

A low-angle photograph of several modern skyscrapers with glass facades, viewed from below. The image is overlaid with a semi-transparent red filter. The text is positioned on the left side of the image.

# TEOCO Data Center Connectivity Overview

## Confidentiality, Copyright Notice & Disclaimer

Due to a policy of continuous product development and refinement, TEOCO (and its affiliates, together “TEOCO”) reserves the right to alter the specifications, representation, descriptions and all other matters outlined in this publication without prior notice. No part of this document, taken as a whole or separately, shall be deemed to be part of any contract for a product or commitment of any kind. Furthermore, this document is provided “As Is” and without any warranty.

This document is the property of TEOCO, which owns the sole and full rights including copyright. TEOCO retains the sole property rights to all information contained in this document, and without the written consent of TEOCO given by contract or otherwise in writing, the document must not be copied, reprinted or reproduced in any manner or form, nor transmitted in any form or by any means: electronic, mechanical, magnetic or otherwise, either wholly or in part.

The information herein is designated highly confidential and is subject to all restrictions in any law regarding such matters and the relevant confidentiality and non-disclosure clauses or agreements issued with TEOCO prior to or after the disclosure. All the information in this document is to be safeguarded and all steps must be taken to prevent it from being disclosed to any person or entity other than the direct entity that received it directly from TEOCO.

TEOCO and Netrac® are trademarks of TEOCO.

All other company, brand or product names are trademarks or service marks of their respective holders.

This is a legal notice and may not be removed or altered in any way.

COPYRIGHT © 2020 TEOCO

ALL RIGHTS RESERVED.

---

**Your feedback is important to us:** At TEOCO, we take many measures to ensure that our documentation is of the highest quality.

If you found errors or feel that information is missing, please report your findings via TEOCO's Customer Support Portal at <http://www.teoco.com/support>.

If you have a Severity 1 operational issue, you may dial 1-866-884-8324 for further assistance after opening a support request via the Customer Support Portal.

---

# Contents

- Introduction..... 1**
- Connecting to TEOCO’s Data Center ..... 1**
  - Virtual Private Network (VPN).....1
  - Guidelines for setting up routing on customer network.....1
  - IP Access Control List .....1
  - Connectivity from users’ homes .....1
  - Software required on workstation for connectivity .....2
  - TEOCO network information .....2
- User access to applications..... 3**
- Corporate e-mail considerations ..... 3**

## Introduction

This document provides information on how TEOCO's Software-as-a-Service (SaaS) customers connect to TEOCO's Data Center and access TEOCO's applications.

## Connecting to TEOCO's Data Center

There are two options for connecting to TEOCO's Data Center:

- Virtual Private Network (VPN)
- Internet Protocol (IP) Access Control List

### Virtual Private Network (VPN)

A VPN extends a private network and the resources contained in the network across public networks like the internet, commonly referred to as a tunnel. TEOCO will work with a customer's IT/Network department to coordinate the setting up of a VPN connection from the customer's central network location to the TEOCO Data Center. TEOCO utilizes common best practices to ensure data security, including hardware-based strong encryption, pre-shared keys, and pass-phrases.

#### Guidelines for setting up routing on customer network

After a VPN tunnel is created from the customer location to the TEOCO Data Center, it is the responsibility of the customer to ensure that the appropriate routing is set up on the customer's side. See [TEOCO network information](#) on page 2 for TEOCO server URL's and required ports.

- When a user enters the URL's for various TEOCO applications into a browser, the local network should route them over the VPN tunnel to TEOCO's servers, not over the public internet.
- If the customer has multiple locations, the customer should arrange for all users to route over the VPN tunnel. The remote locations should have a proper amount of bandwidth to reach the location over the VPN connection. Ping times 50ms or less are recommended from remote location to the TEOCO servers.

### IP Access Control List

An IP Access Control List (ACL) is a list specifying the IP addresses from which users are permitted access to a network. The customer provides TEOCO with all IP addresses from which its users will be accessing TEOCO applications. TEOCO configures its firewall to allow access from these IP addresses.

---

**Note:** TEOCO will not accept IP addresses from users' home broadband access providers, including (but not limited to) cable modem services, DSL services, and dial-up services. See the following section for information on connecting from a user's home.

---

### Connectivity from users' homes

If a customer's users wish to access the TEOCO services from their homes using a broadband connection, there is only one acceptable method: the customer's users must first authenticate to their company's network (VPN) and then route over the already established VPN to TEOCO to gain access to the TEOCO applications. Routes other than from the client's business network will not be supported by TEOCO.

