DoD TeamPage

Configuration Notes

Traction Software

Version 1.0
June 6, 2014

Table of Contents

This guide explains how to configure TeamPage 6 to comply with DoD security requirements, and the configuration options needed to configure it appropriately for running in that environment.

This document supplements the Installation and Configuration Guide (https://teampage.tractionsoftware.com/traction/permalink/Doc351).

For DoD deployments, TeamPage should be configured to run over HTTPS and connected via NTLMv2 to an Active Directory server. This way, the directory server's password requirements will be used, and users will benefit from single sign-on with their workstation login.

Instructions for configuring HTTPS are posted at https://teampage.tractionsoftware.com/traction/permalink/Doc264 .

Instructions for connecting to Active Directory with NTLMv2 using the JESPA libraries are posted at https://teampage.tractionsoftware.com/traction/space/jespaauth . Please note that this link is normally available only to customers who have purchased the JESPA auth option. If you need to review this link in advance, please contact sales@tractionsoftware.com.

The notes below describe the configuration settings needed for testing specific issues in the Certification Document.

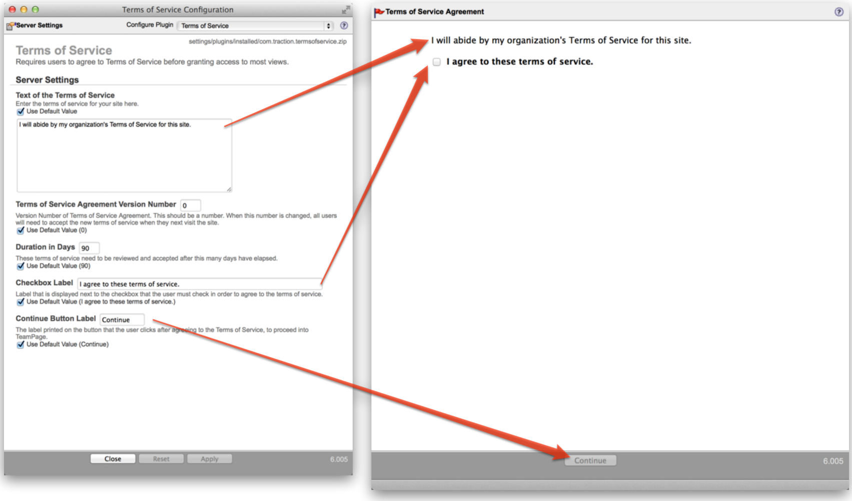
Displaying Terms of Service

2.4 The designer will ensure the application is capable of displaying a customizable click-through banner at logon which prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK." (APP3440 CAT II)

This requirement is addressed via the Terms of Service plug-in, which you can download from https://teampage.tractionsoftware.com/traction/permalink/Customer4532.

To install and configure the plug-in, follow the instructions in that article.

Note that the Terms of Service plug-in *is* compatible with single sign-on solutions such as NTLM.



settings/plugins/installed/com.traction.termsofservice.zip

Terms of Service

Requires users to agree to Terms of Service before granting access to most views.

Server Settings

Text of the Terms of Service
Enter the terms of service for your site here.
☑ Use Default Value
I will abide by my organization's Terms of Service for this site.

Terms of Service Agreement Version Number 0
Version Number of Terms of Service Agreement. This should be a number. When this number is changed, all users will need to accept the new terms of service when they next visit the site.
☑ Use Default Value (0)

Duration in Days 90
These terms of service need to be reviewed and accepted after this many days have elapsed.
☑ Use Default Value (90)

Checkbox Label I agree to these terms of service.
Label that is displayed next to the checkbox that the user must check in order to agree to the terms of service.
☑ Use Default Value (I agree to these terms of service.)

Continue Button Label Continue
The label printed on the button that the user clicks after agreeing to the Terms of Service, to proceed into TeamPage.
☑ Use Default Value (Continue)

I will abide by my organization's Terms of Service for this site.

□ I agree to these terms of service.

Password Storage Compliance

3.4 The designer will ensure the application stores account passwords in an approved encrypted format.(APP3340 CAT I)

Passwords for users are *not stored at all* when the system is configured to use single sign-on. This is the recommended configuration.

