

NUTZERHANDBUCH

SONICCG



BUNDESWEHR

EINSTUFUNG
OFFEN

VERÖFFENTLICHUNG
11.02.2025

ERSTELLER
OFw Cedric Prietz

ANWENDUNGSVERSION
1.2

Inhaltsverzeichnis

Einleitung	1
Allgemeine Nutzung der Webanwendung	2
Anmeldung.....	2
Abmeldung.....	2
Navigationsstruktur.....	3
Grundlegende Funktionen.....	3
Dashboard.....	3
Karte	4
Benutzerrollen	5
Bediener	5
Bearbeiter.....	5
Auswerter.....	5
Auditor.....	6
Administrator.....	6
Funktionen der Benutzerrollen	7
Bediener	7
Terminal	7
Freigegebene Identitäten	11
Bearbeiter.....	12
Dienstposten im Überblick.....	12
Militärische und Zivile Dienstposten.....	13
Dienstposten für Ortskräfte	14
Dienstposten für Gäste	14
Identitäten	15
Ansichten nach Identitätsart	16
Sperrliste für Ortskräfte	17
Anlegen neuer Identitäten.....	18
Berichte zur Militärischen Sicherheit	20
Auswerter.....	22
Berichte	22
Auditor.....	27
Berechtigungen.....	27
Protokolle	28
Buchungshistorie.....	29

Administrator.....	30
Benutzerverwaltung	30
Zonenverwaltung.....	33
Schutzbauten.....	35
Backup.....	37
Fehlersuche und Support.....	38
Häufige Probleme und Lösungen	38
Kontakt zum Support	38
Anhänge.....	39
Glossar.....	39
Betriebshandbuch	39
Versionshistorie	39

Einleitung

Die Webanwendung dient zur Erfassung und Verwaltung von Kontingentangehörigen und Ortskräften innerhalb eines militärischen Camps. Ihr Hauptzweck ist es, den berechtigten Aufenthalt aller Personen zu prüfen und im Alarmfall eine schnelle Übersicht darüber zu ermöglichen, welche Personen sich in welchen Zonen aufhalten. Dies trägt wesentlich zur Sicherheit und Kontrolle innerhalb des Camps bei.

Darüber hinaus bietet die Anwendung umfangreiche Auswertungs- und Berichtsfunktionen, um verschiedene sicherheitsrelevante Informationen bereitzustellen. Sie dient somit als Arbeitsmittel und Nachweis für die Militärische Sicherheit, indem alle relevanten Daten zu den erfassten Personen strukturiert und abrufbar zur Verfügung stehen.

Die Anwendung ist als vollumfassende Softwarelösung konzipiert, die bereichsübergreifende Arbeit unterstützt und die Zusammenarbeit verschiedener Nutzergruppen erleichtert. Durch die zentrale Erfassung und Analyse von Zutritts- und Bewegungsdaten verbessert die Software sowohl die Einsatzfähigkeit als auch die Transparenz der Sicherheitsmaßnahmen.

Allgemeine Nutzung der Webanwendung

Anmeldung

Die Anwendung wird über den Browser des Nutzers aufgerufen. Es wird empfohlen, **Google Chrome** für die bestmögliche Performance und Kompatibilität zu verwenden.

Die Anmeldemaske ist unter der folgenden URL erreichbar:

<https://soniccg.gefstdlwmcd.de>

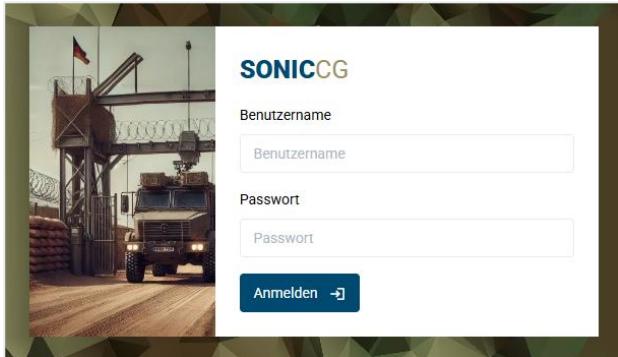


Abbildung 1 : Anmeldemaske

Die Webanwendung ist in die Domänenumgebung eingebunden. Die Anmeldung erfolgt mit einem freigegebenen **Windows-Benutzerkonto** oder mit einem **lokalen Benutzerkonto**, das von den Administratoren eingerichtet wurde.

Abmeldung

Die Abmeldung aus der Anwendung erfolgt bei **längerer Inaktivität automatisch**. Nutzer können sich jedoch auch manuell abmelden. Dazu öffnet man das Benutzerkontextmenü (*Das Bundeswehr-Logo oben rechts in der Anwendung*) und wählt den Punkt „**Abmelden**“ aus.

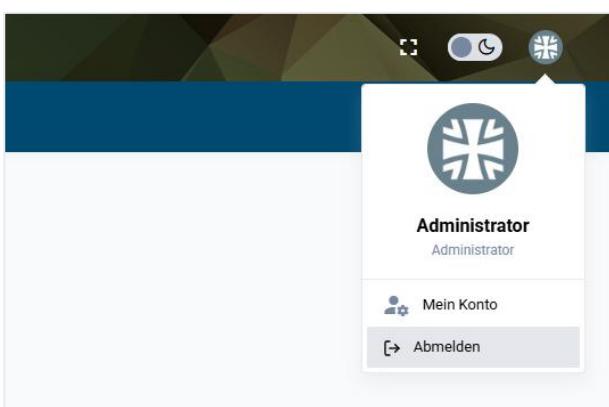


Abbildung 2 : Benutzerkontextmenü

Navigationsstruktur

Die Navigation der Webanwendung besteht aus mehreren **Menüpunkten mit Unterpunkten**, die je nach **Benutzerberechtigung** angezeigt werden. Nutzer sehen nur die Menüpunkte, für die sie aufgrund ihrer Berechtigungsgruppe Zugriffsrechte besitzen.

Die Hauptnavigation befindet sich **permanent am oberen Rand** der Webanwendung und bleibt auch beim Scrollen stets sichtbar. Dadurch wird eine einfache und schnelle Navigation zwischen den verschiedenen Funktionen der Anwendung ermöglicht.

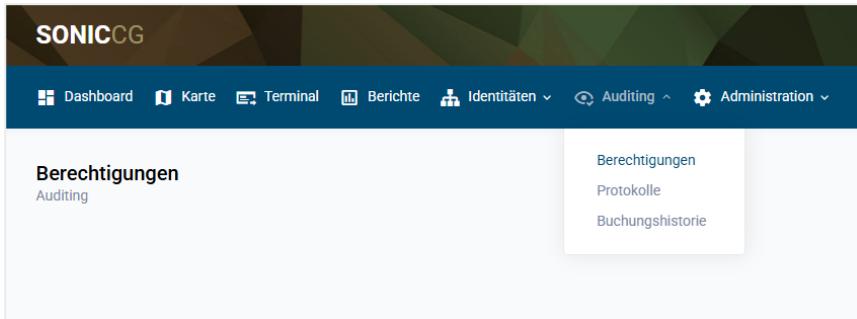


Abbildung 3 : Gesamte Navigation im Administrationsmodus

Grundlegende Funktionen

Dashboard

Das Dashboard ist für alle Nutzer der Anwendung zugänglich und bietet eine zentrale Informationsübersicht. Es zeigt die Gesamtzahl der verfügbaren Soldaten, Zivilisten, Ortskräfte und Gäste sowie eine Ankunfts- und Abflugsübersicht für die kommenden 10 Tage.

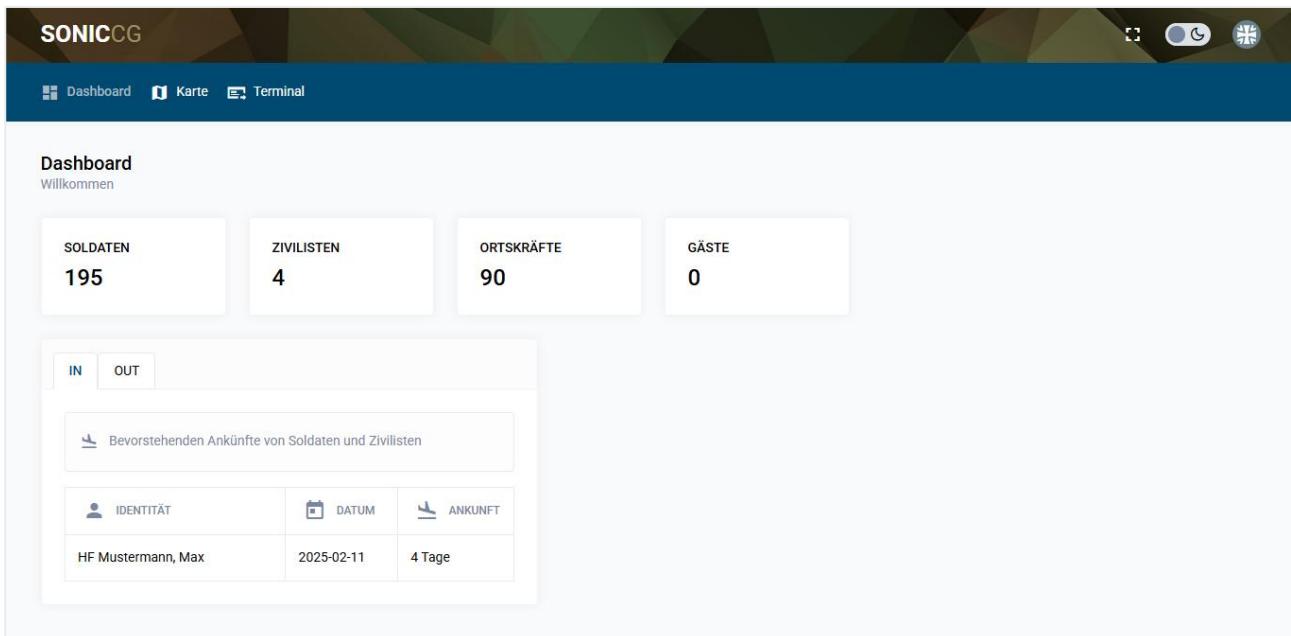


Abbildung 4 : Dashboard

Karte

Die Karte ist für alle Nutzer der Anwendung zugänglich und bietet eine Übersicht über die Schutzbauten, die im Alarmfall aufgesucht werden müssen. Sie dient als visuelle Orientierungshilfe und unterstützt die schnelle Lokalisierung sicherheitsrelevanter Einrichtungen.

In zukünftigen Versionen der Anwendung werden zusätzliche Funktionen integriert, darunter die Möglichkeit, eigene Punkte auf der Karte zu markieren, um individuelle Standorte oder relevante Positionen direkt in der Anwendung zu vermerken.

