



AUTHORIZED CONTACT LIST (ACL)

(Colocation Customers Only)

Overview

To maintain the security of Customer equipment and designated colocation space, Global IP Networks utilizes an **Authorized Contact List (ACL)** to identify individuals authorized to access the Customer's environment and request services on the Customer's behalf.

The ACL is managed through the secure Customer Portal provided at the commencement of service. Because Global IP Networks relies exclusively on the information contained in the ACL when verifying identity and authorizing requests, Customers are strongly encouraged to review and audit their ACL on a regular basis (recommended monthly) to ensure all information remains accurate and up to date.

For security, accountability, and recordkeeping, Global IP Networks also encourages Customers to submit all technical support, service requests, billing inquiries, and account-related communications through the Ticket System available within the Customer Portal.

Managing the Authorized Contact List

Once the initial ACL has been established, all future additions, modifications, or removals of authorized contacts must be approved by a designated Primary Contact.

Changes submitted through the Customer Portal are applied in real time.

To add or modify an Authorized Contact:

1. Log in to the Customer Portal.
2. Navigate to Client Profile.
3. Select View Profile.

4. Under the Authorized Contacts section, select Add Contact or Edit.
-

Authorized Contact Roles

Primary Contact

A contact whose title is designated as Primary Contact is considered an administrator for the Customer account.

Primary Contacts are authorized to:

- Access the data center and Customer equipment
- Request equipment installation, removal, or relocation
- Access technical support and the Customer Ticket System
- Receive account, billing, and invoice information
- View bandwidth utilization and account reports
- Add, modify, or remove Authorized Contacts
- Manage account security settings, including Caller Passwords

Multiple Primary Contacts may be designated if desired. To assign this role, enter Primary Contact as the contact title when creating or editing a contact.

Member

Contacts whose title is anything other than Primary Contact are considered standard Authorized Contacts.

Members may be granted permission to:

- Access the data center and Customer equipment



- Request equipment installation or removal
- Submit and respond to support tickets
- Contact Technical Support by telephone

Members are not authorized to manage the Authorized Contact List unless explicitly promoted to a Primary Contact.

When creating a Member account, the Manage Contact permission within the Client Profile should remain set to No.

ACL Security Policy

To protect Customer assets, Global IP Networks will not add, modify, or remove any Authorized Contact without authorization from a Primary Contact.

Customer Verification

For security purposes, Global IP Networks provides technical support only to verified Authorized Contacts.

Verification methods include:

Support Tickets

Support requests submitted through the Ticket System are verified using the sender's registered email address.

Telephone Support

Telephone requests are verified using the Customer's designated Caller Password.

To configure or update the Caller Password:



1. Log in to the Customer Portal.
2. Navigate to Client Profile.
3. Select View Profile.
4. Under Custom Data / Phone Support, click Edit.
5. Enter or update the Caller Password.

The Caller Password may be a single word or a passphrase selected by the Customer.

Important: Certain requests that could significantly impact Customer services or infrastructure may require additional written authorization from a Primary Contact before action can be taken.

Temporary Third-Party Access

If temporary access is required for a vendor, contractor, consultant, or other third party, the Primary Contact may either:

- Submit a support ticket requesting temporary access for the individual; or
- Add the individual to the Authorized Contact List for the duration of the engagement and remove the contact once access is no longer required.

Global IP Networks recommends removing temporary contacts promptly after their work has been completed to maintain account security.