desired role. The simultaneous use of a central and a local identifier of the same name is not possible. When an LDAP account is removed, the access of this account is also locked again.

3.1.2.2 Authorization for account management

Other accounts (irrespective of their type) can only be managed under an administrator resp. security administrator account. Specifically, this concerns the following functions:

- Create account
- Delete account
- Managing the password and password attributes for local accounts

Security-relevant actions

- There is an initial default password for the pre-defined account `admin`, which you can obtain from Customer Support.

  Change the password immediately after you have logged in for the first time. You may also change the validity time and the other password attributes.

  You can access the password management as follows:

  - in SE Manager: *Authorizations* -> *Users* -> *Password management*
  - in iRMC S5 resp. S6: *Settings* -> *User Management* -> *iRMC Local User Accounts*

- New accounts which are created should be “personalized”.
  This enables the assignment of an account to a person to be recognized immediately from the name.
- When you create an account, you assign a password which must be 6-20 characters in length.

3.1.2.3 Further accounts of the base system

The following accounts are reserved for Customer Support:

- `service`
  The `service` account is used by Customer Support (locally and by means of remote service) as an access and diagnostics account.

  > The `service` account (account with the Service role) is displayed in user management, but it is not subject to account management by an administrator resp. security administrator.
  > The following accounts of the base system are not displayed in the user management and are not subject to account management by an administrator resp. security administrator.

- `tele`
  The `tele` account is used by Customer Support as an access account and by the user to operate the shadow terminal. There is no other functionality available under this account.
- `root` and `vroot`
  The `root` account is locked. The `vroot` account is a virtual account without a shell and without a home directory. It is reserved exclusively for the Support Center to permit the rights of the `service` account to be escalated (extended) further than envisaged.

The following accounts which are also required internally but which are not visible to the user and locked for login also exist:

- `x2kinternal` for internal accesses
- `storman` when the add-on pack STORMAN is installed
- `opensm2` when the add-on pack OPENSM2 is installed
- `openutm` when the add-on pack OPENUTM is installed
- `robar` when the add-on pack ROBAR is installed
- Several further accounts for internal functions, e.g. the AIS account `aisconnect`

3.1.2.4 Accounts for add-on packs

The following is generally applicable for add-on packs:

- Add-ons have as a rule an own role concept.
- In the SE Manager, explicit permissions for individual add-ons are assigned by add-on-specific roles:
  - A prerequisite for access to an add-on is an account with an add-on-specific role.
    Thus, the account has access to all instances of the add-on in the SE administration area.
  - The role or authorization within the individual add-on results from the role defined for the account in the SE Manager.
- The mapping of SEM roles with access to add-ons to the individual add-on internal roles or permissions is shown in the following table ("-" means no access; basic roles not shown do not have access to any add-on):

SEM Basic role	openSM2	openUTM	ROBAR	STORMAN
Administrator	Administration	Master + Administration Write	Administrator	Administrator
Service	Administration	Master + Administration Write	Administrator	Administrator
OPENSM2 administrator	Administration	-	-	-
OPENSM2 information	Monitoring	-	-	-
OPENUTM administrator	-	Master + Administration Write	-	-
OPENUTM operator	-	Administration Write	-	-
OPENUTM information	-	Administration Read	-	-
ROBAR administrator	-	-	Administrator	-
ROBAR operator	-	-	Operator	-
STORMAN administrator	-	-	-	Administrator
STORMAN information	-	-	-	Storage info

3.1.3 Authentication

Access to the SE Manager of an MU is only possible by means of authentication using an account and password. To increase security, multi-factor authentication (MFA) can be configured for each account. In this case, when logging in to the SE Manager, after entering the account and password, a one-time password must be entered additionally in a second step. This is generated with the help of an authentication app.

For local accounts, the password stored in the `/etc/shadow` file is checked for authentication purposes.

A permanently specified PAM configuration (PAM = Pluggable Authentication Modules) is used for authentication purposes. The PAM configuration is used in the following cases:

- SSH login at shell level
- Login on the web interface
- Login on the desktop of the local console

Passwords are hidden during entry (they are displayed as dots) and can consequently not be read by unauthorized persons.

Each authentication is recorded in the audit logging.

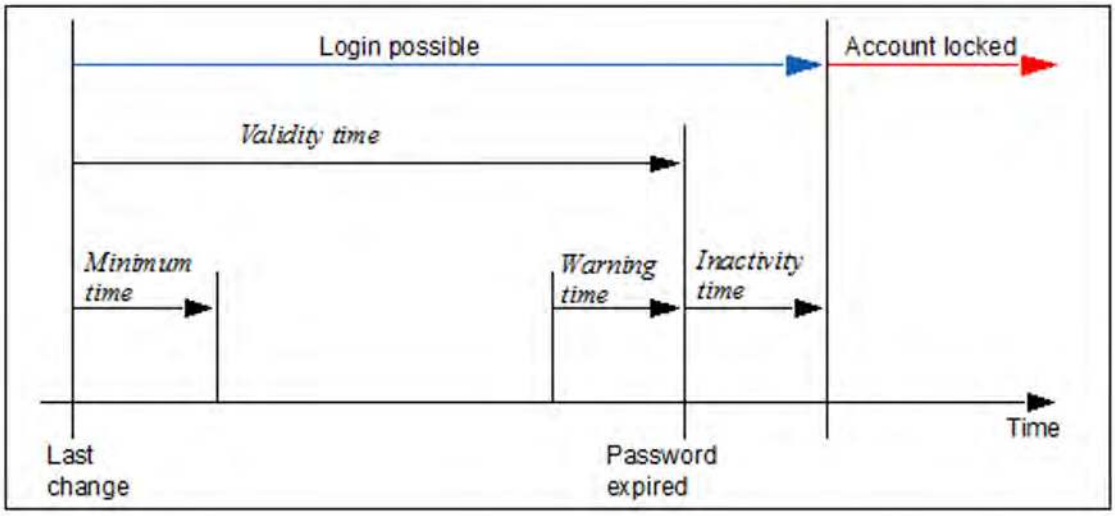
If the login fails in the SE Manager, you can only log in again after a wait time of 10 seconds. This wait time protects against automated trial and error attacks.

3.1.4 Password administration for local accounts

The passwords of the local accounts have the following attributes:
Validity time, *Warning time, Minimum time, Inactivity time*

- During the validity time, which applies from the last time the password was set, it is possible to log in without restriction.
- During the minimum time, non-administrators cannot change their own password.
- During the warning time, a warning is issued that the password will soon no longer be valid. However, it is possible to log in without restrictions.
- During the inactivity time, the password is no longer valid, but it is still possible to log in.
  Directly after a user has logged in, a request to change the password is issued.
- After the inactivity time has elapsed, the account is locked. It can be opened again from an(other) administrator or security administrator account or, if necessary, by Customer Support.
- The value -1 for the *Inactivity time* results in the inactivity time not elapsing.
- The value *99999* for the *Validity time* means, in practice, that you need not change the password.

The figure below shows the relationship between these times.



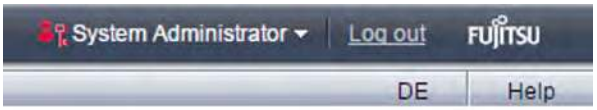
On the basis of the settings for system hardening, customer accounts are created with the following default values for password administration:

- Validity time of the password: 60 days
- Minimum time before the password is changed again: 7 days
  The minimum time is irrelevant for an administrator account and is always displayed as 0.
- Warning time before the password expires: 7 days
- Inactivity time after the password expires: 7 days

Every administrator and security administrator can change individual password administration settings of an account at any time.
Other users can only change the password of their own account. However, this is only possible if the minimum time has elapsed.

When you log in on the web interface, the following situations can occur with regard to the password status and password administration depending on your role:

- If the current account is in the warning time, this is shown by a warning icon in the title bar of the main window:

  In addition, a tool tip shows the user after how many days his/her password will expire.
- If an account is in the inactive time, it is still possible to log in, but a change of password is forced immediately in the login window.

- If the inactivity time has elapsed, the account is locked and it is no longer possible to log in. Intervention by an (other) administrator, security administrator or Customer Support is then required (see "Security-relevant actions").

At shell level, the familiar behavior on Linux systems applies when logging in:

- During the warning time a warning is issued in the course of the login, e.g.:
  `Your password will expire in 2 days.`

  > **Attention!**
  > The `passwd` command must not be used at the shell level!

  In this situation, the user should log in on the SE Manager and change the password even before the warning time expires.
- During the inactivity time a change of password is forced in the course of the login.

  In this situation, the user must act as follows:

  1. Abort the log in to the shell.
  2. Log in on the SE Manager and change the password in the login window.
  3. Repeat the log in to the shell.
- If the inactivity time has elapsed, the account is locked and it is no longer possible to log in. The login fails without any reason being given.

Security-relevant actions

- An administrator or security administrator can adjust the settings for password administration so that they comply with the security policy in the data center.
  The settings can only be changed for individual accounts and not globally for all accounts on the system.
- Each user is requested to maintain their password in accordance with the security policy in their data center.
- It can occur that an account is locked because the inactivity time was exceeded. In this case an(other) administrator or security administrator can cancel the lock for this account for exactly one login. The *Enforce password change* function (see online help) is used for this purpose.
- Customer Support is always able to cancel a lock for an account.

3.1.5 Configuring access to an LDAP server

The *LDAP* tab in the *Authorizations -> Configuration* menu enables you to configure and edit the access to an LDAP server on which the LDAP accounts are managed that can be released for the MUs of the SE server.

¡ In a Management Cluster, you can configure one LDAP server per SE server. Two redundant MUs in one SE server share the same LDAP server.

The LDAP server and the MU(s) must synchronize their time via the same NTP server.

In a Management Cluster, the configurations for each SE server are displayed in individual groups. The LDAP configuration is SE server-specific, but in the default mode it is configured for the involved SE servers together (i.e. they get the same configuration). For more information on the LDAP configuration in the Management Cluster, see the "Cluster Solutions for SE Servers" whitepaper [7].

¡ **Security-relevant actions**

As administrator or security administrator you can configure and edit the access to an LDAP server. For access, you need a valid account on an LDAP server (Bind DN) with a password.

- When you enter or change the access data, you can test if the LDAP server configuration works correctly. You can only work with LDAP accounts if the test was successful.
- As soon as you activate the access and a connection to the LDAP server is established, the released LDAP accounts can be used to log in on the SE Manager.
- As soon as you de-activate the access, the released LDAP accounts can no longer be used.
- As soon as you delete the LDAP configurations, the configuration data are removed and the LDAP accounts can no longer be used to log in on the SE Manager. The valid accounts on an LDAP server still exist.
- The communication between the SE server and the LDAP server can be secured by TLS (port 389 by default) or by LDAPS (port 636 by default).
- If LDAP is used, the port configured in SEM (e.g. the stadard ports 389 resp. 636 - see above), and ports 88 and 750 for Kerberos must be open in the firewall.

3.2 Access to the SE Manager

The description is divided into the following sections:

- Security settings on the administration PC
- Communication with encryption
- Session management

3.2.1 Security settings on the administration PC

The software requirements for the administration PC are described in the "Operation and Administration” manual [2] and in the online help. Of these requirements, the following points are relevant to security:

- **The execution of JavaScript in the web browser is both possible and permissible**.
  If the execution of JavaScript is not permitted on the administration PC, the SE Manager cannot be used.
- **Cookies are permitted in the web browser**.
  If no cookies are permitted on the administration PC, the SE Manager cannot be used.

