Content

1 Introduction ................................................................. 3
  1.1 Why is Security Necessary? ........................................... 3
  1.2 About this Document ................................................ 3

2 Understanding the Mobile System Landscape .................. 4

3 User Management ........................................................ 5
  3.1 Authentication (Identity Management) ............................. 5
    Importance of Authentication ............................................ 5
    Supported Authentication Types ....................................... 5
  3.2 Authorization (Access Management) .............................. 6
    Importance of Authorization ............................................ 6
    Authorization in SAP BusinessObjects Mobile applications ........ 7

4 Network and Communication Security ............................. 9
  4.1 Network Security ........................................................ 9
    Understanding DMZ and Firewall ....................................... 9
    DMZ and Firewall Support in the Mobile System Infrastructure .... 11
  4.2 Communication Channel Security .................................. 12
    Significance of HTTPS .................................................. 12
    HTTPS Support in the Mobile System Infrastructure ............... 12

5 Security of Application Servers ...................................... 15
  5.1 Reverse Proxy Support in the Mobile System Landscape ....... 15
  5.2 URL Mapping Implemented on the Mobile Server ............... 16

6 Support for Security Deployments On the Web Application Server ......................... 17
  6.1 Installing the x509 Client Certificate on Device ................. 18

7 User Data Protection and Privacy Measures Implemented in SAP BusinessObjects Mobile ........................................ 20
  7.1 HTTP Caching .......................................................... 21
  7.2 Features of Application Password ................................. 21
1 Introduction

1.1 Why is Security Necessary?

Mobility is redefining the workplace and the borders between personal and professional, home and office, and device and application are fast disappearing. The number of devices connected to the internet is crossing billions. As the landscape of mobile devices is growing, the threats faced by them are also multiplying. Mobile Application stores are targets for attackers who are looking to maximize the effectiveness and reach of their malicious applications.

Innumerable sorts of security attacks have been witnessed by the software systems over the years. As such, it is essential to identify the vulnerabilities and potential attack points that an attacker may target in a system, and apply adequate security mechanisms to protect the platform and application data.

For Business Intelligence applications, the various security challenges must be addressed by both the BI platform and the mobile devices.

SAP BusinessObjects Mobile implements the fundamental security mechanisms to ensure the safety of network, communication channels, application data, user data, plus the protection of many other aspects of the mobile system landscape.

1.2 About this Document

This guide provides an overview of all aspects of the security strategy provided by the SAP BusinessObjects Mobile solution. It explains user management, data protection, network and communication security, application server security and the purpose of implementing the various security measures.

Security is implemented both at the level of SAP BusinessObjects Mobile applications (clients) and at the overall Mobile system (landscape) level.
2  Understanding the Mobile System Landscape

The figure below depicts the technical and security landscape of the SAP BI Mobile system:

SAP BI Mobile consists of a client-side application for mobile devices and a Mobile server component that communicates with the SAP Business Intelligence (BI) platform server. Using Mobile SAP BI applications, professionals on the move can access business intelligence information from a mobile device, such as a Smartphone or Tablet.

The SAP BusinessObjects Mobile applications (for iOS and Android) are designed specifically to meet the screen size and interactivity constraints of the mobile devices. Business Intelligence documents (including Web Intelligence, Crystal Reports, Dashboards and other types) are displayed on the device with native rendering, single-tap access and device-appropriate user interactivity.

To access SAP BI platform content via the iPhone, iPad or Android devices, users need to download the SAP BusinessObjects Mobile application to their devices.

Although SAP BusinessObjects Mobile can work on data infrastructures like GPRS, the best performance is experienced on 4G+ Wifi networks.

i  Note
- Except the optional components (indicated in the figure), all entities depicted in the figure above of the Mobile system landscape are essential. Omitting any of them, may lead to insecurity of the network, services, data and users of the Mobile system.
- The importance and role of reverse proxy and certain other Mobile system entities shown in the figure above are explained in other sections of this guide.
3 User Management

User Management includes the authentication or identity management of users and the authorization or access management of system or application data. In the SAP BusinessObjects mobile system landscape, user management is implemented at both the BI platform level and the Mobile for Android application level.