In the default out-of-the box configuration (often used for evaluation, or when single sign-on is not enabled), salted password hashes are stored in the Journal.db journal file. A typical entry looks like this:

```
admin:PHYyPjEwMDAwOjNjMWIyZGVjMTZkYjFmYWJmZjlkNDYwMTM0YzU2NjAwYWE
zN2IwODY2MmE5YmMxYjo3Y2Y2YmU0YmY4ZTFiZDdkMTM4MDdhZmRiMTBhYzRlZDBk
MDBkNTI1MGZiMGNhNzc=:1:
```

This is base64 encoded. Decoded, the format is this:

```
<v2>10000:3c1b2dec16db1fabff9d460134c56600aa37b08662a9bc1b:
7cf6be4bf8e1bd7d13807afdb10ac4ed0d00d5250fb0ca
```

First, there is a version number, in this case v2. Next is the number of iterations used in the hash algorithm, in this case 1000. Next, is the password hash, and finally the salt.

Technical Details

- Passwords are hashed with a 192-bit random salt.
- Only the PBKDF2 hash with HmacSHA1 (10,000 iterations) is stored.

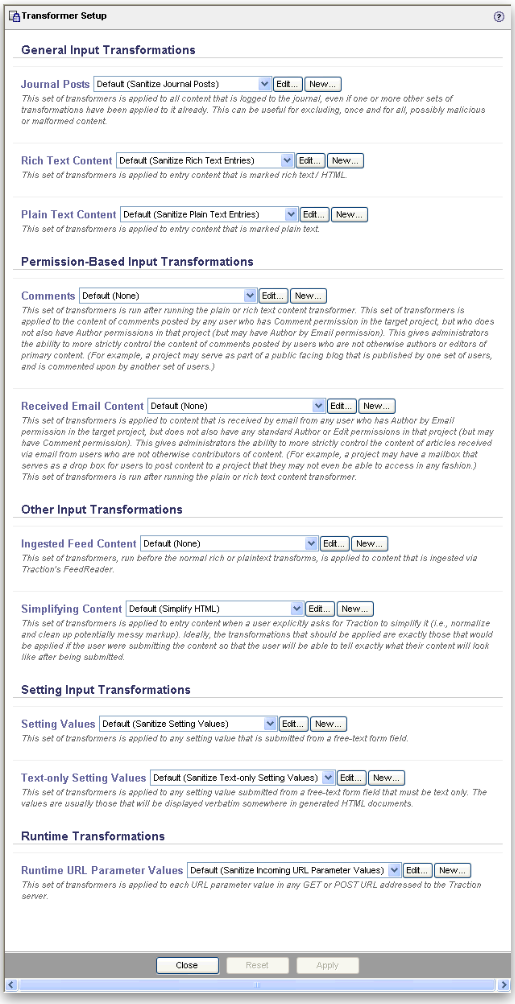
Configuring Cross-Site Scripting Countermeasures

4.8 The designer will ensure the application does not have cross site scripting (XSS) vulnerabilities. (APP3580 CAT I)

In order to prevent cross-site scripting and SQL injection attacks, TeamPage applies configurable transformations to all inputs.

In most cases, the default transformations suffice to guard against attackers embedding JavaScript in form, URL parameters or other inputs, which is the primary way that cross-site scripting attacks are carried out.

If new attacks are discovered, or additional protections needed, the instructions in https://teampage.tractionsoftware.com/traction/permalink/Doc303 explain how to build and test custom transformers.



General Input Transformations

Journal Posts Default (Sanitize Journal Posts)

This set of transformers is applied to all content that is logged to the journal, even if one or more other sets of transformations have been applied to it already. This can be useful for excluding, once and for all, possibly malicious or malformed content.

Rich Text Content Default (Sanitize Rich Text Entries)

This set of transformers is applied to entry content that is marked rich text / HTML.

Plain Text Content Default (Sanitize Plain Text Entries)

This set of transformers is applied to entry content that is marked plain text.

Permission-Based Input Transformations

Comments Default (None)

This set of transformers is run after running the plain or rich text content transformer. This set of transformers is applied to the content of comments posted by any user who has Comment permission in the target project, but who does not also have Author permissions in that project (but may have Author by Email permission). This gives administrators the ability to more strictly control the content of comments posted by users who are not otherwise authors or editors of primary content. (For example, a project may serve as part of a public facing blog that is published by one set of users, and is commented upon by another set of users.)

