LINK® System Security Overview

A Brief Overview of System Security Functionality

ENBRIDGE®

What is LINK® System Security?

LINK® System Security enables customers to establish and maintain security information related to their company.

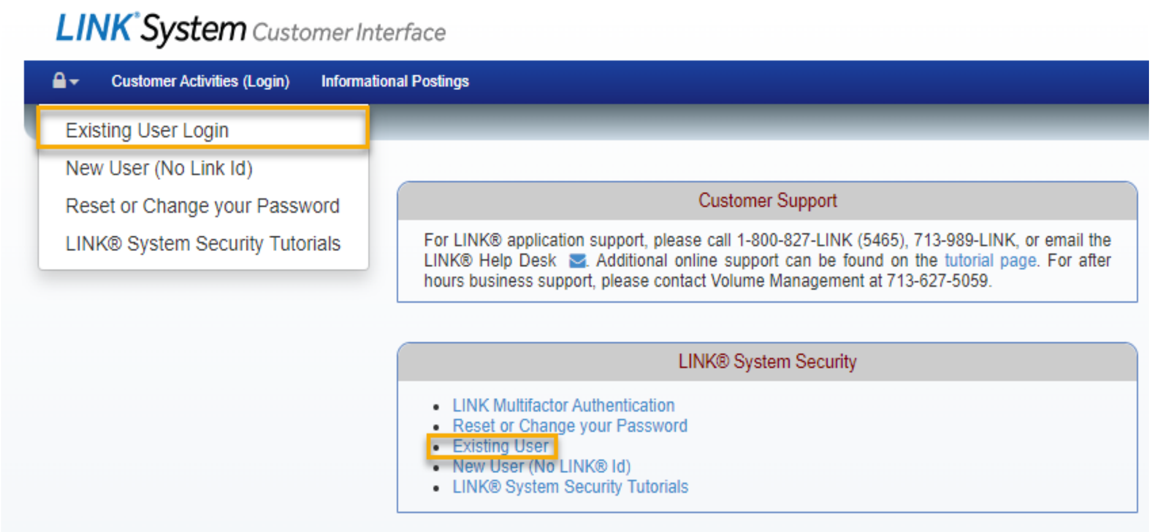
Security information includes:

- Basic company information such as entity name, business type, and DUNS number
- Addresses, Contacts and Notifications
- System Agreements
- Local Security Administrator(s)
- Users
- Agencies
- Affiliations

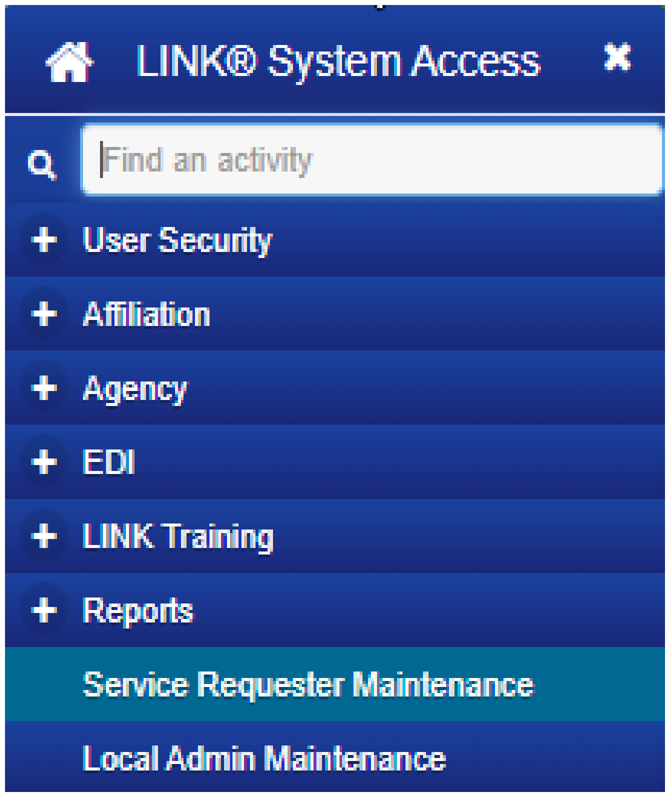
All security information is maintained and updated by Local Security Administrators (LSA)

Where is the LINK® Security Portal?