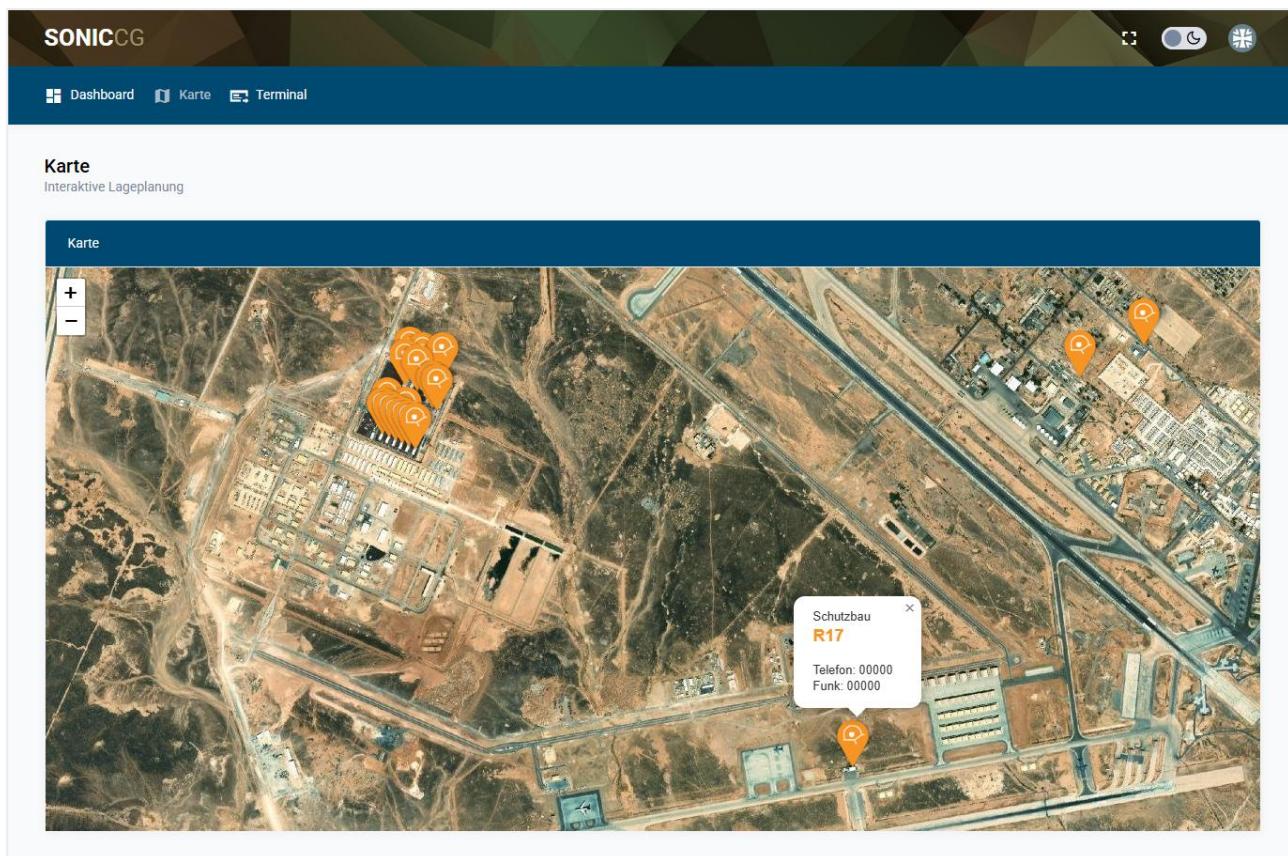


Abbildung 5 : Interaktive Karte

Benutzerrollen

Bediener

Die Benutzerrolle Bediener ermöglicht den Zugriff auf die Terminals der zugewiesenen Zonen, um Personen ordnungsgemäß ein- oder auszubuchen. Bediener sind für die korrekte Erfassung und Überprüfung aller Zutrittsbewegungen verantwortlich und gewährleisten eine lückenlose Nachverfolgbarkeit der ein- und ausgehenden Personen. Im Alarmfall können sie, abhängig von ihrer Berechtigung, über das Terminal eine Alarrrmeldung auslösen, die auf allen angebundenen Windows-Clients innerhalb der Domäne zur sofortigen Alarmierung angezeigt wird. Dies ermöglicht eine schnelle Reaktion auf sicherheitsrelevante Vorfälle und stellt sicher, dass alle notwendigen Maßnahmen unverzüglich eingeleitet werden.

*Die Rolle des Bedieners ist speziell für das Personal der **Force Protection** vorgesehen.*

Bearbeiter

Die Benutzerrolle Bearbeiter ist für die Pflege und Verwaltung aller Identitäten innerhalb der Anwendung verantwortlich. Sie umfasst die Bearbeitung und Aktualisierung von Identitätsdaten, einschließlich der Zuordnung zu Dienstposten und Personen. Bearbeiter verwalten Sperrlisten für Ortskräfte, übergeben Dienstposten und sind für die vollständige und korrekte Pflege aller Datensätze zuständig. Zudem können sie Berichte zur Zonenauswertung und militärischen Sicherheit einsehen und exportieren.

*Die Rolle des Bearbeiters ist speziell für den **SiBe** und den **PersFw** vorgesehen.*

Auswerter

Die Benutzerrolle Auswerter ist für die Erstellung und Analyse sicherheitsrelevanter Berichte zuständig. Auswerter haben die Möglichkeit, Alarmberichte zu erzeugen und zu exportieren, um Ereignisse nachvollziehbar zu dokumentieren. Auswerter können Zonenauswertungen erstellen, die eine Übersicht über alle Personen in den jeweiligen Zonen sowie deren Erreichbarkeit über Funkgeräte ermöglichen. Darüber hinaus haben Auswerter Zugriff auf die Schutzbauauswertung, in welcher im Alarmfall erfasst wird, welche Personen bereits Schutzbauten aufgesucht haben und welche sich noch außerhalb befinden.

*Die Rolle des Auswerters ist speziell für den **J1** und den **Battle Captain** vorgesehen.*

Auditor

Die Benutzerrolle Auditor ist für das Auditing und die Überwachung der Systemnutzung verantwortlich und dient der Einhaltung von Sicherheitsrichtlinien sowie der Überprüfung von Berechtigungsstrukturen innerhalb der Anwendung. Auditoren haben die Berechtigung, die Rollen- und Zonenberechtigungen aller Benutzerkonten einzusehen. Zudem können sie alle Protokolle und Buchungshistorien der letzten 90 Tage einsehen.

*Die Rolle des Auditors ist speziell für den **ISB** vorgesehen.*

Administrator

Die Benutzerrolle Administrator hat uneingeschränkten Zugriff auf alle Funktionen der Anwendung. Administratoren können die Anwendungseinstellungen anpassen und erweitern, einschließlich der Verwaltung von Benutzerkonten, Zonen, Zoneneinstellungen und Schutzbauten. Zudem sind sie für die Vergabe von Berechtigungen sowie das Erstellen und Herunterladen von Backups der Anwendungsdaten berechtigt.

*Die Rolle des Administrators ist speziell für die **Administratoren** sowie den **UserHelpDesk** vorgesehen.*

Funktionen der Benutzerrollen

Bediener

Terminal

Bediener haben im Menüpunkt „Terminal“ die Möglichkeit, sich in ein **Terminal einzuwählen**, für das sie eine Berechtigung besitzen, und darüber die **Buchungen für das Betreten oder Verlassen von Personen in den Zonen zu dokumentieren**.

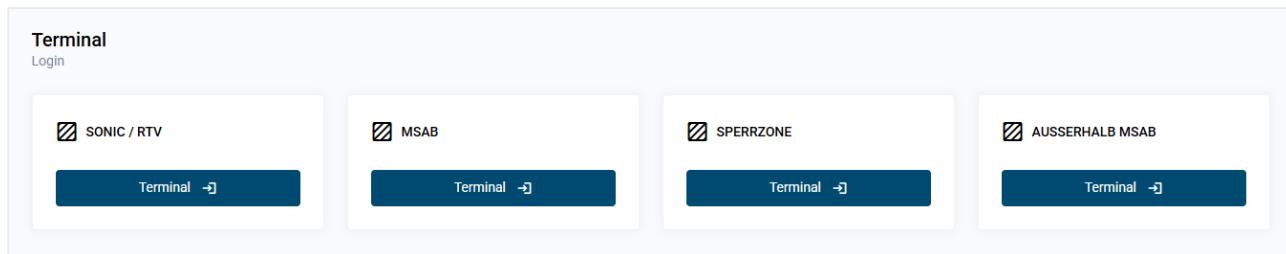


Abbildung 6 : Terminal Login

Buchen von Personen

Jedes Terminal verfügt über zwei **Ansichten**:

- **Aktuelle Zone** – Zeigt Personen an, die sich aktuell in der Zone befinden sollten.
- **Alle** – Listet alle Personen aus allen Zonen auf.

Aktuelle Zone	Alle
KARTE	
GEBUCHT	
SOLDATEN	
001	SF Abendroth, Lea
002	OF Pfeffer, Lisa

Abbildung 7 : Ansicht „Aktuelle Zone“

Aktuelle Zone	Alle
KARTE	
ZONE	
GEBUCHT	
SOLDATEN	
001	SF Abendroth, Lea
002	OF Pfeffer, Lisa

Abbildung 8 : Ansicht „Alle“

Die Buchung einer Person erfolgt durch **Scannen der Zutrittskarte** oder die **manuelle Eingabe der Kartennummer**. Je nach Buchungsart gibt es unterschiedliche Rückmeldungen:

- **Einbuchung**: Die Person wird erfolgreich in die aktuelle Zone eingebucht und erscheint für einige Sekunden mit der Bemerkung „**Gerade eben**“ in der Tabelle, bevor die Buchungssuhrzeit angezeigt wird.

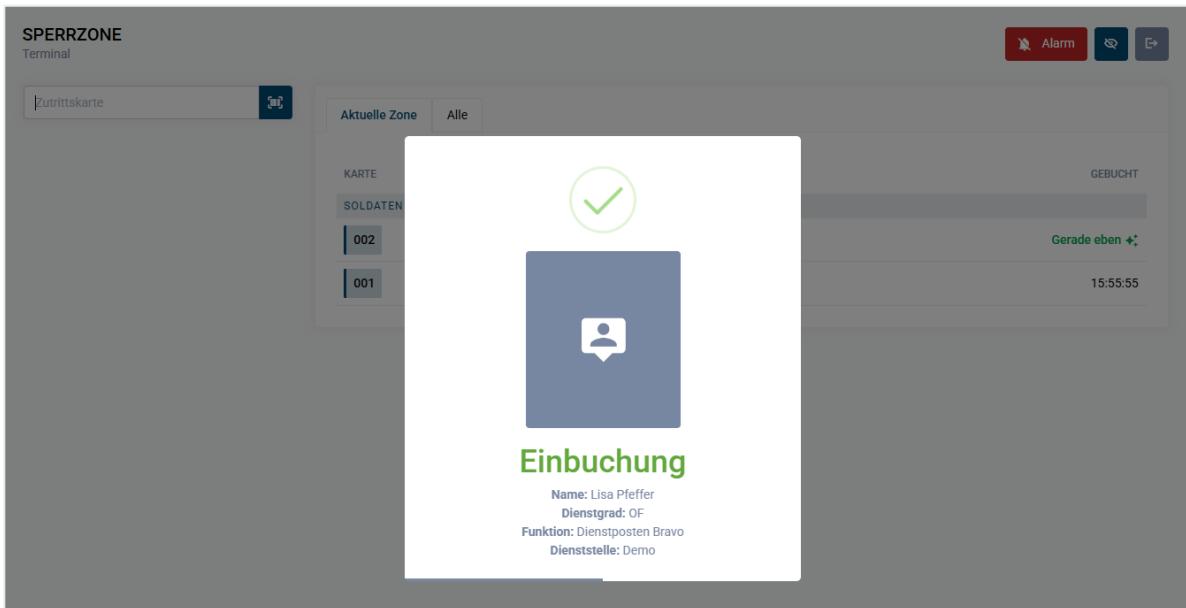


Abbildung 9 Meldung „Erfolgreiche Einbuchung“

- **Ausbuchung**: Die Person wird aus der Zone ausgebucht und automatisch in die **vorgegebene Nachfolgerzone** eingebucht. Dadurch verschwindet sie aus der Ansicht „**Aktuelle Zone**“.

