J.P.Morgan

J.P. Morgan Access® Resiliency Resources for Security Administrators

We have compiled the below list of J.P. Morgan Access® resources to help Security Administrators maintain productivity and avoid potential disruptions to business operations during these challenging times.

Topic	What You Should Know
Personnel and Coverage	• Make sure you have enough active SAs to manage entitlements. If you do not, contact your client service representative immediately to have the proper documentation completed in order to add or amend SAs. • Consider setting up additional users to perform work. • Ensure all user information is current, including email addresses and phone numbers. • Review Default User Limits as well as any individual user level limits that have been set to determine whether adjustments may be required to accommodate your company's needs during alternate work arrangements.
Hardware Tokens	• Carry your token (RSA SecurID® or Feitian) with you should you need to work from home or an alternate location. • If you need a replacement token, please reach out to your client service associate for assistance.

RSA SecurID® Software Tokens	• If you or your users are using your RSA SecurID® hardware token, please convert to the RSA SecurID® software token if this is a viable option for your company.
	• Refer to the following support guides for additional information on RSA SecurID® software tokens:
	  ○ Credential Services User Guide (Pg. 17-19)
	  ○ RSA SecurID® Software Token New User Quick Start Guide
	  ○ RSA SecurID® Software Token FAQs
	• Note: At this time a software token alternative is not available for Feitian token users.

Temporary Token Codes	• SAs can assign temporary token codes to users who do not have their hardware token in their possession.
	• Refer to the following support guide for additional information on assigning and revoking temporary token codes:
	  ○ Credential Services User Guide (Pg. 22-23)
	• If you are unable to assign temporary token codes for your users, review your client credential preferences for "Default Temporary Token Codes Allowed" and makes edits as needed.
	• Refer to the following support guide for additional information on editing client credential preferences:
	  ○ Credential Services User Guide (Pg. 31)

Managing Passwords – Unlocking Users and Resetting Passwords	• **Unlocking Users:** After excessive unsuccessful logon attempts, users are locked out and may not log on until their User IDs are unlocked. One SA can unlock a user; a second SA's approval is not required. • **Resetting Passwords:** If a user forgets a password, a SA can reset it. All password resets (for both password-only and security token users) require approval by a second SA. • Refer to the following support guide for additional information on managing passwords: ○ Credential Services User Guide (Pg. 12-13)
Inactivating/Reactivating Users	• **Inactivating Users:** SAs must inactivate active users if they wish to prevent them from using Access. One SA may inactivate an active user; an approving SA is not required. • **Reactivating Users:** A user becomes inactive if the user has not logged on for an extended period or if an SA has inactivated the user; an approving SA is required to reactivate a user. • Refer to the following support guide for additional information on Inactivating/Reactivating users: ○ Credential Services User Guide (Pg. 10-11)

Machine Registration	• Each time you log on to Access from a new computer or browser, you will be required to register the machine. We will provide you with a new activation code to register the machine.
	• Review Machine Registration settings for your company. If some users need to work from home or other locations, consider enabling multiple machine registration.
	• Refer to the following support guide for additional information on Machine Registration:
	  ○ Credential Services User Guide (Pg. 14-15)
	  ○ New User Quick Start Guide (Pg. 8)

IP Filtering and Location Groups	• If IP filtering and location groups are enabled for your company and users, updates to location groups may be required based on changes to users' work locations. • Refer to the following support guide for additional information on IP Filtering and Location Groups: ○ Credential Services User Guide (Pg. 29-30)
Fraud Prevention	• Be aware of a higher risk for cyber threats. Use diligence to avoid phishing schemes or malware—and encourage employees to be vigilant, share resources and stay alert. • Do not change payment instructions to vendors, suppliers or other payees without validating it through a call back to a known contact using a telephone number from a system of record. Follow your own internal control procedures to change accounts payable remittance information. • Check out additional resources available in the Security Center on www.jpmorganaccess.com.
Additional Support Resources	• When logged on to Access, you can use Support to view a full range of online help articles, FAQs and guides.