

## J.P. Morgan ACCESS<sup>SM</sup> Security Administrators

### Defining the critical role of the SA

J.P. Morgan ACCESS security administrators (SAs) are members of your staff who manage users and users' security credentials. Through SAs, your employees obtain user IDs, passwords, RSA SecurID® tokens and password resets/unlocks.

#### The role of a security administrator

SAs have a wide range of responsibilities, including:

- Managing user access – SAs are responsible for managing new users and existing users.
- Managing security credentials – SAs manage users' credentials to help prevent unauthorized access to your data and transactions.
  - User IDs: SAs distribute user IDs and activate or inactivate users.
  - Passwords: SAs distribute new user passwords and perform password unlocks and resets.
  - SecurID: SAs manage the inventory of SecurID tokens, assign/distribute SecurID tokens to users and assign or revoke temporary token codes.
  - Managing SA designations: SAs should work with the authorized signatories to advise J.P. Morgan when revisions are required.

#### Choosing security administrators

##### *How many do you need?*

You can designate as many SAs as appropriate for your organization. Designating a minimum of two or more SAs is strongly recommended. SAs perform a number of very important functions, and multiple SAs can work as a team, with back-ups, to separately initiate and approve

changes. This helps reduce the risk of internal fraud.

##### *Who is a good candidate?*

SAs should understand your company's operations and audit requirements and be familiar with the J.P. Morgan ACCESS products and services you use. They should also have knowledge of information security and be readily available during normal business hours. You may even choose to have one or more of your SAs on call outside of normal business hours.

Many clients consider designating their risk or security department staff as SAs. Your risk and security teams may already manage employee access to accounts and transactions, making them an ideal choice.

#### Getting started

During the implementation of J.P. Morgan ACCESS, your SAs will:

- Participate in web-based SA training to learn about their role in managing users and distributing security credentials.
- Learn about the J.P. Morgan ACCESS portal functionality and utilities.
- Assign and distribute security credentials to new users.

#### SecurID tokens

As part of the implementation process, your SAs will also receive a package of SecurID tokens for distribution to users. Users entitled to perform sensitive functions, including SAs, are required to enter their token code and password when logging on to J.P. Morgan ACCESS. Users also enter this information when they perform transaction activities that require additional security (such as releasing a transaction).

#### SA responsibilities at a glance

- Manage user access
- Manage user security credentials
- Participate in annual recertification of users' entitlements

#### The tools of a security administrator

The Security Administration application is the primary tool SAs use to manage user access. With Security Administration, SAs perform a number of security-management functions. SAs can retrieve user IDs and initial passwords for new users, activate and inactivate users, and reset or unlock passwords. It also allows SAs to assign or replace a user's SecurID token and to generate or revoke temporary token codes. Additional computer and location-based security controls further enhance your company's control on transaction and data security.

#### Training

J.P. Morgan ACCESS provides online training for Security Administrators and users. Visit our training registration site to register for a session at [jpmorgan.com/visit/wssacesstraining](http://jpmorgan.com/visit/wssacesstraining).

Online help and user guides are also available.

For more information, please contact your J.P. Morgan representative, or visit [jpmorgan.com/wss](http://jpmorgan.com/wss).