



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Roads Office FEDRO

DOCUMENTATION

IAM BSA

User Guide

Edition 2025 V1.00

ASTRA 83057

Legal Notice

Authors / Working group

| | |
|------------------|-----------------------|
| Geringer Jolanda | ASTRA DS-DTI, Vorsitz |
| Gähwiler Daniel | CSI Consulting AG |
| Grau Rolf | CSI Consulting AG |

Working group (Review)

| | |
|-----------------|--------------------------------|
| Crausaz Bernard | ASTRA DS-UARS |
| Jehli Martin | GE V |
| Widrig Bruno | GE XI |
| Schlup Markus | Amstein + Walthert Progress AG |

Translation

CSI Consulting AG, original German version is authoritative

Editor

Federal Office Roads FEDRO
Road Network Division N
Standards and Infrastructure Safety SSI
3003 Bern

Source of supply

The document can be downloaded free of charge from www.astra.admin.ch.

© ASTRA 2025

Reproduction permitted except for commercial use, provided the source is acknowledged.

Table of contents

| | | |
|----------|---|-----------|
| | Legal Notice | 2 |
| 1 | Introduction | 5 |
| 1.1 | Purpose | 5 |
| 1.2 | Scope of Application and Basic Documents | 5 |
| 1.3 | Addressees | 5 |
| 1.4 | Entry into Force and Amendments..... | 5 |
| 2 | Overview | 6 |
| 3 | Set up and Manage an IAM BSA Account | 7 |
| 3.1 | Application for First Time Access..... | 7 |
| 3.2 | Setting up Multifactor Authentication (MFA) | 8 |
| 3.2.1 | MFA Hardware Token | 8 |
| 3.3 | Apply for Roles..... | 8 |
| 3.4 | Other Territorial Units | 8 |
| 3.5 | Forgotten Password | 9 |
| 3.6 | Forgotten MFA Token PIN | 9 |
| 3.7 | MFA Token Lost / Defective / New Hardware | 9 |
| 3.8 | Contact Service Desk..... | 9 |
| 4 | Remote access to Services of the IP network BSA via IAM BSA..... | 10 |
| 4.1 | Access via VPN..... | 10 |
| 5 | Frequently Asked Questions - FAQ | 15 |
| | Glossary | 17 |
| | Bibliography | 18 |
| | List of Changes | 19 |

1 Introduction

1.1 Purpose

The purpose of identity management IAM BSA is to standardise the recording and processing of system access accounts within the IP network BSA.

This document serves as a brief overview and guide for first-time users for the application process:

- Independent application for identities by the users;
- Review and approval of applications by the responsible organisations;
- Central management of access authorisations and identities across the entire lifecycle of the identities with a uniform naming convention and rules;
- Cross-area management and emergency control of identities;
- Regular checking of accesses.

1.2 Scope of Application and Basic Documents

This documentation is a supplementary document to directives FEDRO 73006 OT Security Governance [1] and to the guidelines 13040 IP Network BSA [2] and 13030 OT Security [3], and has the same scope of application.

1.3 Addressees

The document is aimed at the following stakeholders:

- Specialists BSA and FEDRO operations;
- Specialists BSA and operation of the area units;
- Suppliers on behalf of FEDRO.

1.4 Entry into Force and Amendments

This document comes into force on 19.06.2025. The "List of Changes" is documented on page 19.

2 Overview

The identities for the use of the critical infrastructure operated in the IP network BSA are created and managed uniformly via centralised services. Once an identity has been created, it can be assigned to the respective area units as required and receives the necessary rights based on its selected role. Rights and roles are created and assigned by the respective area unit administrators.

Thanks to centralised administration, identities can be changed or blocked centrally depending on the situation.

Multifactor authentication (MFA) is also used to secure access and is assigned to each user in the form of a token. To use the token, the MobilePASS+ software is installed on the user's device. Depending on the application, the token is requested in addition to the user name and password.

The actual access to the respective target systems is communicated to the user by the respective contact person and is not part of this documentation.

