Adapt Delta Release Notes

2023.3 (December 2023)

Adapt Engine 2023.3 Release has been tested on the following browsers: Chrome 93.0 and above, and Firefox 92. Compatibility mode in browsers must be turned off.

Note: Once you have the 2023.3 delta in place, please clear your *Browser Cache* before logging in.

Security Enhancements

2023.3 Description	Release Notes	Issue ID
Stored XSS in calendar event on month view.	A potential security issue was fixed, where an XSS exploit could have been initiated via a maliciously created calendar entry in the month view.	AD-12732
Cross-Tenant Access Control Issue - Calendar Appointments Access.	A potential security issue was fixed, where a request could have been forged to give you access to calendars in a domain you have no access to.	AD-12718
Password Reset Poisoning Leads to Account Take Over	A potential security issue was fixed, where it might have been possible to spoof a password reset link that could be used to hijack a user account. **NOTE:** Your system administrator will need to specify the host URL that password requests will be sent to by setting a value in one of two locations in SysAdmin: • This can be set globally for all domains under *System* > *System Settings* > *Installation Properties* > *System Properties*. • If you have a domain-specific host name, this can be set on a per-domain basis with the second setting in *Domains* > *Domain Settings*. Password reset links will no longer work unless a host URL is specified.	AD-12715

Unauthenticated File Download	A potential security issue was fixed, where a URL to load a report from the reporting server could be used from another browser without logging into Adapt.	AD-12705
Stored XSS on User > Users > [Multiple Locations].	A potential security issue was fixed, where a number of places in the SysAdmin Users section were vulnerable to an XSS exploit.	AD-12669
Stored XSS on Add Document [Multiple Locations].	A potential security issue was fixed, where an XSS vulnerability could be triggered by uploading a compromised document to the document library that would run javascript when the document was previewed. All HTML and PDF documents will now be sanitized for preview, removing all javascript. This does not modify the original document; it just modifies a copy used solely for preview purposes.	AD-12665
XSS in quickfind and workstack entries.	A potential security issue was fixed, where an exploit could occur when malicious content was displayed in popups for quickfind and workstack entries.	AD-12641
Stored XSS in Domains-Templates.	A potential security issue was fixed, where document template names could be used as an XSS exploit.	AD-12636
Implement CSRF for SysAdmin Users section.	CSRF security has been implemented for functionality in the Users section of SysAdmin.	AD-12586
Parent Company QuickFind: Excess characters appear on the workflow when using XSS injections.	A potential security issue that could allow an XSS exploit has been fixed.	AD-12699
Stored XSS in Domains > NextClarkRecruitment > Data Admin Profiles.	A potential security issue that could allow an XSS exploit has been fixed.	AD-12672
Stored XSS in Domains > NextClarkRecruitment > Mailboxes.	A potential security issue that could allow an XSS exploit has been fixed.	AD-12671
Stored XSS in searchName field	A potential security issue that could allow an XSS exploit has been fixed.	AD-12680

Stored XSS in the "Permanent Candidate" names triggering when searching them via Fastfind.	A potential security issue that could allow an XSS exploit has been fixed.	AD-12545
Reflected XSS in SysAdmin report settings	A potential security issue that could allow an XSS exploit has been fixed.	AD-12559
Gather Client OS/browser information when logging into Adapt and before starting ADA	The audit trail logging has been enhanced to include details of which Operating System users are using ADA from. This is included in the output of the login audit trail. To see this, the audit trail must be enabled.	AD-12656
Reflected XSS on Search Bar	A potential security issue that could allow for XSS injection has been fixed.	AD-12664
Add Login/Password Reset Logging Options	The audit trail has been extended to offer a new option to log all password reset requests, along with the IP address they came from. To see this, the audit trail must be enabled. This also requires you to run the appropriate database update script, e.g. V2022.1-mssql-users-dbupgrade.sql for SQLServer	AD-12660

Issue Fixes

2023.3 Description	Release Notes	Issue ID
Chrome browser version 118 handles SPAN field incorrectly.	Google Chrome update 118 changed the way Chrome parses XML containing CDATA segments, which has led to XML responses from the span validator servlet appearing to return one value instead of two, as Chrome has merged the text tags. This has been resolved.	AD-12745
SysAdmin create-modify user doesn't set a default for profiles.	An issue was resolved where, when creating a new user, if domain profiles were added but one was not marked as the default, the user would not be able to log in. The first item will now be set as the default if nothing else is selected.	AD-12741
Corporation can be inactivated despite warning.	An issue was resolved that occurred when modifying the status of a checkbox via a	AD-12733

	businessobject when the checkbox also had an onmodify listener. The checkbox displayed correctly but the changes weren't reflected in the entity's datamodel when the entity was saved.	
Cannot set an email address for entity print notification in SysAdmin domain settings.	An issue was resolved in the SysAdmin domain settings *Print Notification* section, which prevented an email address from being set for entity print notifications.	AD-12731
SysAdmin Users Domain Access - Default Profile is not set correctly each time.	An issue was resolved where, when setting the default domain for a user, the value was correctly set in the database, but the cache update happened outside of the main transaction, meaning the value was not always set correctly.	AD-12730
Users created in Sys Admin have passwords stored incorrectly.	An issue was resolved where, when creating a new user in SysAdmin, their initial password was getting encrypted twice. This caused an incorrect value to be stored in the database, preventing the user from logging in until the password was changed again.	AD-12701
Issue with Tempdesk and Multidrop booking	An issue was found where if you selected multiple candidates - or a single candidate but multiple days - from the bottom table, you could only drop them into the first timeslot in the shifts in the top table. This has now been addressed, and the drop process will prioritize filling shifts that are equal to or later than the drop target's timeslot. This is carried across the table, so on consecutive days it will try to match the drop target's time or later, wrapping around to the earlier shifts if one at the drop time isn't available.	AD-11686
Dropdown/Flyout Menus Closing Too Quickly	The recent iframe removal work caused an issue that led to the batch menu on searches sporadically closing when you navigated between options. This has now been resolved. **Note**: This issue only affected menu elements that had a child submenu, so was only seen on the US config and not seen on the UK standard config.	AD-12692

Users unable to delete tasks in their tasks list that they did not create	An issue was caused by a recent security fix which meant that users could not delete tasks assigned to them that they did not create, e.g. where another user created a task and added you to the "assigned to" list. Now, when you delete such a task, the task is not deleted, but you are unassigned from it, so it no longer appears in your task list.	AD-12661
Calendar - Settings allow you to view other user's calendar not in your user group even though profile dictates otherwise	An issue was resolved with calendar viewing permissions, which occurred when the "see group/see all" options were enabled in SysAdmin for a particular domain profile.	AD-12662
CV Import Duplicate Checker fails to load if the user navigates away during/after the parsing process	An issue was resolved where, if you navigated away from the CV import duplicate checker on finding a potential duplicate record already exists, when returning to the CV import page, you were no longer able to import the CV.	AD-12659
Accessing a Link in formatter tool in SysAdmin gives blank list of available fields	An issue was resolved where extra CSRF security checks had blocked a request that should have been allowed.	AD-12658