

Sicherheitseinstellungen der STARFACE konfigurieren

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Sicherheit"	Reiter "Einstellungen"
	 Admin	 Sicherheit	Einstellungen

Einstellungen

Filter

Richtlinien für SIP-Passwörter

Passwortstärke:

Sicher

Mindestens 16 Zeichen mit wenigstens 3 × a-z, 2 × A-Z und 2 × 0-9. Keine Sonderzeichen erlaubt.

☐ Manuelle Vergabe schwacher Passwörter erlauben

Richtlinien für Benutzer-Passwörter

Passwortstärke:

Sicher

Mindestens 8 Zeichen mit wenigstens 2 × a-z, 2 × A-Z, 2 × 0-9 und 2 × .!@#\$%^&*?_~

☒ Manuelle Vergabe schwacher Passwörter erlauben

Passwortüberprüfung

☒ Passwörter regelmäßig überprüfen

Überprüfungsintervall:

Täglich

Passwortupdate

☒ Unsichere SIP-Passwörter automatisch ändern

Telefon-Administrator-Passwörter

☒ Telefon-Administrator-Passwörter regelmäßig überprüfen

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Berechtigungen:


Alle

Richtlinien für SIP-Passwörter

In diesem Abschnitt wird, via Drop-Down-Menü, die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Telefonkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

Paranoid	Sicher
Mindestens 30 Zeichen	Mindestens 16 Zeichen
5x a bis z	3x a bis z
5x A bis Z	2x A bis Z
5x 0 bis 9	2x 0 bis 9
Keine Sonderzeichen erlaubt	Keine Sonderzeichen erlaubt

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.

**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Telefonkonten.

Richtlinien für Benutzer-Passwörter

In diesem Abschnitt wird via Drop-Down-Menü die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Benutzerkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

Paranoid	Sicher
Mindestens 16 Zeichen	Mindestens 8 Zeichen
4x a bis z	2x a bis z
4x A bis Z	2x A bis Z
4x 0 bis 9	2x 0 bis 9
4x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~	2x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.


**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Benutzerkonten.

Passwortüberprüfung

Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert erfolgt eine Prüfung aller SIP-Passwörter direkt nach dem Speichern der Einstellung und danach immer im darunter eingestellten Zeitabstand. Falls bei der Prüfung ein oder mehrere nicht der Sicherheitsrichtlinie entsprechende Passwörter erkannt werden, erhalten die Administratoren und berechnigte Benutzer eine E-Mail mit einer Liste der betroffenen Telefonkonten.

Passwortupdate

Unsichere Passwörter automatisch ändern: Diese Checkbox betrifft Telefonkonten mit bestehenden Zugangsdaten, die sich mit einer Autoprovisionierungsanfrage an der Anlage melden. Ist diese Option aktiviert und entspricht das Passwort des Telefonskontos nicht der Sicherheitsrichtlinie, vergibt die STARFACE bei der nächsten Anfrage des Telefons automatisch ein neues sicheres Passwort.

**Hinweis:** Diese Einstellung arbeitet unabhängig von der (evtl. erlaubten) manuellen Vergabe schwächerer Passwörter und der regelmäßigen Passwortüberprüfung.

Telefon-Administrator-Passwörter


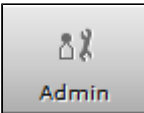

Telefon-Administrator-Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert, wird geprüft ob die Standardpasswörter für den Zugriff auf die Weboberfläche der Telefone geändert worden sind. Ist dies nicht der Fall, werden die Administratoren per E-Mail informiert.

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Benutzerrechte: Über dieses Drop-Down-Menü, wird gesteuert wie umfassend oder eingeschränkt der Pickup auf der STARFACE von Benutzer mit dem Recht "Anzeige und Pickup Anrufer" ist. Dabei stehen die folgenden Auswahlmöglichkeiten zur Verfügung:

Bezeichnung	Beschreibung
Alle	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Benutzern auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
Gruppe	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Mitgliedern innerhalb der gleichen Gruppe(n) auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch bei anderen Gruppenmitgliedern die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.

