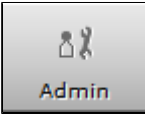


Sicherheitseinstellungen für die Telefone auf der STARFACE

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

In diesem Reiter können die erweiterten Telefoneinstellungen auf der STARFACE vorgenommen werden. Dabei handelt es sich um die Zugangsdaten für die Weboberfläche und die geschützten Menüs der jeweiligen Telefone. Auch die Verschlüsselung für bestimmte Telefonmodelle kann in diesem Reiter aktiviert werden.

Allgemeine Telefonsicherheit	
Neue SIP-Passwörter für alle Telefone generieren: Passwörter übertragen	
Authentifizierung für Telefonmenüs: ☒	
Herstellerspezifische Einstellungen	
	Fanvil
	Gigaset Pro
	Grandstream
	Panasonic
	Snom
	Yealink

Neue SIP-Passwörter für alle Telefone generieren: Ist die Autoprovisionierung aktiviert (siehe [Allgemeine Telefoneinstellungen auf der STARFACE konfigurieren](#)) kann über die Schaltfläche "Passwörter übertragen" die gleichzeitige Änderung der Passwörter für alle SIP-Account (Registrierung des Telefons an der STARFACE) ausgelöst werden. Sind sehr viele Telefone vorhanden wird der Verteilvorgang automatisch gestaffelt durchgeführt.

Diese Option kann z.B. verwendet werden, wenn befürchtet wird das ein oder mehrere SIP-Accounts kompromittiert worden sind.

Authentifizierung für Telefonmenüs: Ab Werk ist der Zugriff auf die Telefonmenüs der STARFACE Benutzer durch einen Sicherheitsmechanismus geschützt. Dies führt jedoch dazu, dass das Telefonmenü auf einigen Telefonmodellen nicht verwendet werden kann, da diese den Zugriffsschutz nicht unterstützen. Um das Telefonmenü auf solchen Telefonen dennoch zu verwenden, kann hier via Checkbox die Authentifizierung global für alle Telefonmodelle deaktivieren werden.



Hinweis: Das Deaktivieren der Authentifizierung für Telefonmenüs stellt, insbesondere bei STARFACE, die direkt über das Internet erreichbar sind, ein erhebliches Sicherheitsrisiko dar.

Für die folgenden 3 Hersteller kann in den herstellerspezifischen Einstellungen die Verschlüsselung aktiviert werden:

- Gigaset
- SNOM
- Yealink

Die Verschlüsselung ist in den Voreinstellungen deaktiviert und muss manuell aktiviert werden.



Hinweis: Es muss sichergestellt werden das die STARFACE über ein valides TLS Zertifikat verfügt, da ansonsten einige verschlüsselte Dienstmerkmale möglicherweise nicht korrekt funktionieren. Für STARFACE Cloudinstanzen ist standardmäßig ein valides TLS Zertifikat hinterlegt.

Die Verschlüsselung umfasst die folgenden Punkte:

- Autoprovisionierung der Endgeräte (HTTPS)
- Telefonmenüs der Endgeräte (HTTPS)
- Telefonie zwischen den Endgeräten und der STARFACE (TLS + SRTP)

Die folgenden Listen führen alle Telefonmodelle des jeweiligen Herstellers auf die eine Verschlüsselung unterstützen:

Hersteller	Modell
Gigaset	N670
Gigaset	N870
Hersteller	Modell
SNOM	710
SNOM	720
SNOM	760
SNOM	D120
SNOM	D305
SNOM	D315
SNOM	D345
SNOM	D375
SNOM	D385
SNOM	D710
SNOM	D712
SNOM	D715
SNOM	D717
SNOM	D725
SNOM	D735
SNOM	D745
SNOM	D765
SNOM	D785
SNOM	D862
SNOM	D865
SNOM	m900
Hersteller	Modell
Yealink	T19
Yealink	T31
Yealink	T41S
Yealink	T42S
Yealink	T46S
Yealink	T46u
Yealink	T48s
Yealink	T53
Yealink	T54
Yealink	T56

Yealink	T57
Yealink	T58
Yealink	T58w
Yealink	VP59
Yealink	CP920
Yealink	CP925
Yealink	CP960
Yealink	CP965

Die Verschlüsselung zwischen den STARFACE Desktop Apps und der Telefonanlage wird unterstützt und ist immer aktiv. Auch die Kommunikation zwischen den STARFACE Mobile Apps und der Telefonanlage ist immer verschlüsselt.