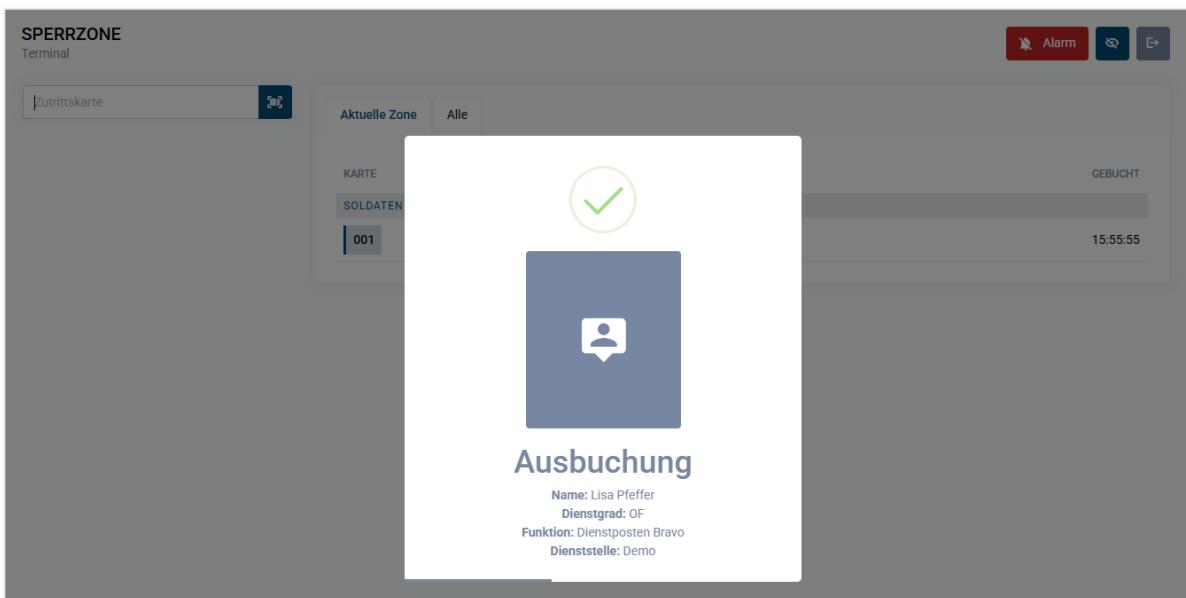


Abbildung 10 Meldung „Ausbuchung“

- **Eingeschränkter Zutritt:** Wird eine Person mit unzureichender Überprüfung in eine **Sicherheitszone** eingebucht, erhält sie nur Zutritt **in Begleitung und nach vorheriger Absprache mit dem Sicherheitsbeauftragten.**

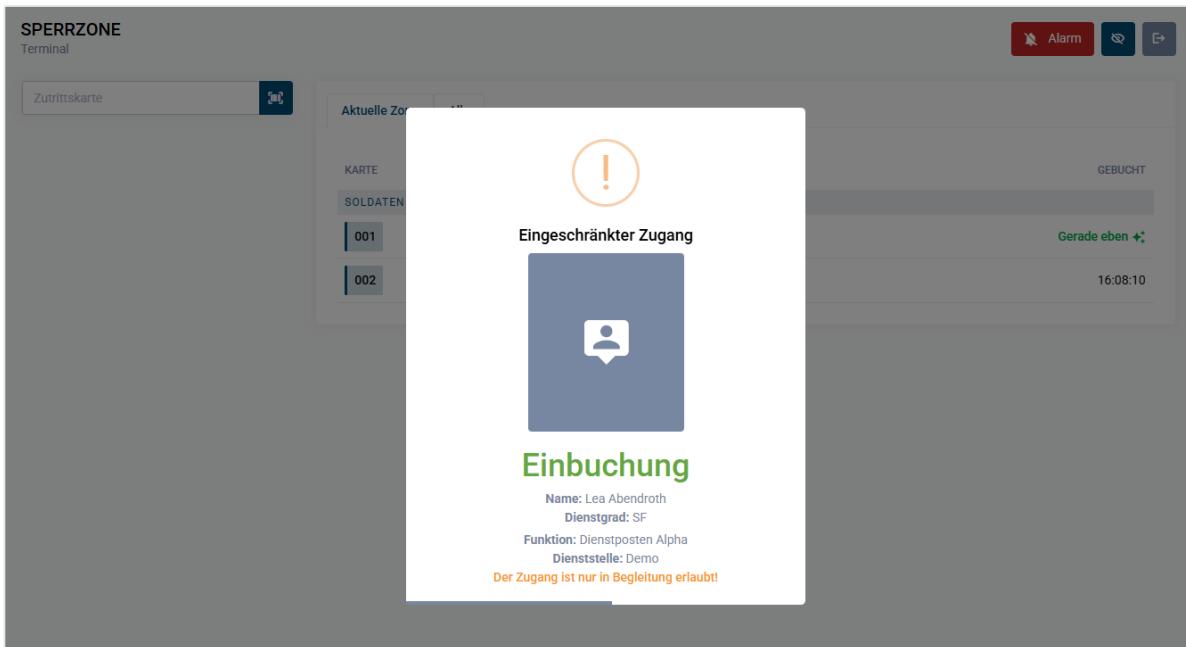


Abbildung 11 Meldung „Eingeschränkter Zutritt“

Fehlermeldungen bei der Buchung

Wenn eine Buchung nicht erfolgreich ist, gibt das Terminal zwei mögliche Fehlermeldungen aus:

- **Fehler: „Die Karte ist keiner Identität zugeordnet“** – Die Karte existiert nicht oder ist keiner Person zugewiesen.
- **Fehler: „Kein gültiger Buchungszeitraum“** – Die Karte ist einer Identität zugeordnet, aber die Gültigkeit ist entweder noch nicht begonnen oder bereits abgelaufen. In diesem Fall sollte der **Bearbeiter** informiert werden, um gegebenenfalls den Zeitraum anzupassen.

Datenschutzmodus

Das Terminal verfügt über einen **Datenschutzmodus**, der über den **Button mit dem durchgestrichenen Augensymbol** aktiviert werden kann. Sobald der Datenschutzmodus aktiv ist, werden **Klarnamen in der Übersicht ausgeblendet** und stattdessen nur **Kartennummern** angezeigt.

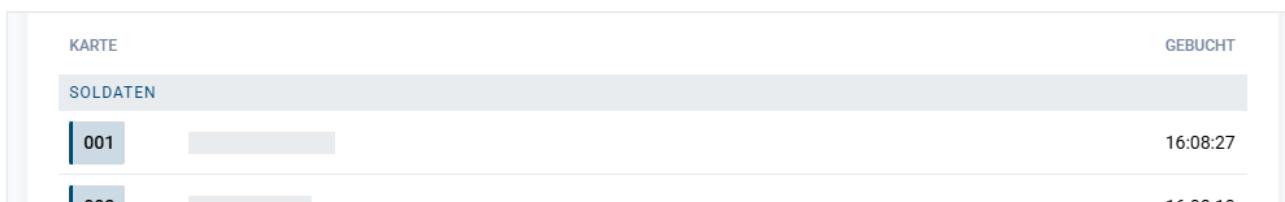


Abbildung 12 Anzeige ohne Klarnamen

Alarmauslösung über das Terminal

In bestimmten Terminals steht ein „**Alarm**“-Button zur Verfügung, mit dem ein Alarm auf den vernetzten Computern ausgelöst werden kann. Beim Drücken des Buttons kann die **Art des Alarms ausgewählt** und ausgeführt werden.

- Ist der Alarm **aktiv**, ändert sich die Beschriftung des Buttons zu „**Deaktivieren**“.
- Die Alarmmeldung kann auf den Computern für **5 Minuten pausiert** werden. Falls der Alarm in dieser Zeit nicht deaktiviert wurde, erscheint die Meldung erneut.
- Erst durch **Deaktivieren des Alarms** verschwindet die Meldung dauerhaft von den Computern.

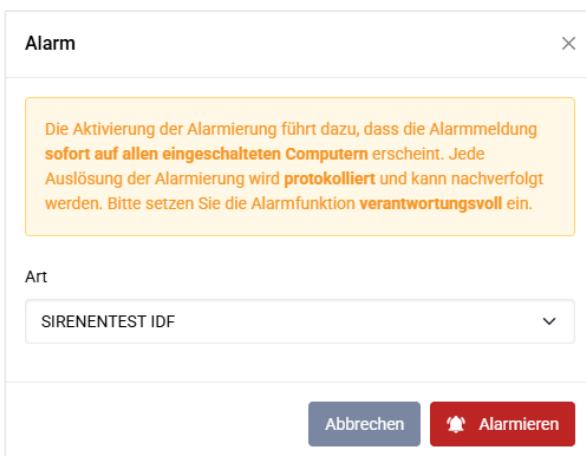


Abbildung 13 Alarmierungsmaske

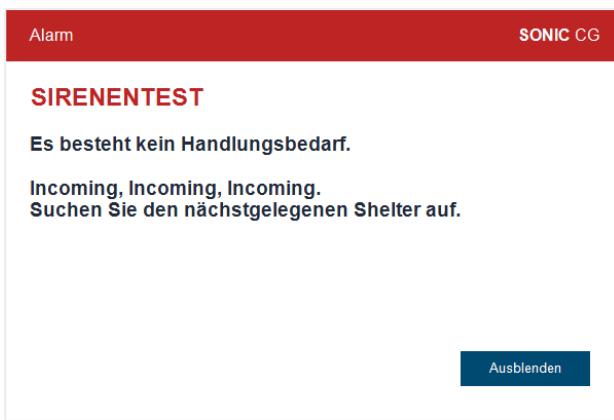


Abbildung 14 Alarmmeldung auf den Computern

Verlassen des Terminals

Um sich aus einem Terminal abzumelden oder sich in ein anderes berechtigtes Terminal einzuloggen, muss der „**Verlassen**“-Button genutzt werden.

Freigegebene Identitäten

Im Menüpunkt „**Identitäten**“ können Bediener die **Daten von freigegebenen Ortskräften** einsehen, um **Ausweisdokumente zu überprüfen und Zutrittszeiträume zu verifizieren**. Diese Funktion erleichtert die **Ausgabe der richtigen Zutrittskarte**.

Es werden nur **Ortskräfte angezeigt**, die eine gültige **Zutrittskarte und einen hinterlegten Zeitraum** besitzen. Zudem muss die **Bedienerfreigabe durch den Bearbeiter** erteilt worden sein. Die Daten dienen dazu, den **Personalausweis oder ein anderes Identitätsdokument** abzulegen und sicherzustellen, dass der Zugang gemäß den festgelegten Berechtigungen erfolgt.

KARTE	NACHNAME	VORNAME	AUSWEIS-ID	MITARBEITERAUSWEIS	OPTIONEN
L001	Harb	Mulham Muhab	LBX52332321223	LSS5235535	Ansehen
L002	Moghadam	Nizar Utbah	CVBNMSD		Ansehen

1 bis 2 von 2 Personen

Information

Die in dieser Liste aufgeführten Personen wurden ausdrücklich zur Einsichtnahme freigegeben. Dies bedeutet, dass Sie die Berechtigung haben, die relevanten Daten dieser Personen einzusehen. Bitte gehen Sie mit diesen Informationen verantwortungsvoll um.

Abbildung 15 Freigegebene Identitäten

Harb, Mulham Muhab
Identität

Stammdaten

Nachname: Harb
Ausweis: LBX52332321223
Vorname: Mulham Muhab
Mitarbeiterausweis: LSS5235535
Geburtstag: 1987-10-14

Foto

Zutrittsberechtigung

Zutritt ab: 2025-01-13
Zutritt bis: 2025-02-18
Karte: L001

Notizen

Das sind Notizen:

- Listeneintrag
- Listeneintrag

Abbildung 16 Detailansicht „Freigegebene Identität“

Bearbeiter

Der **Bearbeiter** ist dafür zuständig, alle relevanten Daten in der Anwendung zu pflegen. Im Menüpunkt "Identitäten" werden **alle Personen** und **Dienstposten** angelegt, bearbeitet oder gelöscht. Auf diese Weise stellt der **Bearbeiter** sicher, dass **alle relevanten Informationen** stets korrekt und aktuell sind.

