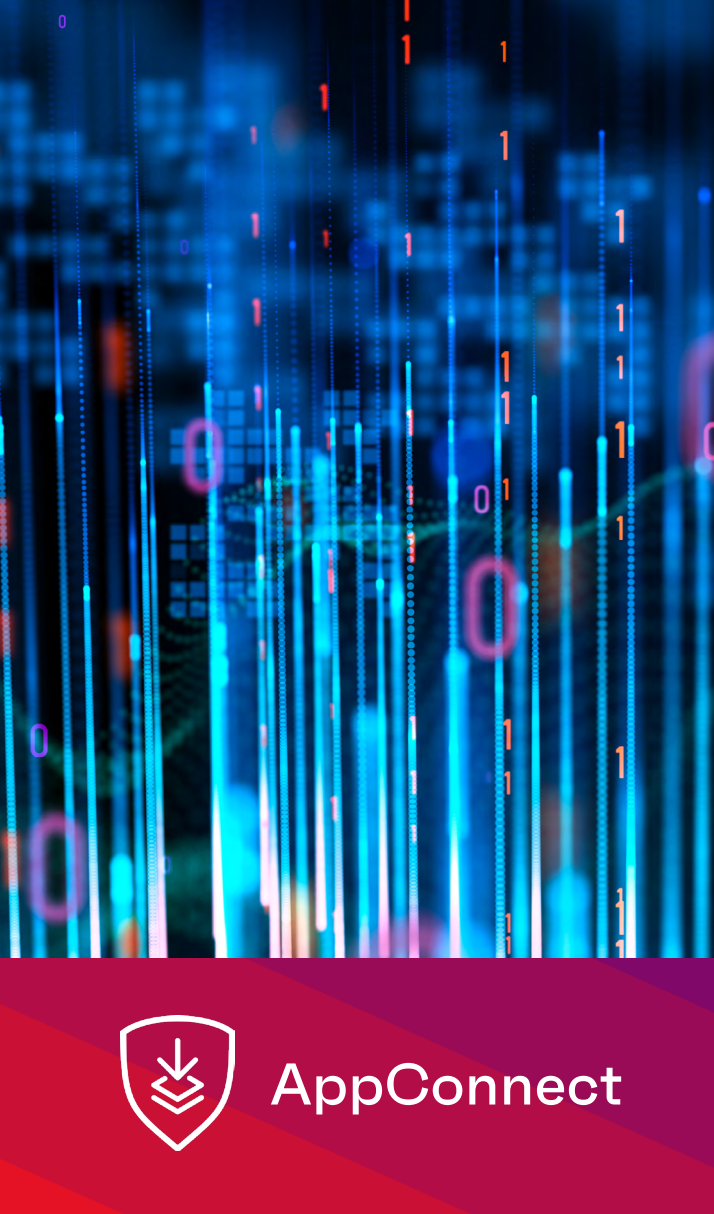




Securing Public Sector Mobile Data With Ivanti AppConnect





AppConnect is Ivanti's mobile software development kit (SDK), providing encryption for iOS mobile devices for data at rest (DAR) and data in transit (DIT). For mobile applications (App) and DAR storage protection, AppConnect uses three different methods to incorporate additional security and management controls into each mobile app. These app security methods are AppConnect, App Wrapping and AppConnect SDK. App DIT is protected by using AppTunnel.

Ivanti Neurons for MDM and Endpoint Manager Mobile offer mobile app management (MAM), mobile content management (MCM) and enterprise mobility management capabilities. Leveraging these solutions, federal, state and local, and education organizations can configure, manage, update and deliver their apps to iOS-based mobile devices. This ensures conformity among all apps and adherence with operational and security policies. The AppConnect container ensures that an organization's apps and their associated enterprise data are securely isolated from the user's personal apps and private data on the mobile device.

App security technologies

Ivanti provides both binary app wrapping and SDK methods to create AppConnect-enabled apps. The app wrapping method modifies the mobile app without rewriting the underlying source code. The Ivanti AppConnect wrapping method takes an app binary, examines it for operating system (OS) application programming interfaces (API) and replaces those interactions with secure APIs. It also adds the functionality to configure a container passcode and code to communicate with the rest of the infrastructure.

A typical use case for the app wrapping method is if your organization has developed an in-house iOS mobile app but does not have the resources to compile the app using the SDK. These apps can be wrapped and then published to a proprietary enterprise app store or deployed as a managed app by Ivanti Neurons for MDM and EPMM Endpoint Manager Mobile.

The AppConnect SDK for iOS method requires the source code. The customer compiles the app using the SDK to incorporate additional security and management controls into the app. This permits the IT administrator to be more particular about which controls are enforced.

For example, if a user becomes unauthorized to use an organization's app and the AppConnect status changes, the IT administrator can notify the user of the status change and enforce additional controls to handle the app logic. If the app generates both secure organization and insecure personal data, then the SDK allows the IT administrator to choose which app data to remove when the app is retired. Retiring an app means that the user is no longer authorized to access the organization's secure data. This means that the organization's data is removed while leaving the user's personal data intact.



The app security layers can be enforced as AppConnect configuration and container policies within Ivanti Neurons for MDM and Endpoint Manager Mobile to manage client-side data loss prevention (DLP) controls.