  The SE Manager generates and uses a number of cookies:
  - One cookie is used to manage the session.
  - Another cookie stores - on a cross-session basis - the language setting selected explicitly by the user in the SE Manager.
  - In addition, further temporary cookies are used to manage current settings (e.g. whether the tree structure is expanded or collapsed) or for other technical purposes (e.g. for variable object lists in the tree structure).

> **Security-relevant actions**
>
> Depending on the configuration, web browsers offer the *Store password* function. You are recommended not to use this function because then a *Show password* function which displays passwords in plain text is as a rule also available.

3.2.2 Communication with encryption

HTTPS (HyperText Transfer Protocol Secure) is always used for communication, whereby encryption protocols SSL 3.0 (Secure Sockets Layer) and TLS 1.3 (Transport Layer Security) beneath HTTPS are supported. TLS 1.1 is used for the internal communication with administered AUs.

Automatic redirection to HTTPS takes place for HTTP calls. This applies both for external communication between the administration PC and one of the systems Server Unit, Management Unit or HNC, and also for internal communication of these systems with each other.

3.2.3 Session management

The SE Manager of the system concerned is protected against unauthorized access both by authentication and by session management.
Following the login, one session whose validity is constantly monitored is set up for each client (browser instance of the calling web browser) and system.

In the *Authorizations* -> *Users* menu the *Sessions* tab informs the administrator about all sessions of users which are currently logged in on the SE Manager. In addition to the information on the user and IP address of the PC, the current individual setting for the session is also displayed.

A session ends in the following cases:

- Explicitly because of *Log out* in the header area of the main window
- Because of a session timeout (default: after 20 minutes of inactivity on the SE Manager)
- An administrator or security administrator may cancel a session

In all cases you are shown the login page to permit you to log in again, immediately in the case of *Log out* and, if the session timed out, with the first action that occurs after the session timeout.

Windows in which terminals are opened are not subject to session management. This guarantees interrupt-free usage of the following additional functions:

- Accesses to the BS2000 console and BS2000 dialog
- Access to the CLI (shell)
- Access to the shadow terminal (Remote Service)
- Access to the SVP console of the SU /390

Security-relevant actions

Each user can change the setting for the session timeout for himself/herself personally:

> Click in the login information in the header area. A list containing the menu item *Individual settings* opens.

> Click *Individual settings*. The *Change individual settings* dialog box opens in which you can enable /disable the session timeout and set the timeout in the range from 5 to 60 minutes.

The individual setting is stored on a browser-specific basis.

In addition to the lock for the administration PC, the following protective measures are also recommended when you leave your workstation:

- Explicit logout from the SE Manager.
- Close all windows which have a terminal loaded.
  If the application has its own lock mechanism (e.g. the console monitors), the window can stay open and the lock mechanism provided can be used.

3.3 Text-based access (at shell level)

Access functions in the SE Manager

When the functions below are called, a terminal which is integrated into the SE Manager is loaded into a separate window:

- Accesses to the BS2000 console and BS2000 dialog
- Access to the SVP of the SU /390
- Access to the CLI with execution rights for a restricted set of CLI commands (see "CLI command reference" in the online help under *General information -> PDF documents*)
- Shadow terminal (on the *Remote Service* tab)

Login and session integration

When the terminal window is called, the session of the SE Manager is checked and no further login is required. Subsequently the terminal window remains open irrespective of the session.

Encrypted communication with Secure Shell

Communication is always encrypted and the SSH protocol is used. This applies for both internal communication (e. g. for the connections to BS2000 consoles on the SU x86) and for external communication (e.g. between the SSH client and the MU).

No rights escalation

No rights escalation is possible in the base operating system using the Linux command `su`.

3.4 Alternative accesses with Secure Shell

For communication at shell level, as an alternative to the terminal integrated into the SE Manager you can use the SSH client PuTTY (Version 0.63 and higher). See section "Alternative access to the BS2000 operating system with PuTTY".

The examples below refer to the SSH client PuTTY.

Secure Shell host key

During system installation, a host key is created on the system.

The first time a connection is set up, you must confirm this host key (depending on the SSH client) as in the following example with PuTTY.

Communication using Secure Shell keys

SSH authentication is possible not only using an account and password, but also by means of an SSH key pair.

This type of authentication should be preferred above all when programming automated procedures because a password then does not need to be coded in plain text.

> **Security-relevant actions**
>
> As administrator you can store SSH key (pairs).
>
> You can provide additional protection for the stored keys by means of “passphrases”.
> The key management associated with this is described in detail in the next section.

3.4.1 Generating the keys

In SSH authentication and encryption are based on the asymmetrical system of public and private keys. Encryption and decryption are performed using different keys. Thereby it is not possible to derive the key for decryption from that used for encryption. For this purpose the user generates a key pair consisting of one public and one private key. The public key is intended for forwarding to other users, whereas the private key is not forwarded by the user.

The two keys are used as follows:

Authentication

- When a user logs in on a remote system, this system generates a random number, encrypts it using the user's public key and returns it to the local system. The appropriate private key is required to decrypt this coded random number; the decrypted date is now sent back to the remote system, where it is checked, thereby the owner of this private key authenticates himself/herself.
- The private key enables signatures to be generated (e.g. for a digital signature). A signature generated with a private key cannot be copied by anyone who does not have this key.

Everybody who has the associated public key can verify whether a signature is genuine.

Encryption

- The public key can also be used to encrypt a message to someone who has the associated private key.
- Only someone who has the associated private key can decrypt such a message.

As the public key is only used to encrypt a message, not too much care must be taken to ensure that it does not fall into the wrong hands (in contrast to the private key).

Generating the keys

Various algorithms are available for generating such key pairs, the best known being RSA and DSA. Under Linux they are generated by calling the `ssh-keygen` command (see http://www.openssh.com). Only Version 2 RSA keys can be used. The minimum key length is 512 bits. In general, 1024 bits are considered sufficient. The keys generated are stored in the local file system:

The RSA authentication identity is stored in the `$HOME/.ssh/id_rsa` file and the public RSA key in the `$HOME/.ssh/id_rsa.pub` file.

The DSA authentication identity is stored in the `$HOME/.ssh/id_dsa` file and the public DSA key in the `$HOME/.ssh/id_dsa.pub` file.

The key pairs can also be generated using a GUI-based tool. In this context the PuTTY key generator is described in the section "PuTTY with PuTTYgen and Pageant".

Distributing the public keys to communication partners

In the next configuration step the user must enter the public key in the `$HOME/.ssh/authorized_keys` file on all remote systems with which he/she wishes to communicate. This can be done, for instance, by copying the local identity file for the public key to the remote systems and appending its content to the `$HOME/.ssh/authorized_keys` file there.

Passphrases

The private key may not fall into the wrong hands. A few separate protection mechanisms are provided in SSH to prevent this. The `ssh` program issues a warning if the local identity file can be read by anyone other than the owner. A passphrase can be specified when a key pair is generated. This passphrase is used to encrypt and decrypt the private key when writing to or reading from the identity file.

You are recommended to protect the private key with a passphrase.

A passphrase is an extension of the password. It can be a sequence of words, numbers, blanks, punctuation marks and other arbitrary characters. Good passphrases are 10 to 30 characters long and contain a sequence of uppercase and lowercase letters, numbers and non-alphanumeric characters which are not easy to guess.

Unlike a password, a passphrase is not transferred to a remote computer as part of the authentication procedure.

There is no way of recovering a lost passphrase. Once it has been lost, a new key pair must be generated and its public key must be distributed to the communication partners.

3.4.2 Using SSH agents

> The use of an SSH agent makes it unnecessary to type in the (normally long and complex) passphrase each time the `ssh` program is called.

In an initialization run for SSH the key pairs are generated, stored in the local files and distributed to the communications partners. The SSH agent is started at the beginning of an interactive session and at the start of a script by calling the `ssh-agent` command (see http://www.openssh.com). The necessary private keys are then transferred to it by means of `ssh-add`. The SSH agent maintains these private keys in encrypted form in the memory. For this decryption process it requires the passphrases, if any were specified.

From this point until the SSH agent is terminated, SSH clients contact the SSH agent automatically for all key-related operations. If a remote connection is to be set up by means of an `ssh` call, the local SSH agent and the remote sshd daemon automatically execute the required authentication procedure.

If a passphrase is used, it needs only be entered once. It is read from the current terminal by `ssh-add` if `ssh-add` was started from the terminal. If no terminal has been assigned to `ssh-add` but the `DISPLAY` and `SSH_ASKPASS` variables are set, the program specified by `SSH_ASKPASS` is executed and an X11 window for reading the passphrase opens. This is useful if `ssh-add` is called in a .Xsession or in a startup script.

Example

```
ssh-keygen -b 1024 -t rsa -C <comment> -N "<passphrase>"
# Generates a 1024 bit RSA key in SSH Version 2 protected by a passphrase
ssh-agent /bin/csh # The path to a shell or a shell script can be specified as an argument
ssh-add # By default loads all keys of the identity file
```

The environment variables which point to the SSH agent's socket must be set to permit the SSH client to communicate with the agent. The `ssh-agent` program supplies the information required for this purpose when it returns:

Example

```
# In SSH Version 2 Notation:
SSH2_AUTH_SOCK=/tmp/ssh-JGK12327/agent.12327; export SSH2_AUTH_SOCK;
SSH2_AGENT_PID=12328; export SSH2_AGENT_PID;
```

These output commands of the `ssh-agent` program can be executed by means of the `eval` command. Please note the reverse quotes (`) here:

```
eval `ssh-agent ...`
```

The `eval` command instructs the shell to execute the `ssh-agent` command and then to execute the commands generated by it. The shell variables `SSH_AUTH_SOCK` and `SSH_AGENT_PID` are then available. After the `eval` `` `ssh-agent` `` command has been executed, the SSH agent's PID is output.

The `eval` `` `ssh-agent` `` command should be included in the ~/.bash_profile file.

Shell scripts

If SSH shell scripts are to be used, the SSH agent can be installed, the correct environment can be set and the agent can be supplied with the necessary keys and passphrases in an initialization phase or in a startup script before the script is started with the `ssh` calls.

In addition, the SSH script must be instrumented in order to set these values in the environment variables. To do this, the output of the `ssh-agent` program must have been stored in an auxiliary file which is then executed in the script by means of the dot command.

Example

```
ssh-agent|head -2 > <auxfile> # Store environment in initialization phase
:
:
:
. <auxfile> # Set environment in script
```

3.4.3 PuTTY with PuTTYgen and Pageant

This section describes how key pairs are generated and how the public keys are distributed with the help of PuTTY (see http://www.chiark.greenend.org.uk/~sgtatham/putty). PuTTY is a free implementation of Telnet and Secure Shell for Win32 and Unix system-based platforms and is useful in interactive mode.

- Key generator PuTTYgen
- Authentication agent Pageant

3.4.3.1 Key generator PuTTYgen

The PuTTYgen (see http://the.earth.li/~sgtatham/putty/latest/htmldoc/Chapter8.html) key generator generates pairs of private and public keys which can be used with PuTTY, PSCP and Plink, and also by PuTTY's authentication agent Pageant.