The screenshot shows the 'Identitäten' dashboard with three main sections:

- DIENSTPOSTEN:** Describes managing service posts with assigned zone permissions. Includes a 'Verwalten' button.
- IDENTITÄTEN:** Describes managing soldiers, civilians, and military personnel. Includes a 'Verwalten' button.
- SCHNELLWAHL:** Describes quick selection for access cards, service posts, and identities. Includes a search input field labeled 'Eingabe'.

Abbildung 17 : Identitäten Dashboard

Dienstposten im Überblick

Ein **Dienstposten** beschreibt die **Position**, die eine Person in der Organisation innehat. Dazu gehört unter anderem, welche **Zutrittskarte** die Person erhält, ob eine **Sicherheitsüberprüfung** notwendig ist und ob **Sperrzonen** betreten werden dürfen. Da die Anwendung unterschiedliche **Arten von Dienstposten** berücksichtigt, sind diese übersichtlich in vier Kategorien eingeteilt:

- **Militärisch**
- **Zivil**
- **Ortskräfte**
- **Gäste**

Jede Kategorie wird in einer eigenen **Ansicht** dargestellt und kann im **Vollbildmodus** betrachtet werden. Diese **Ansichten** sind **durchsuchbar** und **sortierbar**, was bei einer großen Datenmenge für eine gute Übersicht sorgt.

#	ID	BEZEICHNUNG	DIENSTSTELLE	IDENTITÄT	NACHFOLGER	OPTIONEN
100000	Dienstposten Alpha	Demo	001 SF Abendroth, Lea	N001		
100001	Dienstposten Bravo	Demo	002 OF Pfeffer, Lisa	N002		
100002	Dienstposten Charlie	Demo	003 F Baumgaertner, Peter	N003		
100003	Dienstposten Delta	Demo	004 HF Mustermann, Max	N004		

Abbildung 18 : Dienstposten

Militärische und Zivile Dienstposten

Bei **militärischen** und **zivilen** Dienstposten sind die **Übersichten** ähnlich aufgebaut. In der Tabelle finden sich Spalten wie **Dienstposten-ID**, **Bezeichnung**, **Dienststelle**, **Identität** (aktueller Inhaber) und **Nachfolger**. Durch Anklicken der **Dienstposten-ID** gelangt man in die **Bearbeitungsmaske**, wo unter anderem die **Kartennummer** und andere **Stammdaten** angepasst werden können.

Nachfolger-Funktion

Bei militärischen und zivilen Dienstposten kann ein **Nachfolger** hinterlegt werden. Sobald im Formular eine Person als **Nachfolger** ausgewählt wurde, erscheint in der Übersicht der Button "**Übergeben**". Wird dieser Button gedrückt, wird die **Identität des bisherigen Dienstposteninhabers entfernt** und der zuvor eingetragene **Nachfolger** als neue Identität auf dem Dienstposten gesetzt. Beim Festlegen eines Nachfolgers, erhält der Nachfolger automatisch eine **abgeleitete Kartennummer** mit einem vorangestellten "N" (z. B. **001 → N001**).

Diese Funktion ermöglicht einen **formalen Personalwechsel**, ohne bestehende Daten komplett löschen zu müssen. Die veränderte Kartennummer zeigt zudem an, dass es sich bei der neuen Person um den **Nachfolger** handelt.

Abbildung 19 : Übergabebutton bei Nachfolgern

Formulare zum Anlegen und Bearbeiten

Beim Erstellen oder Bearbeiten eines **militärischen** oder **zivilen** Dienstpostens arbeitet der **Bearbeiter mit mehreren Karten**:

- **Stammdaten** (u. a. Dienstposten-ID, Bezeichnung, Dienststelle)
- **Kontakt** (Telefon, Mobilfunk, Funkrufnummer)
- **Identitäten** (Zutrittskarte, aktueller Inhaber, optional Nachfolger)
- **Sicherheit** (erforderliche Sicherheitsüberprüfung, Sperrzonenberechtigung)
- **Notizen** (interne Informationen, nur im Bearbeitungsmodus sichtbar)

Dienstposten für Ortskräfte

Ortskräfte werden über eine eigene **Übersicht** verwaltet. Hier werden **Dienstposten-ID**, **Bezeichnung**, **Arbeitsbereich** sowie die **Identität** (Ortskraft) angezeigt. Ein Klick auf die Dienstposten-ID oder die Identität öffnet die Bearbeitungsmaske.

Beim Anlegen eines neuen **Ortskräfte-Dienstpostens**:

- Wird eine **Zutrittskarte** im Format "L###" (z. B. **L010**) vergeben.
- Gibt es **keine Nachfolger-Funktion**, da Ortskräfte in der Regel unbefristet beschäftigt sind.
- Stehen die **Karten Stammdaten**, **Kontakt**, **Identitäten** und **Notizen** zur Verfügung.

Dienstposten für Gäste

Auch Gäste-Dienstposten erhalten eine eigene **Übersicht**. Hier findet sich pro Eintrag die **Dienstposten-ID**, eine **Bezeichnung**, die **Dienststelle**, die **Identität** (die betreffende Gast-Person) und ein Button zum **Bearbeiten**. Die ID und der Name der Identität verlinken ebenfalls direkt in das Bearbeitungsformular.

Bei **Gäste-Dienstposten**

- Nutzt die Zutrittskarte standardmäßig das Format "G###" (z. B. **G099**).
- Kann ein **Nachfolger** nicht hinterlegt werden, da es sich um eine temporäre Position handelt.
- Stehen die **Karten Stammdaten**, **Kontakt**, **Identitäten**, **Sicherheit** und **Notizen** zur Verfügung.

Identitäten

Die **Identitäten** umfassen alle Personen, die auf einem Dienstposten geführt werden können. Dabei unterscheidet die Software folgende Identitätsarten:

- **Soldaten**
- **Zivilisten**
- **Ortskräfte**
- **Gäste**

Jede Art hat ihre **eigene Ansicht**, welche **durchsuchbar**, **sortierbar** und bei Bedarf im **Vollbild** nutzbar ist. Bei umfangreichen Datenbeständen erleichtert dies das Auffinden und Filtern relevanter Einträge. Abhängig von der ausgewählten Identitätsart werden unterschiedliche **Spalten** angezeigt.

Identitäten							 Neu		
							 Suchen		
Soldaten	Zivilisten	Ortskräfte	Gäste						
NACHNAME	VORNAME	DIENSTGRAD		IN	OUT	KARTEN		OPTIONEN	
Abendroth	Lea	SF	2025-01-05	2025-11-19	Dienstposten Alpha - Demo	 001	 Bearbeiten		
Baumgaertner	Peter	F	2025-01-13	2025-02-08	Dienstposten Charlie - Demo	 003	 Bearbeiten		
Mustermann	Max	HF	2025-02-11	2025-02-26	Dienstposten Delta - Demo	 004	 Bearbeiten		
Pfeffer	Lisa	OF	2025-01-05	2025-05-21	Dienstposten Bravo - Demo	 002	 Bearbeiten		
Rothstein	Marcel	HF	2025-01-06	2025-01-15	Dienstposten Alpha - Demo	 N001	 Bearbeiten		

Abbildung 20 : Identitäten „Soldaten“

Ansichten nach Identitätsart

Soldaten

In dieser Ansicht findest du unter anderem die Spalten **Nachname**, **Vorname**, **Dienstgrad**, **IN-Datum**, **OUT-Datum**, **Dienstposten** (als Link zur Dienstposten-Bearbeitung), **Karte** (Zutrittskartennummer) und **Optionen** (Bearbeiten-Button).

- **IN-/OUT-Datum:** Bei Mouseover zeigt das System an, wie viele Tage noch bis zum jeweiligen Datum verbleiben.
- **Farbkennzeichnung:** Ist das OUT-Datum bereits abgelaufen, erscheint eine **rote** Markierung. Liegt das OUT-Datum innerhalb der nächsten 10 Tage, wird es **gelb** markiert.

Zivilisten

Diese Ansicht ähnelt der „Soldaten“-Übersicht, verzichtet jedoch auf den **Dienstgrad**. Ansonsten gelten dieselben Spalten (z. B. Vorname, Nachname, IN/OUT, Dienstposten, Karte, Optionen) und dieselbe Farbmarkierungs-Logik bei Ablaufdaten.

Ortskräfte

Hier siehst du die Spalten **Nachname**, **Vorname**, **Ausweis-ID**, **Zutritt ab**, **Zutritt bis**, **Dienstposten** (Link), **Karte** (Zutrittskartennummer) und **Optionen** (Bearbeiten).

- **Farbmarkierung:** Wie bei Soldaten/Zivilisten werden bevorstehende Abläufe gelb und abgelaufene Einträge rot markiert.
- **Zusätzliche Buttons** neben der Suchleiste:
 - „**Bedieneransicht**“: Zeigt jene Ortskräfte, für die eine **Bedienerfreigabe** gesetzt wurde (damit Bediener diese im Menü „Freigegebene Identitäten“ sehen können).
 - „**Sperrliste**“: Öffnet die Liste der gesperrten Ortskräfte.

Gäste

Die Gäste-Übersicht enthält die Spalten **Nachname**, **Vorname**, **Zutritt ab**, **Zutritt bis**, **Dienstposten** (Link), **Karte** (Zutrittskartennummer) und **Optionen**. Wiederum gelten die **Farbmarkierungen** bei näher rückenden oder bereits überschrittenen OUT-Daten.

Sperrliste für Ortskräfte

Klickt der Bearbeiter in der „Ortskräfte“-Ansicht auf den Button „**Sperrliste**“, öffnet sich ein separates Verzeichnis aller Personen, die dauerhaft vom Zugang ausgeschlossen sind. Eine so gesperrte Ortskraft kann nicht mehr in der Anwendung angelegt werden, da beim Erfassen einer neuen Ortskraft automatisch die **Ausweisnummer** gegen diese Liste geprüft wird.

Abbildung 21 : Sperrliste

Aufbau der Sperrliste

- Spalten: **Nachname, Vorname, Ausweis-ID, Optionen** (Bearbeiten).
- **Durchsuch- und sortierbare Tabelle**, ähnlich wie die anderen Ansichten.

Neuen Eintrag hinzufügen

- *Karte Stammdaten*: Felder für Nachname, Vorname, Geburtstag, Nationalität, Ausweisnummer, Firma.
- *Karte Begründung*: Formatierbares Textfeld zum Hinterlegen des Sperrgrunds.
- *Karte Notizen*: Formatierbares Textfeld für interne Vermerke, die nicht in Exporten auftauchen.

Export

- Die vollständige Sperrliste lässt sich als **Excel-Datei** exportieren.

Anlegen neuer Identitäten

Für jede Identitätsart (Soldaten, Zivilisten, Ortskräfte, Gäste) steht dem Bearbeiter ein eigenes **Formular** zur Verfügung, das in **mehrere Karten** unterteilt ist. Im Folgenden werden die wichtigsten Unterschiede und Felder beschrieben.

Soldaten anlegen

1. Karte Stammdaten

- **Dienstgrad** (Auswahlfeld; alle Dienstgrade sind hinterlegt)
- **Nachname, Vorname**
- **Sicherheitsüberprüfung** (Keine, Ü1, Ü2, Ü3) – relevant für Dienstposten, die eine bestimmte Stufe erfordern

2. Karte Kommandierung

- **IN-Datum**: Tag, ab dem die Person ihren Zutritt erhält (wird farblich gekennzeichnet, wenn dieser Zeitraum ansteht oder abgelaufen ist)
- **OUT-Datum**: Voraussichtliches Verlassen des Einsatzorts, ebenfalls mit Mouseover-Info und Farbkennzeichnung
- **Eingangszone**: Definiert, in welcher Zone der Soldat ab dem IN-Datum zuerst eingebucht wird
- **Foto**: Optionales Lichtbild, das später z. B. im Terminal angezeigt werden kann

3. Karte Identitäten

- **Dienstposten**: Auswahl aus einer Liste an verfügbaren Dienstposten; ist bereits ein Nachfolgerplatz frei, kann der Soldat automatisch als Nachfolger eingetragen werden

4. Karte Notizen

- Ein **formatierbares Textfeld** für interne Hinweise, nur im Bearbeitungsmodus sichtbar

Zivilisten anlegen

Das Vorgehen bei **Zivilisten** gleicht dem bei Soldaten, **nur ohne Dienstgrad**. Alle anderen Karten (Stammdaten, Kommandierung, Identitäten, Notizen) funktionieren analog, und auch hier kann die Eingangszone, Sicherheitsüberprüfung etc. festgelegt werden.