The customer is responsible for troubleshooting and working with its employees to solve connectivity issues from their homes over the VPN.

## Software required on workstation for connectivity

TEOCO's SaaS environment utilizes Citrix and Business Objects. In order for users to be able to use Citrix and Business Objects in the SaaS environment, users must have certain software installed on their workstation.

- **Additional software required for using Citrix:** ICA Client
- **Additional software required for using Business Objects:** JRE 1.6

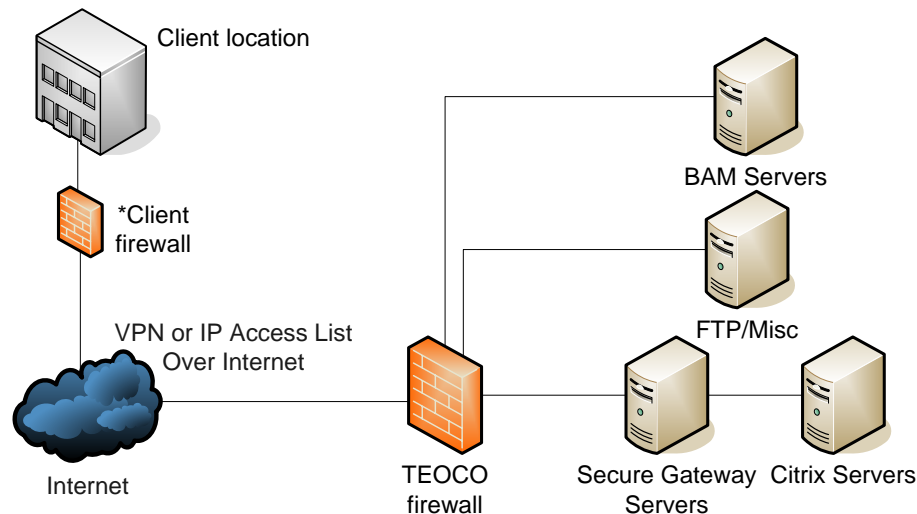
TEOCO will provide this software; however, it is the customer's responsibility to install this software on each workstation that needs access to the TEOCO applications. The software must be installed with administrator rights on the local computer.

## TEOCO network information

The following information will assist the client's IT/Network department with the routing of traffic to the TEOCO servers:

Destination	URL/IP	Required Ports
Main Citrix URL	btp.teocosolutions.com – 68.177.229.0/25	443
Main BAM URL	[client_name].teocosolutions.com – 68.177.229.0/25	443
Citrix Secure Gateway	btpgwy.teocosolutions.com – 68.177.229.0/25	443
FTP/SFTP server	63.146.182.64/26 and 68.177.229.0/25 – IP Access/VPN Access	21/22

(IP blocks given, TEOCO will provide specific IPs as required, addresses are subject to change. [client\_name] will be determined on a per case basis as required)



\* If client has a firewall, then the appropriate changes must be made to allow for ports noted above passing through in both directions.

## User access to applications

In the SaaS environment, TEOCO uses a centralized repository of user information, credentials, and passwords to control access to the applications. Working with the TEOCO Account Manager, the customer provides the required user information for TEOCO to enter. The required user information generally consists of the following:

- First Name
- Last Name
- Email Address
- Applications to which user needs access (e.g., BillTrak Pro)

TEOCO provides the users with their login names and passwords.

If the customer wishes to disable a user, reset a user password, or add a new user, the customer should contact TEOCO by entering an iSupport request.

## Corporate e-mail considerations

In certain scenarios TEOCO systems may send email on behalf of a user on a customer domain. In these instances the successful delivery of the email could be affected depending on the Sender Policy Framework (SPF) settings used by the customers email infrastructure.

SPF is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.

In the instances where TEOCO sends email on your behalf, if SPF is used by the client organization, the SPF settings must be modified to include the TEOCO outbound email servers so they are authorized to send the message since it will appear as if it is coming from the client.

Since TEOCO utilizes an external email provider, Mimecast, the required SPF changes are outlined in the following document:

<https://community.mimecast.com/docs/DOC-2010-connect-application-implementing-spf-for-outbound-email-delivery>

If required, someone from the client side IT organization should be engaged to make the necessary changes to allow email to flow properly.