3 Set up and Manage an IAM BSA Account

3.1 Application for First Time Access

When applying for an identity for the first time, the user is requested to register via the portal by the contact person at FEDRO or the respective territorial unit (TU).

<https://portal.nationalstrassen.admin.ch/>

The following information is required for the application:

- First name and surname of the applicant
(full name as stated on the official identity document)
- Company name of the employer
(full company name as stated in the commercial register)
- Business
(for identity verification)
- Telephone number (mobile)
(for alternative identity verification via SMS)
- Date of birth
(as stated in the official identification document)
- Preferred language of communication
- Copy of an official identity document
(Passport or ID; for ID, the front is sufficient; unpixelated and unblackened; black and white or colour; in JPG or PNG format; file size max. 4MB)
- Operating area
(initial operating area as instructed by the contact person
If further area units are to be served, these are selected in the system at a later date).
- Employee type
(External, area unit employee or federal employee)
- E-mail address of the contact person
(FEDRO / TU contact person who asked you to register).

The information on the form is checked with a time delay by the relevant operating division and approved or rejected accordingly.

The applicant is not automatically informed of a rejection.

As part of the authorisation process, the applicant is successively sent their user name, the initial password, the request to activate multifactor authentication (see section 2.2) and other information by e-mail.

3.2 Setting up Multifactor Authentication (MFA)

For multifactor authentication (MFA), the MobilePASS+ app/software from Thales must be installed on one of the applicant's devices in order to generate the numerical codes required for multifactor authentication.

The Thales SafeNet MobilePASS+ software is available for various platforms and must be installed in advance.

SafeNet MobilePASS+ can be obtained from the respective app stores or directly from the manufacturer:

<https://cpl.thalesgroup.com/access-management/authenticators/mobilepass-otp-download>

Once SafeNet MobilePASS+ has been successfully installed on the applicant's device, the software token can be activated in the SafeNet MobilePASS+ application using the registration email from IAM BSA. To do this, select the "No QR code?" option at the bottom of the screen when prompted to scan a QR code.

To secure the software token, the user must define a separate PIN that protects the software token. This is part of the activation process.

The user can then access the services of the IP network BSA (see chapter 4).

3.2.1 MFA Hardware Token

If the applicant's company policy prohibits the installation of SafeNet MobilePASS+ on one of the applicant's devices or for all users who assign rights and admin users, a hardware token can also be requested in exceptional cases.

A hardware token is ordered via the Service Desk (see Service Desk contact in section 3.8).

3.3 Apply for Roles

A user can apply for additional roles within the IAM BSA system FEDRO. To do this, the user must already be logged into the IP network BSA (see Chapter 4).

Applications are submitted via the web interface of IAM BSA within the IP network BSA:

<https://sailpoint.bd.nationalstrassen.admin.ch/>

The user orders the required accesses under the menu item "Manage Access / Manage My Access" based on the group names known to him. These are granted or rejected by the responsible administrative unit in accordance with the authorisation process.

If the group names are not known, the user must ask their contact person for them.

3.4 Other Territorial Units

Existing users can be registered for additional area units by the respective contact person or area unit administrator within the IAM BSA system. The communication for this takes place outside the system in connection with the assignment and discussion with the respective contact person at the TU.

Be aware: Due to the autonomy requirements and the TU-related administration of identities and authorisations, the user is automatically prompted to set a new password when added to a new territorial unit (analogous to initial registration). This password is then propagated to all operating areas, so that the newly set password can now be used in all units.

If the user is logged in during the automatic password change, they can continue working for about an hour before being locked out due to the change.

3.5 Forgotten Password

If the password is no longer known, a password reset can be initiated via the portal:

<https://portal.nationalstrassen.admin.ch/>

The applicant's identity is confirmed via a security link in the e-mail and a temporary password is issued. This must be changed by the user after successful authentication using the MFA soft token (or, in exceptional cases, a hardware token) at the next login.

Without an MFA token, the password reset must be requested via the Service Desk (for contact details, see section 3.8).