Received Email Content Default (None)

This set of transformers is applied to content that is received by email from any user who has Author by Email permission in the target project, but does not also have any standard Author or Edit permissions in that project (but may have Comment permission). This gives administrators the ability to more strictly control the content of articles received via email from users who are not otherwise contributors of content. (For example, a project may have a mailbox that serves as a drop box for users to post content to a project that they may not even be able to access in any fashion.) This set of transformers is run after running the plain or rich text content transformer.

Other Input Transformations

Ingested Feed Content Default (None)

This set of transformers, run before the normal rich or plaintext transforms, is applied to content that is ingested via Traction's FeedReader.

Simplifying Content Default (Simplify HTML)

This set of transformers is applied to entry content when a user explicitly asks for Traction to simplify it (i.e., normalize and clean up potentially messy markup). Ideally, the transformations that should be applied are exactly those that would be applied if the user were submitting the content so that the user will be able to tell exactly what their content will look like after being submitted.

Setting Input Transformations

Setting Values Default (Sanitize Setting Values)

This set of transformers is applied to any setting value that is submitted from a free-text form field.

Text-only Setting Values Default (Sanitize Text-only Setting Values)

This set of transformers is applied to any setting value submitted from a free-text form field that must be text only. The values are usually those that will be displayed verbatim somewhere in generated HTML documents.

Runtime Transformations

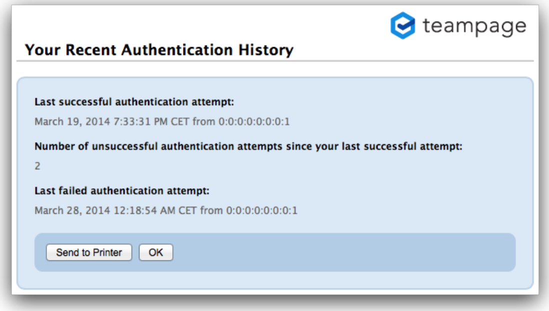
Runtime URL Parameter Values Default (Sanitize Incoming URL Parameter Values)

This set of transformers is applied to each URL parameter value in any GET or POST URL addressed to the Traction server.

Displaying Important Login Information

4.14 The designer will ensure the application has a capability to notify the user of important login information. (APP3660 CAT III)

When logging in directly, after successful authentication, TeamPage can be configured to show a screen with the required information.