1 User authentication

The first layer is user authentication, which ensures that the app is accessed only by an authorized user with the proper credentials. This ensures that the current mobile device user is the authorized user of the device. This can be configured as a passcode or on newer iOS devices with Touch or Face ID.

2 App authorization

The second layer is app authorization, which ensures a registered device meets the organization's operational and security policies for an app to be executed. These can range from ensuring that an iOS device is not jailbroken to enforcing more stringent compliance policies, for example, that no malware or prohibited apps are present on the device. This can be achieved by integrating Ivanti Neurons for MDM and Endpoint Manager Mobile with an app reputation vendor like Appthority, Veracode, FireEye, Lacocon and others that enforce additional app control policies.

3 Access policy

The third layer is access policy, which defines the DLP controls for the app's behavior. These include controls like whether the user can or cannot copy-and-cut, print or open information into other external apps.

4 AppConnect encryption

AppConnect encryption, the fourth layer, ensures that DAR on iOS platforms is stored securely using strong cryptographic algorithms.

AppConnect generates a unique Advanced Encryption Standard (AES) master key on each mobile device using a cryptographically strong random number generator (RNG) from SecureRandom. The AES master key is encrypted within another key that is derived from the user's AppConnect "Secure Apps" passcode using Password-Based Key Derivation Function 2 (PBKDF2). The user's passcode is never stored on the device.

For iOS app-wrapped AppConnect-enabled apps, there is no additional app data encryption when the device passcode is also enabled. For iOS SDK App Connect-enabled apps, additional app data encryption is available if the data encryption API is enabled within the AppConnect SDK.

The current versions of Ivanti Neurons for MDM and Endpoint Manager Mobile allow the mobile device's passcode to be used instead of the AppConnect passcode to secure the AppConnect container using the iOS SDK method.

Additional security layers

The fifth security layer is usage and analytics, which provides visibility into what apps are being used and how often. The sixth layer is selective wipe (i.e., retire or quarantine), which ensures that an organization's data can be securely removed, while leaving user personal data like pictures, music and videos intact on the device.



iOS AppConnect container security

iOS AppConnect implements AES-256 bit Galois/Counter Mode (GCM) encryption. AES-256 GCM provides both data integrity and confidentiality. iOS AppConnect uses the AES master key to encrypt application data stored by AppConnect-enabled apps on the mobile device.

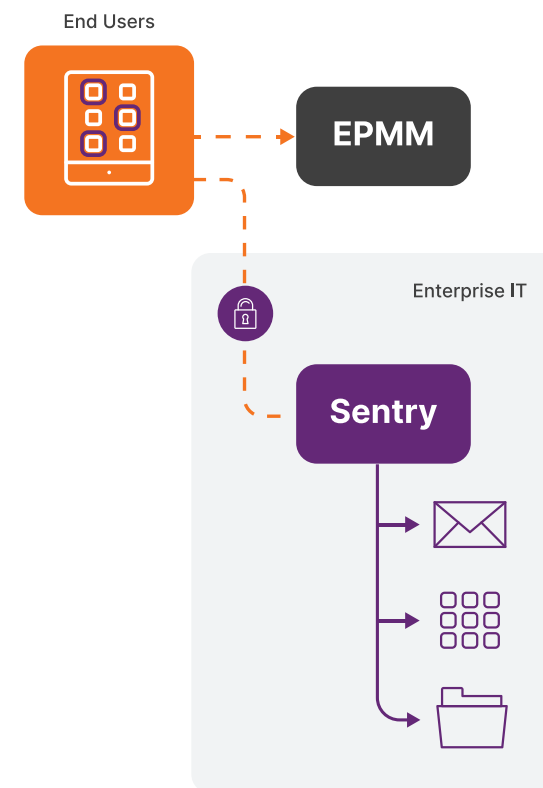
The AppConnect SDK does not use the AES master key to directly encrypt the data. Instead, it generates a unique encryption key for each AppConnect-enabled app. A new encryption key is generated specifically for each AppConnect app on the iOS device. This new encryption key is derived from the previously mentioned AES master key using the HMAC-SHA-256 key derivation function (KDF).

AppTunnel

An important component of Ivanti AppConnect is AppTunnel. It protects data in motion by employing secure tunneling and access control between the mobile device and the organization's application gateway, provided by Ivanti's Sentry component.

AppTunnel provides a set of its own security layers.

- Establish a unique and secure connection that only allows authorized users, apps and devices to traverse the tunnel to sensitive enterprise data sources within the corporate network.
- Use certificate-based identity for authentication between the mobile device and Sentry to prevent man-in-the middle attacks.
- Apply access control list (ACL) rules to block network access if the mobile device becomes compromised or falls out of compliance.



Conclusion

Ivanti's AppConnect solution implements today's strongest cryptographic algorithms that secure public sector DAR and DIT for data loss prevention applications. They employ AES256 GCM ciphers that provide data integrity and confidentiality.

About Ivanti

Ivanti is an enterprise software company that provides a comprehensive IT and security cloud-based platform. Ivanti provides software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing security risk. The Ivanti Neurons platform is cloud-native and is designed as a foundation of unified and reusable services and tools for consistent visibility, scalability and secure solution delivery. Over 34,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com) and follow @Golvanti.



For more information about Ivanti's innovative public sector IT solutions, or to contact us, please visit [ivanti.com/industries/public-sector](https://www.ivanti.com/industries/public-sector).