Account Users guide

Last Modified on 12/18/2025 2:21 pm EST

Account Users: Understanding User Types and Permissions

This guide explains the different types of users who can access customer accounts in Kraken, their permission levels, and how to manage account access.

What Are Account Users?

In Kraken, "account users" refers to anyone who has been granted access to view or manage a customer's energy account. This includes both internal Good Egg Energy staff and external users such as customers and authorized third parties.

Why this matters:

- Different users have different permission levels
- You need to verify user authority before sharing information
- Understanding user types helps you provide appropriate access

---

Internal Users (Good Egg Energy Staff)

1. Customer Service Agents

Who they are: Front-line agents handling customer calls, emails, and chats

Access level: Standard

What they can do:

- View customer account details
- Review billing and payment history
- Process payments
- Update contact information
- Create and update cases
- Send customer communications
- Add account notes
- Set up payment arrangements

What they cannot do:

- Issue credits over $100 (requires supervisor approval)
- Access restricted account flags
- Delete account information
- Override system rules
- Make rate changes

- Disconnect service

Badge color in Kraken: Blue

2. Supervisors

Who they are: Team leads and managers who oversee agents

Access level: Advanced

What they can do:
- Everything agents can do, plus:
- Approve credits over $100
- Override certain system restrictions
- Access detailed agent activity reports
- Reassign cases between agents
- View quality assurance scorecards
- Manage account holds and restrictions

What they cannot do:
- Make system-wide configuration changes
- Access executive-level reporting
- Modify rate structures

Badge color in Kraken: Purple

3. Billing Specialists

Who they are: Team members who handle complex billing issues and disputes

Access level: Specialized

What they can do:
- Everything agents can do, plus:
- Investigate complex billing disputes
- Perform detailed usage analysis
- Issue billing adjustments and credits
- Correct system billing errors
- Recalculate bills manually
- Generate custom billing reports

What they cannot do:
- Approve major account changes
- Access IT system settings
- Modify customer rate plans

Badge color in Kraken: Green

4. Field Service Technicians

Who they are: Technicians who perform on-site work (meter reading, installations, repairs)

Access level: Field operations

What they can do:
- View service address and appointment details
- Access customer contact information
- Update meter readings
- Complete service orders
- Upload photos and documentation
- Add field visit notes
- Update equipment information

What they cannot do:
- View payment history
- Access billing information
- Process payments
- Make account changes

Badge color in Kraken: Orange

5. Collections Specialists

Who they are: Team members who handle past due accounts and payment collections

Access level: Collections

What they can do:
- View account balance and payment history
- Set up payment arrangements
- Process disconnection orders
- Apply late fees
- Track payment commitments
- Send collection notices
- Update account status

What they cannot do:
- Issue billing credits
- Modify usage data
- Access account unrelated to collections

Badge color in Kraken: Red

6. IT Administrators

Who they are: Technical staff who manage the Kraken platform

Access level: System administrator

What they can do:
- Full system access
- Configure system settings
- Manage user accounts and permissions

- Troubleshoot technical issues
- Run system diagnostics
- Access audit logs
- Implement system updates

What they cannot do:
- Make business decisions about customer accounts
- Override business rules without authorization

Badge color in Kraken: Black

7. Executive Team

Who they are: Senior leadership and executives

Access level: Executive

What they can do:
- View all customer accounts
- Access company-wide reports and analytics
- Review high-level metrics
- Monitor system performance
- View escalated cases

What they cannot do:
- Make day-to-day account changes (not their role)
- Access individual agent passwords
- Modify core system configurations

Badge color in Kraken: Gold

External Users (Customers and Third Parties)

1. Primary Account Holder

Who they are: The person whose name is on the energy account

Access level: Account owner

What they can do:
- View all account information
- Make payments
- Update contact information
- Change billing preferences
- View and download bills
- Monitor usage data
- Update payment methods
- Add authorized users
- Request service changes

What they cannot do:

- Access information about other accounts
- Modify historical billing data
- Override disconnection procedures

How they access Kraken: Through the customer portal at goodeggenergy.com/account

2. Authorized Users

Who they are: People the primary account holder has given permission to access the account

Access level: Limited or Full (set by primary account holder)

Limited authorized users can:

- View bills
- View usage data
- View payment history

Full authorized users can:

- Everything limited users can do, plus:
- Make payments
- Update contact information
- Communicate with customer service

What they cannot do:

- Add other authorized users
- Close the account
- Remove themselves from access

How they access Kraken: Through the customer portal with their own login credentials

Important for agents: Always verify that an authorized user has permission to perform the requested action.