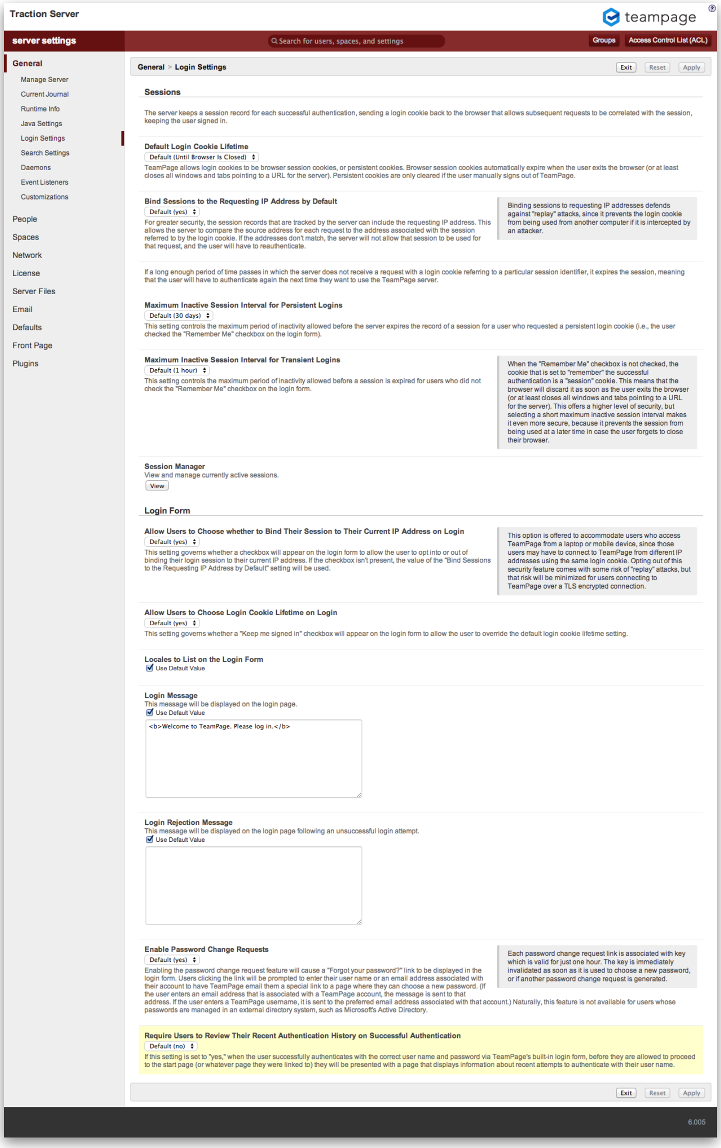
Your Recent Authentication History

Last successful authentication attempt:
March 19, 2014 7:33:31 PM CET from 0:0:0:0:0:0:0:1

Number of unsuccessful authentication attempts since your last successful attempt:
2

Last failed authentication attempt:
March 28, 2014 12:18:54 AM CET from 0:0:0:0:0:0:0:1

To enable the display of this screen, change this setting from *Default (no)* to *yes*.



General > Login Settings

Sessions

The server keeps a session record for each successful authentication, sending a login cookie back to the browser that allows subsequent requests to be correlated with the session, keeping the user signed in.

Default Login Cookie Lifetime
Default (Until Browser Is Closed)
TeamPage allows login cookies to be browser session cookies, or persistent cookies. Browser session cookies automatically expire when the user exits the browser (or at least closes all windows and tabs pointing to a URL for the server). Persistent cookies are only cleared if the user manually signs out of TeamPage.

Bind Sessions to the Requesting IP Address by Default
Default (yes)
For greater security, the session records that are tracked by the server can include the requesting IP address. This allows the server to compare the source address for each request to the address associated with the session referred to by the login cookie. If the addresses don't match, the server will not allow that session to be used for that request, and the user will have to reauthenticate.

Binding sessions to requesting IP addresses defends against "replay" attacks, since it prevents the login cookie from being used from another computer if it is intercepted by an attacker.

If a long enough period of time passes in which the server does not receive a request with a login cookie referring to a particular session identifier, it expires the session, meaning that the user will have to authenticate again the next time they want to use the TeamPage server.

Maximum Inactive Session Interval for Persistent Logins
Default (30 days)
This setting controls the maximum period of inactivity allowed before the server expires the record of a session for a user who requested a persistent login cookie (i.e., the user checked the "Remember Me" checkbox on the login form).

Maximum Inactive Session Interval for Transient Logins
Default (1 hour)
This setting controls the maximum period of inactivity allowed before a session is expired for users who did not check the "Remember Me" checkbox on the login form.

When the "Remember Me" checkbox is not checked, the cookie that is set to "remember" the successful authentication is a "session" cookie. This means that the browser will discard it as soon as the user exits the browser (or at least closes all windows and tabs pointing to a URL for the server). This offers a higher level of security, but selecting a short maximum inactive session interval makes it even more secure, because it prevents the session from being used at a later time in case the user forgets to close their browser.

Session Manager
View and manage currently active sessions.
View

Login Form

Allow Users to Choose whether to Bind Their Session to Their Current IP Address on Login
Default (yes)
This setting governs whether a checkbox will appear on the login form to allow the user to opt into or out of binding their login session to their current IP address. If the checkbox isn't present, the value of the "Bind Sessions to the Requesting IP Address by Default" setting will be used.

This option is offered to accommodate users who access TeamPage from a laptop or mobile device, since those users may have to connect to TeamPage from different IP addresses using the same login cookie. Opting out of this security feature comes with some risk of "replay" attacks, but that risk will be minimized for users connecting to TeamPage over a TLS encrypted connection.

Allow Users to Choose Login Cookie Lifetime on Login
Default (yes)
This setting governs whether a "Keep me signed in" checkbox will appear on the login form to allow the user to override the default login cookie lifetime setting.