Ortskräfte anlegen

1. Karte Stammdaten

- **Nachname, Vorname, Geburtstag**
- **Ausweis** (automatischer Abgleich mit der Sperrliste)
- **Mitarbeiterausweis** (falls vorhanden)

2. Karte Zeitraum

- **Zutritt ab / Zutritt bis** (Farblogik bei Ablauf)
- **Eingangszone** (z. B. falls die Ortskraft mit einer gültigen Karte direkt von außen das Camp betreten kann)

3. Karte Foto

- Optionales Lichtbild für Terminal-Anzeigen

4. Karte Identitäten

- **Dienstposten** (da Ortskräfte keine Nachfolger-Funktion haben, werden nur unvergebene Dienstposten angeboten)
- **Bedienerfreigabe:** Ja/Nein (wenn Ja, kann ein Bediener diese Ortskraft in „Freigegebene Identitäten“ einsehen)

5. Karte Sicherheit

- **Sicherheitsbelehrung** (Datum, 1 Jahr gültig)
- **Letzte Befragung**
- **BAMAD-Registrierungsnummer, BAMAD Abgabe, BAMAD Ergebnis** (jeweils Datumsfelder für militärische Sicherheitsauswertungen)

6. Karte Notizen

- Formatierbares Feld für interne Hinweise

Gäste anlegen

Die **Gast**-Kategorie deckt vorübergehende Personen ab, die zeitlich begrenzten Zugang erhalten.

1. Karte Stammdaten

- **Nachname, Vorname, Geburtstag, Ausweis**

2. Karte Zeitraum

- **Zutritt ab / Zutritt bis**
- **Eingangszone** (wo der Gast ab Zutrittsbeginn eingebucht ist)

3. Karte Identität

- **Dienstposten** (reine Gast-Dienstposten, keine Nachfolger-Funktion)

4. Karte Foto (optional)

5. Karte Notizen (intern)

Berichte zur Militärischen Sicherheit

Über den Menüpunkt „Berichte“ gelangt der Bearbeiter zu verschiedenen Auswertungen. In der Karte „Militärische Sicherheit“ stehen unter anderem folgende Berichte zur Verfügung:

1. Sicherheitsbelehrungen
2. Militärische Abschirmdienst
3. Konflikte (DERZEIT NICHT VERFÜGBAR)

Mit diesen **Berichten zur Militärischen Sicherheit** erhalten Bearbeiter eine gezielte Übersicht über **Ortskräfte**, bei denen wichtige Sicherheitsfristen in Kürze ablaufen oder bereits überschritten sind. Indem die Daten **automatisiert** ausgewertet werden, spart der Bearbeiter Zeit und kann notwendige Maßnahmen (z. B. erneute Sicherheitsbelehrung, Einleitung einer neuen Überprüfung) rechtzeitig einleiten. Alle Berichte lassen sich zudem als **Excel-Datei** exportieren, was eine einfache Weiterverarbeitung oder Archivierung ermöglicht.

Sicherheitsbelehrungen

Im Bericht „**Sicherheitsbelehrungen**“ werden **alle Ortskräfte** aufgelistet, deren Sicherheitsbelehrung **bereits abgelaufen** ist oder **innerhalb der nächsten 30 Tage abläuft**. Auf diese Weise erkennt der Bearbeiter schnell, bei welchen Personen eine neue Belehrung erforderlich ist oder zeitnah ansteht.

- **Exportmöglichkeit:**

Dieser Bericht kann als **Excel-Datei** exportiert werden, wodurch eine externe Weiterverarbeitung (z. B. Weiterleitung an Vorgesetzte oder Sicherheitsabteilungen) erleichtert wird.

NACHNAME	VORNAME	LETZTE BELEHRUNG	STATUS
Hakimi	Saabira Tharwah	2024-01-02	Bereits abgelaufen
Harb	Mulham Muhab	2024-02-23	Läuft ab in 12 Tagen

Gültigkeit: Die Sicherheitsbelehrung ist ein Jahr ab dem Datum der Durchführung gültig.

Ablaufüberwachung: Diese Übersicht zeigt alle Ortskräfte, deren Sicherheitsbelehrung:

- Bereits abgelaufen ist, oder
- In den nächsten 30 Tagen abläuft.

Abbildung 22 Bericht „Sicherheitsbelehrungen“

Militärische Abschirmdienst

Der Bericht „**Militärische Abschirmdienst**“ (BAMAD) prüft unterschiedliche Kriterien zur **Ablaufüberwachung** und **Neubewertung** der Ergebnisse:

1. Ablaufüberwachung

- Zeigt sämtliche Ortskräfte, deren **Ergebnis bereits abgelaufen** ist oder **innerhalb der nächsten 30 Tage abläuft**.
- Dadurch erhält der Bearbeiter einen Hinweis, dass eine **erneute Überprüfung** erforderlich sein könnte.

2. Neubewertung

- Sofern bereits eine neue Überprüfung eingeleitet wurde, erscheint die Ortskraft in der Liste **nur, wenn nach 6 Monaten noch kein neues Ergebnis** vorliegt.
- Auf diese Weise kann der Bearbeiter nachverfolgen, ob ausstehende Überprüfungen rechtzeitig abgeschlossen wurden oder ob Nachfragen nötig sind.

▪ Exportmöglichkeit:

Wie bei den Sicherheitsbelehrungen kann dieser Bericht als **Excel-Datei** exportiert werden, sodass eine Weitergabe an zuständige Stellen oder eine Dokumentation außerhalb der Anwendung möglich ist.

NACHNAME	VORNAME	LETZTES ERGEBNIS	STATUS
Moghadam	Nizar Utbah	2022-06-07	Warten auf Ergebnis seit 255 Tagen
Hakimi	Saabira Tharwah	2023-01-02	Bereits abgelaufen

Information

Gültigkeit: Die Ergebnisse sind zwei Jahre gültig.

Ablaufüberwachung: Diese Übersicht zeigt alle Ortskräfte, deren Ergebnis:

- Bereits abgelaufen ist, oder
- In den nächsten 30 Tagen abläuft.

Neubewertung: Falls bereits eine neue Überprüfung eingeleitet wurde, erscheint diese in der Liste nur, wenn nach 6 Monaten noch kein neues Ergebnis vorliegt.

Abbildung 23 : Bericht „Militärischer Abschirmdienst“

Auswerter

Berichte

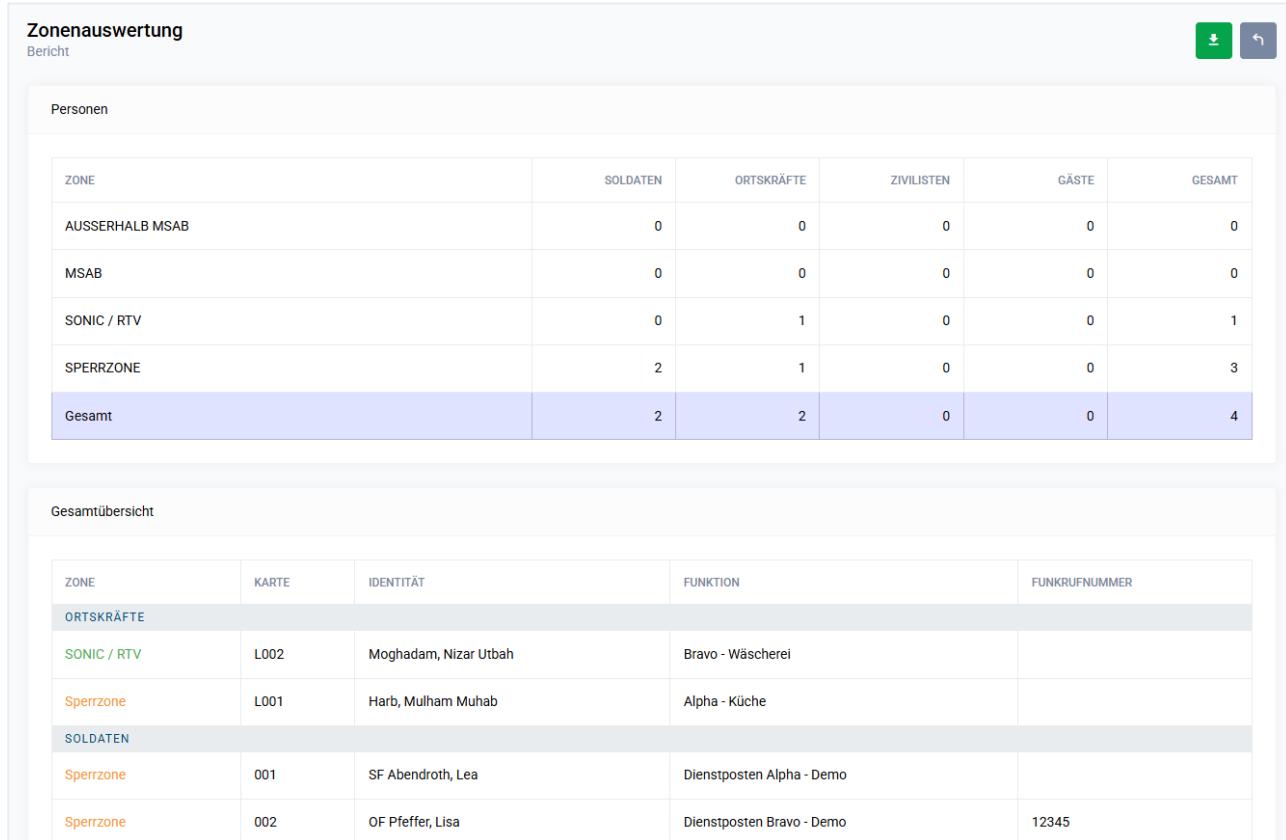
Auswerter haben im Menüpunkt „**Berichte**“ die Möglichkeit, verschiedene **Auswertungen zu erstellen und Berichte anhand von Datensätzen zu generieren**. Diese Berichte dienen der **Analyse und Dokumentation** und können sowohl in der Anwendung betrachtet als auch exportiert werden.



Abbildung 24 Berichte „Alle Berichtsfunktionen“

Zonenauswertung

Die **Zonenauswertung** ermöglicht eine **detaillierte Übersicht darüber, welche Soldaten, Ortskräfte, Zivilisten und Gäste sich aktuell in welcher Zone befinden** und wie diese erreichbar sind. Dies bietet eine schnelle und übersichtliche Möglichkeit zur Lageeinschätzung und Ressourcenplanung.



The screenshot displays the 'Zonenauswertung' report interface. It includes a header with a back button and a save icon. Below the header are two main sections:

- Personen:** A table showing the count of individuals in different zones. The columns are: ZONE, SOLDATEN, ORTSKRÄFTE, ZIVILISTEN, GÄSTE, and GESAMT. The rows include: AUSSERHALB MSAB (0, 0, 0, 0, 0, 0), MSAB (0, 0, 0, 0, 0, 0), SONIC / RTV (0, 1, 0, 0, 0, 1), SPERRZONE (2, 1, 0, 0, 0, 3), and a summary row 'Gesamt' (2, 2, 0, 0, 0, 4).
- Gesamtübersicht:** A table providing detailed information about personnel. It includes columns: ZONE, KARTE, IDENTITÄT, FUNKTION, and FUNKRUFNUMMER. The rows are grouped by category: ORTSKRÄFTE (SONIC / RTV, L002, Moghadam, Nizar Utbah, Bravo - Wäscherei), SOLDATEN (Sperrzone, L001, Harb, Mulham Muhab, Alpha - Küche), and another group of SOLDATEN (Sperrzone, 001, SF Abendroth, Lea, Dienstposten Alpha - Demo) and (Sperrzone, 002, OF Pfeffer, Lisa, Dienstposten Bravo - Demo, 12345).

