**Feasibility Study Document on Tableau**

**Purpose:**

To understand the minimal basic requirements to incorporate Tableau for development and sharing.

**Index:**

1. Comparison between Tableau Online and Tableau Server
2. Online Sync Client
3. Tableau Online Security
4. Tableau Server Security
5. Pricing
6. **Comparison between Tableau Online and Tableau Server**

**Note**: Both Tableau Online and Tableau Server require **Tableau Desktop Professional Edition** for developing and publishing tableau visualizations and workbooks (views and dashboards) and data sources.

Tableau Server is an installed version of Tableau online.

Note: Red color are the cons.

|  |  |  |
| --- | --- | --- |
| **Features** | **Tableau Online** | **Tableau Server** |
| Hardware and system requirements | Hardware and systems maintained by Tableau, outside of your firewall. | You install the software and maintain the systems on your own hardware, inside or outside your company firewall. |
| Users and Permissions | You can purchase and maintain multiple sites, configure users and permissions. | You can create and maintain multiple sites at no additional cost, configure users and permissions. |
| Live Data – Set Connections | Supports live data connections to Amazon Redshift, Google Big-Query, as well as to SQL-based sources hosted on cloud platforms. | Supports live connections to your local data sources and to Google Big-Query and Amazon Redshift. Supports published extracts. |
| Scheduling extracts refresh data – set activities. | Scheduled refreshes for published data: For complete information, see Keep Data Fresh in the Tableau Online Help.   * For extracts of cloud-based data sources, you can schedule refresh tasks directly on Tableau Online. * For extracts of data sources that you maintain on your local network, or for Oracle data hosted in the cloud, or on-Premise data like excels, flat files, SQL server DB’s, you can schedule refresh tasks using the Online sync client that comes with Tableau Desktop. Schedules can be as frequent as every 15 minutes. * You can also update extracts manually using Tableau Desktop, or automate updates using a command-line utility. Select a pre-configured schedule or create a custom schedule. | You can schedule refresh tasks for published extracts. Select a pre-configured schedule or create a custom schedule. |
| Authentication | Authenticate users through Tableau ID (email address and password) or configure a site for single sign-on using SAML. No Guest Access. | Can be configured for local authentication, Active Directory integration, trusted authentication, or single sign-on using SAML or Kerberos. |
| Access Tableau Workbooks | All users accessing views and dashboards published to Tableau Online must be authenticated. | Provides Core Licensing option, which allows guest access. |
| Branding | Custom branding: upload your company logo. | Custom branding: change the logo and the company name that appears in various web browser locations and tooltips. |

1. **Online Sync Client for Tableau Online:**

Gives you the flexibility to leverage behind-the-firewall data sources and on-Premises data sources like locally hosted SQL Db, Excel and Flat Files to keep them fresh.

Requirements to configure online sync client for refreshing extracts/on premise data on Tableau online

* Must have a Site Administrator access role on tableau online
* Need to run the online sync client on 'Service mode' which require to be a local administrator of the computer/machine it is running (Tableau Desktop) on.
* Must be a 64 bit Windows Machine.
* The computer/ machine on which online sync client is installed must be running continuously.

1. **Tableau Online Security:**

Data published to Tableau Online is protected by enterprise-level security features that include:

• Operational security

• Data security and privacy

• Account security

• Security of data in transit

• Application security

* + 1. **Operational Security**
       1. **SOC 2 and ISAE 3402**

Each year, Tableau works with an independent Certified Public Accounting firm to perform an in-depth audit of the control objectives and activities for Tableau Online. Tableau is proud to announce that the control procedures for our Tableau Online service have been verified in a SOC 2 Type II report prepared under terms of the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance Engagements (ISAE) No. 3402. The Tableau Online SOC 2 Type II report is available upon request.

* + 1. **Data Security and Privacy**
       1. **Privacy Shield**

With respect to personal data relating to residents of the European Economic Area (EEA), Tableau is a certified Active Participant in the Privacy Shield Framework and is subject to the investigative and enforcement powers of the Federal Trade Commission.

* + - 1. **Backup and Recovery**

Backups are made of all critical components. Backup media is encrypted and always maintained in a secured facility. Disk-based backups are stored in secured data center facilities. Backups made to external backup providers are encrypted in transit and in storage. Only approved system administrators have access to backups.

Per Tableau Online backup policy, daily backups are retained for 31 days.