Locales to List on the Login Form
☑ Use Default Value

Login Message
This message will be displayed on the login page.
☑ Use Default Value

```
<b>Welcome to TeamPage. Please log in.</b>
```

Login Rejection Message
This message will be displayed on the login page following an unsuccessful login attempt.
☑ Use Default Value

Enable Password Change Requests
Default (yes)
Enabling the password change request feature will cause a "Forgot your password?" link to be displayed in the login form. Users clicking the link will be prompted to enter their user name or an email address associated with their account to have TeamPage email them a special link to a page where they can choose a new password. (If the user enters an email address that is associated with a TeamPage account, the message is sent to that address. If the user enters a TeamPage username, it is sent to the preferred email address associated with that account.) Naturally, this feature is not available for users whose passwords are managed in an external directory system, such as Microsoft's Active Directory.

Each password change request link is associated with key which is valid for just one hour. The key is immediately invalidated as soon as it is used to choose a new password, or if another password change request is generated.

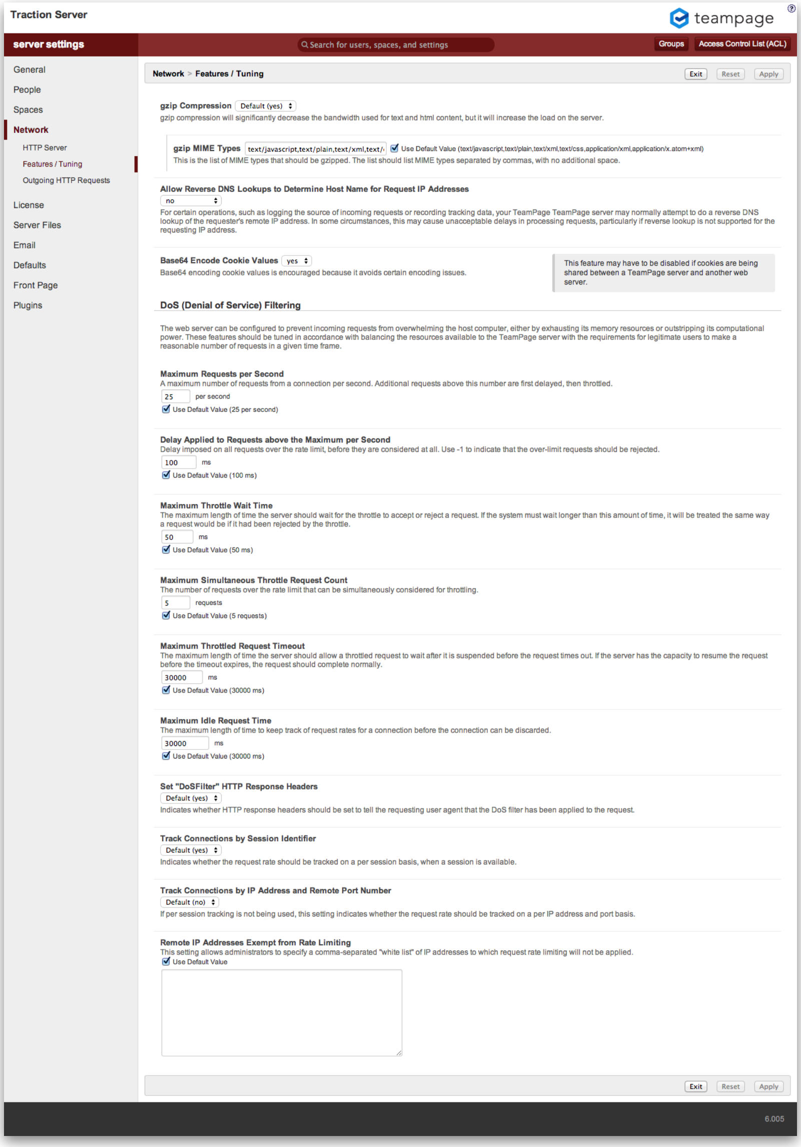
Require Users to Review Their Recent Authentication History on Successful Authentication
Default (no)
If this setting is set to "yes," when the user successfully authenticates with the correct user name and password via TeamPage's built-in login form, before they are allowed to proceed to the start page (or whatever page they were linked to) they will be presented with a page that displays information about recent attempts to authenticate with their user name.