The general procedure for generating a new key pair using PuTTYgen is as follows:

> Select the type of key (RSA for SSH Version 2, or DSA for SSH Version 2) and specify the key length.

> Click *Generate* and during generation move the mouse pointer in the window area.

  When the key has been generated, the layout of the window changes: the entire key is displayed and then the *Key fingerprint* box shows the fingerprint value, a short name for the generated key.

> Enter a passphrase in the *Key passphrase* and *Confirm passphrase* boxes. If these boxes are left empty, the private key is stored in the file in unencrypted form. This should not occur without a cogent reason.

> Click *Save private key*.

  PuTTYgen then opens a dialog box to ask for the storage location.

> Select a directory and a file name.

  The file is stored in the format used by PuTTY (file name extension .ppk).

> Click *Save public key*.

  PuTTYgen then opens a dialog box to ask for the storage location.

> Select a directory and a file name.

The public key does not necessarily need to be stored locally on disk. You can also copy it directly to PuTTY sessions which run on the remote servers concerned. Proceed as follows to do this:

> Set up a connection to these servers by means of PuTTY.

> Then switch to the $HOME/.ssh located there and open the `authorized_keys` file with an editor (if no public key exists there yet, one must first be generated).

> Switch to the PuTTYgen window, select the entire text in the *Public key for pasting into authorized_keys file* box, and copy it to the clipboard.

> Return to the PuTTY window and enter the data from the clipboard in the open file. Pay attention that all the data is contained in one line.

> Save the file.

3.4.3.2 Authentication agent Pageant

PuTTY's authentication agent Pageant (see http://the.earth.li/~sgtatham/putty/latest/htmldoc/Chapter9.html) keeps the decrypted private keys in the memory and, if required, generates signatures and handles the authentication procedure.

You list the keys stored by Pageant as follows:

> Start the Pageant program.

> Right-click the Pageant icon in the taskbar.

  A menu opens.

> Select *View Keys*.

  Pageant's main window opens, which incorporates a list box containing all the private keys currently stored by Pageant.

If the required key is not yet included, enter it as follows:

> Click *Add Key*.

  Pageant then opens the dialog box *Select Private Key File*.

> From this dialog box select the file which belongs to your private key and click *Open*.

  Pageant then loads the private key into the memory. If the key is protected by a passphrase, Pageant requests this passphrase.

  As soon as the key is loaded, it appears in the list box of the main Pageant window.

You can now start PuTTY and open an SSH connection to a system which accepts your key. PuTTY recognizes that Pageant is running, fetches the key automatically from Pageant, and uses it for authentication purposes. You can now open further PuTTY connections without having to type in the passphrase each time.

3.5 Access via the local console

Access to the local console and physical access to the system is as a rule already protected because various locks and restrictions apply when accessing the data center.

On the local console on the SE server (rack console) you can operate the console switch using a hot key and switch between the existing units of the types Management Unit, HNC, Server Unit x86 and Application Unit.

For Application Units, see the section "Access via the local console".

Access to the Management Unit with Linux desktop

When you access the Management Unit via the local console, the user interface you obtain is a Linux desktop.

You can log in under any account.

The functionality of the desktop is identical for all accounts.

The Firefox web browser is anchored in the *Computer* menu. You can use it to call the SE Manager (addressed, for instance, with *https://localhost*).

As with remote operation, further authentication must be provided for the SE Manager with the current account. After you have logged in successfully, the SE Manager offers the functionality for the user role which corresponds to the account.

Other functions of the desktop on the local console include functions for calling a terminal window, for locking the screen, for configuring the screen saver and the mouse, and for logging out.

Security-relevant actions

- When you leave your workstation, at least the screen should be locked.
  Caution: the screen contents survive beyond a logout and login.
- If you are absent from the workstation for a lengthy period, you are recommended to log out. The screen contents are then lost.
- In the event of inactivity, the screen saver locks the desktop.
  The default timeout setting for the desktop is 10 minutes. You can adjust this setting to your requirements.

3.6 Access to the iRMC of the Management Unit

The iRMC of the Management Unit can be used optionally. It must be connected to the public management network MANPU to permit this.

Access to the iRMC is possible via the SE Manager:
In the *Hardware -> Units -> [<se-server> ->] <mu> -> Information* menu the *System* tab shows the field *iRMC address* with a link to the iRMC.
Via this link you can open the iRMC's web interface.

The predefined account `admin` is available to the administration on the iRMC.

The following functions are recommended for administration purposes:

- Powering the Management Unit on/off (System *Power Button* from the iRMC's web interface)
  Power On enables the Management Unit to be started up remotely.
- Changing the local password (by command only)

Security-relevant actions

- **User management**
  - The SE server is delivered with an initial password for the pre-defined `admin` account, which you can obtain from Customer Support resp. can be seen on the ID card as of MU M5. At iRMC level `admin` has the operator privilege and the additional privilege of console redirection. No further configuration possibilities are available.
    Change the password immediately after you have logged in for the first time!
    This is possible with the M2000 command `rmcPasswdAdmin` which is executable under any administrator account.
  - Further (personalized) accounts can be created by Customer Support on request. These should not, however, be equipped with higher privileges than the predefined account `admin`. However, since administrative activities are extremely rare on the iRMC of the Management Unit, there is no need for further accounts.

CAUTION!

You are urgently recommended not to change the password of the `service` account or to delete this account. If you do, the serviceability of the iRMC is not guaranteed, and the serviceability of the Management Unit is consequently also impaired.
However, if such a measure is necessary, it must always be agreed on with the Support Center.
Nor may the function account `x2kinternal` be changed, otherwise the functionality of the SE Manager will be impaired.

- **Protection functions**
  - You can log out from the iRMC's web interface by means of *Logout*. When you leave your workstation, this can be used as an alternative or in addition to the locking mechanisms of the administration PC.

3.7 Protected access to the BIOS and the bootloader

The BIOS of the Management Unit, HNC and Server Unit x86 is protected by a password which is known to Customer Support.

The bootloader GRUB (GRand Unified Bootloader) which is used by Linux is also protected by a password which is known by Customer Support.

> **i** By default the rack console (local console) is attached to the Management Unit. When you switch over the console switch (see section "Access via the local console"), you can reach BIOS and GRUB of the HNC or SU x86 via the local console.

4 Secure access to systems

This chapter describes secure access to the BS2000 operating system on the Server Units, and to the systems on the Application Units.

- Secure access to BS2000 systems
  - Security in the BS2000 operating system
  - Downloading KVP logging files
  - Alternative access to the BS2000 operating system with PuTTY
- Secure access to systems on Application Units
  - Configuration changes
  - Access to the iRMC / Management Board of the Application Unit
  - Integration of Application Unit into the SE Manager
  - Access via the local console

4.1 Secure access to BS2000 systems

The description is divided into the following sections:

- Security in the BS2000 operating system
- Downloading KVP logging files
- Alternative access to the BS2000 operating system with PuTTY

4.1.1 Security in the BS2000 operating system

The BS2000 operating system provides basic functions for system security. For details, see the “Introduction to System Administration” manual [8].

More extensive security functions in BS2000 are implemented by the software product SECOS, which consists of the following components:

- SRPM (System Resources and Privileges Management),
- GUARDS (Generally Usable Access contRol aDministration System)
- GUARDDEF (GUARDs DEFault protection)
- GUARDCOO (GUARDs COOwner protection)
- SAT (Security Audit Trail)
- SECOS-KRB (Kerberos authentication)

These SECOS components are provided by management systems and interfaces which enable each individual user to define a customized set of rights and duties.

Details are provided in the SECOS manuals ([9] and [10]).

4.1.2 Downloading KVP logging files

The KVP logging files contain the BS2000 operating system history at console and KVP level.

The history contains up to 40 KVP logging files per KVP. When 40 files exist, the oldest is deleted when a new KVP logging file is created.

How far back in time the history goes depends largely on how many messages the system concerned issues.

As administrator or BS2000 administrator you can download the KVP logging files and store them on the administration PC for further use.

You can access the KVP logging files via the respective BS2000 system:

- in Native BS2000 mode via the *KVP logging* tab under *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>)* -> *BS2000*
- in VM2000 mode via the *KVP* tab under *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>)* -> *<bs2000-vm>*

Alternatively, access is possible via the *KVP* tab under *Devices* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>).*

Security-relevant actions

Download confidential data:
When managing the KVP logging files on the administration PC, remember that these files may contain confidential BS2000 data. You must consequently ensure that only trusted persons can access these downloaded files.

4.1.3 Alternative access to the BS2000 operating system with PuTTY

If you use the access to the BS2000 console and BS2000 dialog integrated into the SE Manager, data transmission between the administration PC and the Server Unit and Management Unit takes place at base system level in encrypted format and is consequently secure.

Alternatively secure access to the BS2000 console, SVP console (only SU /390) and BS2000 dialog can be achieved using the SSH client PuTTY (Version 0.63 and higher) under the following conditions:

- There is a connection to the MU.
- A valid administrator, BS2000 administrator or BS2000 operator account (the latter only remote!) is specified. Authentication with password entry or installed ssh key is required.
- The CLI command `bs2Console`, `svpConsole` or `bs2Dialog` with the relevant parameters is specified as the follow-up command. BS2000 operators are granted access only in accordance with their individual rights.
- To avoid line breaks, for a BS2000 console the number of columns should be set to 132. For a BS2000 dialog a character set must be specified which supports the display and the shortcuts which are required in the BS2000 dialog.

Examples for the alternate BS2000 operation under PuTTY can be found in the appendix of the "Operation and Administration" manual [2]. A detailed syntax description of the CLI commands is provided in the CLI command reference, see the SE Manager‘s online help under *General information -> PDF documents*.

4.2 Secure access to systems on Application Units

As administrator you install in-house software (e.g. software for data backup or databases) on the Application Units and perform other administration and configuration tasks both at application and operating system level.

The administration measures on the Application Unit are solely the customer’s responsibility. Consequently you are also responsible for the security of all accesses to the Application Unit and of your iRMC / Management Board (operating system security, password management, forbidding insecure services, administration of the iRMC / Management Board, serviceability, etc.).

> The security in the Application Units has no influence on the security in the other systems on the SE server.

4.2.1 Configuration changes

By default, Application Units are integrated into the status monitoring and the remote service procedures of the SE server. This requires configuration measures in the SNMP configuration of the Application Unit.

SNMP configuration

The Management Unit starts queries to the SNMP agent on the Application Unit in order to obtain information about managing the Application Units.

Details of how to integrate the Application Unit into the status monitoring are described in the “Operation and Administration” manual [2] and in the online help.

Security-relevant actions

- When you define or modify the SNMP configuration required for status monitoring, you should ensure that only SNMP queries from the Management Unit are allowed.
- Port 161 in the firewall must be opened for the SNMP queries.
- If you want to monitor the Application Unit or applications running on it by means of SNMP or one or more management stations, the information on the actions which are relevant to security is provided in the section "SNMP".

4.2.2 Access to the iRMC / Management Board of the Application Unit

For Application Unit PY, access is via the iRMC, for Application Unit PQ via the Management Board.