Go to https://link.enbridge.com



Under the lock icon, select “Existing User Login”



Entity Types Within LINK®

Two types of companies can be established:

- All Business Purposes
  - Business entity where users perform typical business functions such as requesting contracts, nominating, establishing PDAs, reviewing allocations or obtaining invoices.
- Upstream/Downstream
  - Business entity where it is used solely as an upstream or downstream entity for nomination purposes. No business functions are performed.

Local Security Administrators (LSAs)

- Each pipeline or storage facility tariff requires a Local Security Administrator for an “All Business Purposes” company.
  – LSAs are designated employees at a customer company that acts as an administrative authority for their employer

- The Local Security Administrator is responsible for:
  – Establishing and maintaining Service Requester contact and notification information.
  – Creating and managing user ids.
  – Creating and modifying appropriate security rights for each user id.
  – Maintaining user account information.
  – Adding and terminating user ids when a status change occurs.
  – Creating, approving, and renewing agency agreements
  – Creating affiliation agreements
  – EDI setup

- Enbridge recommends having multiple Local Security Administrators in case the primary is out of the office

LSA Security Functions

System Agreements
User IDs
Contact Maintenance
Agencies
Affiliations

System Agreements

- A LINK® System Agreement must be executed, or a valid service agreement must exist, before access is granted to Enbridge pipelines or Storage facilities.
- The agreement binds the executing company to the terms and conditions of the appropriate tariff.
- The agreement must be executed by someone authorized to bind the requesting company to such legal agreement.
- All business units on the LINK® System require system agreements prior to use
  - LINK has a grouped agreement of the top eight most commonly used business units for customer convenience.
    - BUs included: AGT, BGS, BSP, EHP, ETNG, MBHP, SGSC, TE
  - All other business units must be filed individually
- Please see the “System Agreement Execution Process” tutorial for more details

User IDs

- LINK ID
  - To access LINK® each user must have a LINK ID
    - LINK IDs will all start with “LNK”
    - For Example: LNKUSER123
  - Each LINK ID has different access rights and permissions to view and edit information within LINK
    - If you are unable to access or view a piece of information it is most likely because your ID does not have the appropriate access rights assigned
- Access Rights
  - Each users is denied or allowed to “Inquire Only” or “Update and Inquire” access rights
  - Roles include:
    - Capacity Release
    - Contracts
    - Nominations
    - Meter Confirmations
    - OBA Imbalance Verification
    - View Invoice
    - View Measured Volumes
    - Update for Order 698
    - View Gas Quality
- **Please see the “LINK® ID Setup/Edit” tutorial for more details about ID management**

Contact Information

- Pipeline and Storage tariffs require customers to maintain contact information within LINK®. Local Security Administrators are responsible for maintaining and updating contact information for their company as needed.

- Contact information includes
  - Names (person or department).
  - Addresses.
  - Notification associations.
  - E-mail addresses.
  - Telephone numbers

Contact Uses

- Contact uses define how a contact is used.
  - For example, if Enbridge has a question about who to contact regarding nominations, the person assigned the "Nominations" contact use type would be called.

- Customers can define key contacts to receive important e-mails.
  - For example, the person assigned the "Mail/Deliver Invoice To" contact use type would receive an e-mail notification when monthly invoices are ready.

- Every service requester must have at least one default General Use contact. This person would receive correspondence for other contact use types (such as Nominations or Mail/Deliver To) if a contact for that particular use type is not specified.

- More than one person can be configured for a contact use type. In that case, the person or department marked as the "default" contact use type would be contacted first.

Agency Relationships

- LINK® Security provides the ability for one business entity to act as an agent for another business entity in order to manage or view business activities.

- Agencies are established at the business unit level. If a principal has an agent for two (or more) business units, an agency agreement must be established for each business unit.