Customizing Denial of Service Mitigation

The following requirement addresses

> 5.1 The designer will ensure the application provides a capability to limit the number of logon sessions per user and per application. (APP3410 CAT II)

Denial of service filtering is enabled by default. You can configure the default settings as needed for your deployment using the *Server Settings* > *Network* > *Features/ Tuning* > *DoS Filtering* controls.



Network > Features / Tuning

gzip Compression Default (yes)
gzip compression will significantly decrease the bandwidth used for text and html content, but it will increase the load on the server.

gzip MIME Types text/javascript,text/plain,text/xml,text/ ☑ Use Default Value (text/javascript,text/plain,text/xml,text/css,application/xml,application/x.atom+xml)
This is the list of MIME types that should be gzipped. The list should list MIME types separated by commas, with no additional space.

Allow Reverse DNS Lookups to Determine Host Name for Request IP Addresses
no
For certain operations, such as logging the source of incoming requests or recording tracking data, your TeamPage TeamPage server may normally attempt to do a reverse DNS lookup of the requester's remote IP address. In some circumstances, this may cause unacceptable delays in processing requests, particularly if reverse lookup is not supported for the requesting IP address.

Base64 Encode Cookie Values yes
Base64 encoding cookie values is encouraged because it avoids certain encoding issues.

This feature may have to be disabled if cookies are being shared between a TeamPage server and another web server.

DoS (Denial of Service) Filtering

The web server can be configured to prevent incoming requests from overwhelming the host computer, either by exhausting its memory resources or outstripping its computational power. These features should be tuned in accordance with balancing the resources available to the TeamPage server with the requirements for legitimate users to make a reasonable number of requests in a given time frame.

Maximum Requests per Second
A maximum number of requests from a connection per second. Additional requests above this number are first delayed, then throttled.
25 per second
☑ Use Default Value (25 per second)

Delay Applied to Requests above the Maximum per Second
Delay imposed on all requests over the rate limit, before they are considered at all. Use -1 to indicate that the over-limit requests should be rejected.
100 ms
☑ Use Default Value (100 ms)

Maximum Throttle Wait Time
The maximum length of time the server should wait for the throttle to accept or reject a request. If the system must wait longer than this amount of time, it will be treated the same way a request would be if it had been rejected by the throttle.
50 ms
☑ Use Default Value (50 ms)

Maximum Simultaneous Throttle Request Count
The number of requests over the rate limit that can be simultaneously considered for throttling.
5 requests
☑ Use Default Value (5 requests)

Maximum Throttled Request Timeout
The maximum length of time the server should allow a throttled request to wait after it is suspended before the request times out. If the server has the capacity to resume the request before the timeout expires, the request should complete normally.
30000 ms
☑ Use Default Value (30000 ms)

Maximum Idle Request Time
The maximum length of time to keep track of request rates for a connection before the connection can be discarded.
30000 ms
☑ Use Default Value (30000 ms)

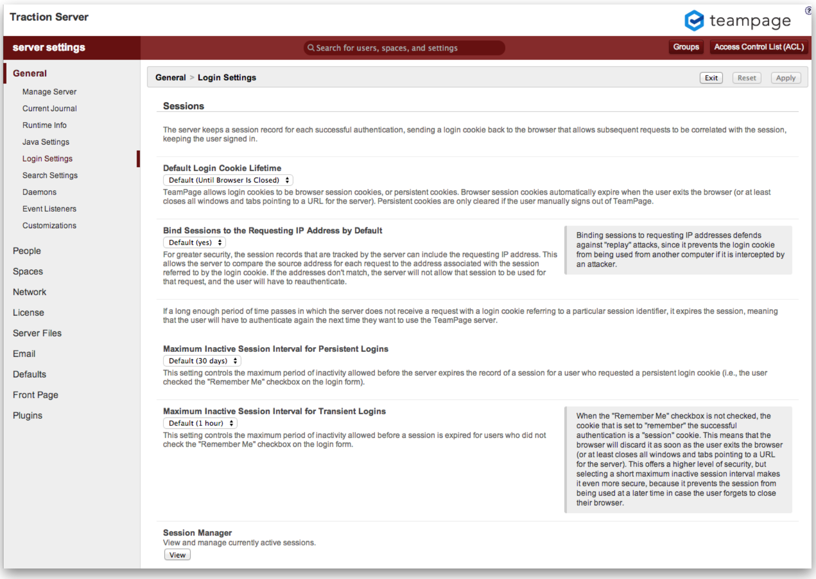
Set "DoSFilter" HTTP Response Headers
Default (yes)
Indicates whether HTTP response headers should be set to tell the requesting user agent that the DoS filter has been applied to the request.