The administrator creates user accounts and manages existing user accounts. This involves setting the authentication type, assigning a user role and assigning the user to a pre-defined group. By assigning a user to groups or otherwise, the administrator can control the rights of individual users or groups of users for accessing specific objects (documents) and performing various actions on the objects, such as downloading objects, refreshing objects, scheduling objects and viewing object instances.

3.1 Authentication (Identity Management)

3.1.1 Importance of Authentication

Implementing proper identity management or authentication is the first step towards ensuring a secure application. Using various authentication techniques such as phishing, eavesdropping, wiretapping, stealing, social engineering or reproduction of fingerprints, an attacker can easily gain invalid access to valuable system resources and data.

Authentication means validating the identity claimed by a user through the information that he or she knows (as in the case of passwords) or some other data that the system has based on his or her actions in the recent past (as in the case of session cookies), and other mechanisms.

The user’s identity must only be corroborated on fields that

- Have been set by a trusted system, for example an application server or an Identity Provider.
- Are signed or integrity protected and cannot be modified by an attacker as such.

A secure system protects sensitive authentication information of users by techniques such as password hashing for storage, encryption for data transfer and careful cookie management to avoid illegal access.

3.1.2 Supported Authentication Types

The SAP BusinessObjects Mobile software uses standard authentication types to validate user identity. Before setting up the user accounts and groups within BI platform, the administrator needs to decide the type of authentication that he or she wants to use.

SAP BusinessObjects Mobile applications support the following authentication types:
<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>This is the default authentication and is automatically enabled when the system is first installed. This should be used by the administrator when he or she prefers to create distinct accounts and groups for use within the BI platform, or when there is no existing hierarchy of users and groups in an LDAP directory server or Windows AD server.</td>
</tr>
<tr>
<td>LDAP</td>
<td>If an LDAP directory server is setup, the administrator can use existing LDAP user accounts and groups on the BI platform. When he or she maps the LDAP accounts to the BI platform, users are able to access BI platform applications with their LDAP user name and password. This eliminates the need to re-create individual user and group accounts within the BI platform.</td>
</tr>
<tr>
<td>Windows AD</td>
<td>The administrator can use existing Windows AD user accounts and groups in the BI platform. When an AD account is mapped to the BI platform, users are able to log on to BI platform applications with their AD user name and password. This eliminates the need to recreate individual user and group accounts within the BI platform.</td>
</tr>
<tr>
<td>SAP</td>
<td>The administrator can map existing SAP roles to BI platform accounts. When doing so, users are able to log on to BI platform applications with their SAP credentials. This eliminates the need to recreate individual user and group accounts within the BI platform.</td>
</tr>
</tbody>
</table>

For the application to authenticate the user with the types mentioned above, the administrator must:

- Ensure that the appropriate prerequisites are satisfied.
- Perform additional configuration steps on the SAP BusinessObjects BI platform server and SAP BusinessObjects Mobile server.

For the details of these prerequisites and additional configuration information, refer to the Administrator and Report Designer's Guide available at http://help.sap.com/Bomobileios

### 3.2 Authorization (Access Management)

#### 3.2.1 Importance of Authorization

Authorization limits the accessibility of a software or platform's data to a particular set of users who can perform specific actions based on the rights or permissions granted to them. The goal of authorization is to ensure that users perform only legitimate actions. Authorization defines what a user can do and is critical for data protection, fraud prevention and general legislation compliance.

Authorization is often explained using the analogy of locks and keys. The assets of a system are protected by locks. Users get keys (rights or permissions) to open locks.

This concept is illustrated in the following example:
In the following figure, each lock represents an authorization attribute or condition imposed by the administrator that must be met by the user to access the asset. All locks of an asset need to be "opened" to access or work on an asset. The locks and their respective keys are depicted by the same color code:

- **Asset 1**: Neither Bob nor John have sufficient keys to unlock the asset. As such, neither of them can access Asset 1.
- **Asset 2**: Bob has the required (red and yellow) keys to unlock the asset. John does not have the red key. Hence, Bob can access Asset 2, while John cannot.
- **Asset 3**: Only the yellow key is required to unlock the asset. Both Bob and John have the yellow key and so both of them can access Asset 3.

### 3.2.2 Authorization in SAP BusinessObjects Mobile applications

In the SAP BusinessObjects Mobile system, individual users or groups can access the BI platform content based on the rights granted to them by the application administrator.