* + - 1. **Data Governance**

Your data is your own, even when stored in Tableau Online. Only individuals you authorize have access to data or workbooks stored in your site—Tableau employees and other customers do not have access to your data. The only exception is a small and controlled number of trusted Tableau administrators that are responsible for managing the systems that run the service. There is a documented process for authorizing users with this level of access, and all administrative-level access is reviewed and approved on a quarterly basis.

Something to keep in mind is that the bulk of your data remains securely stored in your own data sources. Only workbooks, data extracts and cached data are stored within Tableau Online.

Tableau does have access to, and may monitor, metrics that have to do with system utilization, account status, and performance. Such metrics include:

• Total storage used by account and by user

• Total bandwidth used by account and by user

• Total number of workbooks and views by account and by user

• Access dates and times by user (logins)

• Number and type of data sources (e.g., SQL Server, Salesforce.com) by account and by user

• Dates and times of data refresh by account and by user

• Site performance metrics

**Data enters Tableau Online in one of four ways:**

1. By publishing a workbook with the data embedded in it.

2. By “pushing” data from an on premises source to a Tableau data extract. This method always results in a data extract, not a real-time connection, so there is no need to create a virtual private network (VPN) or secure tunnel into your corporate environment. For data sources that Tableau Online cannot reach directly, you can publish data extracts and use the Tableau Online sync client to schedule automatic refreshes.

3. Connecting to a web service via an application programming interface (API). For most cloud data sources, such as Salesforce.com and Google Analytics, the API connection is used to generate data extracts which can be scheduled to update regularly.

4. Direct connection to data hosted on a cloud platform. For these data sources, Tableau Online can create a real time live connection or one that is extract-based.

* + 1. **User Security**

**Access and Authentication**

Only users you explicitly add to your site have access to your content and workbooks. Administrators that you designate are responsible for all account management functions including adding and removing users and assigning permissions. Account management is completely in your control. If a user is no longer authorized in your site, simply remove them and they will no longer have access to content stored in Tableau Online.

There are two methods of authentication available within Tableau Online and you have the flexibility to configure your site to use one or both of them.

1. **Tableau Account**

Tableau Accounts are used by default and are secured in a Tableau-maintained identity store. This method of authentication provides site administrators the ability to quickly configure users without the need to integrate with a separate identity provider. The accounts are managed by customers and enable secure authentication to Tableau Online. The account is also used to access other Tableau services and resources such as the Tableau Website, Tableau Customer/Partner Portal, and Tableau Forums.

Users are authenticated using their email address as the username and a user-selected password. When administrators add users to their site, an email is sent to the user with instructions on how to setup their password.

Administrators do not set user passwords nor can they retrieve stored passwords. Passwords are salted and hashed using a strong hashing algorithm.

Accounts are locked out after 10 failed attempts for a period of 10 minutes and the lockout time doubles for each successive lockout. A user may have no more than five concurrent sessions which timeout after eight hours.

Passwords are required to be a minimum of eight characters in length and must include letters and numbers.

1. **SAML**

SAML allows administrators to configure their site for single sign on using their own SAML 2.0 capable identity provider (IdP). For additional information refer to the Site Authentication section of the Online Product Guide.

Note: Features related to SAML and single sign-on are currently only available by request. To request these features, contact Tableau Support.

Tableau Online enforces a session time-out after a two hour period of inactivity.

**Roles and Permissions**

Access within Tableau Online is controlled through a combination of site roles and permissions. Every user added to Tableau Online must have an associated site role. The site role is assigned by the administrator and determines the levels of permissions allowed for a user, including whether a user can publish, interact with, or only view content published to Tableau Online. Additional details on Site Roles can be found here. Permissions are assigned to content (projects, workbooks, views, and data sources) and can be assigned to individual users or groups. When you specify permissions, you use rules to specify who is allowed to work with that content.

Permissions can be used to grant permissions such as create, view, modify, and delete. Permissions assigned to a projects control the default access level all workbooks and views published to the project. Administrators can create groups such as “Finance Users” to make permission management easier.

* + 1. **Transmission (Network) Security**
       1. **Encryption**

All communication between the client (Tableau Desktop or a supported browser) and Tableau Online is encrypted using TLS which provides protection of data in transit.

Connections to data sources may or may not be encrypted based on encryption capabilities of the data source. Customers should understand the encryption options available for the data sources they plan to use.

In addition, Tableau products have many built-in security mechanisms to help prevent spoofing, hijacking, and SQL injection attacks. Tableau also actively tests its products for vulnerabilities and responds to new threats with regular updates.

