SECURITY DOCUMENT

Documentation for XTM Version 10.3

Published by XTM International Ltd.

Updated May 2017

XTM-International Ltd, PO Box 2167, Gerrards Cross, SL9 8XF, UK

Tel.: +44 (0)1753 480479 email: sales@xtm-intl.com http://www.xtm-intl.com

Table of Contents

Table of Contents 3

Introduction 4

XTM Architecture 4

XTM Cloud Environments 4

Physical security 4

Access Management 4

Access Control 5

Identification and Authentication 6

Data Transmissions 6

Auditing and Logging 6

Application timeout after a period of inactivity 7

Application Monitoring 7

Database connections 7

Application Security 7

Application Error Handling 7

Web services 7

Business Continuity / Disaster Recovery 8

Server Management 8

Server data access 8

Data protection 8

Fire-fighter account controls 8

Introduction

This document summarises the data and application security aspects of XTM. It covers both XTM Cloud, the SaaS version of XTM, and XTM Suite, the traditionally licenced software installed on a customer's Server.

XTM Architecture

XTM is written in Java and runs on servers under Windows Server or Linux. Users access the program entirely via a web browser. XTM currently supports Internet Explorer and Firefox.

XTM Cloud Environments

All XTM International's servers run Centos v7.0 and use the HTTPS protocol. The system uses at least TLS v1 with at a minimum of 2048-bit cipher strength.

XTM cloud exists in the following environments that are installed on different servers:

- Production servers for customers
- Stage server for customer testing
- Beta server for XTM staff and selected users
- Testing server for XTM International

The XTM Cloud production servers are deployed in one zone which is protected by a firewall and only allows HTTPS and SSH connections. For hosted servers the customer can decide whether to use HTTPS.

Physical security

XTM International currently uses three hosting centres for XTM Cloud servers:

1. France, Roubaix
2. USA, St. Louis, MO
3. Canada, Montreal

These state of the art hosting facilities provide the following physical security:

- Multiple redundant internet connections
- Fully automatic room climate control and air moistening
- UPS and voltage filters
- Fire protection
- 230V power supply
- Early detection system for smoke
- 24 hour security service
- Video surveillance
- Admission control
- Diesel generators

Access Management

An XTM administrator can create, grant, modify and revoke access to the application for project managers and linguists. Project managers can create, grant, modify and revoke access to the system to linguists.

XTM International works with the system administrators and project managers to set the role-based access for users and ensure that the least privilege principle is consistently implemented.

Access Control

XTM has the following access control features:

Feature	Administrator control - Description
Allowed logon attempts	If the user makes the specified number of invalid logon attempts then their account will be locked and they will not be able to access the system. In order to unlock the account the administrator needs to go to the Users tab and select unlock account from the menu icon in the left hand column of the users listing.
Disable account after non-use	If the user does not log into their account during the period of days specified then the account will be locked. The account will then need to be unlocked by the administrator as described above.
Computer activation level	This setting specifies who will need to go through the PC activation process on first log in. The process involves generating an automatic email to the user which contains a link to download a cookie.
Password duration	This field specifies the number of days that user passwords will be valid. After this period the user will have to change their password.
Check against previous passwords	This field specifies the number of previous passwords that cannot be used as the current password.
Minimum password length.	This field specifies the number of characters required in the password
Use brute force dictionary	This dictionary defines the words that cannot be used as or in a password. By default the following words and components are excluded: • User • Guest • Admin • User's first or last name • Sys • Test • Pass • Super
Force password change at first log in	Check box to enforce this measure
Password strength	There are 3 levels of password strength which define the mixture of characters in the password. Characters are split into 4 groups: ● Upper-case letters, ● Lower-case letters, ● Numbers ● Non-alphanumeric symbols. The password strength is thus: ● Simple — Must use characters from at least 1 group. ● Medium — Must use characters from at least 2 of the groups. ● Strong — Must use characters from at least 3 of the groups.

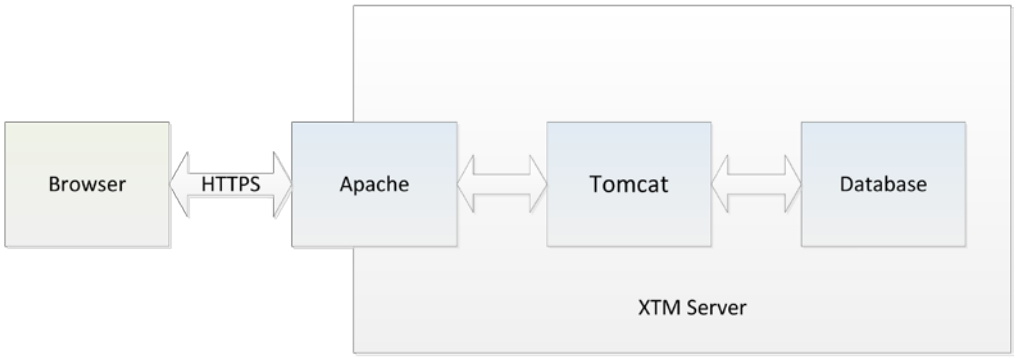
Identification and Authentication

XTM may either connect to an LDAP service for user authorisation or perform the authentication itself.