3.6 Forgotten MFA Token PIN

If the MFA token PIN has been forgotten, the Service Desk must be contacted (for contact details, see section 3.8).

3.7 MFA Token Lost / Defective / New Hardware

If the MFA token is lost, the Service Desk must be informed immediately (for contact details, see section 3.8) so that the token can be blocked.

If the token is defective (e.g. does not display a token code), the Service Desk must also be contacted in order to analyse the error and possibly have a replacement token assigned.

The Service Desk is also used to move a soft token to new hardware (laptop or mobile).

3.8 Contact Service Desk

The Service Desk responsible for IAM BSA FEDRO can be contacted as follows:

E-Mail: noc@axpo-systems.com

Phone: 0800 99 74 38

4 Remote access to Services of the IP network BSA via IAM BSA

4.1 Access via VPN

For remote access to the services of the IP network BSA it is possible to access the jump server in the BD locations from the Internet via [Checkpoint Mobile Agent](#) through the basic service locations BD-A and BD-B.

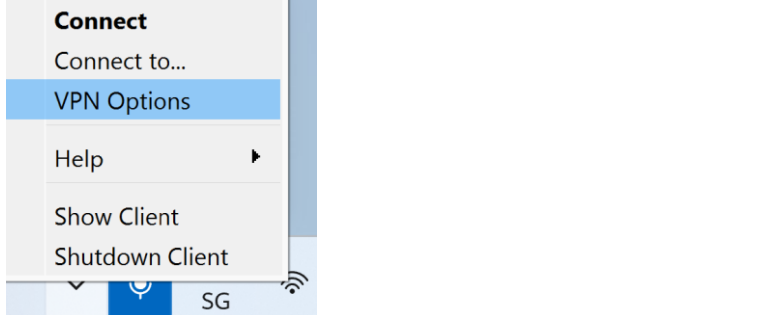
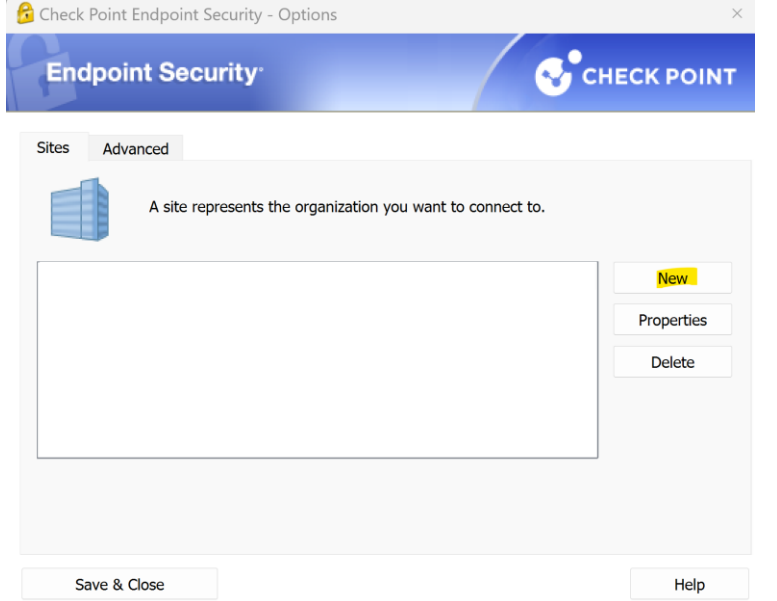
The Checkpoint Mobile Agent required for this can be obtained directly from the manufacturer (select "Checkpoint Mobile Agent" during installation):