Track Connections by Session Identifier
Default (yes)
Indicates whether the request rate should be tracked on a per session basis, when a session is available.

Track Connections by IP Address and Remote Port Number
Default (no)
If per session tracking is not being used, this setting indicates whether the request rate should be tracked on a per IP address and port basis.

Remote IP Addresses Exempt from Rate Limiting
This setting allows administrators to specify a comma-separated "white list" of IP addresses to which request rate limiting will not be applied.
☑ Use Default Value

Additional protections can be achieved by shortening sessions and binding them to the IP address of the user's computer. These controls are on this admin page:



General > Login Settings

Sessions

The server keeps a session record for each successful authentication, sending a login cookie back to the browser that allows subsequent requests to be correlated with the session, keeping the user signed in.

Default Login Cookie Lifetime

Default (Until Browser Is Closed)

TeamPage allows login cookies to be browser session cookies, or persistent cookies. Browser session cookies automatically expire when the user exits the browser (or at least closes all windows and tabs pointing to a URL for the server). Persistent cookies are only cleared if the user manually signs out of TeamPage.

Bind Sessions to the Requesting IP Address by Default

Default (yes)

For greater security, the session records that are tracked by the server can include the requesting IP address. This allows the server to compare the source address for each request to the address associated with the session referred to by the login cookie. If the addresses don't match, the server will not allow that session to be used for that request, and the user will have to reauthenticate.

Binding sessions to requesting IP addresses defends against "replay" attacks, since it prevents the login cookie from being used from another computer if it is intercepted by an attacker.

If a long enough period of time passes in which the server does not receive a request with a login cookie referring to a particular session identifier, it expires the session, meaning that the user will have to authenticate again the next time they want to use the TeamPage server.

Maximum Inactive Session Interval for Persistent Logins

Default (30 days)

This setting controls the maximum period of inactivity allowed before the server expires the record of a session for a user who requested a persistent login cookie (i.e., the user checked the "Remember Me" checkbox on the login form).

Maximum Inactive Session Interval for Transient Logins

Default (1 hour)

This setting controls the maximum period of inactivity allowed before a session is expired for users who did not check the "Remember Me" checkbox on the login form.

When the "Remember Me" checkbox is not checked, the cookie that is set to "remember" the successful authentication is a "session" cookie. This means that the browser will discard it as soon as the user exits the browser (or at least closes all windows and tabs pointing to a URL for the server). This offers a higher level of security, but selecting a short maximum inactive session interval makes it even more secure, because it prevents the session from being used at a later time in case the user forgets to close their browser.

Session Manager

View and manage currently active sessions.

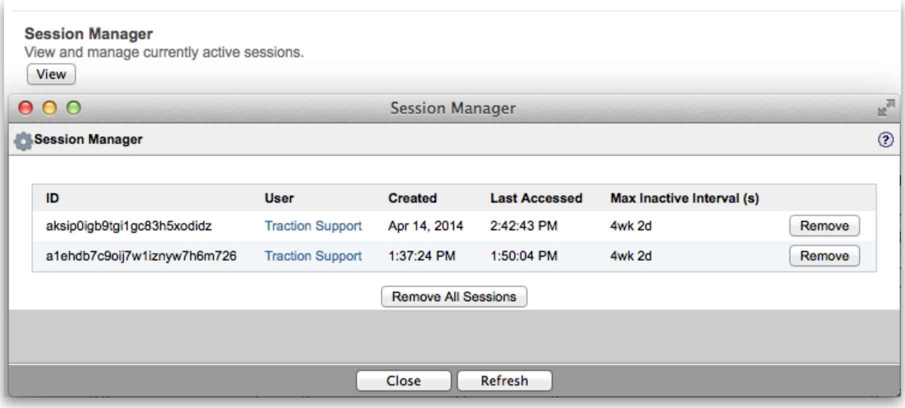
View

Terminating Sessions

5.2 The designer will ensure the application provides a capability to automatically terminate a session and log out after a system defined session idle time limit is exceeded. (APP3415 CAT II)

The session idle time is controlled by the session settings shown above.