* + - 1. **Application Security**

Application security is a combination of secure design practices that include defining security requirements, threat modeling, code reviews, and security testing. Automated and manual

Vulnerability testing is done as a part of the development process and third-party security firms are leveraged to conduct penetration testing of applications prior to major releases. Tableau is committed to working with third-party security experts to test, discover, validate, and address security concerns.

Additionally, Tableau has implemented a third-party vulnerability scanning service that continuously scans the company’s Internet-facing resources and services for vulnerabilities including Tableau Online. Any findings generate an alert which is triaged to assess severity and impact. Priority of any remediation efforts that may be required is based on this assessment.

**Conclusion**

The Tableau Online service is built and operated based on a robust security model that is informed by industry best practices and validated by third party security experts. Tableau understands how important your data is and takes the responsibility to protect it very seriously.

For Further Information please read the Tableau Online Security Whitepaper referring below link:

**https://www.tableau.com/sites/default/files/whitepapers/securityinthecloud.pdf**

1. **Tableau Server Security:**

There are three general components to enterprise application security, and this paper will cover them in greater depth for Tableau Server:

1. Authentication

2. Authorization

3. Network–transmission security

1. **Authentication**

Tableau Server supports several forms of industry standard authentication including Active Directory, LDAP, Kerberos, OpenID Connect, SAML, Trusted Tickets, and certificates. Tableau Server also has its own built-in user identity service called Local Authentication.

Once a user signs in, Tableau Server provides a customizable experience including language and locale, a personalized start page, and an overview of personally-authored content. Tableau Server retains user information across sessions for a consistent personalized experience. Tableau does this by creating and maintaining an account for each named user on the system. In addition, authors and publishers can use server-wide identity information to control the level of authorization other users have to the underlying data for views they publish.

1. **User identity**

As mentioned above, you can manage user identities with Active Directory or by storing them within the server using Local Authentication. We describe the difference between these two methods of managing user authentication below.

1. **Active directory**

When customers choose to integrate Tableau Server with Active Directory as the identity store, Active Directory manages all usernames and passwords.

Even though users and groups are centrally managed by Active Directory, Tableau Server stores a copy of the usernames and groups in its own repository. Tableau does not store passwords when configured for Active Directory authentication. Users and groups can be synchronized with Active Directory either manually by an administrator or programmatically using the **tabcmd** command-line utility or REST API.

1. **Local authentication**

Tableau Server also contains a built-in user management and authentication service called Local Authentication. This method is used by organizations who choose not to use Active Directory or who are deploying to clients external to AD. When using Local Authentication, Tableau Server is responsible for managing users, groups, and the entire authentication process. The administrator has the option of storing passwords on Tableau Server. However, the option to delegate passwords and user information to an external service, such as OpenID or SAML, is also an option. User lists can easily be imported to Tableau Server, and most user management functions can be performed programmatically via tabcmd or REST API. This makes it easy to provision Tableau users as part of your automated provisioning process.

1. **LDAP**

Tableau Server on Linux introduces support for authenticating to any LDAP provider with Windows support coming soon. All of the same authentication and user management features available with an Active Directory server are available for any Directory Service that supports the LDAP protocol and any of the following authentication mechanisms: GSSAPI, simple bind, simple bind with Kerberos. Work with your IT department to determine what works for you.

1. **Single sign-on and integration with external authentication services**

Tableau Server supports several types of single sign-on (SSO) solutions as well as mutual SSL (client certificate authentication).

Mutual SSL provides a secure automatic sign-in experience with Tableau across all devices. With mutual SSL, when a client (Tableau Desktop on Windows, a web browser, or tabcmd.exe) with a valid certificate connects to Tableau Server, Tableau Server confirms the existence of a valid client certificate and automatically signs in the user with the username it finds in the certificate.

With SSO, users don't have to explicitly sign in to Tableau Server. Instead, the credentials they use to authenticate with other external authentication services (for example, signing in to their corporate network) can be used to seamlessly authenticate them onto Tableau Server without prompting a log in screen. SSO establishes the user's identity externally and maps it to a user identity defined in the Tableau Server identity store.

When you configure Tableau Server for use with an external authentication service for SSO, the external authentication service handles all authentication. However, Tableau Server will manage user access to Tableau resources based on the site roles stored in the identity store. See the authorization section below for more details.

1. **Tableau Server supports integration with the following external authentication services:**

**SAML**: You can configure Tableau Server to use SAML (security assertion markup language) for SSO. With SAML, an external identity provider (IdP) authenticates the user's credentials, and then sends a security assertion to Tableau Server that provides information about the user's identity. You can use SAML to access Tableau Server regardless of your Active Directory or local authentication configuration. You can also configure Tableau Server to use a different SAML IdP for each site, known as Site-Specific SAML.