Using the iRMC / Management Board of an Application Unit is mainly intended for the following scenarios:

- User management on Application Unit

  Security-relevant actions

  - The `semuser` account is used by the SE Manager as fixed access and may not be deleted by the administrator resp. security administrator (see also section "Integration of Application Unit into the SE Manager").
    After configuration by the Customer Support, the `semuser` account is protected with an initial password, which you can obtain from Customer Support. **Change this password immediately after startup.**
  - It is possible to create further (personalized) accounts. When you do so, note the privilege strategy predefined on the iRMC / Management Board.
    You should disable accounts which are not used.

- Powering on/off the Application Unit
  For this purpose the predefined account `admin` is available to the administration on the iRMC / Management Board.
- Remote access to the Application Unit console using the “Video Redirection” function. The functionality corresponds to Access via the local console.

  Security-relevant actions

  Protection functions

  - You can log out from the iRMC’s / Management Board‘s web interface by means of *Logout*.
    When you leave your workstation, this can be used as an alternative or in addition to the locking mechanisms of the administration PC.
  - The iRMC’s / Management Board‘s web interface can also be protected against unauthorized access by a *Session Timeout*. The session times out if no activity is detected on the web interface for a particular period (timeout period).
    You must then log in again.
  - This behavior can be configured resp. viewed in the following iRMC menus:
    - iRMC S5 resp. S6 Web Server: under *Settings -> Services -> Web Access -> Session Timeout*
    - If needed, the service can configure this for you.
    - The session timeout configuration applies to all accounts.

4.2.3 Integration of Application Unit into the SE Manager

Access to the iRMC / Management Board of Application Unit

To integrate the Application Unit into the SE Manager (status information, switching on / off, etc.), access to the iRMC / Management Board of the Application Unit is required.

When the Customer Support configures an Application Unit it sets up the fixed account `semuser` with the privileges "*LAN Channel Privilege Administrator*, *Serial Channel Privilege User*" and an initial password.

Details of how to integrate the Application Unit into the status monitoring are described in the “Operation and Administration” manual [2] and in the online help.

Access to the Application Unit

This access is required if the Application Unit is operated with the operating system VMware vSphere ESXi.

The administrator or AU administrator provides an account on the AU and configures it and the access password in the SE Manager:

- *Hardware -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (AU<model>) -> Management -> IP configuration*, action *Change access data* in the respective access data group.

4.2.4 Access via the local console

When you toggle the console switch (see the section "Access via the local console"), you obtain access to the Application Unit's operating system via the local console. The type of access (e.g. shell or desktop) depends on the operating system installed.

You are responsible for providing and managing access accounts.

The range of commands and functions available depends on the operating system used.

Security-relevant actions

- When you leave your workstation you should log out explicitly using the method which corresponds to the interface, e.g. at shell level with the `exit` command.
- Switching over the console switch or switching the console off does not result in an automatic logout.

5 Remote service (via AIS Connect)

Remote service ensures that when a fault occurs a service call is sent to the Support Center from the customer system's Remote Service Endpoint and that Customer Support has the opportunity of establishing a remote access.

The connection is set up over the internet. AIS Connect is configured at the Remote Service Endpoint for this purpose. The Remote Service Endpoint on an SE server is the Management Unit.

When access is permitted, the initiative for connection setup always lies with the customer side in the form of regular contacts of the service agent with the Support Center, which can be reached over the internet. When necessary, the Support Center employs these connection setup options to log in on the customer side.

Jobs from the Support Center to the service agent on the Management Unit (e.g. file transfer, remote access) are received by the latter. The service agent executes these jobs by, for example, establishing the tunnel for them in the case of remote access.

With an SSH session, the service engineer at the Support Center obtains access to the Management Unit under the `tele` account. Since `tele` is only an access account without any further functionality, the service technician generally subsequently changes to the `service` account to perform the maintenance work.

Remote service satisfies stringent security requirements:

- The initiative for connection setup always comes from the customer side. This ensures that only the configured Support Center obtains access to the customer system.
- File transfer always takes place in encrypted format.
- The customer can use the shadow terminal function to observe the work of Customer Support or even to intervene in it. Several security levels can be set.
- The customer can inform himself or be informed about the currently open AIS Connect connections. In emergency situations, they can intervene and terminate an existing connection.
- The work of Customer Support is logged. The customer can read these logs and at all times trace which actions Customer Support performed.
- AIS Connect also supports integration into a proxy server configuration (see "Using the "shadow terminal" function").

Outgoing connections are service calls and regular messages of the system program PRSC (Periodical Remote System Check) which are sent to Customer Support once a week.

Incoming connections are connections which Customer Support creates in order to clear a fault or to implement preventive measures. To do this, Customer Support sets up a connection to the Remote Service Endpoint (Management Unit) and then, if required, switches to the system to be serviced (e.g. the BS2000 system).

If it is necessary, as an administrator (and to a lesser extent as an operator) you can change the remote service configuration or intervene in a service operation which is currently running, see the "Operation and Administration" manual [2].

> **Important!**
>
> Please discuss every change to the remote service configuration with the Support Center, otherwise you will put the serviceability of your SE server at risk.

5.1 Service account

On a Management Unit the `service` account is provided for Customer Support on the base system. Under this account the service engineer works on all available interfaces (web interface, Linux desktop of the local console, shell level), both locally on site and also remotely via the remote service access.

The `service` account can also access the BS2000 console. The following must be taken into consideration when logging entries on the BS2000 console:

- In the KVP logging files it is possible to distinguish the account (e.g. `admin` or `user1`) under which an entry was made.
- In BS2000, on the other hand, only the console (e.g. C0) enables you to recognize who made an entry in the CONSLOG files.
  Consequently console entries of different users are only unambiguously identifiable if every user uses a different console (console mnemonic) when accessing the console.
  To achieve such differentiation, you can assign the BS2000 operator accounts different consoles (by means of individual access rights). For administrator accounts, BS2000 administrator accounts and in particular for Customer Support, it is only possible to reach an agreement on using particular unambiguous consoles.

Security-relevant actions

- Change the console for BS2000 operator accounts
  In the SE Manager, *Authorizations* -> *Users* -> *Operator rights* enables you to enter the console access to a system with a specific console. The change takes effect immediately.
- Define the console in the BS2000 operating system
  It must be ensured that the assigned consoles are defined in BS2000 so that the console access functions.
  You define the consoles in the `/BEGIN OPR` section of the BS2000 parameter files (e.g. `SYSPAR.BS2.nnn`) using the keyword `DEFINE-CONSOLE`. Here the `TELESERVICE=YES` parameter ensures that the console is not taken away from Customer Support (i.e. the console cannot become either a standby console for another console or a master).
  Details on configuring the console are provided in the manual “Introduction to System Administration” [8].

5.2 Logging support operations

The sessions, both SSH and VNC sessions, are always logged. You can view logging files of SSH sessions using the CLI command `aisLog`. You can load logging files of VNC sessions onto your PC and view them there in the web browser.

For information, see the “Operation and Administration” manual [2].

> ¡ As logging files of VNC sessions can become very large, the administrator must check and, if necessary, delete them from time to time.

5.3 Using encryption

Communication always takes place using HTTPS (HyperText Transfer Protocol Secure). The underlying encryption protocols SSL 3.0 (Secure Sockets Layer) and TLS 1.2 (Transport Layer Security) are supported.

5.4 Using the "shadow terminal" function

With the remote service standard configuration the Support Center can at all times access the system and perform its work without any assistance or permission from the customer.

You can adjust the remote service configuration to your security criteria (e.g. lock or open the service access).

The SE Manager provides all the functions you require to administer the service access. You can change the service access and the usage of the shadow terminal at any time (lock it or open it with different settings). You can observe the work the service engineer performs, participate in it or have yourself guided by the engineer.

Irrespective of the access setting, you receive information on the current Teleservice sessions (name of the service engineer and access type) and the current status of the AIS agent.

Security-relevant actions

- Change the Customer Support access:

  The following settings are possible for the service access of AIS Connect:

  - Access permitted, without shadow
    Customer Support obtains access to the system at all times and does not need to inform you to do this. No shadow terminal is available to track the activities of Customer Support.
  - Access permitted, shadow possible
    Customer Support obtains access to the system at all times and does not need to inform you to do this. A shadow terminal can be opened to track the activities of Customer Support.
  - Access permitted, shadow mandatory
    Customer Support obtains access to the system only if you open a shadow terminal beforehand. You can track the support activities on the shadow terminal.
  - Access not permitted
    Customer Support obtains no access to the system.
- Change the AIS proxy configuration:

  If the internet connection is established via a proxy server, the IP address of the proxy server, the port number and, if required, the account and password for the proxy authorization are entered in the AIS proxy configuration.

  If your proxy server configuration changes, you must adjust the AIS proxy configuration accordingly. You must adjust the firewall settings on the proxy server. Only if you do so is serviceability retained.

You execute the specific actions in the SE Manager as administrator or shadow terminal operator (not AIS proxy configuration). The functions are provided in the *Remote Service* tab under *Service -> Units* [*<se server> (SE<model>) ->*] *<unit> (MU)*.

In a multi-MU configuration, you have to perform the same actions on each MU!

A description of how you work with the shadow terminal is contained in the section “Managing the service access” in the “Operation and Administration” manual [2].

5.5 Monitoring the current usage of the service access

Display of remote service sessions

On SEM page *Service -> Remote service sessions* the AIS Connect sessions and AIS Connect logging files are displayed.

The *AIS Connect sessions* group displays the sessions that currently use the service accesses to the Management Unit and to the external assets.

> ¡ Displaying the sessions is only possible in case of direct MU connection, not in case of connection via a gateway.

You can delete a session by using the *Delete* icon. This will abort the current usage of the service access.

> ¡ Because this may abort an important service operation, it should only be done in emergency situations.

In an SE server configuration with multiple MUs, you will receive a complete overview over all service accesses when you view the sessions on each MU.

Notification about remote service sessions (ssh only)

- You can get timely information about the establishment of remote service sessions on ssh level as follows:
  - Each time a service technician logs in remotely, an event is generated for the RemSrv component.
    These events can be seen in SEM in the menu *Logging -> Event Logging*.
  - You can register in Alarm Management for a notification by mail for this component. Then you will be informed immediately about every new remote service session.
    You can configure this in the menu *Logging -> Alarm Management*.
- Additional options:
  - You can force the service technician to identify himself personally when logging in and name the current task. The service technician's specifications become part of the event and are also visible in the alarm mail.
  - You can provide the service technician with information at login that can help him with his work, e.g. information about contact persons in the data center.
  - The necessary configuration options can be found in the menu *Service -> Configuration -> Remote Service Access*.
- In an SE server configuration with several MUs, these settings are global resp. MU-spanning.

5.6 Access to external assets

AIS Connect enables Customer Support connections to be configured via the Management Unit to selected storage systems which in this context are referred to as *external assets*.

These connections are configured by Customer Support in agreement with the customer.

The SE Manager displays the configured external assets in the *Remote Service* tab under *Service -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (MU)*.
As administrator, security administrator or shadow terminal operator you can at all times modify the Customer Support access to specific external assets (allow or not allow).

Security-relevant actions

- Changing Customer Support access to external assets:

  The following settings are possible:

  - Access allowed
    Customer Service has access to the external asset at all times.
  - Access not allowed
    Customer Support obtains no access to the external asset.

  Even in the *Access not allowed* status it is ensured that the Teleservice messages are forwarded to the Support Center.

  In an SE server configuration with multiple MUs, you have to make the same settings on each MU.