- The agency can be for all of a business entity's functions or only a subset of those functions. Within a specific function, agencies can be assigned more granularly to a contract or meter level. Functions that can be assigned for an agency include:
  - Capacity Release - Perform Capacity Release functions or view capacity release information. This can be contract specific.
  - Contracting – Request, maintain or view contract information. For existing contracts, this can be contract specific.
  - Nominations – Perform nominations or view nominations for all contracts, a group of contracts or a single contract.
  - Meter Confirmations – Confirm meters, set PDAs, view allocations and imbalances for all meters/contracts or a subset of those.
  - OBA Imbalance Verifier – update OBA verification information for all OBA contracts or a subset of contracts.
  - View Invoice – view invoice information.
  - View Measured Volumes – view measurement information for all meters, a group of meters or a specific meter.
  - Update for Order 698 Power Plants – update power plant information resulting from Order 698.
  - View Gas Quality – view gas quality information for all meters, a group of meters or a specific meter.

Agency Relationships (Cont.)

- Either the Principal or Agent can submit a proposal to create or amend an agency relationship through on-line screens.
- The Principal may
  - Select to retain their update rights as well as assign such rights to an agent.
  - Assign an Agent the right to see data prior to the Agency.
  - Allow the Agent to act as their Local Security Administrator
  - Allow the Affiliates of Agent to access the Principal’s data.
- Per tariff, agency relationships must be renewed on an annual basis.
  - E-Mail warnings will be sent to the Local Security Administrator of the Principal and Agent 60 and 30 days before an Agency expires.
  - Upon an Agency expiration, an e-mail notification will be sent to the LSA of both the Principal and the Agent.
- **Please see the “Agency Setup” tutorial for details about setting-up and configuring agency agreements**

Agency Relationships (Cont.)

- Either the Principal or Agent can submit a proposal to create or amend an agency relationship through on-line screens.

- The Principal may
  - Select to retain their update rights as well as assign such rights to an agent.
  - Assign an Agent the right to see data prior to the Agency.
  - Allow the Agent to act as their Local Security Administrator
  - Allow the Affiliates of Agent to access the Principal's data.

- Per tariff, agency relationships must be renewed on an annual basis.
  - E-Mail warnings will be sent to the Local Security Administrator of the Principal and Agent 60 and 30 days before an Agency expires.
  - Upon an Agency expiration, an e-mail notification will be sent to the LSA of both the Principal and the Agent.

Affiliations

- LINK® provides the ability for access to be shared between a group of Affiliated companies. Not to be confused with Marketing Affiliations, Security Affiliations simply means a group of business entities that are closely related.
- Affiliations can be proposed or amended by any party but must be confirmed by the counter parties.
- Local Security Administrator access can be shared if desired as an optional component of the Affiliation.
- Affiliations are an all or nothing agreement since they are at a business entity level. However, the Security Administrator of one company in an Affiliation, can chose not to assign specific rights to employees from other business entities involved in the Affiliation.
- Please see the “Affiliation Setup” tutorial for details about setting-up and configuring the affiliation

Warning

ENBRIDGE

- **Customers are responsible for managing the configuration of their entity's security in a way that appropriately protects proprietary data and information.**
  - Agency and affiliation agreements must be especially monitored to prevent information from being inappropriately shared

- The example below show cases how improper security management may lead to a data breach:

Principal A

Principal A enters into an update-all agency with Agent A. Agent A creates the proposal and (1) Authorizes the Agent to be the Local Security Administrator, (2) Allows the Agent's Affiliates to Access the Principal's data and (3) Allows the Agent to view prior data. Principal A accepts.

Agent A

Agent A has also entered into Security Affiliation with Affiliates B, C and D and shared LSA's between each company.

Affiliate B ⟷ **Affiliate C** ⟷ **Affiliate D**

However, Security Affiliate D is the competitor of Principal A. Because of the rights that have been established in the chain beginning with Principal A, Competitor D has full access to Principal A's data and can manage user ids of Principal A.

Questions?

Email link-help@enbridge.com or call 1-800-827-5465 for LINK® application support