**Kerberos**: If Kerberos is enabled in your environment and Tableau Server is configured to use Active Directory authentication, you can provide users with access to Tableau Server based on their Windows identity. You cannot use Kerberos if your Tableau Server is configured for local authentication.

**Integrated Windows authentication**: If you have Tableau Server configured with Active Directory authentication, you can enable automatic logon. Automatic logon uses Microsoft SSPI to sign in users based on their Windows username and password. Users are not prompted for credentials, which creates an experience similar to single sign-on (SSO) and Kerberos.

**OpenID**: OpenID Connect is a standard authentication protocol that lets users sign in through a compatible identity provider. After they've successfully signed in to their identity provider, they are automatically signed in to Tableau Server. To use OpenID Connect with Tableau Server, the server must be configured to use local authentication; Active Directory authentication is not supported.

**Trusted authentication**: Trusted authentication (also known as trusted tickets) lets you set up a trusted relationship between Tableau Server and one or more web servers. When Tableau Server receives requests from a trusted web server, it assumes that the web server has already handled the necessary authentication. Tableau Server receives the request with a redeemable token or ticket and presents the user with a personalized view which takes into consideration the user’s role and permissions.

**Guest user or anonymous access**

Note: This option is only available with a core-based Tableau Server license.

Tableau Server can be set up to allow anonymous access to views via a guest account. This is useful for deploying content to large user communities such as the public web or to communities where the identity of the user is not required, such as a corporate intranet. The guest license allows users without an account on Tableau Server to see and interact with embedded views.

To prevent accidental anonymous access to sensitive data, the ability to access Tableau Server as a guest is disabled by default. When enabled, the guest license is assigned to an automatically generated guest user. Since guest users are anonymous, meaning there is no way to identify who they are, Tableau provides only a single guest user because they are universal.

Anonymous users can load webpages containing embedded visualizations without ever having to log in to Tableau Server, but you can choose to require credentials to access the intranet or the page hosting the view. Anonymous users cannot browse the repository; they can only access embedded views (URLs that have the: “embed=true” parameter set). For simplicity, if an anonymous user requests a view that does not have the embedded flag, Tableau Server will interpret it as a request for an embedded view. This means that URLs shared via email or linked from other web pages will be properly processed for anonymous users and made accessible. Note that only guest accessible views (as defined in permissions) will be rendered for anonymous users; any view restricted from guest users will not render regardless of the “embed” flag.

Guest user permission to content can be controlled with the full scope of roles, permissions, and data security available to all other user types on Tableau Server. When Tableau Server receives a request for an embedded view, it first checks to see if the user is logged in (i.e. the request is accompanied by a login session cookie for a logon that has not expired). If the user is not actively logged in, then the request is processed as a guest user, if enabled.

Guest user access will not work when Active Directory authentication is set to enable automatic login, due to ambiguity in handling invalid credentials.

1. **Logging out**

An often-neglected area of authentication is terminating a session. Tableau Server has automatic session timeouts based on length of inactivity. Administrators can change the default length of the idle duration timeout. Tableau Server also allows an absolute session timeout to be configured.

When using Active Directory authentication with automatic login enabled, users have a “switch user” option rather than a “sign out” option. This is because they would be automatically logged back in if they initiated a log out. For all other authentication scenarios, users get a “sign out” option so they can manually log out when finished with their session.

For integrated environments, such as views embedded in a portal, it is useful to programmatically force a logout on Tableau Server in addition to the logout for the portal. You can easily do this by calling a logout URL from the client: https://<Tableau Server>/ manual/auth/logout.

1. **Authorization**

Once you properly authenticate a user and grant them access to the system, the next step is to authorize what content and server permissions they have. In Tableau Server, site role and permissions provide administrators with fine-grained control over what data, content, or objects a user can access and -- what actions a user or group can perform on that content. These actions are often referred to as capabilities and include the ability to view and interact, add comments, save workbooks, and connect to data sources, among others.

You can also group users to apply permissions in batches more easily. Tableau Server provides you the flexibility to set permissions (allow, deny, or unspecified/inherited) on each piece of content (project, data source, workbook, and individual views within workbooks) and for specified users/ groups. When permissions are not explicitly set on a piece of content, Tableau will apply a default set of permissions. These default permissions will depend on the default settings at the time the content was created and are inherited from the parent of that content. Permissions do not control what data will appear inside of a view.