Users can hold the rights of only a BI Viewer, which means they can access and perform specific actions on the documents, but not modify or upload them from their devices.

The application administrator must grant the following minimum rights to authorize the user:

- **Object level rights:**
  Users must have the following minimum rights:
  - **View** rights for folders, categories and documents: This right enables users to access the required folders and categories; download documents, view documents and synchronize the downloaded documents with the mobile server.
  - **Refresh** rights for documents: This right authorizes users to refresh the documents.

- **Application level rights:**
  The administrator must grant users the following rights at the application level:
  - Rights to log on to Web Intelligence
  - Rights to enable formatting for reports
Note

The administrator grants rights to individual users from the Central Management Console (CMC) on the BI platform.

- For information on how to assign mobile specific user rights using the CMC, refer to the *Mobile Server Deployment and Configuration Guide*.
- For information on how the access rights are assigned in general, see the *Business Intelligence Platform Administrator’s Guide*. 
4  Network and Communication Security

4.1  Network Security

Network hosts in a mobile system landscape provide various services to the internet such as web, email, application files and confidential information and are vulnerable to attack by hackers, intruders and all sorts of malicious users. This section gives an overview of the security mechanisms that are applied to protect the components of the mobile system network.

4.1.1  Understanding DMZ and Firewall

A DMZ, or De militarized Zone, is a physical or logical subnetwork that contains and exposes an organization’s external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization’s local area network (LAN). This means that an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

In a network, the hosts most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, web and Domain Name System (DNS) servers. Because of the increased potential of these hosts being attacked, they are placed into their own sub-network to protect the rest of the network if an intruder were to succeed in attacking all of them.

Hosts in the DMZ have limited connectivity to specific hosts in the internal network but communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients.

A DMZ configuration typically provides security from external attacks.

Note

A DMZ is also referred to as a Perimeter Network.

Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are:

- Web servers
- Mail servers
- FTP servers
- VoIP (Voice over Internet Protocol) servers
Architecture

There are many different ways to design a network with a DMZ. Two of the most basic methods are with a single firewall, also known as the three legged model, and with dual firewalls.

Single Firewall

A single firewall with at least three network interfaces can be used to create a network architecture containing a DMZ. The external network is formed from the Internet Service Provider(ISP) to the firewall on the first network interface, the internal network is formed from the second network interface, and the DMZ is formed from the third network interface. The firewall becomes a single point of failure for the network and must be able to handle all of the traffic going to the DMZ as well as the internal network.

The figure below illustrates the single firewall architecture.

Notice that the various service hosts are placed within the DMZ.
Dual Firewall

This implementation uses two firewalls to create a DMZ. The first firewall (also called the “front-end” firewall) must be configured to allow traffic destined for the DMZ only. The second firewall (also called “back-end” firewall) allows only traffic from the DMZ to the internal network. Dual firewalls provide a more secure infrastructure.

In some organizations, the two firewalls are provided by two different vendors. If an attacker manages to break through the first firewall, it may take more time to break through the second one if it is made by a different vendor, and thus less likely to suffer from the same security vulnerabilities if any are found.

The figure below illustrates the dual firewall architecture.

![Dual Firewall Architecture Diagram]

4.1.2 DMZ and Firewall Support in the Mobile System Infrastructure

The SAP BusinessObjects Mobile server supports deployments in the DMZ environment. The SAP BusinessObjects Mobile client on the extranet interacts with the SAP BusinessObjects BI platform server on the intranet using the DMZ environment.

To enable this deployment, perform the following:

1. Configure the `-requestPort` and `-port` parameters for the following servers:
○ CMS (for authentication, querying InfoStore, and browsing the repository)
○ Web intelligence report server
○ Adaptive processing server

2. Open the listening ports (`-requestPort` parameter) for the servers mentioned above on the internal firewall.

3. Open the Web application server port on the external firewall.

The communication between the SAP BusinessObjects Mobile client and SAP BusinessObjects Mobile server uses the HTTPS protocol. The SAP BusinessObjects Mobile server communicates with SAP BusinessObjects BI platform Central Management Server (CMS), Web Intelligence Servers, and Adaptive Processing Servers in Corba mode.