Niemand	Niemand kann einen Pickup für ein eingehendes Gespräch durchführen. Es wird auch nicht bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
---------	---

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Sicherheit"	Reiter "Einstellungen"
	 Admin	 Sicherheit	Einstellungen

Einstellungen
Filter

Richtlinien für SIP-Passwörter ⓘ

Passwortstärke: Sicher

Mindestens 16 Zeichen mit wenigstens 3 × **a-z**, 2 × **A-Z** und 2 × **0-9**. *Keine Sonderzeichen erlaubt.*

☐ Manuelle Vergabe schwacher Passwörter erlauben

Richtlinien für Benutzer-Passwörter

Passwortstärke: Sicher

Mindestens 8 Zeichen mit wenigstens 2 × **a-z**, 2 × **A-Z**, 2 × **0-9** und 2 × **.:!@#\$%^&*?_~**

☒ Manuelle Vergabe schwacher Passwörter erlauben

Passwortüberprüfung

☒ Passwörter regelmäßig überprüfen

Überprüfungsintervall: Täglich

Passwortupdate

☒ Unsichere SIP-Passwörter automatisch ändern

Telefon-Administrator-Passwörter

☒ Telefon-Administrator-Passwörter regelmäßig überprüfen

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Berechtigungen:


Alle

Richtlinien für SIP-Passwörter

In diesem Abschnitt wird, via Drop-Down-Menü, die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Telefonkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

- Sicher: Mindestens 16 Zeichen
3x a bis z
2x A bis Z
2x 0 bis 9
Keine Sonderzeichen erlaubt
- Paranoid: Mindestens 30 Zeichen
5x a bis z
5x A bis Z
5x 0 bis 9
Keine Sonderzeichen erlaubt

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.

**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Telefonkonten.

Richtlinien für Benutzer-Passwörter

In diesem Abschnitt wird via Drop-Down-Menü die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Benutzerkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

- Sicher:

Mindestens 8 Zeichen
2x a bis z
2x A bis Z
2x 0 bis 9
2x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~
- Paranoid:

Mindestens 16 Zeichen
4x a bis z
4x A bis Z
4x 0 bis 9
4x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.

**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Benutzerkonten.


Passwortüberprüfung

Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert erfolgt eine Prüfung aller SIP-Passwörter direkt nach dem Speichern der Einstellung und danach immer im darunter eingestellten Zeitabstand.

Falls bei der Prüfung ein oder mehrere nicht der Sicherheitsrichtlinie entsprechende Passwörter erkannt werden, erhalten die Administratoren und berechnigte Benutzer eine E-Mail mit einer Liste der betroffenen Telefonkonten.

Passwortupdate

Unsichere Passwörter automatisch ändern: Diese Checkbox betrifft Telefonkonten mit bestehenden Zugangsdaten, die sich mit einer Autoprovisionierungsanfrage an der Anlage melden. Ist diese Option aktiviert und entspricht das Passwort des Telefonskontos nicht der Sicherheitsrichtlinie, vergibt die STARFACE bei der nächsten Anfrage des Telefons automatisch ein neues sicheres Passwort.

**Hinweis:** Diese Einstellung arbeitet unabhängig von der (evtl. erlaubten) manuellen Vergabe schwächerer Passwörter und der regelmäßigen Passwortüberprüfung.

Telefon-Administrator-Passwörter


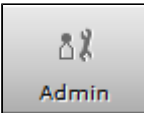

Telefon-Administrator-Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert, wird geprüft ob die Standardpasswörter für den Zugriff auf die Weboberfläche der Telefone geändert worden sind. Ist dies nicht der Fall, werden die Administratoren per E-Mail informiert.

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Benutzerrechte: Über dieses Drop-Down-Menü, wird gesteuert wie umfassend oder eingeschränkt der Pickup auf der STARFACE von Benutzer mit dem Recht "Anzeige und Pickup Anrufer" ist. Dabei stehen die folgenden Auswahlmöglichkeiten zur Verfügung:

Bezeichnung	Beschreibung
Alle	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Benutzern auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
Gruppe	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Mitgliedern innerhalb der gleichen Gruppe(n) auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch bei anderen Gruppenmitgliedern die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.

Niemand	Niemand kann einen Pickup für ein eingehendes Gespräch durchführen. Es wird auch nicht bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
---------	---

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Sicherheit"	Reiter "Einstellungen"
	 Admin	 Sicherheit	Einstellungen

Einstellungen
Filter

Richtlinien für SIP-Passwörter

Passwortstärke: Sicher

Mindestens 16 Zeichen mit wenigstens 3 × **a-z**, 2 × **A-Z** und 2 × **0-9**. Keine Sonderzeichen erlaubt.