Herstellerspezifische Einstellungen: Hier können zentral die Passwörter für den Administrationsmodus und, falls vorhanden, den Benutzermodus der verschiedenen von der STARFACE unterstützten Telefonmodelle gepflegt werden. Die hinterlegten Passwörter entsprechen nach der Grundinstallation den Standardpasswörtern der jeweiligen Hersteller und sollten aus Sicherheitsgründen geändert werden.

Ändert man die Passwörter für den Zugriff auf die Weboberfläche der Telefone, wird beim Speichern die Provisionierung der Passwörter für alle an der Anlage konfigurierten Endgeräte des jeweiligen Herstellers einmalig ermöglicht. Die Endgeräte werden automatisch benachrichtigt und holen sich, sobald es kein aktives Gespräch gibt, die neue Konfiguration von der STARFACE.



Hinweis: Bitte beachten Sie zur Nutzung des Administrations- und Benutzermodus auf den Telefonen die jeweilige Dokumentation des Herstellers.

Digest-Authentifizierung: Durch diese auswählbare Sonderoption bei den Snom-Endgeräten werden die Zugangsdaten nicht im Klartext, sondern verschlüsselt an das Telefon übermittelt.

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

In diesem Reiter können die erweiterten Telefoneinstellungen auf der STARFACE vorgenommen werden. Dabei handelt es sich um die Zugangsdaten für die Weboberfläche und die geschützten Menüs der jeweiligen Telefone. Auch die Verschlüsselung für bestimmte Telefonmodelle kann in diesem Reiter aktiviert werden.

Allgemeine Telefonsicherheit	
Neue SIP-Passwörter für alle Telefone generieren:	<button>Passwörter übertragen</button>
Authentifizierung für Telefonmenüs: ☒	
Herstellerspezifische Einstellungen	
	Fanvil
	Gigaset Pro
	Grandstream
	Panasonic
	Snom
	Yealink

Neue SIP-Passwörter für alle Telefone generieren: Ist die Autoprovisionierung aktiviert (siehe [Allgemeine Telefoneinstellungen auf der STARFACE konfigurieren](#)) kann über die Schaltfläche "Passwörter übertragen" die gleichzeitige Änderung der Passwörter für alle SIP-Account (Registrierung des Telefons an der STARFACE) ausgelöst werden. Sind sehr viele Telefone vorhanden wird der Verteilvorgang automatisch gestaffelt durchgeführt.

Diese Option kann z.B. verwendet werden, wenn befürchtet wird das ein oder mehrere SIP-Accounts kompromittiert worden sind.

Authentifizierung für Telefonmenüs: Ab Werk ist der Zugriff auf die Telefonmenüs der STARFACE Benutzer durch einen Sicherheitsmechanismus geschützt. Dies führt jedoch dazu, dass das Telefonmenü auf einigen Telefonmodellen nicht verwendet werden kann, da diese den Zugriffsschutz nicht unterstützen. Um das Telefonmenü auf solchen Telefonen dennoch zu verwenden, kann hier via Checkbox die Authentifizierung global für alle Telefonmodelle deaktivieren werden.



Hinweis: Das Deaktivieren der Authentifizierung für Telefonmenüs stellt, insbesondere bei STARFACE, die direkt über das Internet erreichbar sind, ein erhebliches Sicherheitsrisiko dar.