Abbildung 25 Zonenauswertung

Folgende Funktionen stehen in der Zonenauswertung zur Verfügung:

- **Echtzeit-Übersicht** über die aktuelle Personallage der Zonen.
- **Ermittlung von Gesamtzahlen**, um statistische Auswertungen zu ermöglichen.
- **Exportmöglichkeit** in verschiedene Formate:
 - **PDF-Export** zur strukturierten Dokumentation.
 - **EXCEL-Export** zur weiteren Bearbeitung und Analyse.
 - **Direkte Ansicht innerhalb der Anwendung** für eine schnelle Übersicht.

Schutzbauten

Der **Bericht für die Schutzbauten** ist eine essenzielle Auswertung im **Alarmierungsfall**. Er bietet eine **Gesamtübersicht über alle verfügbaren Schutzbauten**, einschließlich deren **Kommunikationsmittel zur Erreichbarkeit**. Falls bereits Personen in einem Schutzbau eingetragen sind, wird die **aktuelle Anzahl der im Schutzbau befindlichen Personen** angezeigt.

Schutzbauten							
Schutzbauten					Information		
BEZEICHNUNG	TELEFON	FUNK	PERSONEN	OPTIONEN			
R01	6401	22168	0	 Verwalten			
R02	6402	22169	0	 Verwalten			
R03	6403	22170	0	 Verwalten			
R04	6404	22171	0	 Verwalten			

Abbildung 26 Übersicht „Schutzbauten Bericht“

Eintragen von Personen im Alarmierungsfall

Im Alarmfall begeben sich alle Personen gemäß **Protokoll** in die Schutzbauten, und deren Kartennummern werden dokumentiert. Der **Auswerter** kann über den **Button „Verwalten“** einen Schutzbau auswählen, um Personen dort zu registrieren.

- Der **Auswerter kontaktiert den Schutzbau** per Telefon oder Funk und erhält die **Kartennummern der anwesenden Personen**.
- Diese werden im Feld „**Personenerfassung**“ eingegeben und per **Enter-Taste oder Mausklick** zur Liste hinzugefügt.
- Bereits in einem anderen Schutzbau erfasste Karten sind **nicht mehr wählbar**.
- Nach vollständiger Erfassung aller Personen muss der **Button „Speichern“** gedrückt werden, um die Daten zu sichern.
- Dieses Verfahren wird für alle Schutzbauten wiederholt.

The screenshot shows a user interface for managing personnel in a shelter. At the top left, it says 'R01 Schutzbau'. On the right, there are buttons for 'Speichern' (Save), 'Abbrechen' (Cancel), and 'Schließen' (Close). Below this, a section titled 'Personenerfassung' contains a text box with instructions: 'Tragen Sie alle Kartennummern ein, die in diesen Schutzbau eingebucht werden sollen. Anschließend müssen Sie nur noch auf „Speichern“ klicken, um alle Personen in diesem Schutzbau zu erfassen.' There are two input fields containing 'x 001' and 'x 002'. To the right, a map shows the shelter's layout with several buildings and a location marker. At the bottom, there are two buttons: one with a phone icon labeled '6401' and another with a mobile phone icon labeled '22168'.

Abbildung 27 Schutzbau „Personenerfassung“

Zurücksetzen von Schutzbauten

Falls fehlerhafte Eintragungen vorgenommen wurden, gibt es zwei Möglichkeiten zum Zurücksetzen:

- **Einzelne Personen entfernen:** Falsch erfasste Personen können aus der **Mehrfachauswahl entfernt** werden, bevor der Schutzbau gespeichert wird.
- **Komplettes Zurücksetzen eines Schutzbau:** Über „**Verwalten**“ kann ein Schutzbau vollständig zurückgesetzt werden, wodurch **alle Eintragungen in diesem Schutzbau gelöscht** werden.
- **Gesamtes Zurücksetzen aller Schutzbauten:** In der **Gesamtübersicht** kann über einen **roten Button** die **Lösung aller Eintragungen** durchgeführt werden. Dies sollte nach **jedem abgeschlossenen Alarm** sowie nach **Export und Sicherung der Daten** erfolgen.



Abbildung 28 Zurücksetzen „Schutzbauten Bericht“

Bericht exportieren

Nach vollständiger Erfassung von allen Personen in den Schutzbauten sollte der **Bericht als PDF-Datei exportiert** und für die Auswertung genutzt werden.

Der Bericht beinhaltet:

- **Welche Personen sich in welchem Schutzbau befinden** und deren Erreichbarkeit.
- **Personen, die keinem Schutzbau zugewiesen wurden**, mit Angaben zur **aktuellen Zone und Erreichbarkeit**.

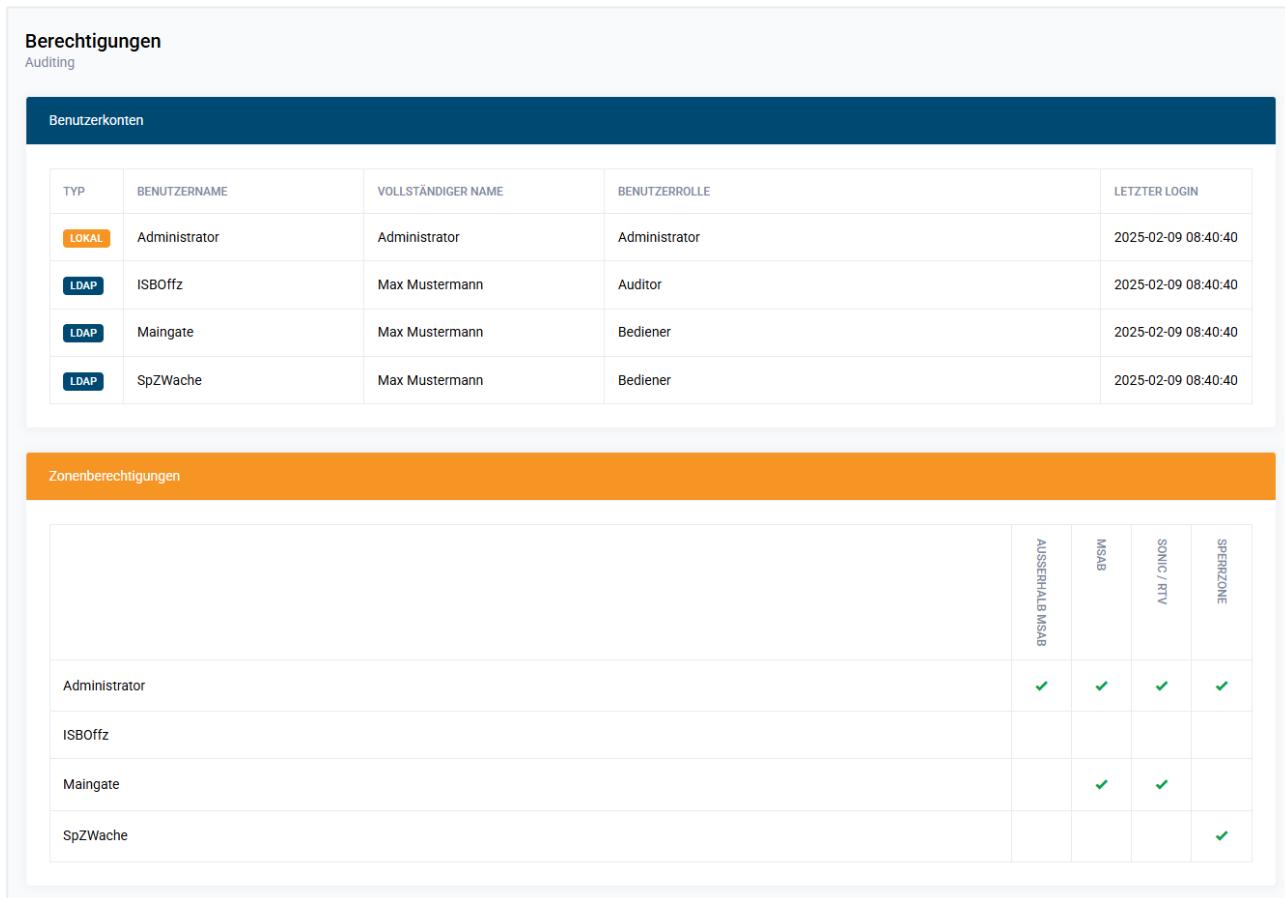
SONICCG		VS-NfD	Schutzbautenbericht
Keine Schutzraumzuordnung			
KARTE	IDENTITÄT	FUNK	ZONE
002	OF Pfeffer, Lisa	12345	Sperrzone
001	SF Abendroth, Lea		Sperrzone

Abbildung 29 : Beispiel von exportierten PDF-Bericht

Auditor

Berechtigungen

Auditoren haben im Menüpunkt „**Berechtigungen**“ die Möglichkeit, alle Benutzer der Anwendung sowie deren zugewiesene **Benutzerrollen** einzusehen. Zusätzlich wird eine **automatisch generierte Zonenberechtigungen-Matrix** bereitgestellt, die anzeigt, welche Nutzer Zugriff auf welche **Terminals** haben. Des Weiteren enthält die Seite eine **Rechte-Matrix**, die detailliert darstellt, welche Benutzerrolle über welche **Berechtigungen innerhalb der Anwendung** verfügt. Dies ermöglicht Auditoren eine umfassende Kontrolle und Überprüfung der Zugriffsrechte.



The screenshot shows two main sections: 'Benutzerkonten' and 'Zonenberechtigungen'.

Benutzerkonten:

TYP	BENUTZERNAME	VOLLSTÄNDIGER NAME	BENUTZERROLLE	LETZTER LOGIN
LOKAL	Administrator	Administrator	Administrator	2025-02-09 08:40:40
LDAP	ISBOffz	Max Mustermann	Auditor	2025-02-09 08:40:40
LDAP	Maingate	Max Mustermann	Bediener	2025-02-09 08:40:40
LDAP	SpZWache	Max Mustermann	Bediener	2025-02-09 08:40:40

Zonenberechtigungen:

	AUSSERHALB MSAB	MSAB	SONIC / RTV	SPERRZONE
Administrator	✓	✓	✓	✓
ISBOffz				
Maingate		✓	✓	
SpZWache				✓

Abbildung 30 : Auditing von Berechtigungen

Protokolle

Im Menüpunkt „**Protokolle**“ haben Auditoren die Möglichkeit, alle **protokollierten Ereignisse** der Anwendung einzusehen. Dazu gehören **erfolgreiche und fehlgeschlagene Anmeldungen**, Änderungen an **Administrationseinstellungen**, Anpassungen an **personenbezogenen Daten von Identitäten und Berechtigungen** sowie der **Download von Berichten und anderen Protokollen**. Alle Protokolleinträge werden für **90 Tage** gespeichert.

