Tornado
Deployment Security Guide

Version 2.10

December 2024

docmosis

Trademarks
Docmosis is a registered trademark of Docmosis Pty Ltd.
https://www.docmosis.com

Microsoft Word and MS Windows are registered trademarks of the Microsoft Corporation.
http://office.microsoft.com/en-us/default.aspx
http://www.microsoft.com/windows/

Adobe® PDF is a trademark of the Adobe Corporation.
http://www.adobe.com/products/acrobat/adobepdf.html

LibreOffice is a trademark of LibreOffice contributors and/or their affiliates.
http://www.libreoffice.org

TABLE OF CONTENTS

1. INTRODUCTION

Tornado is a stand-alone, self-hosted document generation engine that other software applications can use to generate documents based on templates.

Tornado can be hosted on Linux or Windows servers, or using a containerized approach such as Docker. It is well suited to running in private data centres, or on public cloud services such as AWS or Azure

This document explains the fundamentals of securing Tornado and the environment around Tornado.

Tornado should, typically, not be public-facing since exposure to the internet creates one of the highest risks to IT systems. The principle of minimal access should be applied when configuring and maintaining Tornado. Applications and staff accessing Tornado would usually do so over a LAN (local private networks).

Docmosis has developed features to help secure Tornado, but security rests with the devops and security teams installing, configuring and maintaining Tornado. The teams responsible for hosting Tornado should have a detailed understanding of the environment in which Tornado runs and are ultimately responsible for balancing security risks against accessibility, usability and other concerns.

2. THE THREE ACCESS POINTS OF TORNADO

There are three ways a Tornado system can be accessed:

1. The Tornado Console.
2. The REST API.
3. The server itself.

Securing a Tornado environment involves securing these points of access. There may be other aspects (such as backups, cold standby servers, etc) that provide other forms of access to the files of a Tornado system. These other aspects must be addressed by the relevant team but are not discussed further in this document.

2.1. The Tornado Console

The Tornado Console provides a web-based interface to view and configure Tornado via a web browser. It also provides the ability to execute tests to render templates into documents. Access to the Tornado Console should be limited to the staff that require it. The relevant security aspects for the console, discussed later, are:

- Network access / firewalls
- TCP/IP port
- Administrative password (Tornado configuration)
- HTTPS/SSL configuration

2.2. The REST API

The REST API provides access to the main function of Tornado: to allow software applications to generate documents. As a minimum, having network access from the application to the Tornado host and port is required. The security aspects that are relevant to the REST API are:

- Network access / firewalls
- TCP/IP port
- API/Access key (Tornado configuration)
- HTTPS/SSL configuration

2.3. The Server Itself

Access to the server running Tornado software should to be limited to the staff who manage the systems. Server access is fundamental to the security of a Tornado installation since, once logged onto the server, many security features can be bypassed. The administrative and security team should manage the security of the operating system including access, updates and monitoring.

3. BUILT IN SECURITY FEATURES

Tornado has several application-level features that can be used to assist with security. These are controlled via Tornado configuration settings. The settings can be viewed and adjusted using the Tornado Console or via launch parameters (e.g. Docker launch configuration).

3.1. Administrative Password

The administrative password controls access to the Tornado Console. Once the password is configured, access to the console and configuration requires the password. Note: HTTPS/SSL configuration is important for protecting the password from network penetration.

There are no minimum length or complexity requirements enforced by Tornado. Passwords should be created to meet the procedures/policies of the organization hosting Tornado.

3.2. API Key for REST calls

Access to the main API functions of Tornado (e.g. rendering a document) can be controlled by setting the API key. This key is independent of the password. Once set, all API calls will be required to provide the key to be permitted to operate.

There are no minimum length or complexity requirements enforced by Tornado. The API Key should be created to meet the procedures/policies of the organization hosting Tornado.

3.3. HTTPS configuration

Tornado may be configured to be very “network-local” or “network-private” to the clients using it. In such an environment, the network itself may be considered secure enough that there is no benefit to encrypting the communications.

Where appropriate, HTTPS/SSL can be configured so that all traffic to / from Tornado will be encrypted. This protects the configuration (e.g. password, API Key) as well as any documents and application data that is travelling across the network from any other devices that might be on the same network.

HTTPS can be configured by a network appliance such as a load balancer so that the encryption is provided outside of Tornado (such as in “SSL-termination”) or it can be configured within Tornado itself. The teams managing the Tornado installation should utilize the encryption mechanism (if any) as they require.

The configuration within Tornado involves installing certificates into the Java installation and the use of cryptographic tools (such as Java’s keytool). The certificates may be private self-signed or signed by public auhorities depending on the security requirements and facilities of the Tornado clients. The settings are Java settings (e.g. javax.net.ssl.trustStore) and are listed in the *Tornado Installation & Configuration Guide*.

3.4. Outbound Communications

Tornado does not require any out-bound communication. There are no license key checks or status checks that involve external connections. This means outbound network access can (and should) be limited as required.

