TRUIST

Reference

Truist Treasury Manager
Security Overview

Truist Treasury Manager is a secure cash management solution that lets you manage your account activity, transfer funds between accounts, and view transaction details. Security is a key component of Treasury Manager. Truist employs various security protocols to mitigate the risk of fraud and unauthorized access. We use technology to help protect your account and identify unauthorized activity.

Data Security

Encryption

Treasury Manager uses 128-bit encryption to protect data in transit from your company to Truist. This includes the entry of all IDs and passwords.

Firewalls and Security

Firewalls and other computer systems provide network security to protect against unauthorized access to Truist systems from both inside and outside Truist.

Sign-on Process

Browser Security Software

Treasury Manager works with IBM Security Trusteer Rapport* software to help provide an added layer of protection for your company's online experience. When users sign on to Treasury Manager from a computer with Trusteer Rapport installed, this browser security plug-in helps verify that they are actually connecting to our Treasury Manager site. Protecting the session and encrypting the data helps you prevent malware attacks such as pharming, keylogging, and session hijacking.

Accessing Treasury Manager from a publicly shared or home computer can increase the risk that your Treasury Manager sign-on credentials could be compromised. This can potentially lead to unauthorized access to your accounts, including fraudulent payments. Examples of publicly shared computers include those at hotel kiosks, airports, coffee shops and shared business centers. These computers are in the public domain and often have malware, viruses and keyloggers installed. Truist highly encourages you to access Treasury Manager only from a computer that has anti-virus software and Trusteer Rapport installed.

User Credentials and Authority Levels

To access Treasury Manager, each user is authenticated by the entry of unique security codes, consisting of the Company ID, a User ID, and User Password. The User Password is individually selected by each user and stored in an encrypted manner. Your company security administrator (CSA, or in some cases referred to as a primary administrator) is responsible for adding, deleting, or suspending users; resetting passwords; and defining or limiting each user's access to specific accounts, information, services, and transaction types.

Security Challenge Questions

As an additional security procedure to authenticate users, Treasury Manager employs risk monitoring and security challenge technology. This technology is similar to authentication technology employed for credit cards. An alternative to hardware-based tokens, an internal Truist risk monitoring application establishes a user's profile, which is based in part on a user's sign-on activity and IP address information.

When a user first accesses Treasury Manager, the user is prompted to select challenge questions and answers. Users are prompted to answer the selected questions in the event the Truist risk monitoring application detects what it identifies as uncharacteristic sign-on behavior, based on the user's profile. For example, a user who typically works in the main office but signs on from a workstation in another office may be prompted by a challenge question to help authenticate the user's identity.

Time Out

Treasury Manager will time out and suspend access if a session is idle for more than 30 minutes. Access can be regained by re-entering user credentials.

Security Administration and User Entitlements

Audit Reports by User Profile

To help address internal security audit requirements, the company security administrator has access to detailed User Profile and User Activity Reports. The User Profile Report provides detail about a user's entitlements, including services, accounts and payment and approval limits. The User Activity Report includes detailed information about the daily activity audit log for each user. This includes payment and template creation, approvals, deletions, and positive pay exception decisions. These reports can be exported and saved for audit reporting purposes.

Dual Approval and Segregation of Duties

Transaction-initiation services, such as account transfers, ACH payments, and wire transfers, all provide for dual approval, meaning one user would initiate a transaction, but a different user would approve the transaction for release. By segregating duties, you can reduce the risk of compromised sign-on credentials, which could lead to unauthorized access. Dual approval is strongly recommended for initiation of transactions, whether they are internal account transfers or ACH or wire transfer transactions.

Dual Administration

To help prevent unauthorized access to Treasury Manager, Truist highly recommends dual approval over the single security administrator function. With this control in place, tasks such as setting up new users, making changes to passwords, and entitling user access to services and accounts go into a pending status after being entered. Another CSA's authority is required to approve those changes before they take effect.

ACH Origination Security

The Treasury Manager ACH service allows you to originate ACH debits and credits through the creation of templates, file import or one time payments. This service provides several important security features, including:

- Dual approval of ACH batches, ACH File Upload, or individual ACH transactions
- Approval limits by user and ACH transaction types
- Confidential batches to limit specific users from seeing information such as payroll data
- The Preferred Recipient List to help control access to sensitive recipient information

Wire Transfer Security

The Treasury Manager Wire Transfer service allows you to initiate domestic and international wire transfers, import wire transfers, establish repetitive wires and view wire activity. You can submit a wire by selecting a specific account or by using a template. After the information has been entered and reviewed, the wire is released according to approval procedures and user payment limits. Truist strongly recommends that you do not grant a single user the ability to initiate and approve wires. If your company does not intend to send international wires or drawdown wires, Truist will not activate these payment types.

- **Approvals and Entitlements** — Treasury Manager allows for separate and distinct input, approval and release functions for up to three separate users, thus segregating wire transfer duties among internal staff according to your specifications. Additional user entitlements such as per wire and daily dollar limits by user and dynamic approval levels by transaction type can be set up by the CSA.
- **Tokens** –Treasury Manager requires the use of a hard or soft token for wire payment approvals. Each user will be required to authenticate using this token prior to the release of wire payments.
- **Wire Advices** — Detailed Online Courier wire advices can be sent automatically to your email address to advise you on a real-time basis about incoming wire debits or credits to your accounts. To help you control the type of wire advices you receive, you can specify whether you want to receive wire advices for outgoing or incoming wires (or both), as well as set a threshold by dollar amount.

Complementary Fraud Control Services

Treasury Manager's Positive Pay feature gives you an effective tool for identifying fraudulent checks so that appropriate action can be taken to mitigate your risk. Positive Pay increases your company's control over check payments. You transmit your check issue records to Truist as checks are written, and we match certain information from your check issue records to those features of checks paid against your account. If a check does not match your issue record, Truist notifies you. You can then research the check and enter your pay/return decision online.

Additional ACH fraud prevention solutions offered by Truist include ACH Fraud Control with ACH Positive Pay, ACH Blanket Block, and Universal Payment Identification Codes (UPIC). For more information regarding fraud control services, please contact your Treasury Consultant.

Getting Help

Click the **User Materials** link at the top right of any page or visit the Treasury Manager page of the **Treasury Resource Center** at truist.com/treasuryresourcecenter to access reference materials.

If you need additional assistance, contact Treasury Solutions Client Services at treasuryclientservices@truist.com or **800-774-8179**. Representatives are available from 8 am to 8 pm ET, Monday through Friday on bank business days.

* Trusteer Rapport or other secure browsing software downloaded to or accessed by your computer or mobile device (the Software) is provided by IBM. You and your company agree that (i) use of the Software is subject to IBM's terms and conditions and privacy policy; (ii) Truist makes no representations or warranties of any kind related to the Software and has no responsibility for the performance, compatibility or availability of the Software, or for damages of any kind that may be caused by the Software; and (iii) protections offered by use of the Software can be achieved only when the Software is used in connection with access to specific Truist products which are designed to interact with the Software. When used with those services, the Software may make certain fraud detection information available to Truist. Truist has no obligation to provide you any notices with respect to such information.