Cookie Policy Notice

digitate.com/cookie-policy-notice

Tata Consultancy Services Limited/Digitate uses cookies (small text files placed on your device) and similar technologies to provide Digitate websites (digitate.com, studio.digitate.com, studiov1.digitate.com, store.digitate.com) and to help collect data. The text in a cookie often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well.

Our Use of Cookies and Similar Technologies.
Tata Consultancy Services/Digitate uses cookies and similar technologies for several purposes, which may include:

- Storing your Preferences and Settings. Settings that enable our website to operate correctly or that maintain your preferences over time may be stored on your device.
- Sign-in and Authentication. When you sign into our website using your credentials, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- Security. We use cookies to detect fraud and abuse of our websites and services.

In addition to the cookies Tata Consultancy Services/Digitate sets when you visit our websites, third parties may also set cookies when you visit Tata Consultancy Services'/Digitate sites. In some cases, that is because we have hired the third party to provide services on our behalf. We use cookies from Google reCAPTCHA to prevent abuse of the website and enhance its security (read Google's privacy policy). Tata Consultancy Services/Digitate sets cookies that are technical and necessary for the function of the website(s), for example, that allow you to browse the website and use the different options included in this for the management of the website(s) and enable its functions and services, such as controlling data traffic and communication, identifying the session, managing payment, controlling any fraud linked to service security, completing event sign up or participation requests, counting visits for the purposes of invoicing the licenses for the software/products which allow the service to operate (website, platform or application or products), using safety elements during browsing, storing contents for video or audio broadcasting, enabling dynamic contents (for example, loading animation for a text or image) or share contents in social media.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the main reasons we typically set cookies. If you visit one of our websites, the site may set some or all of the following cookies:

Cookie Name	Description	Cookie Category	Website Name	Expiry
STUDIO_ID	This cookie is used by the application to manage the browsing session	First Party – Strictly Necessary	studio.digitate.com	Session
XSRF-TOKEN	This cookie is used for securing the application from cross site request forgery	First Party – Strictly Necessary	studio.digitate.com	Session
ApplicationGatewayAffinity	This cookie is used by the Application Gateway to maintain sticky session.	First Party – Strictly Necessary	studio.digitate.com	Session

ApplicationGatewayAffinityCORS	This cookie is used by the Application Gateway in addition to ApplicationGatewayAffinity to maintain sticky session even on cross-origin requests.	First Party – Strictly Necessary	studio.digitate.com	Session
userLanguage	This cookie is used by application to keep the user preferred language during the browsing session	First Party – Strictly Necessary	studio.digitate.com	Session
STUDIOID	This cookie is used by the application to manage the browsing session	First Party – Strictly Necessary	studiov1.digitate.com	Session
ApplicationGatewayAffinity	This cookie is used by the Application Gateway to maintain sticky session.	First Party – Strictly Necessary	studiov1.digitate.com	Session
ApplicationGatewayAffinityCORS	This cookie is used by the Application Gateway in addition to ApplicationGatewayAffinity to maintain sticky session even on cross-origin requests.	First Party – Strictly Necessary	studiov1.digitate.com	Session
ApplicationGatewayAffinity	This cookie is used by the Application Gateway to maintain sticky session.	First Party – Strictly Necessary	store.digitate.com	Session
ApplicationGatewayAffinityCORS	This cookie is used by the Application Gateway in addition to ApplicationGatewayAffinity to maintain sticky session even on cross-origin requests	First Party – Strictly Necessary	store.digitate.com	Session
__sT	This cookie is used by the application to manage the browsing session	First Party – Strictly Necessary	store.digitate.com	Session
__xT	This cookie is used for securing the application from cross site request forgery	First Party – Strictly Necessary	store.digitate.com	Session
__utma	Used to distinguish users and sessions. The cookie is created when the javascript library executes and no existing __utma cookies exists. The cookie is updated every time data is sent to Google Analytics.	First Party – Strictly Necessary	digitate.com	Session
__utmt	Used to throttle request rate.	First Party – Strictly Necessary	digitate.com	Session

__utmb	Used to determine new sessions/visits. The cookie is created when the javascript library executes and no existing __utmb cookies exists. The cookie is updated every time data is sent to Google Analytics.	First Party – Strictly Necessary	digitate.com	Session
__utmc	Not used in ga.js. Set for interoperability with urchin.js. Historically, this cookie operated in conjunction with the __utmb cookie to determine whether the user was in a new session/visit.	First Party – Strictly Necessary	digitate.com	Session
__utmz	Stores the traffic source or campaign that explains how the user reached your site. The cookie is created when the javascript library executes and is updated every time data is sent to Google Analytics.	First Party – Strictly Necessary	digitate.com	Session
__utmv	Used to store visitor-level custom variable data. This cookie is created when a developer uses the _setCustomVar method with a visitor level custom variable. This cookie was also used for the deprecated _setVar method. The cookie is updated every time data is sent to Google Analytics.	First Party – Strictly Necessary	digitate.com	Session
cookie_notice_accepted	Cookie notice accepted	First Party – Strictly Necessary	digitate.com	Session

How to Control Cookies

You can set your browser:
• To allow all cookies
• To allow only 'trusted' sites to send them
• To accept only those cookies from websites you are currently using.

We recommend not to block all cookies because digitate.com website(s) use those to work properly.

Please read below points to find out how to manage cookies in the major browsers.

Google Chrome:

Click on the “Menu” tab in the upper-right corner and then click on “Settings”.
To block cookies:
Settings → Click on “Advanced” to expand → Under Privacy and Security, Click on “Content Settings” → Click on “Cookies” → To block cookies, Click on toggle button next to this line “Allow sites to save and read cookie data (recommended)“ → This will block the cookies.
To check cookies:
Settings → Click on “Advanced” to expand → Under Privacy and Security → Click on “Content Settings” → Click on “Cookies” → See all cookies and site data → Click on the website and check the cookies used in that particular site.

Mozilla Firefox:

Click on the Menu tab in the upper-right corner → Click on Options → In the left side navigation, Click on Privacy and Security → Under History, Select “Use Custom setting for history” from the Drop down → Click on Show Cookies Buttons → Select the file which you want to remove and then click on remove selected button.

Internet Explorer:

Open Internet Explorer → Click on Tools menu in the upper-right corner → Click on Internet Options → This will open a window with many tab → Click on Privacy tab → Under Settings, move the slider to the top to block all cookies or to the bottom to allow all cookies → Then click Apply.
Open Internet Explorer → Click on Tools menu in the upper-right corner → Click on Internet Options → This will open a window with many tabs → Click on Privacy tab → Click on Sites button → Enter site name and then click Allow or Block button → If user clicks block button, that website is not allowed to use cookies in IE → Then click Apply.

Safari:

Open Safari → Click on Preferences from Safari menu → Go to Privacy tab → Click on “Remove all Website data” to remove all the stored data → Click Remove now button from the pop-up → Click on Details button under “Remove all Website data” → Select the sites you want to remove the data → Click Remove → Click Done.
To find information relating to other browsers, visit the browser developer’s website.