### 4.2 Communication Channel Security

#### 4.2.1 Significance of HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol (HTTP) with Secure Socket Layer (SSL) or Transport Layer security (TLS) protocol. HTTPS provides secure identification of a web server in the network and encrypted communication between the interacting entities (client and server or two servers). HTTPS connections are used for sensitive transactions on the World Wide Web and corporate information systems.

HTTPS is syntactically identical to the HTTP scheme used for normal HTTP connections, but it also signals the browser to use an added encryption layer of SSL/TLS to protect the traffic. SSL is especially suited for HTTP since it can provide some protection even if only one side of the communication is authenticated. This is the case with HTTP transactions over the Internet, where typically only the server is authenticated (by the client examining the server’s certificate).

The main idea of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted. The trust inherent in HTTPS is based on major certificate authorities that come pre-installed in browser software.

> **Recommendation**

Use TLS 1.2 Protocol on the Client Server as it uses SHA 256 based encryption, thereby enhancing the security.

#### 4.2.2 HTTPS Support in the Mobile System Infrastructure

The SAP BusinessObjects Mobile server supports encrypted communication with the SAP BusinessObjects Mobile client. To encrypt the communication between the SAP BusinessObjects Mobile application (on device) and the SAP BusinessObjects Mobile server, you must configure HTTPS on your Web Application Server.
We recommend that you configure HTTPS on your Web application server to ensure the security of the communication channel in your set up. For information on how to configure HTTPS, refer to the documentation of your Web Application Server.

### Note

With effect from the 5.1 release, the SAP BusinessObjects Mobile application for iOS allows HTTPS connections to only trusted servers. A trusted server is a server with secure server certificates signed by certificate authorities (CAs) that are trusted by iOS. If the server is not trusted, and users try to add a server connection in the application, they encounter an error. For more information, refer to the related topic provided at the bottom.

### Related Information

Ensuring that the Mobile Server is Trusted [page 13]

#### 4.2.2.1 Ensuring that the Mobile Server is Trusted

If you are using HTTPS to connect to your SAP BusinessObjects Mobile server, the SAP BI application (for iOS and Android) only allows connections to trusted servers. In order for the application to establish successful connections to a server, it is essential that one of the following conditions is met:

- **Your server is trusted.** This means that the server has secure server certificates from a Certificate Authority (CA), and these CAs are trusted by iOS (such as Verisign, Thawte and others listed at [http://support.apple.com/kb/ht5012](http://support.apple.com/kb/ht5012))
- **The root certificate** of your server is **installed on the client device** (iPhone or iPad) as a profile, which means when the connection to the server is added in the application, the device can verify the server certificate.

If one of the above conditions is not met, and you try to add a server connection in the application, you encounter an error like this:

Connection to the server could not be established (MOB06031) (HTTP-1202) Details: The certificate for this server is invalid. You might be connecting to a server that is pretending to be <server1.servers.xxcompany.com>, which could put your confidential information at risk.

If you are not using a root certificate that is preinstalled on the user’s device, you can distribute it in one of the following ways:

- Using the Mobile Device Management (MDM) tools
- Sending the root certificate as an email attachment
- Hosting the root certificate on a server and sharing the link

### Note

Self-signed root certificates are not supported.
For example, to retrieve the root certificate of a trusted server and to share it with other users, follow the procedure below:

1. Open your browser settings and open the certificates (depending on your browser, the Manage Certificates or Certificates option may appear in one of the tabs).
2. In the Certificates window, access the **Trusted Root Certification Authorities** tab as shown in the figure below:

   ![Certificate Management Window](image)

3. Select the trusted root certificate corresponding to your server, and choose **Export**. The Certificate Export wizard appears.
4. Follow the prompts to export the certificates.

The certificate is saved on your machine. Attach the certificate to an e-mail and send it to the required recipients. Alternatively, host the root certificate on a server and send the URL to the users.

When users receive the certificate on their iOS device, they can choose the **Install** option when they tap the file or URL. Once installed, the certificate appears on the device as a profile, and users can check the installation on their iPhone or iPad: **Settings > General > Profiles**.
5 Security of Application Servers

Access to the SAP BusinessObjects Business Intelligence platform servers and the SAP BusinessObjects Mobile server is secured by setting up reverse proxy servers in the system. This section explains the architecture of reverse proxy servers and how they are implemented in the mobile infrastructure.