1. **Network – Transmission Security**

Administrators often use network security devices to protect access to Tableau Server deployed on-premises from untrusted networks and the Internet. However, even in these cases, credentials still need to be securely transmitted across the network. When access to Tableau Server is not restricted, transmission security becomes even more critical to protecting sensitive data and credentials, and preventing malicious use of Tableau Server. Regardless of your situation, Tableau Server has robust transmission security capabilities.

There are three main network interfaces to Tableau Server: client to Tableau Server, Tableau Server to database, and communication between Tableau Server components. Each one of these interfaces is described below. In addition to these broad security capabilities, Tableau pays special attention to the storage and transmissions of passwords at all layers and interfaces.

1. **Client to Tableau Server**

In this case, “client” means a web browser, Tableau Desktop, tabcmd, or REST API applications. By default, these communications use standard HTTP requests and responses which are suitable for most internal deployments. For external or other sensitive deployments, Tableau Server can be configured for HTTPS (SSL/TLS) with customer supplied security certificates. When Tableau Server is configured for HTTPS, all content and communications between clients is encrypted and uses the HTTPS protocol. SSL/TLS should be enabled for all deployments where security is a concern.

When Tableau Server is configured for HTTPS, the browser and HTTPS library on the server negotiate a common encryption level. Tableau uses OpenSSL as the server-side HTTPS library and it is preconfigured to use currently accepted standards. Each web browser accessing Tableau Server via SSL uses the standard HTTPS implementation provided by that browser. This works even in embedded situations and results in a seamless experience for the end user with no security warnings, pop-ups, or exceptions.

Tableau Desktop communicates with Tableau Server using either HTTP or HTTPS. Protecting the transmission of passwords securely requires HTTPS to be enabled.

1. **Communication between Tableau Server and the Database**

Tableau Server makes dynamic connections to databases to process result sets and to refresh extracts. Tableau uses native drivers to connect to databases whenever possible. Tableau relies on a generic ODBC adapter when native drivers are not available. All communications to the database are routed through these drivers. As such, configuring the driver to communicate on nonstandard ports or provide transport encryption is part of the native driver installation, and this type of configuration is transparent to Tableau.

1. **Communication between Tableau Server Components**

This section only applies to distributed deployments of Tableau Server. There are two aspects to communication between Tableau Server components: trust and transmission. Each server node in a Tableau cluster uses a stringent trust model to ensure that it is receiving valid requests from the other nodes in the cluster. Trust is established by a whitelist of IP address, port, and protocol. If any of these are invalid, the request is ignored. All members of the cluster can communicate with each other. It is recommended that Tableau Server be firewalled off from unsecure servers.

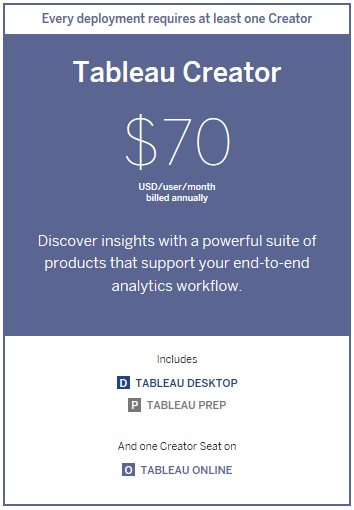
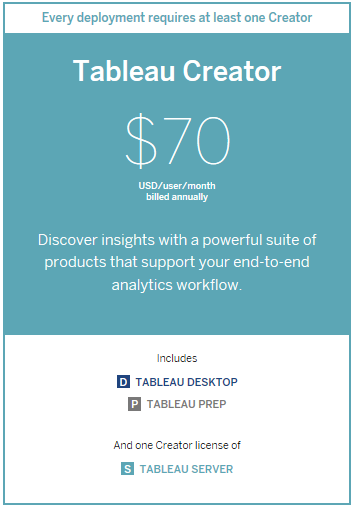
For Further Information please read the Tableau Server Security Whitepaper referring below link:

[**https://www.tableau.com/sites/default/files/whitepapers/tableau\_server\_platform\_security\_1.pdf**](https://www.tableau.com/sites/default/files/whitepapers/tableau_server_platform_security_1.pdf)

1. **Pricing:**

The Price is same both Tableau Online and Tableau Server, 70$ per user per month.

**Tableau Online Tableau Server**

[](https://www.tableau.com/pricing/teams-orgs#online) [](https://www.tableau.com/pricing/teams-orgs)