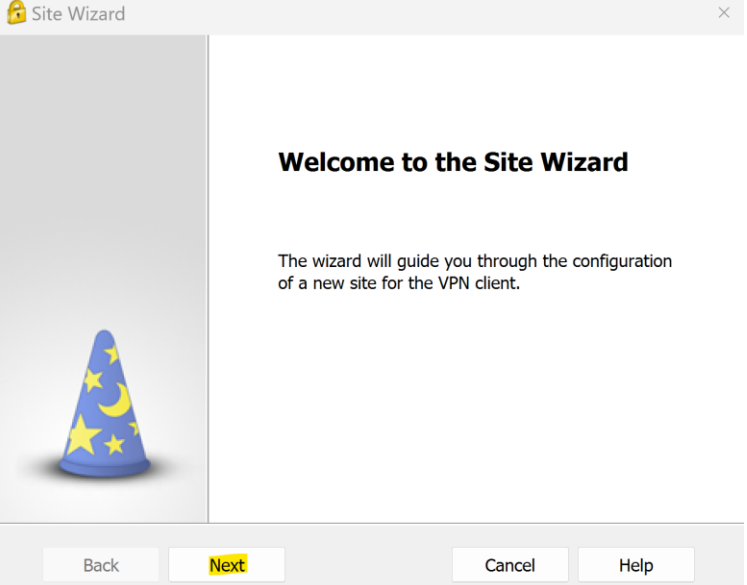
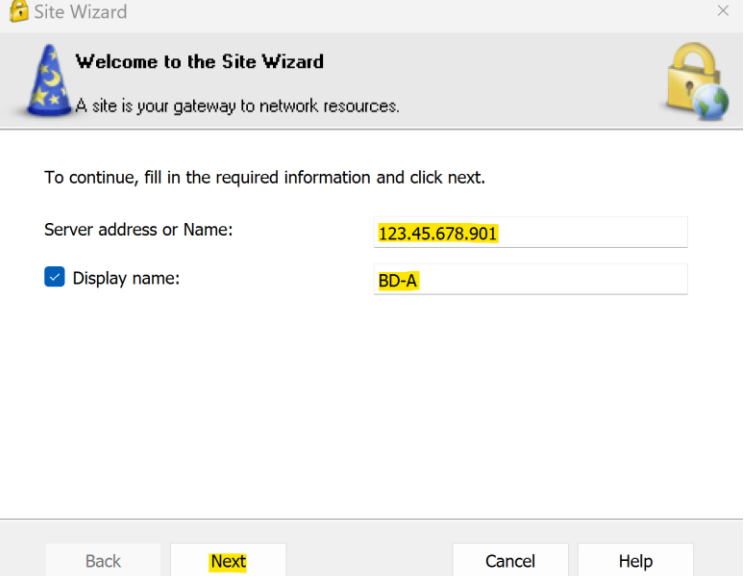
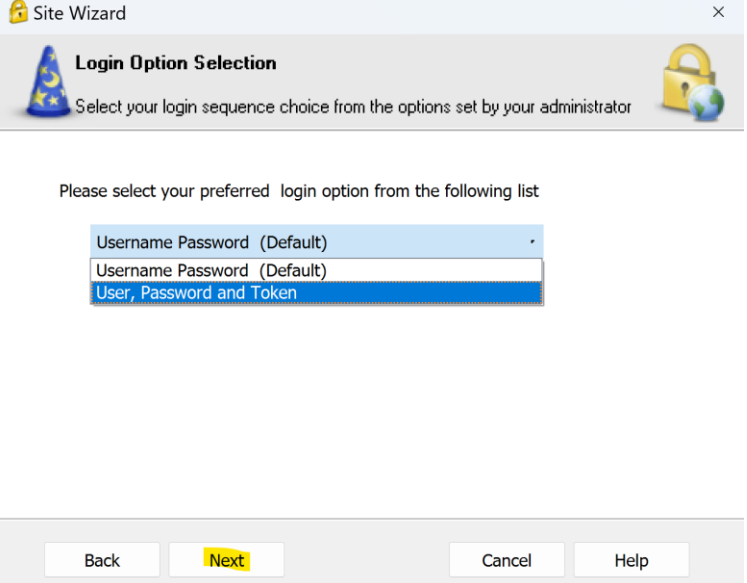
<https://www.checkpoint.com/quantum/remote-access-vpn/#downloads>