There are exceptions to the need for outbound access. For example, Tornado can be instructed (during a document generation request) to fetch images from remote URLs or obtain templates from Amazon S3, Microsoft Azure or Google Cloud. In these cases, outbound network access will need to be allowed as required to facilitate these specific locations.

3.5. Monitoring

Tornado provides some monitoring features that can assist with reliability/stability monitoring:

3.5.1. The “ping” API

Tornado will respond to an HTTP/HTTPS call to “/ping” to confirm connectivity. This is a trivial call that provides a simple HTTP response code to confirm reachability. A response code of 200 on success means Tornado is reachable and can be used by monitoring systems for basic connectivity testing.

3.5.2. The “status” API

A HTTP/HTTPS call to “/status” is like the “/ping” service, but provides a deeper introspection and a JSON result indicating the operational status of the Tornado server. It can confirm that the service is able to render documents beyond simply being reachable.

4. NETWORK SECURITY

With an understanding of the inbound and outbound communications from the previous sections and through the use of firewalls, the Tornado server should be limited to the minimal required access.

4.1. Inbound Networking

Inbound networking must allow access to:

1. The port(s) that Tornado is configured to run on. All access (the Tornado Console and the REST API) is via a single port (typically) and that port can be configured
2. Port 8080 is used by default and does not encrypt traffic
3. An SSL port can be configured and it is recommended that if configured, the non-ssl port is disabled (and of course blocked by the firewall configuration)
4. The firewall/network may also be configured to consider the source of the network traffic to limit access to only where it is expected to originate.

4.2. Outbound Networking

Tornado does not require outbound network access except as used by the application developers calling the Tornado REST API. Via the API, Tornado can be instructed to source images from URLs and templates from Amazon or Microsoft sources. Typically, all outbound network access should be blocked with regards to Tornado except as required by the teams developing the software that interacts with Tornado.

5. OPERATING SYSTEM SECURITY

The administrative team should ensure that the server running Tornado is secured. This includes configuring network access and passwords to ensure authorised access.

Tornado itself should be run under a user account with basic user privileges. It should not be a “root”/administrative user and should not be able to escalate privileges (e.g. via “sudo”).

6. SEPARATION OF ENVIRONMENTS

It is common for development of software to include multiple environments. For example: production, test and development. Each of these environments uses the same software but will have varying configuration, passwords and access.

Developing with Tornado supports the separation of environments. In a software project, it is expected that if there is a dev, test and production environment for the software, each is paired with a dev, test and production Tornado server (or set of servers). Each environment will be configured to support the related environment – dev will often be low scale and local to the developers, but prod will have separate passwords, be isolated and often run at a different scale (hardware, parallelism etc).

The security concerns addressed in earlier sections of this document apply to all environments. The degree of security configuration varies - where production data is in use typically the security requirements are more stringent. Each environment needs to be considered as to how it should be secured with the ultimate objective being to make sure the production systems are never compromised. Distinct hardware, security settings (such as passwords, keys and TCP/IP ports) and user-access to the servers will help to protect the production environment.

7. SOFTWARE UPDATES

Tornado is a "stack" of components:

- The operating system
- Java/JVM
- LibreOffice
- Fonts
- Tornado Software

From time to time these components need to be reviewed for security updates. Given the nature of document generation, stability and consistency of output are key objectives. Documents must always render as designed. Even seemingly innocuous changes (such as adding a new font) can have small effects which can potentially change the layout of a document in undesirable ways.

The best approach to any updates to the Tornado stack is a test-and-update approach. This entails performing updates in a test environment, running tests, then updating the production environments. This is typical approach for most software systems.

The testing stage includes:

1. Accuracy testing – ensuring that the generated documents are consistent with documents generated before the updates. This can involve both manual and automated tests.
2. Performance testing – ensuring the performance has not degraded (or better still improved)
3. Reliability/Stability testing – ensuring no new issues have occurred that degrade the robustness of the system.

Deciding when to perform updates is completely dependent on the environment in which Tornado runs. Often, multiple important updates will be available which makes the test-and-update approach appropriate and worth the effort.

Sometimes minor security updates (such as an OS patch) may be executed in a manner that has a reduced testing requirement because the effect on document production is expected to be zero. In such a case, expedited/minimized testing may be appropriate.

Sometimes, the opposite is true. Security updates may be identified as "urgent and severe", but because of the nature of the vulnerability and the already-implemented security measures, the urgency is mitigated. A decision to delay updates may be appropriate until a full test-and-update approach can be used.

8. GETTING HELP

The Docmosis team is always available to provide assistance and assist with questions about security. We are not experts with regards to your system, but we are with respect to Tornado.

Contact support whenever you have a question: https://www.docmosis.com/support/

Docmosis Pty Ltd

Address
Suite 8 / 5 Hasler Road,
Osborne Park,
WA 6017 Australia

Website
https://www.docmosis.com

Resources
https://resources.docmosis.com

docmosis