5.1 Reverse Proxy Support in the Mobile System Landscape

Significance of Reverse Proxy Servers

Like a proxy server, a reverse proxy server is an intermediary between the client and the Web application server, but it is used the other way around. Instead of providing a service to internal users wanting to access an external network, a reverse proxy server provides an external network with indirect access to internal resources. For example, back office application access, such as an email system, could be provided to external users (to read emails while outside the company) but the remote user would not have direct access to his email server. Only the reverse proxy server can physically access the internal email server.

Reverse proxy is an extra layer of security, which is particularly recommended when internal resources need to be accessed from the outside. Usually such a reverse proxy mechanism is provided by using an application layer firewall.

Like a proxy server, reverse proxy also provides efficiency advantages such as load distribution, caching of static and dynamic content, and content compression. From the perspective of security, it gives the following advantages to the system:

- Reverse proxies hide the existence and characteristics of the original server(s).
- Application firewall features of a reverse proxy can protect against common web-based attacks. Without a reverse proxy, removing malware or initiating takedowns, for example, can become difficult.
- In the case of secure websites, the SSL encryption is sometimes not performed by the web server itself, but is instead offloaded to a reverse proxy that may be equipped with SSL acceleration hardware.

Implementation in the Mobile Landscape

The mobile platform is deployed in an environment with one or more reverse proxy servers. The reverse proxy server communicates with SAP BusinessObjects Mobile client(s) and is typically deployed in front of the SAP BusinessObjects Mobile server in order to hide the mobile and BI platform servers behind a single IP address. This configuration routes all Internet traffic that is addressed to private web application servers through the reverse proxy server, hiding private IP addresses.
Because the reverse proxy server translates the public URLs to internal URLs, it must be configured with the URLs of the Mobile platform applications that are deployed on the internal network. Once reverse proxy is enabled for the server, the client can access the mobile application using the appropriate reverse proxy URL.

5.2 URL Mapping Implemented on the Mobile Server

When users add Mobile server connections in the SAP BI application on their mobile device, they specify the Mobile `<Server-URL>` for each connection. After creating connections, when the user chooses a connection, the application creates a specific request URL to invoke the Web application server (Mobile server).

Users need not enter the complete URL for a Mobile server. Instead, the application re-constructs the URLs in the following manner:

- If the user enters: `x.com:8080` in the `<Server-URL>` field, the application contacts `http://x.com:8080/MobileBIService/MessageHandlerServlet` using HTTP POST.
- If the user enters: `http://x.com:8080` in the `<Server-URL>` field, the application contacts `http://x.com:8080/MobileBIService/MessageHandlerServlet` using HTTP POST.
- If the user enters: `https://x.com:8080` in the `<Server-URL>` field, the application contacts `https://x.com:8080/MobileBIService/MessageHandlerServlet` using HTTPS POST.

**Note**

1. If a user is setting up a reverse proxy server, all communications received over the URL: `http://external-hostname:port/MobileBIService/MessageHandlerServlet` must be mapped to `http://internal-hostname:port/MobileBIService/MessageHandlerServlet`. All the query parameters in the URL (such as `?x=a&y=b`) must also be mapped.
2. If user is setting up a load balancer, he/she must ensure that cookie-based persistence (for session data) is set up for the server that first serves the client request. If the load balancer faces issues with cookie-based persistence, ensure that IP based persistence is set up.
6 Support for Security Deployments On the Web Application Server

Ensure that you have implemented either of the following scenarios on your Web application server (on which you have installed the SAP BusinessObjects Mobile server):

- Basic authentication (for example Siteminder)
- Form based authentication (for example Siteminder, Webseal)
- X509 certificate (two way client certificate)

When users add connections to the SAP Mobile server (with either of the above security deployments) using the SAP BusinessObjects Mobile application on their devices, they see a security interface which asks for authentication. The following sections explain the three scenarios listed above.

a. Basic Authentication

1. Using the Settings screen of the application, users add a connection to the CMS with basic authentication deployed on it. (As an administrator, you provide the specific server details to the application users.)
2. On choosing the new connection in the Settings screen, the application displays the basic Authentication dialog box, asking the user to enter his/her credentials.
3. User is logged in to the connection, and can browse the BI documents available on the server.

b. Form Based Authentication

1. Using the Settings screen of the application, users add a connection to the CMS with form based authentication deployed on it. (As an administrator, you provide the specific server details to the application users.)
2. On choosing the new connection in the Settings screen, the application displays a form, asking the user to provide additional information.