A description is provided in the section “Managing service access” in the “Operation and Administration” manual [2] and in the online help.

6 Configuration and diagnostic data

The description is divided into the following sections:

- Configuration data backup
- Diagnostic data

6.1 Configuration data backup

You use a CSR backup (CSR = Configuration Save and Restore) to back up the configuration data of a unit (Management Unit, HNC or Server Unit x86) in an archive.

CSR backups are retained when reinstallation takes place.
In a single-MU configuration, you can use a CSR backup to recreate the configuration of the respective base system as of the time of the backup.

In a multi-MU configuration, there is a difference between MU-specific and MU-global data.

- For MU-specific data:
  The current MU-specific data are replaced by the old data.
- For MU-global data:
  The current MU-global data are not changed, only old, no longer existing MU-global data are restored. The MU-global data are the configured authorizations (accounts, LDAP configuration, IP based access rights), the configuration of the alarm management, the configured Application Units, the configured applications, the configuration of the FC networks, the configured SU Clusters.

> **Security-relevant actions**
>
> As administrator, BS2000 administrator or AU administrator, in the SE Manager you can download configuration data backup archives to the administration PC in order to back them up in case a disaster occurs.
> If required, as administrator you can also upload the backup.
>
> The CSR backup contains base system data which is relevant to security. However, it contains no customer data from your BS2000 systems which are run on or with it.

The data collected in the archives cannot simply be used in the form it is to intrude in or compromise the system. Nevertheless, you should take care:

- When managing the archives on the administration PC, ensure that only trusted persons can access these archives.
- When uploading, ensure that the data in an archive is activated only on the required target system and on no other system beside this.

Recommendation: For the purpose of data security, perform a CSR backup after every configuration change and store it in accordance with your security policy.

Note: A CSR backup contains no account passwords.

6.2 Diagnostic data

An administrator can generate diagnostic data on the units (Management Unit, HNC and Server Unit x86) and make this data available to Customer Support when the latter requires this support.
This function is also accessible for the user roles BS2000 administrator and BS2000 operator.

Security-relevant actions

In the SE Manager, as administrator, BS2000 administrator or BS2000 operator you can download diagnostic data to the administration PC in order, for example, to send it by email to Customer Support.

The diagnostic data contains base system data which is relevant to security.
However, it contains no customer data from your BS2000 systems which are run on or with it.

The diagnostic data collected in the archives cannot simply be used in the form it is to intrude in or compromise the system. Nevertheless, you should take care:
When managing the diagnostic data on the administration PC and sending it to the Support Center, ensure that these diagnostic data can only be accessed by trusted persons.

7 Network security

The description is divided into the following sections:

- Network services
- IP-based access restriction
- Security at Net Unit level
- Net-Storage
- SNMP

7.1 Network services

The table below describes the services which are released in the base system of the Management Unit. Using ACL the services can be restricted further for specific networks, see section "Security at Net Unit level".
HNC and SU x86 are protected by default and are not described in detail.

Type	Name and Port	Application
TCP	ssh (22)	Communication at shell level (e.g. BS2000 console/dialog, SVP console, shadow terminal)
TCP	domain (53)	Integration into the Domain Name Service (DNS)
TCP	http (80)	Communication via this port is always redirected to https (443).
TCP	kerberos (88)	Optional: for Kerberos
TCP	snmp (161)	For reading SNMP access by management stations
TCP	snmptrap (162)	For receiving SNMP traps from the hardware monitoring
TCP	ldap (389)	Optional: for the Lightweight Directory Access Protocol (LDAP)
TCP	https (443)	Communication between the browser (e.g. on the administrator PC) and the system's web interface (e.g. SE Manager)
TCP	ldaps (636)	Optional: LDAP protocol over TLS/SSL
TCP	rfile (750)	Optional: for Kerberos version IV
TCP	iascontrol-oms (1156)	PRSC/prscx (Periodical Remote System Check) regularly sends sign of life messages to the Support Center
TCP	nfs (2049)	Optional: Network File System (NFSv4) [RFC5665]
TCP	caupc-remote (2122)	Optional: AIS gateway
TCP	storman (4178)	Optional: for communication with StorMan (add-on)
TCP	5800	Browser access to the VNC shadow functionality of the remote service (AIS Connect)
TCP	rfb (5900)	VNC viewer access to the VNC shadow functionality of the remote service (AIS Connect)
TCP	10021-10022	In the case of an SKP network (redundant SKP) for SKP-SKP communication
TCP	rs2_rctd (13333)	For remote service connections of BS2000
UDP	domain (53)	Integration into the Domain Name Service (DNS)
UDP	kerberos (88)	Optional: for Kerberos

UDP	ntp (123)	Integration into the Network Time Protocol (NTPI) [RFC5905]
UDP	snmp (161)	For reading SNMP access by management stations
UDP	snmptrap (162)	For receiving SNMP traps from the hardware monitoring
UDP	syslog (514)	For monitoring components (SYSLOG)
UDP	dhcpv6-client (546)	Optional: the DHCPv6 client port is used when a LAN interface is configured accordingly
UDP	loadav/kerberos-iv (750)	Optional: for Kerberos version IV
UDP	multicast-ping (9903)	For monitoring components [RFC6450]
ICMP	-	Internet Control Message Protocol (ping)

Table 1: Ports for incoming connections

These ports are released for incoming connections by means of the packet filter (SuSEfirewall2) which is installed on all the systems. All other ports are locked.

All ports are released for outgoing connections in the packet filter.

A port for incoming connections which is released in the packet filter does not constitute a security risk provided the service using this port is not started because the system blocks every connection attempt.

Note on HNC and SU x86

When using the Net-Storage functionality via the MANPU and DANPU networks, there are direct outgoing connections on these units, but these do not pose a security risk.

Settings of the external firewall

The ports described in table1 may need to be enabled in the external firewall. Exceptions are TCP 10021-10022, which serve the redundant SKP functionality of the MUs within the SE server.

In addition, if necessary, ports for further optional functions with outgoing connections must also be enabled.

- If LDAP is used the LDAP port set in SEM (depending on the chosen protocol 389 or 636 by default), and ports 88 and 750 for Kerberos.
- For the SNMP queries, port 161 must be open in the firewall.
- For traps, port 162.

Examples:

- Connection to an LDAP server, TCP port 389 by default
- NFSv4 port TCP 2049 using Net-Storage functionality
- In the case of ROBAR, the ports required for access to the storage systems must be unlocked.

7.2 IP-based access restriction

The administrator can configure access to the SE server and thus to the SE Manager in such a manner that access is possible only for explicitly entered IP addresses or for IP addresses from an explicitly entered IP network.
In a management cluster the configuation can be done server-specific.

The current setting is shown by the *IP-based access rights* tab in the menu *Authorizations* -> *Configuration*.

By default the list for access restrictions is empty, and access is permitted without restriction for all IP addresses.

Security-relevant actions

- You can alternately deactivate and activate the whole configuration of the IP-based access restriction. (status active/inactive)
  The deactivation might be useful for maintenance or tests, or if one wants to first prepare the configuration and then activate it as a whole.
- With the first entry (IP address or IP network) in activated state you enable the IP-based access restriction to the SE server. Access is then only possible for IP addresses which are entered either explicitly or via an IP network.
  Therefore you should always **observe** the following:
  Make sure that at activation your own IP address (or the subnetwork) is part of the configuration. Otherwise you will lock yourself out and will lose access to the SE server!
- When you delete the last entry from the list for access restriction, access to the SE server is once again possible for all IP addresses without restriction, irrespective of the current status of the configuration.
  The deletion of the entire configuration in one step is also possible.
- In a management cluster the configuration can be done server-specific. Therefore, in a management cluster all actions can be executed server-specific or for the whole management cluster.

7.3 Security at Net Unit level

The services for the various networks can be further restricted at Net Unit level by means of ACL.

You can lock or release individual TCP/UDP ports (services) for the DANPU<xx>, MANPU, MONPU, DANPR<xx>, and MONPR<xx> networks:

- Either the administrator defines an ACL list of the type "permit" in which all released services (ports) are explicitly entered.

  > **i** After the ACL of the type "permit" has been configured, the list is initially empty. Access to the network is thus locked for all services (ports).

- Or the administrator defines an ACL list of the type "deny" in which all the locked services (ports) are explicitly entered.

One ACL list each can be defined for IPv4 and IPv6.

7.4 Net-Storage

As net clients the units HNC and Server Unit x86 support BS2000 access to a Net-Storage. In this case the HNC is the net client for the BS2000 systems which run on the SU /390, and the SU x86 is the net client for BS2000 systems which run on it.

The configuration of the access to a Net-Storage is administered in the SE Manager for each net client:

- The net client requires access rights for the net server which provides the Net-Storage. A user ID and a group ID are entered which have the necessary access rights to the released storage on the net server.
- Each Net-Storage connection must be configured in the network.

7.5 SNMP

Central SNMP integration of the SE server is administered using the SE Manager on the Management Unit. The preconfiguration is created in such a manner that you can also use SNMP to monitor the other units on the management stations provided a configuration for SNMP integration exists on the Management Unit (read access, trap receiver):

- Queries regarding the Server Unit /390 are possible on the Management Unit (see the private MIBs).
- Management stations can address the SNMP agent on the Server Unit x86 or HNC and query data (the SNMP agent supports the MIB-II and private MIBs for queries).
- In defined error situations (e.g. status changes) the SNMP agent on the Server Unit x86 or HNC sends traps to management stations.
- On Application Units, on the other hand, you must configure SNMP yourself.

The following private MIBs must be imported to the management station in order to permit access in read mode and to enable the traps to be interpreted:

- `/usr/share/snmp/mibs/FUJITSU-SESERVER-MIB.txt`
- `/usr/share/snmp/mibs/FUJITSU-SU390-MIB.txt`

At the Management Units and Server Units x86, ServerView RAID periodically checks hardware components. These events are reported by trap, even in good case with the weight `NOTIFICATION`. Text example of such a successful test: "*Patrol Read started*" and "*Patrol Read finished*".

In order for ServerView RAID's traps to be correctly represented by the management station, the MIB `/usr/share/snmp/mibs/FSC-RAID-MIB.txt` must be imported to the management station.

> ¡ The traps usually contain neither the trap weight nor the message text. This information can only be read from the MIB.

Access to MIB files on the Management Unit is, for example, possible under any administrator account with `scp` (secure copy).

> ¡ **Security-relevant actions**
>
> - When creating the SNMP configuration, ensure that only trusted management stations can access the Management Unit resp. the Server Units of the SE server by configuring the read community with a restriction to the management station.
>   - As far as possible use only specific read communities (not *public*).
>   - Grant access only to precisely defined management stations (by specifying their host names).
> - When creating the SNMP configuration, ensure that traps are sent only to trusted management stations from the Management Unit resp. the Server Units of the SE server.
>   - As far as possible use only one specific trap community (not *public*).
>   - Enter only the management stations intended for this purpose as trap receivers.

8 Security of the base system

The description is divided into the following sections:

- Hardening the base system
- Software signature
- Digital certificates
  - Confirming/importing a certificate in the web browser
  - Using the standard certificate
  - Creating and activating a new self-signed certificate
  - Requesting an SSL certificate
  - Uploading and activating a customer-specific certificate

8.1 Hardening the base system

The Fujitsu Server BS2000 SE Series with Management Unit, HNC and Server Unit x86 are systems which satisfy stringent security requirements. The statically implemented security of a hardened system which cannot be influenced by administration activities is involved here.