To terminate an active session, open the session manager by clicking the View button.



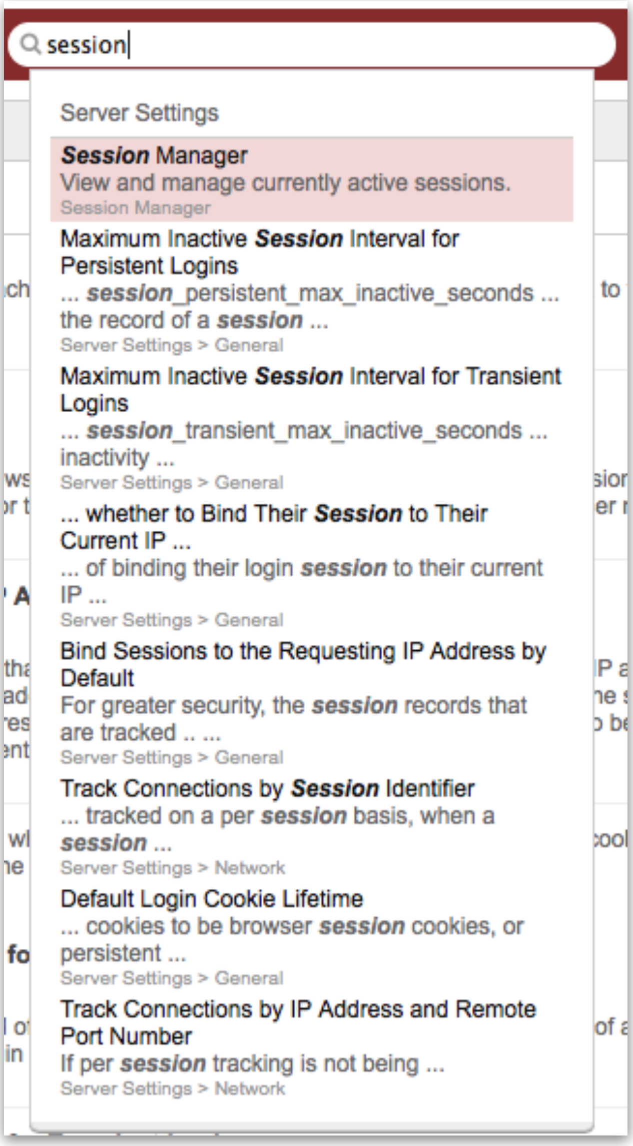
Session Manager

View and manage currently active sessions.

ID	User	Created	Last Accessed	Max Inactive Interval (s)	
aksip0igb9tgi1gc83h5xodidz	Traction Support	Apr 14, 2014	2:42:43 PM	4wk 2d	Remove
a1ehdb7c9oij7w1iznyw7h6m726	Traction Support	1:37:24 PM	1:50:04 PM	4wk 2d	Remove

To immediately terminate the session, click the Remove button next to the session you wish to terminate.

Tip: You can also access any admin view or settings by typing a few characters of its name into the search box at the top of the setup pages.



session

Server Settings

Session Manager
View and manage currently active sessions.
Session Manager

Maximum Inactive ***Session*** Interval for Persistent Logins
... ***session***_persistent_max_inactive_seconds ... the record of a ***session*** ...
Server Settings > General

Maximum Inactive ***Session*** Interval for Transient Logins
... ***session***_transient_max_inactive_seconds ... inactivity ...
Server Settings > General

... whether to Bind Their ***Session*** to Their Current IP ...
... of binding their login ***session*** to their current IP ...
Server Settings > General

Bind Sessions to the Requesting IP Address by Default
For greater security, the ***session*** records that are tracked .. ...
Server Settings > General

Track Connections by ***Session*** Identifier
... tracked on a per ***session*** basis, when a ***session*** ...
Server Settings > Network

Default Login Cookie Lifetime
... cookies to be browser ***session*** cookies, or persistent ...
Server Settings > General

Track Connections by IP Address and Remote Port Number
If per ***session*** tracking is not being ...
Server Settings > Network