>Note

The form fields can be customized on the Web application server and UI features such as company logo can be included in the form. The form configured on the Web application server is displayed in the same way as in the application in a container on device.

3. User is logged in to the connection, and can browse the BI documents available on the server.
c. Certificate Based Authentication

1. Users first install the X509 certificate on the device. Information on how to install the certificate is provided in the sub-topic of this chapter.

2. Using the Settings screen of the application, users add a connection to the CMS with certificate based authentication deployed on it. (As an administrator, you provide the specific server details to the application users.)

3. When you choose the new connection in the Settings screen, the application displays a dialog box stating that the connection requires a certificate. User chooses Yes to display the certificate.

4. Application displays the available certificates and asks for the right certificate.

5. User selects the certificate (installed in step 1) from the list.

6. User is logged in to the connection, and can browse the BI documents available on the server.

   **Note**

   1. Installed certificates can be removed from the application by choosing the Clear Data Remove Certificates option in the Settings screen.
   2. The application supports basic authentication and certificate based authentication for hyperlink objects as well.

6.1 Installing the x509 Client Certificate on Device

For adding or accessing a client certificate based connection in the application, users need to first install the certificate on their device. SAP BusinessObjects Mobile applications support the set ups that are deployed based on the x509 certificate.

x509 certificate is usually of the format "<>.p12" or "<>.pfx"

The procedures below are for users who install the certificate (received via email or accessed from a Web application server) on their device:

**Installing the certificate received as an email attachment**

1. On your desktop, download the certificate (*.p12) file.

2. Change the certificate file extension from ".p12" to ".mcert" and send it to the email account configured on your device. This ensures that the certificate file is in a recognizable format for the application.

3. On your device, double-click the certificate that you emailed to your account. The application is launched.

   - If the certificate is password protected, a dialogue box appears on the screen asking you to enter the password. For the installation to complete successfully, enter the password and choose OK. The message for successful certificate installation appears.
If the certificate you are installing already exists on your device, on performing step 3 in the above task, a dialogue box appears saying: "This certificate <ID> already exists". If you want to delete the existing certificate from the app, choose *Delete* in the dialogue box. Else, choose *Cancel*.

**Installing the certificate hosted on a Web Application Server**

1. On your device, access the following link emailed to you by the administrator:
   
   SAPBI://action=downloadcert&certurl=<Download URL>

2. If you access the link above:
   
   The application is launched and the certificate file is downloaded from the URL location (certurl). A dialogue box appears asking you to enter the password. Enter the password and choose OK. The certificate is installed successfully on the device.

   *Note*

   If the certificate is not password protected, the application is installed directly on accessing the link.

   An example of the parameter "Download URL" is http://<IP address>:<Web Application server machine port>/Resource/<Certificate File>;

   *Note*

   If the certificate you are installing already exists on your device, on accessing the link, a dialogue box appears saying: "This certificate <ID> already exists". If you want to delete the existing certificate from the application, choose *Delete* in the dialogue box. Else, choose *Cancel*. 
User Data Protection and Privacy Measures Implemented in SAP BusinessObjects Mobile

User data is the data or information which is personal to an individual user. In the context of the SAP BusinessObjects Mobile applications, this includes the downloaded reports, cached data and application logon credentials of the user. To ensure the security of user data, the following features are implemented on the software:

- The downloaded documents are persisted on the device in encrypted format using the SQL Cipher AES 256 algorithm and FIPS compliant AES algorithm.

  **Note**

  For iPad/iPhone devices with iOS version 8 or above, these encrypted documents are not uploaded to iCloud.

- Users have the same authorizations as defined on the SAP Business Intelligence (BI) platform server, even for the downloaded or offline documents.

- Users have the option of saving their password for a connection in the application. However, in the server configuration, this option is disabled by default (`savePassword=false`). If a user enables the Save Password option while configuring the connection on his or her device, the password is encrypted using the FIPS compliant AES algorithm and stored with the iOS keychain.

  **Note**

  For information on the password enhancements implemented in the application, see the sub-topic of this chapter.

- In the default configuration of the application, the option to download and view documents locally on the device is disabled (`offlineStorage=false`). Users can only access the documents available on the server in online mode of working. Based on requirements, administrator can enable this option in the server configuration file at the Central Management Console (CMC).