3. Property Managers

Who they are: Professional managers who oversee rental properties on behalf of property owners

Access level: Multi-account management

What they can do:

- Manage multiple customer accounts
- View bills for all managed properties
- Make payments on behalf of tenants
- Update contact information
- Request service starts/stops for tenant turnover
- Download bulk billing reports

What they cannot do:

- Access accounts outside their managed portfolio
- Override tenant account settings without authorization

How they access Kraken: Through a specialized property manager portal

4. Power of Attorney / Legal Representatives

Who they are: Individuals with legal authority to manage someone else's affairs

Access level: Full proxy access

What they can do:
- Everything the primary account holder can do
- Act on behalf of the customer in all matters

What they cannot do:
- Access the account without proper documentation

Required documentation:
- Notarized power of attorney document
- Government-issued ID
- Proof of relationship (if applicable)

Important for agents: POA documents must be reviewed and approved by our legal team before granting access. Never grant POA access without proper documentation on file.

5. Third-Party Service Providers

Who they are: Companies or individuals authorized to access account information for specific purposes (e.g., energy brokers, solar installers, auditors)

Access level: Limited, time-bound

What they can do:
- Access specific information needed for their service
- View usage data (if authorized)
- Request service changes on customer's behalf

What they cannot do:
- Make payments
- Change account settings
- Access information beyond their authorization

Authorization process:
- Customer must complete Third-Party Authorization Form
- Access is granted for specific time period (typically 30-90 days)
- Automatically expires unless renewed

Managing Account Users

Adding an Authorized User (Agent Process)

When a primary account holder requests to add an authorized user:

1. **Verify primary account holder identity**

    - Confirm name, account number, and security information

2. **Get authorized user information**
    - Full name
    - Email address
    - Phone number
    - Relationship to account holder

3. **Determine access level**
    - Limited (view only)
    - Full (view and make changes)

4. **Add user in Kraken**
    - Navigate to Account > User Management
    - Click "Add Authorized User"
    - Enter user details
    - Select permission level
    - Save changes

5. **Confirmation**
    - System sends invitation email to authorized user
    - User must accept invitation and create their own login
    - Document the addition in account notes

Removing an Authorized User

Who can request removal:

- Primary account holder
- The authorized user themselves
- Legal authority (with proper documentation)

Process:

1. Verify identity of person requesting removal

2. Navigate to Account > User Management
3. Select the authorized user
4. Click "Remove User"
5. Confirm action
6. Document removal in account notes

Important: System sends notification email to the removed user.

Modifying User Permissions

Only the primary account holder can change an authorized user's permission level:

1. Verify primary account holder identity
2. Navigate to Account > User Management
3. Select the authorized user
4. Update permission level
5. Save changes
6. Document change in account notes

Verifying User Authority

Before sharing information or making changes, always verify the person has authority:

For Phone Calls

Ask verification questions:

- Account number
- Service address
- Last four digits of SSN or account password
- Recent payment amount or bill amount

For authorized users:

- Name on the account
- Relationship to account holder
- Authorized user's email on file

For In-Person Visits

Require:

- Government-issued photo ID
- Recent bill or account statement

For Email Requests

Be cautious:

- Verify sender's email matches email on file
- For sensitive requests, require phone verification
- Never send full account details via email

Common Scenarios

"My spouse should have access to the account"

Response:"I can certainly help you add your spouse as an authorized user. I'll need some information from you to set that up. Your spouse will receive an email invitation and will need to create their own login to access the account."