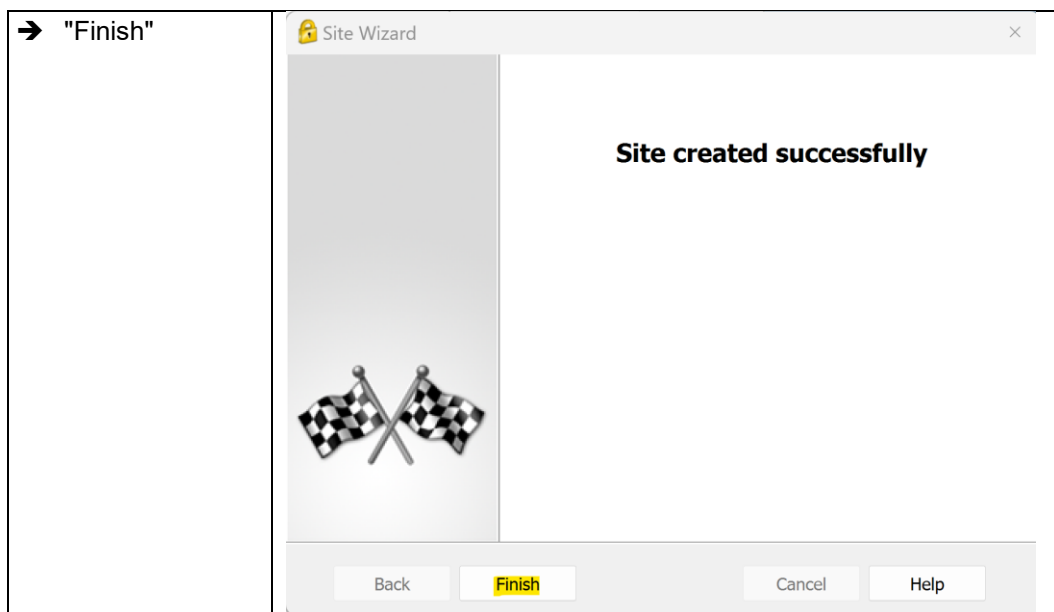
Once Checkpoint Mobile Agent has been successfully installed on the applicant's device, it can be configured as follows for access to the jump hosts in the basic services.

The addresses required for access to the respective target systems are communicated to the user by the respective contact person.

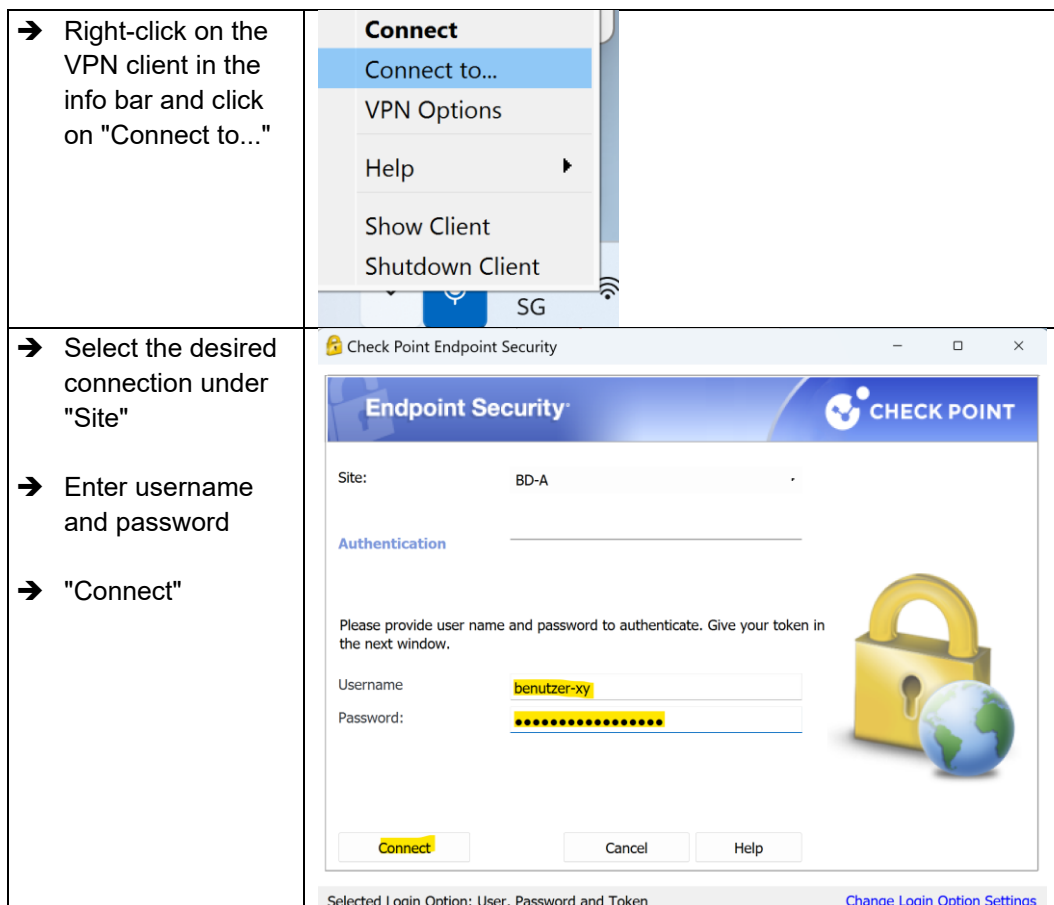
The configuration must be carried out separately for BD-A and BD-B:

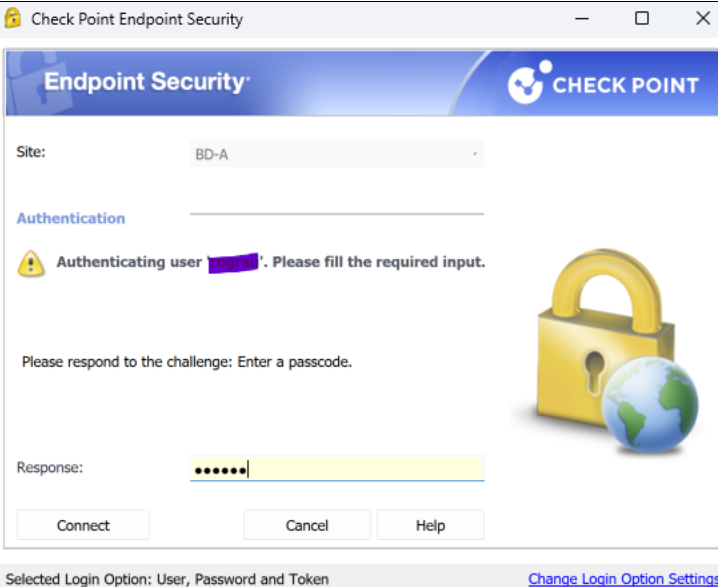
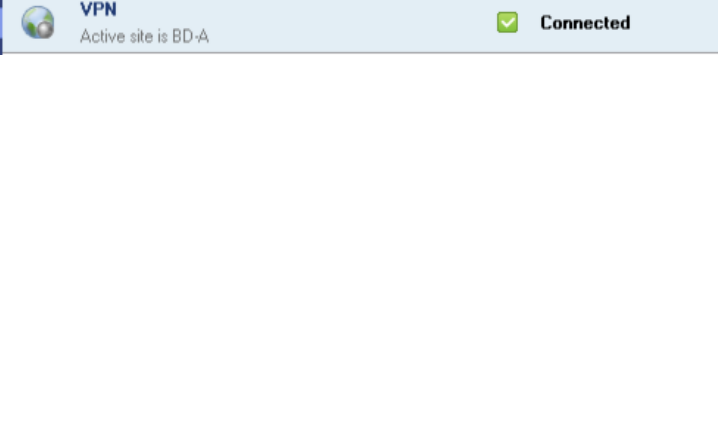
| | |
|---|--|
| <p>➔ Right-click on the VPN client in the info bar and click on "VPN Options"</p> |  |
| <p>➔ "New"</p> |  |