☐ Manuelle Vergabe schwacher Passwörter erlauben

Richtlinien für Benutzer-Passwörter

Passwortstärke: Sicher

Mindestens 8 Zeichen mit wenigstens 2 × **a-z**, 2 × **A-Z**, 2 × **0-9** und 2 × **.:!@#\$%^&*?_~**

☒ Manuelle Vergabe schwacher Passwörter erlauben

Passwortüberprüfung

☒ Passwörter regelmäßig überprüfen

Überprüfungsintervall: Täglich

Passwortupdate

☒ Unsichere SIP-Passwörter automatisch ändern

Telefon-Administrator-Passwörter

☒ Telefon-Administrator-Passwörter regelmäßig überprüfen

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Berechtigungen:


Alle

Richtlinien für SIP-Passwörter

In diesem Abschnitt wird, via Drop-Down-Menü, die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Telefonkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

- Sicher: Mindestens 16 Zeichen
 3x a bis z
 2x A bis Z
 2x 0 bis 9
 Keine Sonderzeichen erlaubt
- Paranoid: Mindestens 30 Zeichen
 5x a bis z
 5x A bis Z
 5x 0 bis 9
 Keine Sonderzeichen erlaubt

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.

**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Telefonkonten.

Richtlinien für Benutzer-Passwörter


In diesem Abschnitt wird via Drop-Down-Menü die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Benutzerkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts sind:

- Sicher:

Mindestens 8 Zeichen
2x a bis z
2x A bis Z
2x 0 bis 9
2x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~
- Paranoid:

Mindestens 16 Zeichen
4x a bis z
4x A bis Z
4x 0 bis 9
4x Sonderzeichen : . ! @ # \$ % ^ & * ? _ ~

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.

**Hinweis:** Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Benutzerkonten.


Passwortüberprüfung

Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert erfolgt eine Prüfung aller SIP-Passwörter direkt nach dem Speichern der Einstellung und danach immer im darunter eingestellten Zeitabstand.

Falls bei der Prüfung ein oder mehrere nicht der Sicherheitsrichtlinie entsprechende Passwörter erkannt werden, erhalten die Administratoren und berechnigte Benutzer eine E-Mail mit einer Liste der betroffenen Telefonkonten.

Passwortupdate

Unsichere Passwörter automatisch ändern: Diese Checkbox betrifft Telefonkonten mit bestehenden Zugangsdaten, die sich mit einer Autoprovisionierungsanfrage an der Anlage melden. Ist diese Option aktiviert und entspricht das Passwort des Telefonskontos nicht der Sicherheitsrichtlinie, vergibt die STARFACE bei der nächsten Anfrage des Telefons automatisch ein neues sicheres Passwort.

**Hinweis:** Diese Einstellung arbeitet unabhängig von der (evtl. erlaubten) manuellen Vergabe schwächerer Passwörter und der regelmäßigen Passwortüberprüfung.

Telefon-Administrator-Passwörter


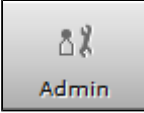

Telefon-Administrator-Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert, wird geprüft ob die Standardpasswörter für den Zugriff auf die Weboberfläche der Telefone geändert worden sind. Ist dies nicht der Fall, werden die Administratoren per E-Mail informiert.

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Benutzerrechte: Über dieses Drop-Down-Menü, wird gesteuert wie umfassend oder eingeschränkt der Pickup auf der STARFACE von Benutzer mit dem Recht "Anzeige und Pickup Anrufer" ist. Dabei stehen die folgenden Auswahlmöglichkeiten zur Verfügung:

Bezeichnung	Beschreibung
Alle	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Benutzern auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
Gruppe	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Mitgliedern innerhalb der gleichen Gruppe(n) auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch bei anderen Gruppenmitgliedern die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.

Niemand	Niemand kann einen Pickup für ein eingehendes Gespräch durchführen. Es wird auch nicht bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
---------	---

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Sicherheit"	Reiter "Einstellungen"
	 Admin	 Sicherheit	Einstellungen

Einstellungen
Filter

Richtlinien für SIP-Passwörter

Passwortstärke: Sicher

Mindestens 16 Zeichen mit wenigstens 3 × **a-z**, 2 × **A-Z** und 2 × **0-9**. Keine Sonderzeichen erlaubt.