Protokolle
Auditing

Einträge

30 Einträge anzeigen Suchen

TYPE	BESCHREIBUNG	BENUTZER	IP-ADRESSE	DATUM
Benutzerkonto	Daten von Benutzerkonto "SpZWache" aktualisiert	Administrator	X.X.X.X	2025-02-09 09:32:26
Backup	Backup Heruntergeladen	Administrator	X.X.X.X	2025-02-09 09:22:32
Schutzbauten	Schutzbau "R11" aus dem System entfernt	Administrator	X.X.X.X	2025-02-09 08:55:34
Login	Erfolgreiche Anmeldung	Mustermann	X.X.X.X	2025-02-08 14:41:50
Identität	Identität "Mustermann, Max" bearbeitet	Administrator	X.X.X.X	2025-02-07 13:32:06
Login	Fehlgeschlagener Anmeldeversuch	test	X.X.X.X	2025-02-07 13:28:52

Information

Einträge werden **automatisch gelöscht**, sobald sie älter als **90 Tage** sind. Dies trägt zur Optimierung unserer Datenverwaltung als auch zur Einhaltung der Datenschutzstandards bei.

Abbildung 31 : Protokoll

Export von Protokollen

Das Protokoll kann als **PDF-Datei** exportiert werden. Dabei kann entweder ein **individueller Zeitraum** ausgewählt oder der **gesamte verfügbare Zeitraum** an Protokollen exportiert werden. Diese Funktion ermöglicht eine gezielte Analyse und Dokumentation sicherheitsrelevanter Ereignisse.

Protokoll Exportieren

Beim Export von Protokollen können Sie optional einen gewünschten Zeitraum festlegen. Wird kein Zeitraum ausgewählt, erfolgt der Export für den gesamten verfügbaren Zeitraum. Der Exportvorgang wird ebenfalls protokolliert.

Von Bis

Abbrechen Download

Abbildung 32 : Protokoll Exportieren

Buchungshistorie

Im Menüpunkt „**Buchungshistorie**“ können Auditoren alle **Terminalbuchungen** einsehen, um nachzuvollziehen, **welche Person zu welcher Zeit in welcher Zone gebucht wurde**. Diese Daten ermöglichen eine lückenlose Nachverfolgung der Zutrittsbewegungen innerhalb der Anwendung. Die Buchungshistorie wird für **90 Tage** gespeichert und anschließend automatisch gelöscht. Die **Datentabelle ist vollständig durchsuchbar**, sodass gezielt nach bestimmten Personen, Buchungszeiten oder Zonen gefiltert werden kann.

KARTE	IDENTITÄT	VERLASSEN	BETRETEN	DATUM
001	SF Abendroth, Lea	Außerhalb MSAB	MSAB	2025-02-06 13:54:53
001	OSG Theissen, Angelika	SONIC / RTV	Sperrzone	2025-02-06 13:48:04
001	OSG Theissen, Angelika	Sperrzone	SONIC / RTV	2025-02-06 13:47:58
002	OF Pfeffer, Lisa	SONIC / RTV	Sperrzone	2025-02-05 07:59:28

Abbildung 33 : Buchungshistorie

Export der Buchungshistorie

Die Buchungshistorie kann als **PDF-Dokument** exportiert werden. Dabei kann ein **individueller Zeitraum** oder der **gesamte verfügbare Zeitraum** an Buchungen gewählt werden.

Beim Export von der Buchungshistorie können Sie optional einen gewünschten Zeitraum festlegen. Wird kein Zeitraum ausgewählt, erfolgt der Export für den gesamten verfügbaren Zeitraum. Der Exportvorgang wird ebenfalls protokolliert.

Von Bis

Abbrechen **Download**

Abbildung 34 : Buchungshistorie Exportieren

Administrator

Benutzerverwaltung

Die **Benutzerverwaltung** bietet Administratoren eine zentrale Übersicht über alle Benutzerkonten des Systems. Über die Administrationsoberfläche können sowohl **lokale Benutzerkonten** als auch **Domänenbenutzerkonten** verwaltet werden.

TYP	BENUTZERNAME	VOLLSTÄNDIGER NAME	BENUTZERROLLE	LETZTER LOGIN	OPTIONEN
LOKAL	Administrator	Administrator	Administrator	2025-02-08 08:46:37	
LDAP	Mustermann	Max Mustermann	Bediener	2025-02-08 14:41:50	Bearbeiten

Abbildung 35 : Benutzerkontenverwaltung

Hinzufügen von Benutzerkonten

Lokale Benutzerkonten werden über den Button „**Hinzufügen**“ erstellt. Dabei müssen der **Benutzername**, **vollständige Name** und die **Benutzerrolle** sowie ein **Passwort** festgelegt werden.

Abbildung 36 : Neues Benutzerkonto

Domänenbenutzerkonten werden automatisch registriert, wenn sich ein Benutzer erstmals anmeldet und Mitglied der **bei der Installation definierten Domänengruppe** ist. Diese Benutzer werden standardmäßig mit der Rolle „**Bediener**“ ohne **Zonenberechtigungen** angelegt.

Bearbeiten von Benutzerkonten

Die **lokalen Benutzerkonten** können vollständig über die Anwendung bearbeitet werden.

The screenshot displays a user interface for managing local user accounts. On the left, under the heading 'Mustermann' (User) - 'Benutzerkonto', there is a 'Benutzerdaten' section containing fields for 'Benutzername' (Mustermann), 'Vollständiger Name' (Max Mustermann), and 'Rolle' (Bearbeiter). A 'Speichern' (Save) button is located at the bottom of this section. On the right, there is a 'Passwort' (Password) section with fields for 'Neues Passwort' and 'Passwort bestätigen', and a 'Speichern' button. At the top right of the interface are buttons for 'Löschen' (Delete) and navigating back.

Abbildung 37 : Bearbeiten eines Lokalen Benutzerkontos

Bei **Domänenbenutzern** können lediglich die **Benutzerrolle** und – falls die Rolle „Bediener“ zugewiesen wurde – die **Zonenberechtigungen** angepasst werden. Andere Informationen wie **Benutzername, vollständiger Name und Passwort** werden aus der Domäne übernommen und können nicht verändert werden.

The screenshot shows the same user interface as Abbildung 37, but for a domain user account ('Mustermann' - 'Benutzerkonto'). The 'Benutzerdaten' section is identical. In the 'Passwort' section, there is a message box stating: 'Da dieses Benutzerkonto ein Domänenkonto ist, kann das Passwort nur auf dem Domänencontroller zurückgesetzt werden.' (As this user account is a domain account, the password can only be reset on the domain controller.)

Abbildung 38 : Bearbeiten eines Domänenbenutzers

Bearbeiten von Zonenberechtigungen

Für die Rolle „**Bediener**“ können Administratoren festlegen, auf welche Terminals der Benutzer Zugriff hat. Bei Auswahl dieser Rolle erscheint automatisch ein **Mehrfachauswahl-Feld**, in dem die entsprechenden Zonenberechtigungen zugewiesen werden können.

The screenshot shows a user profile for 'Mustermann' under 'Benutzerkontos'. The 'Benutzerdaten' tab is active, displaying the username 'Mustermann' and full name 'Max Mustermann'. The 'Rolle' dropdown is set to 'Bediener'. Under 'Zonenberechtigungen', there is a list with 'MSAB' and 'Sperrzone' selected. The 'Passwort' tab on the right contains a note: 'Da dieses Benutzerkonto ein Domänenkonto ist, kann das Passwort nur auf dem Domänencontroller zurückgesetzt werden.' A 'Speichern' (Save) button is at the bottom.

Abbildung 39 : Bearbeiten von Zonenberechtigungen

Löschen von Benutzern

Beim Löschen eines Benutzerkontos ist zu beachten, dass **lokale Benutzerkonten dauerhaft entfernt werden** und bei Bedarf manuell neu erstellt werden müssen. **Domänenbenutzerkonten** sollten zuvor aus der **Domänengruppe entfernt** werden, da sie sonst bei der nächsten Anmeldung automatisch als **Bediener ohne Zonenberechtigungen** neu registriert werden.

The dialog box is titled 'Benutzerkonto Löschen'. It contains a message: 'Möchten Sie das Benutzerkonto dauerhaft löschen? Dieser Vorgang kann nicht rückgängig gemacht werden.' Below is a note: 'Um das Benutzerkonto endgültig zu löschen, entfernen Sie bitte die Zuordnung des Benutzers zur Gruppe „CampGuard_Nutzer“ auf dem Domänencontroller. Andernfalls wird das Konto beim nächsten Login automatisch neu erstellt.' At the bottom are 'Abbrechen' and 'Löschen' buttons.

Abbildung 40 : Benutzerkonto Löschen

Zonenverwaltung

Die **Zonenverwaltung** bietet eine Übersicht über alle bereits angelegten Zonen sowie deren zugeordneten Eigenschaften.

ZONENNAME	AUSGANGSZONE	ALARM	EINGESCHRÄNKTE	OPTIONEN
SONIC / RTV	MSAB	Nein	Nein	Bearbeiten
MSAB	Außerhalb MSAB	Nein	Nein	Bearbeiten
Sperrzone	SONIC / RTV	Ja	Ja	Bearbeiten
Außerhalb MSAB	MSAB	Nein	Nein	Bearbeiten

Abbildung 41 : Zonenverwaltung

Hinzufügen und Bearbeiten von Zonen

Administratoren können **neue Zonen erstellen** oder bestehende Zonen bearbeiten. Beim Erstellen oder Bearbeiten müssen verschiedene Eigenschaften konfiguriert oder angepasst werden, darunter der **Name der Zone, die Ausgangszone, ob es sich um eine eingeschränkte Zone handelt, die Farbe der Zone für die Darstellung in der Anwendung und ob aus dieser Zone ein Alarm ausgelöst werden kann**. Änderungen an bestehenden Zonen ermöglichen die Anpassung dieser Attribute, um Berechtigungen oder Darstellungen innerhalb der Anwendung zu aktualisieren.

Abbildung 42 : Zone Bearbeiten

Löschen von Zonen

Beim Löschen einer Zone wird automatisch das zugehörige **Terminal entfernt**. Zudem werden alle eingebuchten Personen aus dieser Zone **automatisch ausgebucht** und müssen einer neuen Zone zugewiesen werden. Diese Personen erscheinen in der Übersicht mit dem Status „**Keine Buchungshistorie**“, bis sie erneut eingebucht wurden.

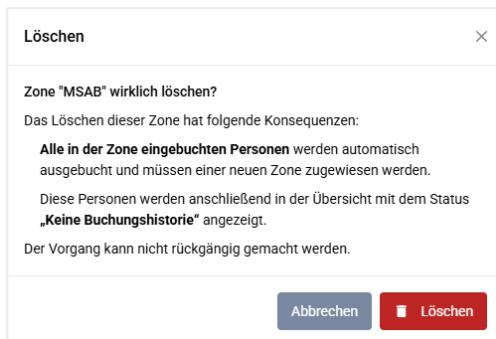
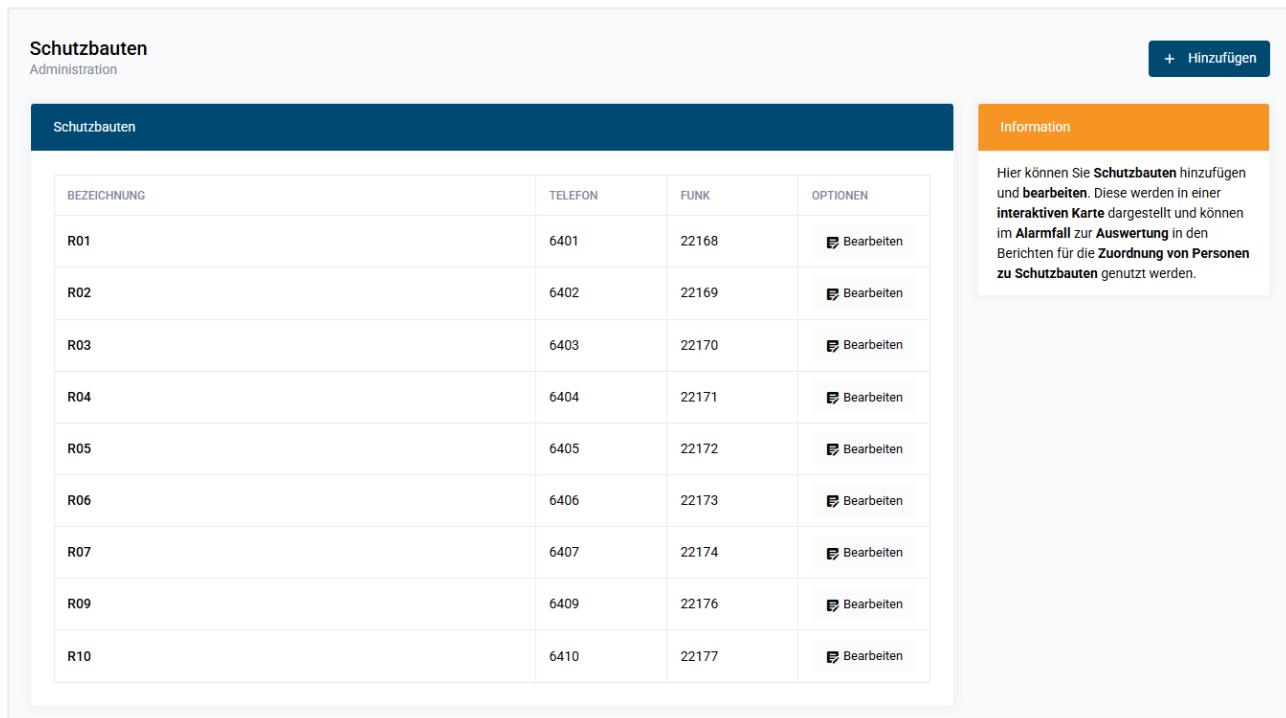