Für die folgenden 3 Hersteller kann in den herstellerspezifischen Einstellungen die Verschlüsselung aktiviert werden:

- Gigaset
- SNOM
- Yealink

Die Verschlüsselung ist in den Voreinstellungen deaktiviert und muss manuell aktiviert werden.



Hinweis: Es muss sichergestellt werden das die STARFACE über ein valides TLS Zertifikat verfügt, da ansonsten einige verschlüsselte Dienstmerkmale möglicherweise nicht korrekt funktionieren. Für STARFACE Cloudinstanzen ist standardmäßig ein valides TLS Zertifikat hinterlegt.

Die Verschlüsselung umfasst die folgenden Punkte:

- Autoprovisionierung der Endgeräte (HTTPS)
- Telefonmenüs der Endgeräte (HTTPS)
- Telefonie zwischen den Endgeräten und der STARFACE (TLS + SRTP)

Die folgenden Listen führen alle Telefonmodelle des jeweiligen Herstellers auf die eine Verschlüsselung unterstützen:

Hersteller	Modell
Gigaset	N670
Gigaset	N870
Hersteller	Modell
SNOM	710
SNOM	720
SNOM	760
SNOM	D120
SNOM	D305
SNOM	D315
SNOM	D345
SNOM	D375
SNOM	D385
SNOM	D710
SNOM	D712
SNOM	D715
SNOM	D717
SNOM	D725
SNOM	D735
SNOM	D745

SNOM	D765
SNOM	D785
SNOM	m900
Hersteller	Modell
Yealink	T19
Yealink	T31
Yealink	T41S
Yealink	T42S
Yealink	T46S
Yealink	T46u
Yealink	T48s
Yealink	T53
Yealink	T54
Yealink	T56
Yealink	T57
Yealink	T58
Yealink	T58w
Yealink	VP59
Yealink	CP920
Yealink	CP925
Yealink	CP960
Yealink	CP965

Die Verschlüsselung zwischen den STARFACE Desktop Apps und der Telefonanlage wird unterstützt und ist immer aktiv. Auch die Kommunikation zwischen den STARFACE Mobile Apps und der Telefonanlage ist immer verschlüsselt.

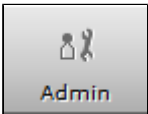
Herstellerspezifische Einstellungen: Hier können zentral die Passwörter für den Administrationsmodus und, falls vorhanden, den Benutzermodus der verschiedenen von der STARFACE unterstützten Telefonmodelle gepflegt werden. Die hinterlegten Passwörter entsprechen nach der Grundinstallation den Standardpasswörtern der jeweiligen Hersteller und sollten aus Sicherheitsgründen geändert werden.

Ändert man die Passwörter für den Zugriff auf die Weboberfläche der Telefone, wird beim Speichern die Provisionierung der Passwörter für alle an der Anlage konfigurierten Endgeräte des jeweiligen Herstellers einmalig ermöglicht. Die Endgeräte werden automatisch benachrichtigt und holen sich, sobald es kein aktives Gespräch gibt, die neue Konfiguration von der STARFACE.



Hinweis: Bitte beachten Sie zur Nutzung des Administrations- und Benutzermodus auf den Telefonen die jeweilige Dokumentation des Herstellers.

Digest-Authentifizierung: Durch diese auswählbare Sonderoption bei den Snom-Endgeräten werden die Zugangsdaten nicht im Klartext, sondern verschlüsselt an das Telefon übermittelt.

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

In diesem Reiter können die erweiterten Telefoneinstellungen auf der STARFACE vorgenommen werden. Dabei handelt es sich um die Zugangsdaten für die Weboberfläche und die geschützten Menüs der jeweiligen Telefone.

