

VoIP Security

Version 1.0.0 | Updated 2026-09-05 | 1 min read

Preparation / invited access

In this guide: [Before you start](#) | [Steps](#) | [Verify the result](#) | [Help and related information](#)

Keep endpoint credentials, transport protection and call-routing ownership separate.

Before you start

Use the access and features actually assigned to your account. Keep a rollback or recovery route before changing existing service settings.

Steps

1. Use unique endpoint credentials and the required TLS/SRTP settings.
2. Restrict administrative access and keep provider recovery details protected.
3. Revoke a lost endpoint through the normal authorized process.
4. Check unusual routing or charges with the account owner; never alter emergency-calling registration automatically.

Verify the result

Only intended endpoints register and the secure calling path remains intact. A configuration badge is not a substitute for a real call check.

Help and related information

Contact support, service status, and Customer Access. Never send passwords or recovery codes.