| | |
|--|---|
| <p>→ "Next"</p> |  <p>The wizard will guide you through the configuration of a new site for the VPN client.</p> <p>Buttons: Back, Next, Cancel, Help</p> |
| <p>→ Server address or name: Specify the address of the desired basic service location, according to the information provided by the contact person</p> <p>→ Display name: e.g. "BD-A" or "BD-B"</p> <p>→ "Next"</p> |  <p>To continue, fill in the required information and click next.</p> <p>Server address or Name: 123.45.678.901</p> <p><input checked="" type="checkbox"/> Display name: BD-A</p> <p>Buttons: Back, Next, Cancel, Help</p> |
| <p>→ Select "Username, Password and Token"</p> <p>→ "Next"</p> |  <p>Please select your preferred login option from the following list</p> <ul style="list-style-type: none"> Username Password (Default) Username Password (Default) User, Password and Token <p>Buttons: Back, Next, Cancel, Help</p> |

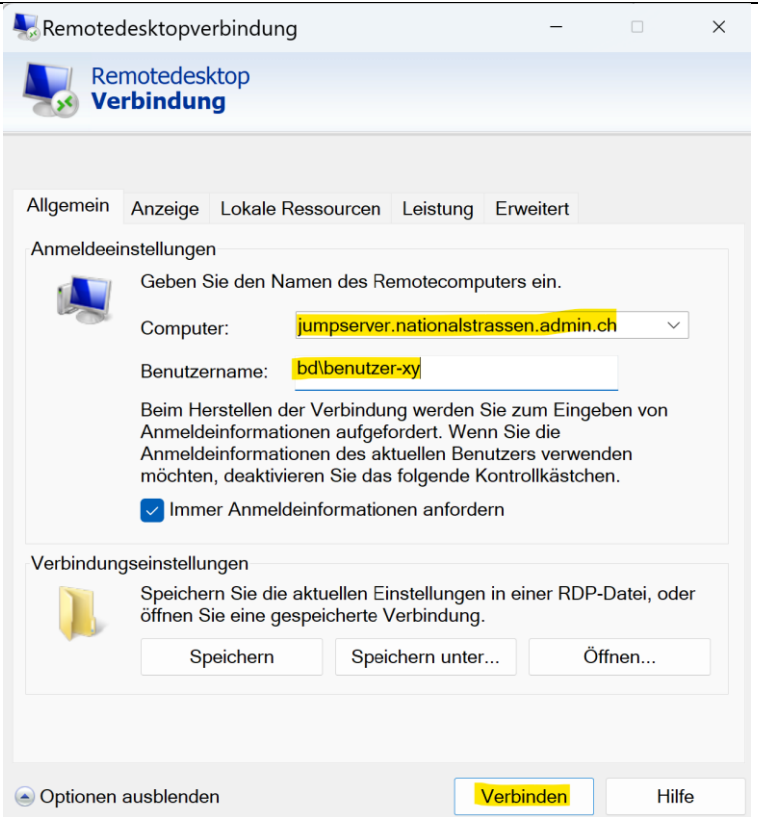


The connection is established as follows:



| | |
|--|---|
| <p>→ Enter MFA token from SafeNet MobilePASS+</p> <p>→ "Next"</p> |  |
| <p>→ If the login is successful, this is announced with a corresponding sound and the window is closed.</p> <p>→ The successful connection is displayed when the Checkpoint Mobile Agent is opened again</p> |  |

A Jump Server can then be logged into via a remote desktop connection:

| | |
|---|---|
| <ul style="list-style-type: none"> ➔ Start the remote desktop connection app. ➔ Computer: Enter the address of the desired jump server, according to the information provided by the contact person ➔ Benutzername: Enter the bd\Username ➔ «Verbinden» (connect) |  |
|---|---|

After a successful connection to the jump server, the target systems of the respective BD location can be accessed:

- Using a web browser to access a web application;
- With the help of RDP (Remote Desktop Connection app) to other servers;
- With the help of a file explorer to file storage.