Process: Add authorized user with full access

"I'm calling on behalf of my elderly parent"

Response:"I understand you'd like to help your parent with their account. To protect their privacy, I need to either speak directly with them to get verbal authorization, or you'll need to provide us with a power of attorney document. Would your parent be available to speak with me briefly?"

Process: Either get verbal authorization from account holder while they're present, or request POA documentation

"I manage this rental property"

Response:"Thank you for letting me know you're the property manager. For me to discuss the account with you, I'll need to verify that the account holder has added you as an authorized user or property manager. Can you provide me with your name and contact information so I can look that up?"

Process: Verify property manager is listed as authorized user before proceeding

"I need to remove my ex-spouse from my account"

Response:"I can help you remove an authorized user from your account. Let me verify your identity first, then I'll remove their access immediately."

Process: Verify identity, remove authorized user, document in notes

"The account is in my roommate's name, but I pay half the bills"

Response:"I understand you contribute to the bill payments. However, I can only discuss account details with the primary account holder or someone they've authorized. Your roommate would need to add you as an authorized user for you to have access to account information. Would you like me to explain to your roommate how to do that?"

Process: Do not provide account access without proper authorization

Security and Privacy Considerations

Why We're Strict About User Verification

Legal requirements:

- We're required by law to protect customer privacy
- We cannot share account information with unauthorized parties

Customer protection:

- Prevents identity theft
- Protects against fraudulent account changes
- Ensures only authorized parties can make changes

Company protection:

- Reduces liability
- Prevents fraud and abuse
- Maintains customer trust

Red Flags

Be alert for potential unauthorized access attempts:

Warning signs:

- Caller cannot answer verification questions
- Caller becomes hostile when asked to verify identity
- Caller pressures you to "just give them the information"
- Email address or phone number doesn't match records
- Caller knows some information but not security details
- Multiple failed verification attempts

If you suspect fraud:

1. Do not provide any account information
2. Document the attempt in account notes
3. Flag the account for supervisor review
4. Report to your supervisor immediately

User Activity Logging

All user actions in Kraken are automatically logged:

What's tracked:

- User login and logout times
- Accounts accessed
- Information viewed
- Changes made

- Payments processed
- Communications sent

Why it matters:
- Creates accountability
- Enables audit trails
- Helps investigate issues
- Protects against unauthorized access

Viewing user activity: Supervisors and authorized personnel can view user activity logs through the Kraken reporting module.

Best Practices

1. Always Verify Identity

Never skip verification steps, even if the caller seems legitimate.

2. Document Everything

Add notes whenever you add, modify, or remove authorized users.

3. Be Courteous but Firm

If someone isn't authorized, explain the policy kindly but don't make exceptions.

4. Protect Customer Privacy

Only share information with properly verified users.

5. Know Your Limits

Escalate to a supervisor if you're unsure about granting access.

6. Keep Authorization Current

Review authorized user lists periodically to ensure they're still appropriate.

7. Educate Customers

Explain to customers how authorized users work and why we need verification.

Quick Reference: User Types

User Type	Access Level	Can Process Payments	Can View Bills	Can Make Changes
Agent	Standard	Yes	Yes	Yes (within limits)
Supervisor	Advanced	Yes	Yes	Yes

User Type	Access Level	Can Process Payments	Can View Bills	Can Make Changes
Billing Specialist	Specialized	Yes	Yes	Yes (billing)
Field Technician	Field	No	No	Limited
Primary Account Holder	Owner	Yes	Yes	Yes (own account)
Authorized User (Full)	Full	Yes	Yes	Yes (limited)
Authorized User (Limited)	Limited	No	Yes	No
Property Manager	Multi-account	Yes	Yes	Yes (managed accounts)
Power of Attorney	Proxy	Yes	Yes	Yes

Remember: When in doubt about whether to grant access, verify with a supervisor. It's better to protect customer privacy than to risk an unauthorized disclosure.

Last updated: December 2024
Version: 1.0
Questions? Contact your supervisor or IT Support at ext. 3000