Abbildung 43 : Zone Löschen

Schutzbauten

Die **Schutzbautenverwaltung** ermöglicht Administratoren das **Einsehen, Bearbeiten, Hinzufügen und Löschen** von Schutzbauten. Alle eingetragenen Schutzbauten werden in einer **interaktiven Karte** dargestellt und können im **Alarmfall für Berichte und die Zuordnung von Personen zu Schutzbauten** genutzt werden.



The screenshot shows a user interface for managing structures. At the top, there's a header bar with the title "Schutzbauten" and a sub-header "Administration". On the right of the header is a blue button labeled "+ Hinzufügen". Below the header is a dark blue navigation bar with the text "Schutzbauten". The main content area contains a table with 10 rows, each representing a structure (R01 to R10). The columns are labeled "BEZEICHNUNG", "TELEFON", "FUNK", and "OPTIONEN". The "OPTIONEN" column contains a "Bearbeiten" button for each row. To the right of the table is an orange "Information" box containing text about adding and editing structures, their representation on an interactive map, and their use in reports and personnel assignments during an emergency.

BEZEICHNUNG	TELEFON	FUNK	OPTIONEN
R01	6401	22168	 Bearbeiten
R02	6402	22169	 Bearbeiten
R03	6403	22170	 Bearbeiten
R04	6404	22171	 Bearbeiten
R05	6405	22172	 Bearbeiten
R06	6406	22173	 Bearbeiten
R07	6407	22174	 Bearbeiten
R09	6409	22176	 Bearbeiten
R10	6410	22177	 Bearbeiten

Abbildung 44 : Schutzbautenverwaltung

Hinzufügen und Bearbeiten von Schutzbauten

Beim **Erstellen oder Bearbeiten eines Schutzbau** können verschiedene Informationen hinterlegt oder aktualisiert werden. Dazu gehören die **Bezeichnung des Schutzbau**, die **Rufnummer und die Funknummer**. Zusätzlich besteht die Möglichkeit, die **Position direkt auf der interaktiven Karte** festzulegen oder zu ändern, indem der Standort angeklickt wird. Dies gewährleistet eine genaue Visualisierung innerhalb der Anwendung.

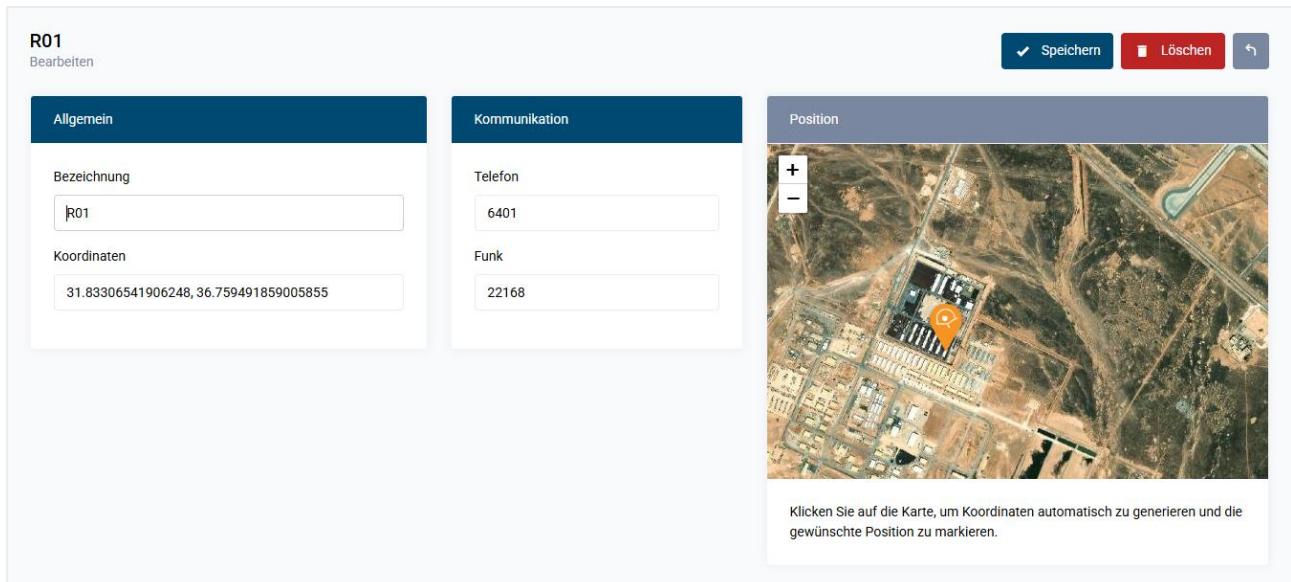


Abbildung 45 : Schutzbau Bearbeiten

Löschen von Schutzbauten

Das **Löschen eines Schutzbau** entfernt diesen vollständig aus der Anwendung. Nach dem Löschen wird der Schutzbau **nicht mehr in der interaktiven Karte angezeigt** und kann auch **nicht mehr für Auswertungen in Berichten genutzt** werden.



Abbildung 46 : Löschen eines Schutzbau

Backup

Administratoren können über die Administrationsoberfläche ein **vollständiges Backup der Anwendung** erstellen und exportieren. Das Backup umfasst die gesamte **Datenbank sowie alle hochgeladenen Dateien** und wird als **ZIP-Datei** gespeichert. Nach Abschluss des Backup-Prozesses wird die Datei **automatisch heruntergeladen** und steht zur **externen Sicherung** bereit. Dieses Backup kann zur **Wiederherstellung bei der Neuinstallation der Anwendung** genutzt werden.

Backup
Administration

Hier haben Sie die Möglichkeit, ein vollständiges Backup aller relevanten Daten des Systems herunterzuladen. Dieses Backup umfasst:

Datenbank:
Eine vollständige Sicherung der Sonic Camp Guard-Datenbank. Diese enthält sämtliche wichtige Informationen und Systemdaten, die zur Verwaltung und Überwachung des Camps benötigt werden. Die Datenbank wird als **.sql**-Datei exportiert, um eine einfache Wiederherstellung zu gewährleisten.

Uploads:
Der komplette Inhalt des **/uploads/** Ordners, der alle hochgeladenen Dateien, wie Berichte, Bilder und andere Dokumente, enthält, die während des Betriebs des Systems gespeichert wurden.

Herunterladen

Hinweise

- Das Backup wird als ZIP-Datei bereitgestellt, die sowohl die Datenbank- als auch die hochgeladenen Dateien enthält.
- Nach dem Klicken auf den "Herunterladen"-Button wird die ZIP-Datei generiert und automatisch auf Ihr Gerät heruntergeladen.
- Sicherheitstipp:** Bewahren Sie diese Datei sicher auf, da sie wichtige Daten enthält. Laden Sie die Datei nur auf sichere Speicherorte herunter.

Abbildung 47 : Backup Herunterladen

Wiederherstellen eines Backups

Bei einer Neuinstallation kann eine zuvor erstellte Backup-Datei direkt während der Einrichtung ausgewählt und **automatisch wiederhergestellt** werden. Dadurch werden die **Datenbank und alle hochgeladenen Dateien** vollständig in das System eingespielt, sodass die Anwendung ohne Datenverlust weiter genutzt werden kann.

Wiederherstellung

Die Wiederherstellung wird nur ausgeführt, wenn eine gültige Backupdatei ausgewählt wurde.

Datei

Datei auswählen Keine ausgewählt

Abbildung 48 : Wiederherstellungsmaske

Fehlersuche und Support

Häufige Probleme und Lösungen

Derzeit sind keine bekannten Fehler oder Probleme in der Anwendung vorhanden. Sollte es dennoch zu unerwarteten Schwierigkeiten kommen, wird empfohlen, sich zunächst an den UserHelpDesk zu wenden. Dieser bietet Unterstützung bei allgemeinen Anwendungsfragen und kann auftretende Probleme analysieren.

Für systemkritische Fehler oder nicht selbstständig lösbarer Probleme informiert der UserHelpDesk die Administratoren, die weiterführende Maßnahmen zur Fehlerbehebung einleiten können.

Kontakt zum Support

Für allgemeine Fragen zur Nutzung der Anwendung oder zur Verwaltung von Inhalten wie Zonen, Schutzbauten oder Nutzerberechtigungen ist der UserHelpDesk zuständig.

ANSPRECHPARTNER	UserHelpDesk
APPARAT	44444

Die Administratoren des Gefechtsstandes sind verantwortlich für den technischen Betrieb der Webanwendung und der dahinterliegenden Server.

ANSPRECHPARTNER	Administratoren
APPARAT	6051 / 6052

Falls Softwarefehler auftreten oder die Administratoren ein Problem nicht eigenständig beheben können, kann der Entwickler im Inland kontaktiert werden.

ANSPRECHPARTNER	OFw Cedric Prietz
E-MAIL	CedricPrietz@Bundeswehr.org
APPARAT	90 8303 54618

Anhänge

Glossar

Es werden keine Bezeichnungen verwendet, die nicht durch den normalen Nutzer der Anwendung zu verstehen sind. Fachbegriffe und technische Ausdrücke werden, sofern notwendig, innerhalb der Anwendung oder im zugehörigen Betriebshandbuch erläutert, um eine klare und verständliche Nutzung zu gewährleisten.

Betriebshandbuch

Das Betriebshandbuch steht als eigenständiges Dokument zur Verfügung, in dem weiterführende Informationen zur Installation und Konfiguration der Anwendung beschrieben sind. Zudem enthält es Angaben zu den technischen Voraussetzungen der Serverarchitektur sowie zur rechtlichen Lage der Anwendung innerhalb der Bundeswehr.

Das Betriebshandbuch dient als zentrale Referenz für Informationssicherheitsbeauftragte und Administratoren, um eine ordnungsgemäße Einrichtung, Wartung und Nutzung der Anwendung sicherzustellen.

Versionshistorie

Die Versionshistorie dokumentiert die veröffentlichten Versionen der Anwendung.

VERSION	DATUM	HINWEISE
1.0	14.09.2024	Erste Nutzung der Anwendung nach Entwicklung
1.1	03.11.2024	Einführung neuer Funktionen
1.2	05.02.2025	Erweiterung um neue Funktionen und Erstellung eines Nutzerhandbuchs