☐ Manuelle Vergabe schwacher Passwörter erlauben

Richtlinien für Benutzer-Passwörter

Passwortstärke: Sicher

Mindestens 8 Zeichen mit wenigstens 2 × **a-z**, 2 × **A-Z**, 2 × **0-9** und 2 × **.:!@#\$%^&*?_~**

☒ Manuelle Vergabe schwacher Passwörter erlauben

Passwortüberprüfung

☒ Passwörter regelmäßig überprüfen

Überprüfungsintervall: Täglich

Passwortupdate

☒ Unsichere SIP-Passwörter automatisch ändern

Telefon-Administrator-Passwörter

☒ Telefon-Administrator-Passwörter regelmäßig überprüfen

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Berechtigungen:

Alle

Richtlinien für SIP-Passwörter

In diesem Abschnitt wird via Drop-Down-Menü die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Telefonkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts werden direkt unter dem Drop-Down-Menü angezeigt.

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.



Hinweis: Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Telefonkonten.

Richtlinien für Benutzer-Passwörter

In diesem Abschnitt wird via Drop-Down-Menü die minimal erforderliche Passwortstärke für die Komplexität der Passwörter der Benutzerkonten auf der STARFACE konfiguriert. Die detaillierten Anforderungen an die Komplexität des Passworts werden direkt unter dem Drop-Down-Menü angezeigt.

Manuelle Vergabe schwacher Passwörter erlauben: Diese Option erlaubt die Konfiguration von Telefonkonten mit unsicheren Passwörtern, wobei vor dem Speichern keine Warnung ausgegeben wird.



Hinweis: Es wird dringend dazu geraten keine unsicheren Passwörter zuzulassen für die Benutzerkonten.

Passwortüberprüfung

Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert erfolgt eine Prüfung aller SIP-Passwörter direkt nach dem Speichern der Einstellung und danach immer im darunter eingestellten Zeitabstand.

Falls bei der Prüfung ein oder mehrere nicht der Sicherheitsrichtlinie entsprechende Passwörter erkannt werden, erhalten die Administratoren und berechnete Benutzer eine E-Mail mit einer Liste der betroffenen Telefonkonten.

Passwortupdate

Unsichere Passwörter automatisch ändern: Diese Checkbox betrifft Telefonkonten mit bestehenden Zugangsdaten, die sich mit einer Autoprovisionierungsanfrage an der Anlage melden. Ist diese Option aktiviert und entspricht das Passwort des Telefonkontos nicht der Sicherheitsrichtlinie, vergibt die STARFACE bei der nächsten Anfrage des Telefons automatisch ein neues sicheres Passwort.



Hinweis: Diese Einstellung arbeitet unabhängig von der (evtl. erlaubten) manuellen Vergabe schwächerer Passwörter und der regelmäßigen Passwortüberprüfung.

Telefon-Administrator-Passwörter

Telefon-Administrator-Passwörter regelmäßig überprüfen: Ist diese Checkbox aktiviert, wird geprüft ob die Standardpasswörter für den Zugriff auf die Weboberfläche der Telefone geändert worden sind. Ist dies nicht der Fall, werden die Administratoren per E-Mail informiert.

Globale Privatsphäreneinstellungen für Telefonie

Gruppen-Pickup und Sichtbarkeit von Anruferdaten bei Vergabe passender Benutzerrechte: Über dieses Drop-Down-Menü, wird gesteuert wie umfassend oder eingeschränkt der Pickup auf der STARFACE von Benutzer mit dem Recht "Anzeige und Pickup Anrufer" ist. Dabei stehen die folgenden Auswahlmöglichkeiten zur Verfügung:

Bezeichnung	Beschreibung
Alle	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Benutzern auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
Gruppe	Alle Benutzer mit dem Recht "Anzeige und Pickup Anrufer " können bei allen anderen Mitgliedern innerhalb der gleichen Gruppe(n) auf der STARFACE einen Pickup eines eingehenden Gesprächs durchführen. Zusätzlich wird bei einem klingelnden Gespräch bei anderen Gruppenmitgliedern die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.
Niemand	Niemand kann einen Pickup für ein eingehendes Gespräch durchführen. Es wird auch nicht bei einem klingelnden Gespräch die Rufnummer des Anrufers auf der BLF des Angerufenen angezeigt.

Die Dokumentation für die abgekündigten Versionen der STARFACE finden sich in unserem Archiv:

[Link zum Archiv](#)