Allgemeine Telefonsicherheit	
Neue SIP-Passwörter für alle Telefone generieren: Passwörter übertragen	
Authentifizierung für Telefonmenüs: ☒ Verschlüsselung zu unterstützten Telefonen aktivieren: ☐	
Herstellerspezifische Einstellungen	
▶	Fanvil
▶	Gigaset Pro
▶	Grandstream
▶	Panasonic
▶	Snom
▶	Yealink

Neue SIP-Passwörter für alle Telefone generieren: Ist die Autoprovisionierung aktiviert (siehe [Allgemeine Telefoneinstellungen auf der STARFACE konfigurieren](#)) kann über die Schaltfläche "Passwörter übertragen" die gleichzeitige Änderung der Passwörter für alle SIP-Account (Registrierung des Telefons an der STARFACE) ausgelöst werden. Sind sehr viele Telefone vorhanden wird der Verteilvorgang automatisch gestaffelt durchgeführt.

Diese Option kann z.B. verwendet werden, wenn befürchtet wird das ein oder mehrere SIP-Accounts kompromittiert worden sind.

Authentifizierung für Telefonmenüs: Ab Werk ist der Zugriff auf die Telefonmenüs der STARFACE Benutzer durch einen Sicherheitsmechanismus geschützt. Dies führt jedoch dazu, dass das Telefonmenü auf einigen Telefonmodellen nicht verwendet werden kann, da diese den Zugriffsschutz nicht unterstützen. Um das Telefonmenü auf solchen Telefonen dennoch zu verwenden, kann hier via Checkbox die Authentifizierung global für alle Telefonmodelle deaktivieren werden.



Hinweis: Das Deaktivieren der Authentifizierung für Telefonmenüs stellt, insbesondere bei Telefonen, die direkt über das Internet erreichbar sind, ein erhebliches Sicherheitsrisiko dar.

Verschlüsselung zu unterstützten Telefonen aktivieren: Ist diese Checkbox aktiviert, werden die Telefongespräche zwischen der Telefonanlage und den Telefonen, die diese Option unterstützen, via SRTP verschlüsselt. Zum aktuellen Zeitpunkt, wird die Verschlüsselung von den folgenden Modellen unterstützt:

Hersteller	Modell
Snom	D120
Snom	D305
Snom	D315
Snom	D345
Snom	D375
Snom	D385
Snom	D712
Snom	D715
Snom	D717
Snom	D735
Snom	D745
Snom	D765
Snom	D785

Die Verschlüsselung zwischen den STARFACE Desktop Apps und der Telefonanlage wird unterstützt und ist immer aktiv. Auch die Kommunikation zwischen den STARFACE Mobile Apps und der Telefonanlage ist immer verschlüsselt.

Herstellerspezifische Einstellungen: Hier können zentral die Passwörter für den Administrationsmodus und, falls vorhanden, den Benutzermodus der verschiedenen von der STARFACE unterstützten Telefonmodelle gepflegt werden. Die hinterlegten Passwörter entsprechen nach der Grundinstallation den Standardpasswörtern der jeweiligen Hersteller und sollten aus Sicherheitsgründen geändert werden.

Ändert man die Passwörter für den Zugriff auf die Weboberfläche der Telefone, wird beim Speichern die Provisionierung der Passwörter für alle an der Anlage konfigurierten Endgeräte des jeweiligen Herstellers einmalig ermöglicht. Die Endgeräte werden automatisch benachrichtigt und holen sich, sobald es kein aktives Gespräch gibt, die neue Konfiguration von der STARFACE.



Hinweis: Bitte beachten Sie zur Nutzung des Administrations- und Benutzermodus auf den Telefonen die jeweilige Dokumentation des Herstellers.

Digest-Authentifizierung: Durch diese auswählbare Sonderoption bei den Snom-Endgeräten werden die Zugangsdaten nicht im Klartext, sondern verschlüsselt an das Telefon übermittelt.

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

In diesem Reiter können die erweiterten Telefoneinstellungen auf der STARFACE vorgenommen werden. Dabei handelt es sich um die Zugangsdaten für die Weboberfläche und die geschützten Menüs der jeweiligen Telefone.