The base system of the Management Unit, HNC and Server Unit x86 is a Linux system based on SUSE Linux Enterprise Server (SLES) 15.

The base system is used exclusively to administer the systems themselves. No normal user operation with customer applications takes place.

These systems are characterized by the following features:

- Only signed software components which are required for operation are installed.
- The base system software which is used on the systems is supplied on a CD/DVD which contains a checksum. During installation the checksum is used to check whether all the packages on the CD are uncorrupted, i.e. their status is the same as that when they were produced.
- Nonprivileged accounts are used for user access.
- These accounts are equipped with clearly defined (and restricted) functions and access rights as part of a differentiated role concept.
- No access to the system is possible outside of this role concept.
- A rights escalation is not possible in the context of this role concept.
  Access to the `root` account is locked. Rights which are required for maintenance/diagnostics or for updates by Fujitsu Customer Support are implemented by extended rights of the *Service* role.
- The role and user strategies enable personalized accounts to be configured and passwords and password attributes to be managed.
- Actions which lead to configuration or status changes are logged and can be assigned to the persons who perform them.
- The data traffic between administration PCs and the base system is always encrypted.
- All unused network services are disabled.
- Each firewall within a system restricts network access to the network ports required.

The configuration of the base systems is based on the recommendations of the Center for Internet Security (CIS, *http://www.cisecurity.org*).
Deviations from these recommendations occur only with functions which are required for operating the base system (e.g. a web server which provides the user interface is always active for the SE Manager in the base operating system). These deviations from the CIS recommendations do not lead to security gaps.

The base systems of the SE servers are regularly examined by Fujitsu for potentially security-relevant vulnerabilities. In particular, the security advisories and notices published by the Fujitsu PSIRT (Product Security Incident Response Team) and the results of security scans are taken into account. The potential vulnerabilities are evaluated taking into account the hardening and the deployment scenarios of the SE appliances and, taking into account their risk potential, are remedied as required as part of the update process for the SE systems.

In principle, an SE infrastructure is always IT-Grundschutz certifiable according to the rules issued by the BSI (Bundesamt für Sicherheit in der Informationstechnik) and can therefore also be part of environments that must be operated in a KRITIS-compliant manner (critical infrastructure).

- The system components are largely preconfigured on delivery or can be configured as part of the actual construction of an SE infrastructure in such a way that the technical requirements resulting from the relevant system components of the IT-Grundschutz compendium are met.
- With its properties, an SE infrastructure thus also fundamentally supports the implementation of requirements resulting from relevant process building blocks of the IT-Grundschutz compendium.
- However, the internal network architecture of an SE infrastructure does not itself contain a P-A-P structure (Packet filter – Application Layer Gateway – Packet filter) and does not provide a DMZ (demilitarized zone) concept.
  - An SE infrastructure deliberately does not represent a "data center in a box" concept, but it does fit seamlessly into BSI IT-Grundschutz-compliant data center network architectures.
  - In its basic configuration, an SE infrastructure presents itself to the data center network as a simple "compute node".
  - Optionally, however, an SE infrastructure can also implement several virtual network segments using the internal network within the data center network. The Net Unit then represents a "top-of-rack switch".

8.2 Software signature

The software used on the Management Unit, HNC and Server Unit x86 is supplied in packages which are provided with a signature.

- The packages of the underlying base software Linux SLES 15 are signed by the vendor.
- The specific packages for the Management Unit, HNC and Server Unit x86 are signed by Fujitsu.

During installation the signature is used to check whether the status of a package is unaltered, i.e. corresponds to the production status.

If the signature check fails, installation of the package is rejected.

8.3 Digital certificates

To use HTTPS/SSL, not only an SSL key pair is required on the Management Unit, but also a (digital) SSL certificate. This server certificate performs the following two tasks:

- The certificate is always system-specific (contains the FQDN) and proves the online identity of the system concerned for the browser on the administration PC.
- The certificate provides the public key with which the browser encrypts its messages to the server on the administration PC.

A self-signed, system-specific certificate which was generated on the system is preinstalled as the standard certificate on each Management Unit.

You can also use other certificates instead of the preinstalled self-signed certificate. The following options are available:

- Use of a self-signed certificate
  The certificate must comply with the X.509 standard with PEM encoding and the certificate file must have the suffix .key.

  A certificate of this type is preinstalled on the system as the standard certificate. It must be explicitly confirmed or imported on any browser with which the SE Manager operates.

- Use of a customer-specific certificate (signed by a customer CA)

  If the customer-specific policy specifies the use of such a certificate, it can simply be installed.

  The certificate is as a rule derived from a customer-specific root certificate. Such a certificate is known to the browsers the customer uses and is accepted without an inquiry (i.e. without being confirmed or imported).

- Use of a commercial certificate (signed by a root CA)

  A certificate of this type is created for a fee by a trusted root certification authority (CA) and is therefore known to all browsers. Consequently every browser accepts such certificates without an inquiry.

8.3.1 Confirming/importing a certificate in the web browser

If the web interface called uses a self-signed certificate (i.e., for example, the preinstalled standard certificate), web browsers reject the call for the page because, from their viewpoint, the certificate is not trusted.

To permit pages of the SE Manager to be loaded in the browser at all, you must either temporarily accept the certificate error or you can download the Management Unit's CA certificate and import it permanently in the browser.

The procedures described in principle below are based on Firefox browser and differ according to the browser used and the version. You will find details of the specific procedures in your browser's online help.

Downloading a CA certificate and installing it in the browser

To prevent a certificate error in future, you can download the current Management Unit's CA certificate (if necessary the customer-specific CA certificate) and install it in the browser.

> ¡ In an SE server configuration with multiple MUs, you have to perform the same actions for each MU.

> Select *Authorizations -> Certificates ->* [<*mu-name*> (MU)], *Certificates* tab. The table displays the current certificate of the MU:

> In the *Issued by (CN)* row click the *Download CA certificate* icon.

The `sslCertCA` command serves to display, copy, or output the current CA certificate of the MU.

After the download, you can install the certificate in your browser.

> Open the certificate file (standard name **<*mu-name*>-ca.crt**) and answer the security warning that displays "*Unknown Publisher*" by clicking *Open*.

The information of the certificate is shown:

> Select *Install Certificate...*.

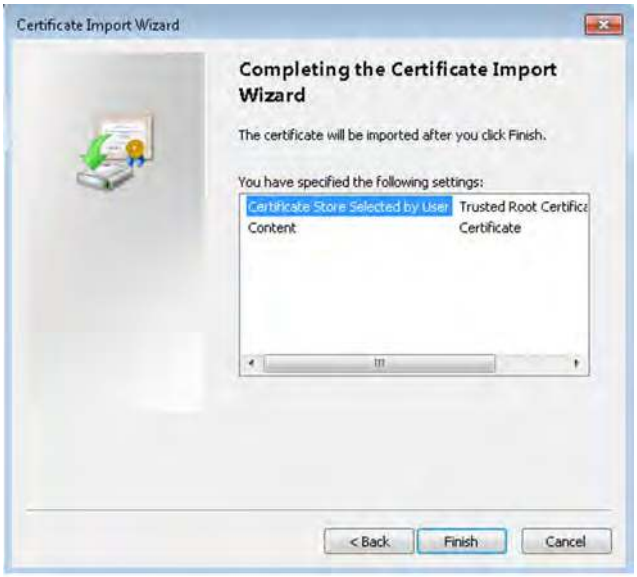
The browser's certificate import wizard takes you through certificate installation step by step.

> Click *Next*.

> Select *Place all certificates in the following store* option and click *Browse...*:

> Select *Trusted root certification authorities* as the certificate memory and click *OK* and then *Next*:

> Confirm the request that now displays your selection again by clicking *Finish*.



> Confirm the subsequent security warning, which contains the certificate name and the "fingerprint" with *Yes*. The certificate will now be installed.

> After successful import, terminate the certificate import wizard by selecting *OK*:

Temporarily accepting a certificate error

> Open your web browser.

> In the browser window call the SE Manager of the required system.

The web browser reports a certificate error.

> Confirm that the website should be loaded.

You are shown the login page. The browser's address bar displays *Certificate Error* as a warning.

You obtain information on the possible security risk when you click *Certificate Error*. Check the certificate displayed. Continue only if no doubts exist about the certificate.

The certificate has now been temporarily accepted for this session, and you can now work with the SE Manager of this system.

8.3.2 Using the standard certificate

A self-signed, system-specific certificate is preinstalled on the Management Unit. This is not known directly by the web browsers, nor is it derived from a known root certificate.

A standard certificate is automatically generated and activated each time the Management Unit is renamed (the FQDN is changed). The new standard certificate must then of course be accepted by or imported to the browsers.

The main features of this certificate are:

- The *Common name (CN)* is identical to the fully qualified domain name (FQDN) of the base operating system.
- The Validity period is 10 years.
- The fingerprint which unambiguously identifies the certificate is generated using the SHA-1 algorithm and RSA encryption.

As the browser does not know the self-signed certificate, when the SE Manager is called it requests the user to accept the certificate temporarily for the current session or to import it permanently.

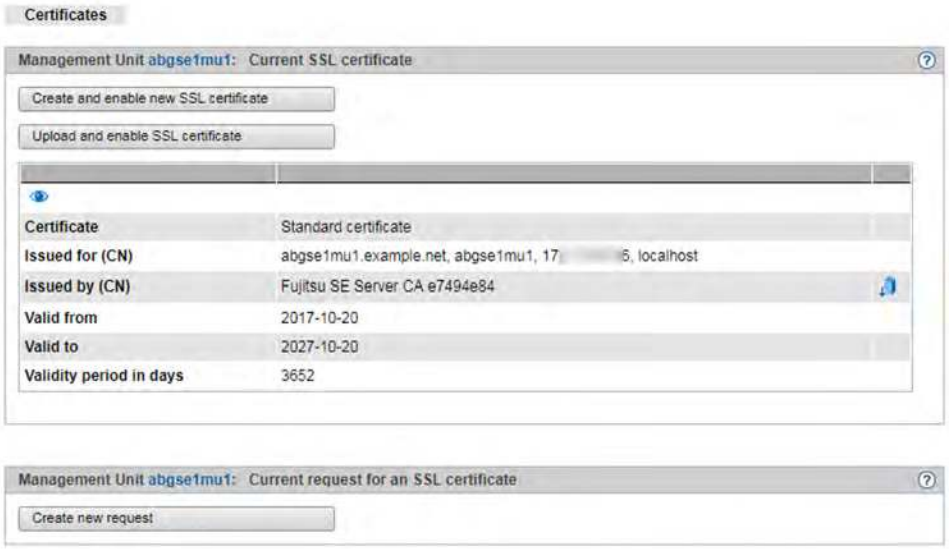
If you call the SE Manager on the local console, you must also confirm or import the standard certificate, because the browser used on the desktop of the local console does not know the certificate, either.
You are granted access to the SE Manager of the system component only if the certificate is temporarily accepted or permanently imported.

If in doubt, you should first read and cross-check the certificate before accepting it temporarily or importing it permanently.

Displaying the current certificate

> Select *Authorizations* -> *Certificates* ->[<*mu-name*> *(MU)*], *Certificates* tab.