When the authorisation is performed internally, firstly the password entry is hidden on sign in. Then the username and password are sent over the HTTPS encrypted connection to the server.

At the server the authenticated Class connects to the appropriate database tables. All passwords are encrypted using SHA1 algorithm. The username and password pair is checked against the appropriate database entry. The user roles, which govern user access to different XTM modules, are also extracted from the database.

On first login the user is directed to the password reset page and encouraged to change the initial password.



XTM login security diagram

Data Transmissions

By default users need to register their PC in order to access XTM Cloud. This is achieved through the installation of a cookie. The link for the cookie is sent to the user's email address. This feature may be deactivated at the system level by an administrator if it is deemed to be unnecessary.

For XTM Cloud the communication between the end user and XTM uses HTTPS. This is optional for XTM Suite or Private Cloud implementations.

If a file is uploaded for processing and the upload is faulty then the user will receive a message that the file is corrupted.

Auditing and Logging

The XTM components that have logging capabilities are configured to produce a security audit log. These are:

- Apache HTTP Server log
- PostgreSQL log
- System log
- XTM log

The following events are logged within XTM

- User logon and logoff
- XTM Editor: Opening, saving and navigation to another page.

On XTM Cloud and hosted servers managed by XTM international, all the logs are retained for 90 days, except for the PostgreSQL log which is retained for 7 days.

To ensure that the log files are secured during system restarts, they stay on a mirrored HDD RAID ARRAY and are backed up onto an external machine daily.

Application timeout after a period of inactivity

In XTM Editor the user pings the server every 10 seconds. When a translator enters a page the segments are locked for other users. If the pings are not detected, when for example the browser or PC has crashed or if the user simply closes the browser without logging out, XTM releases the locked segments quickly. If no user activity is recorded for a period of 60 minutes then XTM closes the session.

XTM project manager session timeout after 60 minutes of user inactivity, however if the browser or the computer is closed then the session expires within 4 minutes.

XTM TM Manager and XTM Terminology Manager sessions timeout after 60 minutes of user inactivity if the browser is open, and within 20 minutes if the browser of computer is closed.

Application Monitoring

XTM Cloud and hosted servers managed by XTM International are proactively monitored by Nagios to ensure that all systems, applications and services, are functioning properly. In the event of a failure, Nagios alerts XTM International's technical staff of the problem, allowing them to begin remedial action before outages affect end-users.

Database connections

XTM applications connect to the database with the minimum privileges required.

Application Security

XTM does not permit cross-site scripting or SQL injection.

Application Error Handling

XTM displays an error message to the user on the web page with a link to a page containing the details of the error can be viewed in the log.

The XTM Software development life cycle process (SDLC) process ensures testing of potential intrusion threats such as SQL injection and session hijacking. This includes testing that error conditions cannot be forced, or that if error conditions are encountered that they cannot be used to breach the security mechanisms of the system.

Web services

The standard implementation of XTM does not expose web services.

XTM has the option to connect to a number of different machine translation engines in order to provide translators with machine translations of text. These options require the XTM administrator to set have an account with the MT provider

There is also an optional API to integrate XTM with third party applications called XTM Connect. It can be set up with or without SSL; on XTM Cloud SSL is used. Each web service method has a LoginAPI object which contains three fields: Company, User, and Password. These fields have to be filled every time you call the web service method.

Business Continuity / Disaster Recovery

Data in XTM Cloud is stored in a database and also in data files. This data is backed up as follows:

In case of HDD failure, the XTM Cloud server cluster is equipped with mirrored disk arrays. XTM data is written to a storage array on the local machine and in addition it is simultaneously written to a storage array on another server in the cluster.

The databases and data files are backed up every day locally and also onto an external server. We store

- The last 15 copies of the databases
- The last 3 copies of the data files

In case of hardware failure damaged components can be replaced in few hours or the whole service can be relocated to other machine using data from the latest backup.

After every configuration change that can affect current procedures, the business continuity/disaster recovery procedures are tested and revisited to ensure they provide the required level of business continuity in emergency scenarios.

The XTM Support SLA and Redmine issue tracking system ensure that details of any application incident are logged and managed correctly.

Server Management

Each administrator has a separate account to the server and there are no shared IDs.

Server data access

No directories can be accessed from web clients. There is a generic error page to hide the actual error message or warning returned.

Data protection

XTM International has a core team of developers and support engineers. If any staff leave the team, then they immediately lose all access rights to all development, testing and production systems.

Only staff working on specific issues have access to production data and if the data is copied by staff for testing purposes it is deleted on completion of the tests. All PCs and laptops used by XTM support and development staff have their disks encrypted.

Production data is not stored on mobile media.

Fire-fighter account controls

In order to provide high quality support required of the SLA there are privileged accounts (fire-fighter accounts) that the XTM technical team use to access XTM Cloud. These accounts which allow access to customer’s data are password protected and use is monitored via the log. Access to all production servers, including XTM Cloud is protected via two-factor authentication.

XTM International Ltd, PO Box 2167, Gerrards Cross, SL9 8XF, UK
Tel.: +44 (0)1753 480479 email: sales@xtm-intl.com http://www.xtm-intl.com