Allgemeine Telefonsicherheit	
Neue SIP-Passwörter für alle Telefone generieren:	Passwörter übertragen
Authentifizierung für Telefonmenüs: ☒	Verschlüsselung zu unterstützten Telefonen aktivieren: ☐
Herstellerspezifische Einstellungen	
▶	Aastra
▶	Alcatel
▶	Fanvil
▶	Gigaset Pro
▶	Grandstream
▶	Openstage
▶	Panasonic
▶	Patton
▶	Polycom
▶	Snom
▶	Tiptel
▼	Yealink

Neue SIP-Passwörter für alle Telefone generieren: Ist die Autoprovisionierung aktiviert (siehe [Allgemeine Telefoneinstellungen auf der STARFACE konfigurieren](#)) kann über die Schaltfläche "Passwörter übertragen" die gleichzeitige Änderung der Passwörter für alle SIP-Account (Registrierung des Telefons an der STARFACE) ausgelöst werden. Sind sehr viele Telefone vorhanden wird der Verteilvorgang automatisch gestaffelt durchgeführt.

Diese Option kann z.B. verwendet werden, wenn befürchtet wird das ein oder mehrere SIP-Accounts kompromittiert worden sind.

Authentifizierung für Telefonmenüs: Ab Werk ist der Zugriff auf die Telefonmenüs der STARFACE Benutzer durch einen Sicherheitsmechanismus geschützt. Dies führt jedoch dazu, dass das Telefonmenü auf einigen Telefonmodellen nicht verwendet werden kann, da diese den Zugriffsschutz nicht unterstützen. Um das Telefonmenü auf solchen Telefonen dennoch zu verwenden, kann hier via Checkbox die Authentifizierung global für alle Telefonmodelle deaktivieren werden.



Hinweis: Das Deaktivieren der Authentifizierung für Telefonmenüs stellt, insbesondere bei Telefonen, die direkt über das Internet erreichbar sind, ein erhebliches Sicherheitsrisiko dar.

Verschlüsselung zu unterstützten Telefonen aktivieren: Ist diese Checkbox aktiviert, werden die Telefongespräche zwischen der Telefonanlage und den Telefonen, die diese Option unterstützen, via SRTP verschlüsselt. Zum aktuellen Zeitpunkt, wird die Verschlüsselung von den folgenden Modellen unterstützt:

Hersteller	Modell
Snom	D120
Snom	D305
Snom	D315
Snom	D345
Snom	D375
Snom	D385
Snom	D712
Snom	D715
Snom	D717
Snom	D735
Snom	D745
Snom	D765
Snom	D785

Die Verschlüsselung zwischen den STARFACE Desktop Apps und der Telefonanlage wird unterstützt und ist immer aktiv. Auch die Kommunikation zwischen den STARFACE Mobile Apps und der Telefonanlage ist immer verschlüsselt.

Herstellerspezifische Einstellungen: Hier können zentral die Passwörter für den Administrationsmodus und, falls vorhanden, den Benutzermodus der verschiedenen von der STARFACE unterstützten Telefonmodelle gepflegt werden. Die hinterlegten Passwörter entsprechen nach der Grundinstallation den Standardpasswörtern der jeweiligen Hersteller und sollten aus Sicherheitsgründen geändert werden.

Ändert man die Passwörter für den Zugriff auf die Weboberfläche der Telefone, wird beim Speichern die Provisionierung der Passwörter für alle an der Anlage konfigurierten Endgeräte des jeweiligen Herstellers einmalig ermöglicht. Die Endgeräte werden automatisch benachrichtigt und holen sich, sobald es kein aktives Gespräch gibt, die neue Konfiguration von der STARFACE.



Hinweis: Bitte beachten Sie zur Nutzung des Administrations- und Benutzermodus auf den Telefonen die jeweilige Dokumentation des Herstellers.

Digest-Authentifizierung: Durch diese auswählbare Sonderoption bei den Snom-Endgeräten werden die Zugangsdaten nicht im Klartext, sondern verschlüsselt an das Telefon übermittelt.

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

[Link zum Archiv](#)