An overview of the most important attributes of the current certificate is displayed in the work area.



Certificate

Type of certificate: *Standard certificate* or *User-defined*

Issued by (CN)

FQDN of the server for which the certificate was issued.

Issued by (CN)

Issuer of the certificate (e.g. organization). In the case of user-specific certificates this is also the FQDN of the server for which the certificate was issued.

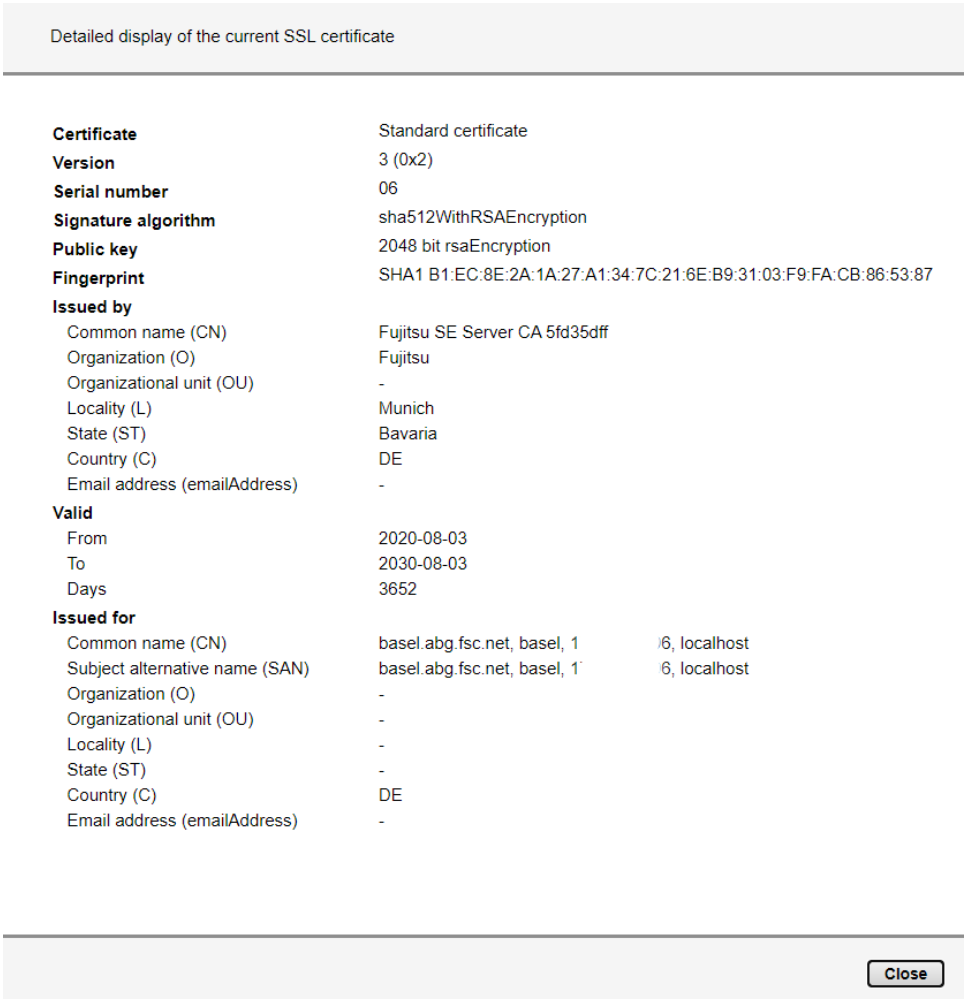
Information on the attributes *Valid from*, *Valid to*, *Validity period in days* and *Email address (emailAddress)* is provided in the online help.

Detailed display of the certificate

> Select *Authorizations* -> *Certificates* -> [<*mu-name*> *(MU)*], *Certificates* tab.

> Click the *Details* icon ( ).

All the attributes of the certificate are displayed in a dialog.



8.3.3 Creating and activating a new self-signed certificate

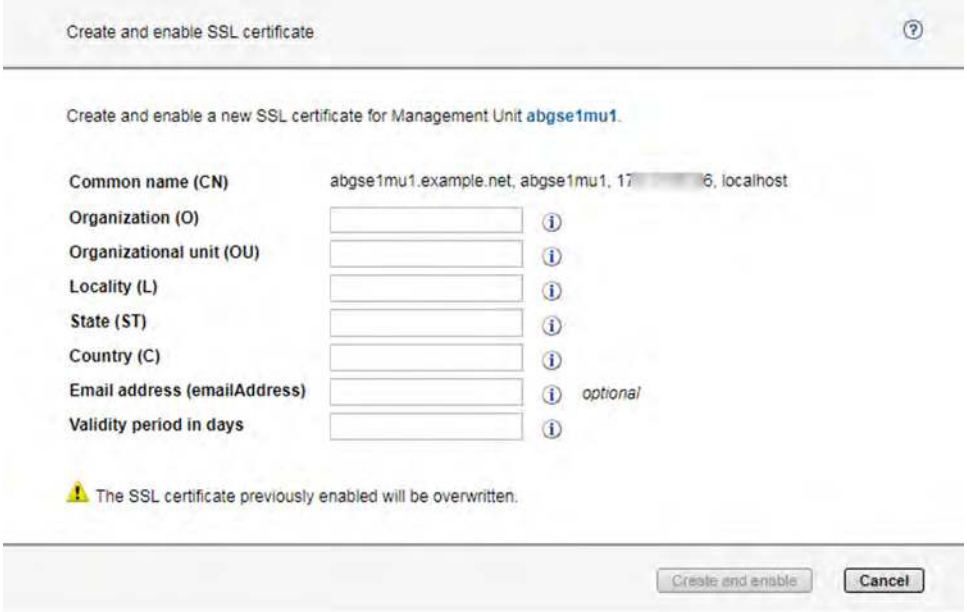
The preinstalled standard certificate contains data which is naturally not customer-specific.

If you want to work with a certificate with customer-specific data, you can at any time create and use such a certificate. This action can also be necessary when you want to renew a certificate. Proceed as follows:

> Select *Authorizations* -> *Certificates* -> [<*mu-name*> *(MU)*], *Certificates* tab.

> Click *Create and enable new SSL certificate* above the table.

A dialog opens:



Enter the most important data for the certificate. The value for the *Common name (CN)* is predefined and contains the system's fully qualified domain name (FQDN). Information on the attributes *Organization (O)*, *Organizational unit (OU)*, *Locality (L)*, *State (ST)*, *Country (C)*, *Email address (emailAddress), Validity period in days* is provided in the online help.

> Click *Create and enable*.

The certificate is created, activated immediately and displayed as the current certificate.

Notes:

- When a certificate is activated, the web server is also automatically rebooted.
- As the web browser does not know how trustworthy the new certificate is, like the standard certificate it must be explicitly accepted or imported (see the section "Confirming/importing a certificate in the web browser").

8.3.4 Requesting an SSL certificate

When you want to use a system-specific certificate which was signed by a CA (certification authority), the SE Manager supports you in creating the request:

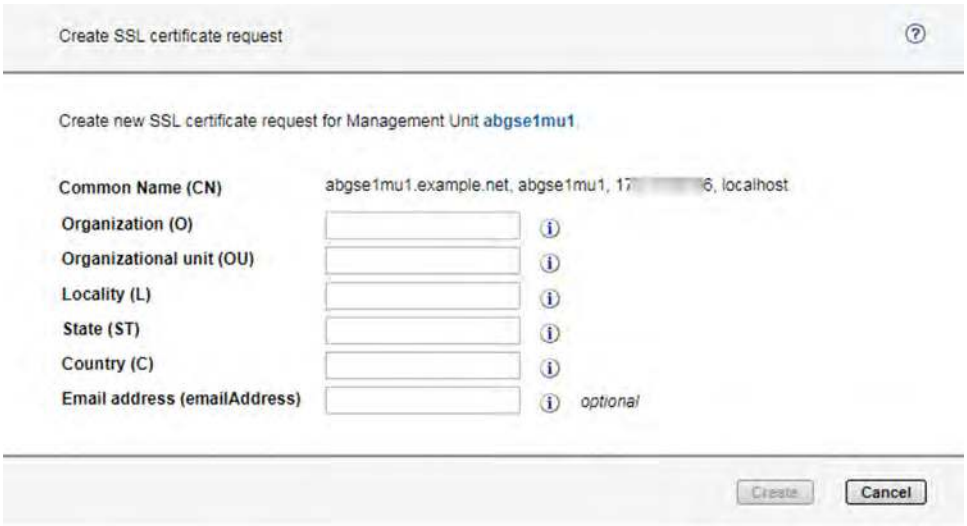
> Select *Authorizations* -> *Certificates* -> [<*mu-name*> *(MU)*], *Certificates* tab.

The *Current request for an SSL certificate* group shows whether a request has already been submitted: if one has, the attributes for the requested certificate are displayed.

> Click *Create new request* in the *Current request for an SSL certificate* group.

> ℹ Any request which has already been created is overwritten.

A dialog opens:



Enter the most important data for the requested certificate. The value for the *Common name (CN)* is predefined and contains the system's fully qualified domain name (FQDN). Information on the attributes *Organization (O)*, *Organizational unit (OU)*, *Locality (L)*, *State (ST)*, *Country (C)*, *Email address (emailAddress)* is provided in the online help.

> Click *Create*.

The request is created and displayed in the *Current request for an SSL certificate* group. To enable you to send the request to the certification authority by email, first download it to your administration PC using the *Download request* icon.

When the signed certificate is returned to you, enter the certificate in the system: see the section "Uploading and activating a customer-specific certificate" and section "Using the standard certificate".

Notes:

- When the certificate signing request is created, it is linked to the system's standard SSL key. If this key is changed in the system in the time between the certificate signing request being created and the signed certificate being entered in the system, the certificate cannot be used.
- A new standard SSL key is created when reinstallation takes place or when the host name is changed.

Consequently reinstallation should not take place and the host name should not be changed in the time between the certificate signing request being created and the signed certificate being entered in the system.

8.3.5 Uploading and activating a customer-specific certificate

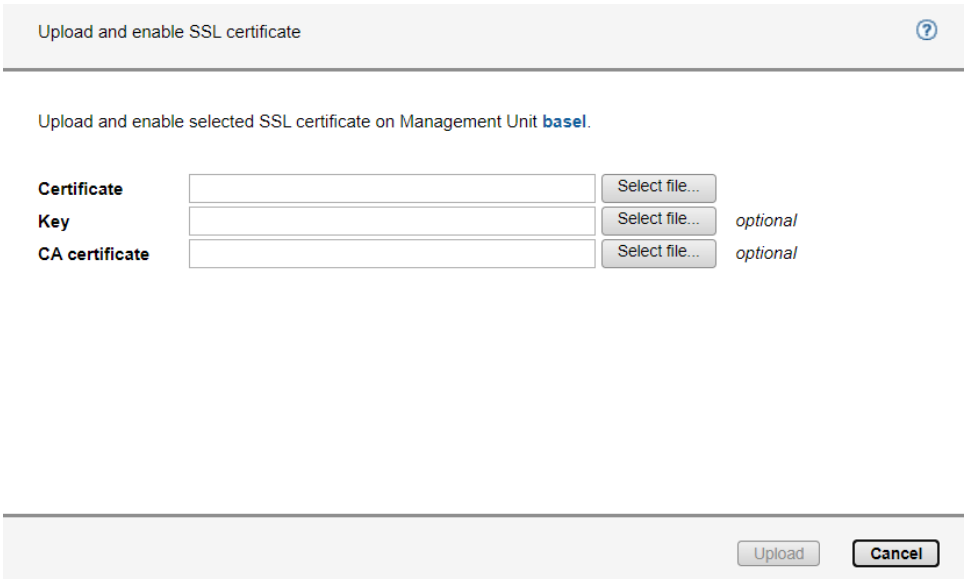
Instead of a self-signed certificate generated in the system (standard certificate or user-defined certificate), you can use a certificate of your own to access the system's SE Manager.