- If offline storage of documents is enabled, there is a "Time to Live" parameter in the server configuration file at the CMC, with a default value of 365 days (`offlineStorage.ttl=365`). This means that the downloaded documents expire after 365 days and are automatically removed from the local memory of device. The administrator can choose to set a lower value for `ttl` (for example 5 days) based on the specific data protection requirements.

- For BI documents having private or confidential data, administrators can secure the documents by assigning them to a "Confidential" category on the BI platform. Users can access a secure document only while they are connected to the Mobile server. Once the user closes the document, it is deleted from the device memory.

- If you are using an iOS 8 (or later version) device, and have registered your finger print (using the Device Settings), you can enable touch ID in the application and use it to log on without needing to enter the application password. You can also use touch ID to access documents that have been protected.
Note

1. For information on configuring the various security parameters (such as `savePassword` and `offlineStorage`) on the Mobile server; and on securing BI documents, refer to the Administrator and Report Designer’s guide available at http://help.sap.com/bomobileios or at http://help.sap.com/bomobileandroid.

2. Advanced capabilities such as wiping the application data from the device are not supported in the SAP BusinessObjects Mobile software at this point in time.

### 7.1 HTTP Caching

Static content is cached in the following:

- Hyperlinks
- Dashboard
- Lumira Cloud and Server

The mobile application stores HTTP cache when users access hyperlinks, analysis application documents, and SAP Lumira BI content on the device. Administrators can disable the HTTP cache on the mobile client by setting the `feature.http.cache.disabled` property to `true` in Client Settings in CMC.

- By default HTTP caching is supported for all HTML content that you view using the application. However, you can disable it by defining the property `feature.disable.http.caching` with a value of ‘false’ in client settings on the Mobile server. For information on how to define or edit the client settings using the CMC on the server, refer to the Administrator’s Guide available on http://help.sap.com/bomobileios.

- By choosing the `Clear Data` option in the Settings screen, the cached static content is deleted from the local memory.

- The life cycle of cache depends on the cache control headers sent from the database.

### 7.2 Features of Application Password

The application password acts as a source of input for encryption of user data, where other users cannot decrypt the data without this input.

Here are some features of the SAP BusinessObjects Mobile application password:

- By default, the application password is not enabled in the application, until users add a connection to the BI platform server. When users add a BI platform server connection, the application forces them to create an application password (this is because user-specific or personal information comes on the device only after a connection is created).

  However, if users have not created a single connection, yet, they wish to enable the application password, they can do so using the Settings screen of the application. (Settings screen appears on tapping the [Settings] icon which is next to the current connection name in the left hand navigation panel.)
The above behavior applies if the user has performed a fresh installation of the application. If a user has upgraded the existing installation with a newer version of the application from the iTunes store, server connections would already exist in the application, and so the password would remain enabled.

**Password prerequisites:**

Password length must be minimum eight characters.

For entering the password, the application allows a maximum of twenty attempts. If the attempts exceed this number, the application forces the user to reset the application.

Resetting the application erases the application password and all the SAP BI content downloaded on the device.

By choosing the [Clear Data] [Remove Application Data] option in the of the [Settings] screen, all BI data of the application is deleted from the local memory. However, this does not delete the application password.

Users can change the password and set the "Application password timeout" parameter using the [Settings] screen.

The Application password timeout parameter defines the duration of inactivity. Once this is exceeded, the application forces the user to enter the password to resume the application activity. This applies to the scenario when the user has switched over to other applications, and returns to the SAP BusinessObjects Mobile application after some time. The default value of this parameter is 5 minutes.

You can customize the password settings in the Central Management Console (CMC) by choosing [Applications] [SAP BusinessObjects Mobile] [Client Settings]

If you set savePassword=true, the Save Password option appears in the Connection settings screen of the application. Otherwise, it does not appear for the user.

If for a server, the administrator has set the value of offlineStorage.appPwd parameter to true, users cannot disable the application password (for the particular server connection) while using the application. If this parameter has the false (default) value, users can disable the application password using the [Settings] screen of the application.

Other parameters associated with offline storage (such as "time to live") apply to the password as well.

For information on the workflow of a particular action (such as disabling application password), use the embedded Help provided in the application.
Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).