See also the additional instructions on using the basic services in the main directory of the OPERATIONS file storage (O:) for further assistance.

Important:

- It is currently possible to access a Jump Server in BD-A from the perimeter FW in BD-A or from the perimeter FW in BD-B to BD-B - but not across locations;
- Two(!) simultaneous RDP sessions are available per Jumphost. It is therefore important not to keep the RDP session open for an unnecessarily long time and to disconnect it once the work is complete.

5 Frequently Asked Questions - FAQ

Are there alternatives to the IAM BSA, such as eIAM?

No, the services within the critical infrastructure, which is operated in the IP network BSA, can only be accessed with the help of IAM BSA.

What does it cost to use the IAM BSA?

Use of the IAM BSA is free of charge.

Which e-mail address should I register with the IAM BSA?

Enter your main e-mail address that you want to use in the long term. Do NOT enter any disposable e-mail addresses. This e-mail address will be forwarded by IAM BSA together with your first name and surname to the applications you use. It is also required for the self-service password reset.

Can I have multiple IAM BSA accounts?

There is only one account per natural person.

Can one and the same IAM BSA account be used by several people?

An IAM BSA account always represents exactly one natural person, regardless of whether they are using the IAM BSA for themselves or on their behalf. This natural person is responsible for the correct use of the IAM BSA account, the applications that can be accessed with it and the transactions carried out with this authentication. This means that this person is also responsible for the secure storage and correct use of the associated access data (e.g. passwords or tokens).

Do I need security questions in the IAM BSA for support?

No security questions are required to identify a user during a subsequent support call; e.g. for a password reset, the user receives an email with a generated token and a confirmation link. The system checks this and only triggers the reset if the tokens match.

What happens if the data initially entered, e.g. telephone number or employee type, changes?

If necessary, the data entered initially can be changed later via the contact person.

Can I use other multifactor authentication (MFA) software than Thales SafeNet MobilePASS+?

No, when using the Thales app, the token is also encrypted - this cannot be enforced for other apps.

Why does my password change automatically, when I am assigned to a new TU?

Due to the autonomy requirements and the TU-related administration of identities and authorisations, the user is automatically prompted to set a new password when added to a new territorial unit (analogous to initial registration). This password is then propagated to all operating areas, so that the newly set password can now be used in all units. If the user is logged in during the automatic password change, they can continue working for about an hour before being locked out due to the change.

Glossary

Glossary IP network BSA

See FEDRO Guideline 13040 “IP network BSA”.

Glossary IAM BSA

| Term/Abbreviation | Meaning |
|-------------------|---|
| 2FA | 2 Factor Authentication |
| AD | Active Directory |
| BD-A, BD-B | Basic services location A, basic services location B |
| BIT | Federal Office of Information Technology and Telecommunications |
| DNS | Domain Name Service |
| Forest | Collection of Active Directory domains with a common global catalog, directory schema, and directory configuration. |
| IAM | Identity and Access Management |
| IIS | Internet Information Server |
| IKT | Information and communication technologies |
| IP | Internet Protocol |
| MFA | Multifactor authentication |
| MS | Microsoft |
| PAM | Privileged Access Management |
| RAS | Privileged Remote Access |
| RBAC | Remote Access Service |
| RDP | Remote Desktop Protocol |
| SAS PCE | SafeNet Authentication Service Private Cloud Edition |

Bibliography

FEDRO instructions and guidelines

-
- [1] Federal Roads Office FEDRO, “**OT Security Governance**”, *Instructions ASTRA 73006*, www.astra.admin.ch.
 - [2] Federal Roads Office FEDRO, “**IP-Netz BSA**”, *Guideline ASTRA 13040*, www.astra.admin.ch.
 - [3] Federal Roads Office FEDRO, “**OT Security**”, *Guideline ASTRA 13030*, www.astra.admin.ch.
-

List of Changes

| Edition | Version | date | Changes |
|----------------|----------------|-------------|--|
| 2025 | 1.00 | 19.06.2025 | Entry into force of the 2025 edition (German, French, Italian and English versions). |