A certificate signing request was generated in the system for the certificate (see the section "Requesting an SSL certificate") and sent to a certification authority. As soon as the certificate signed by the CA (certification authority) is available to you, you can upload and activate it:

> Select *Authorizations* -> *Certificates* -> [<*mu-name*> *(MU)*], *Certificates* tab.

> Click *Create and enable SSL certificate*.

A dialog opens.



Certificate

> Click *Select file...* to select a certificate file on your administration PC.

Key

If necessary, select a suitable key file. A key file is required only if the certificate was created on another system. If nothing is specified, the default key is used.

> Click *Select file...* to select a key file on your administration PC.

CA certificate

If necessary, select a CA certificate file.

> Click *Select file...* to select a CA certificate file on your administration PC.

> Click *Upload* to start the file upload.

The files specified are uploaded into the target system, activated immediately and displayed as the current SSL certificate.

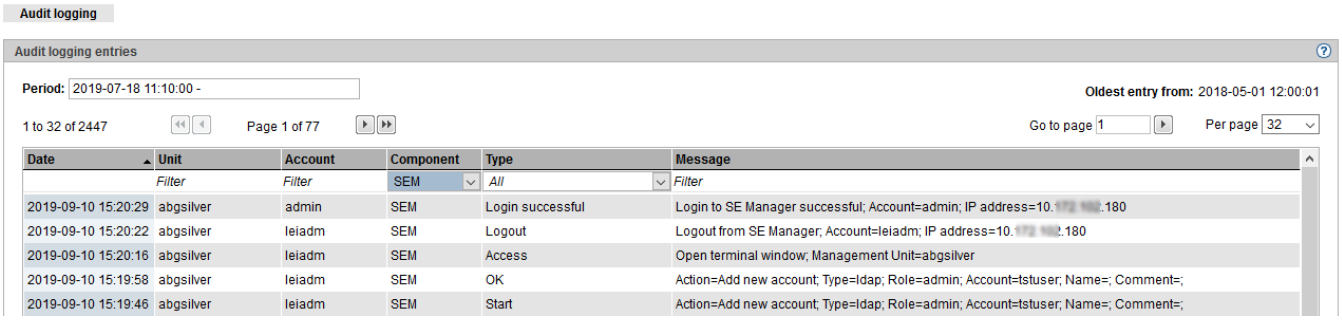
Notes:

- When a certificate is activated on the target system, the web server is also automatically rebooted with the new certificate. A brief interruption of the SE Manager’s connection to the system can occur.
- If the web browser used (on the administration PC or local console) knows that the new certificate is trusted or knows its root certificate, no further action is required.
- If the web browser does not know that a certificate is trusted, the certificate must be explicitly confirmed or imported (see the section "Confirming/importing a certificate in the web browser").

9 Logging actions (audit logging)

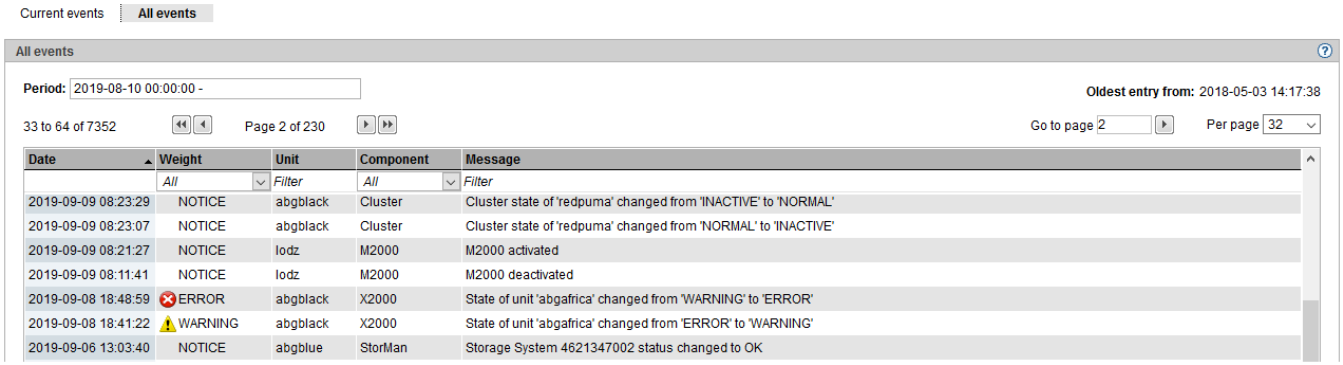
The internal audit logging function logs all actions that are executed on a Unit (MU, SU, HNC) of the SE server configuration via the SE Manager, an add-on or a CLI command and that cause a configuration change or status change in the system. Logins and logouts are also logged. Pure display functions are not logged.

Thanks to the logging entries, the administrator can always use the *Audit logging* tab under *Logging -> Audit logging* to review who performed which action with which result and when. This enables in particular all actions in the system which are relevant to security to be assigned unambiguously to an “originator”.



10 Event logging and alarm management

The *Event logging* function logs all events that occur und displays the logged events under *Logging -> Event logging* in the *All events* tab. To provide a better overview, the recent events that you have not yet seen are also displayed in the *Current events* overview. The Dashboard displays a summary of this tab in the *Events* tile.

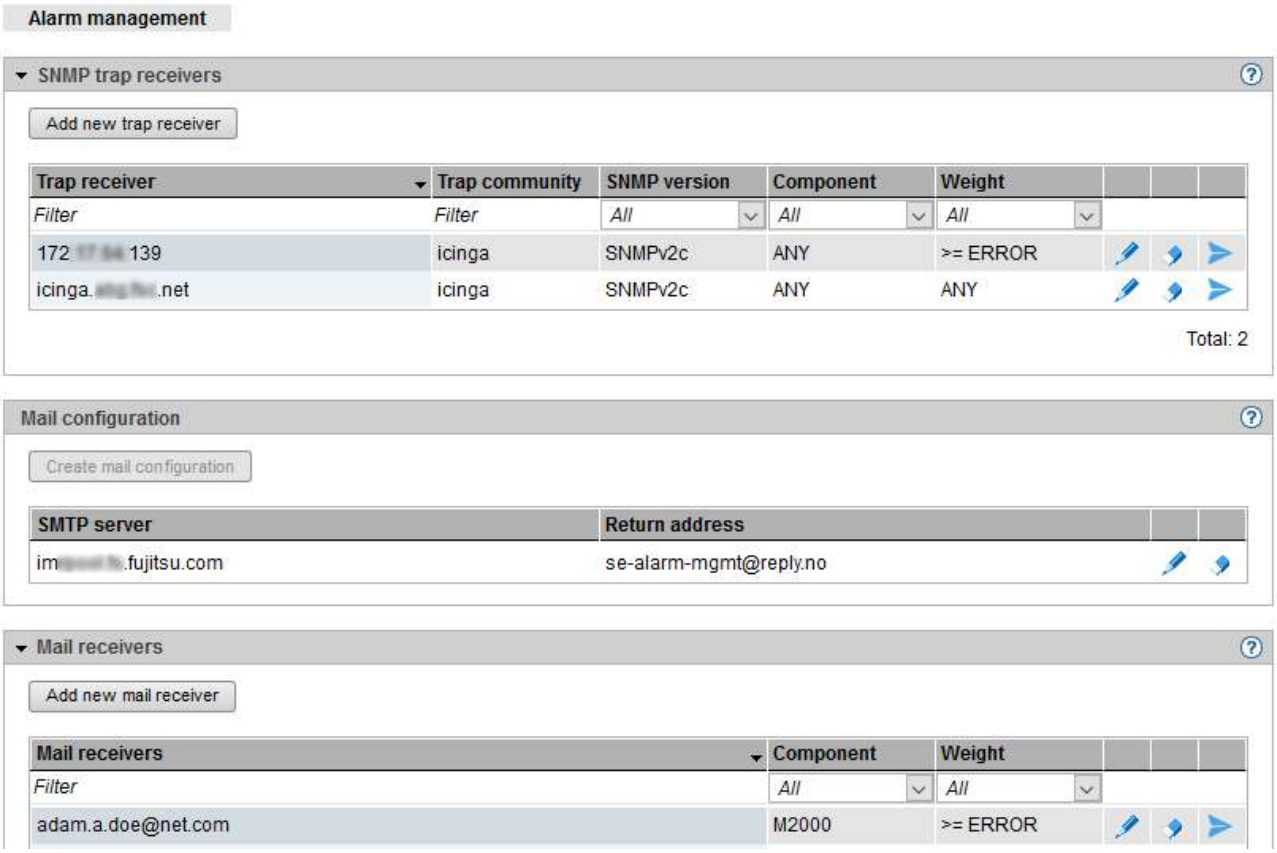


If you use the *Acknowledge current events* button to remove the currently displayed events from the *Current events* table, the *Events* tile reflects this change. The acknowledged events are only displayed in the *All events* tab.

The currently possible events with messages are listed in the online help of the SE Manager under "General information".

With the *Alarm management* you can configure automatic SNMP trap or email messages for events with certain weights and/or from certain components; this enables you to recognize important events like error situations earlier and to react quickly if necessary, even in large SE server configurations.

The SE Manager displays the alarm management configuration in the *Logging -> Alarm management* menu.



Security-relevant actions

Since a message can mean that sensitive data are sent to the outside, you should always thoroughly check the specified address when configuring a new SNMP trap or email receiver. Use the *Test* function to send a test trap or test email to the new receiver to see whether the message is sent to the correct receiver.

11 Related publications

You can find the following BS2000 manuals on the manual server with the BS2000 documentation at https://bs2manuals.ts.fujitsu.com.

Other manuals, for example descriptions of the Fujitsu PRIMERGY and PRIMEQUEST servers, can be found on the general Fujitsu support pages at https://support.ts.fujitsu.com/.

[1] **Fujitsu Server BS2000 SE Series**
Quick Guide
User Guide

[2] **Fujitsu Server BS2000 SE Series**
Operation and Administration
User Guide

[3] **Fujitsu Server BS2000 SE Series**
Basic Operating Manual

[4] **Fujitsu Server BS2000 SE Series**
Server Unit /390
Operating Manual

[5] **Fujitsu Server BS2000 SE Series**
Server Unit x86
Operating Manual

[6] **Fujitsu Server BS2000 SE Series**
Additive Components
Operating Manual

[7] **Fujitsu Server BS2000 SE Series**
Cluster Solutions for SE Servers
Whitepaper

[8] **BS2000 OSD DX**
Introduction to System Administration
User Guide

[9] **SECOS**
Security Control System - Access Control
User Guide

[10] **SECOS**
Security Control System - Audit
User Guide