APPC-10SLBe Security Features

PRO DVX | ALWAYS ON

ProDVX Europe B.V.
Europalaan 10
5232 BC, Den Bosch
The Netherlands

+31(0)73 737 0345
sales@prodvx.com

APPC-10SLBe Security Features

Introduction

The APPC-10SLBe puts great emphasis on device security. This document aims to outline the various security features that make it our most secure device to date.

Security on Android 11

The APPC-10SLBe comes with a fully certified version of Android 11 with Google Mobile Services, preinstalled on the device. This operating system comes with a host of security features that are designed to provide optimal security. Fundamental to Android is the protection of user privacy.

Starting from Android 9, privacy highlights included limiting background apps' access to device sensors, restricting information retrieved from Wi-Fi scans, and new permission rules and permission groups related to device state and Wi-Fi scans. These changes affect all apps running on Android 9, regardless of target SDK version.

From Android 10 and above, the privacy and controls that users have over data and app capabilities were extended. In total, they provide users and IT administrators with better clarity about how data and user location can be accessed. The work profile creates a separate, self-contained profile on Android devices that isolates corporate data from personal apps and data. This can be added to personal devices in a BYOD setting or on a company-owned device used for both work and personal purposes. With this separate profile, the user’s personal apps and data are outside IT control, on the other hand, corporate data and account is under full control of IT security.

Devices that run Android 8.0 and above use random MAC addresses when probing new networks, while not currently associated to a network. On Android 9.0, the device can use a randomized MAC address when connecting to a Wi-Fi network if enabled by a developer option. In Android 10 and above, the system transmits randomized MAC addresses by default.

Additionally, device IMEI and serial numbers are unable to be accessed. In addition to data-at-rest security—protecting information stored on the device—Android provides network security for data-in-transit to protect data sent to and from Android devices.

The ProDVX APPC-10SLBe offers the following security updates policy: all official security patches and updates are collected into a single package within 3 months and are available for updating according to the rules established by the customer's IT security. Every month, Google publishes Android Security Bulletins to update users, partners, and customers on the latest fixes. These security updates are available for Android versions for three years from the date of release.

Google Play Services

Google Play Services, along with its security component, Google Play Protect, collectively ensure a multi-layered defense against potential threats. The synergy of these components creates a comprehensive security ecosystem that addresses various dimensions of device and data protection.

A pivotal role of Google Play Protect is to authenticate and verify the integrity of applications. Through advanced scanning and verification mechanisms, Play Protect identifies and eliminates potentially harmful apps, thereby mitigating the risk of malware and other security vulnerabilities that could compromise your Android Panel PC.

Google Play Services also establishes a secure communication channel between your device and Google's servers. This involves the use of robust encryption protocols, reducing the likelihood of unauthorized access or interception during data transmission. This secure infrastructure is crucial for safeguarding sensitive information, such as login credentials and personal data.

Additionally, Google Play Protect contributes to device protection through features like Find My Device. In the event of loss or theft, users can leverage this functionality to locate, lock, or remotely wipe their Android Panel PC, enhancing both data security and privacy.

The continuous background updates delivered by Google Play Services play a vital role in maintaining the security posture of your device. This ensures that your Android Panel PC receives the latest security patches promptly, addressing emerging threats and vulnerabilities in real-time.

In summary, the collaborative efforts of Google Play Services and Play Protect create a robust defense mechanism for your Android Panel PC. From app-level security checks and secure communication protocols to device tracking and prompt security updates, this integrated approach significantly enhances the overall safety and security of your Android Panel PC.

Android Enterprise

Android Enterprise serves as a robust safeguard for businesses managing and securing Android devices in the enterprise landscape. As organizations increasingly adopt technology, Android Enterprise delivers a comprehensive set of features tailored to enhance productivity and bolster the security of the APPC-10SLBe in professional settings.

Key components, such as Work Profiles, establish dedicated spaces on devices for work-related apps and data, ensuring the separation of personal and work information for heightened security and privacy. Managed Profiles, employed on company-owned devices, create distinct spaces for work-related activities, aiding in the management and security of corporate data.

Device Management APIs provided by Android Enterprise empower mobile device management (MDM) solutions to efficiently control various aspects of Android devices, from application deployment to security settings. The APPC-10SLBe supports three efficient enrollment methods that streamline the device setup process:

1. Zero-touch Enrollment automates configuration, ensuring devices adhere to security policies from the start and reducing the risk of misconfigurations.
2. NFC Enrollment allows quick provisioning through NFC-enabled tags, requiring physical proximity for an added authentication layer.
3. ADB Enrollment, enabling enrollment via USB for flexibility, maintains security by requiring a physical connection, thus reducing the risk of unauthorized access.

The Enterprise App Store feature allows companies to curate their own app stores or use third-party app stores for the seamless distribution of enterprise-specific applications. Security features embedded in Android Enterprise, such as secure boot and encryption, fortify corporate data and uphold a secure environment. Bulk App Deployment simplifies the process of deploying and managing apps on multiple devices simultaneously, ensuring uniformity across the organization.

To fully enable Android Enterprise on the ProDVX APPC-10SLBe for your organization, two additional components are requisite: a Google account and a certified EMM provider. An EMM (Enterprise Mobility Management) provider plays a crucial role in managing and securing mobile devices within an enterprise. The Android Enterprise Recommended program aids organizations in selecting EMM providers that meet stringent standards set by Google, encompassing criteria like robust security features, effective device management capabilities, support for streamlined provisioning methods, and the ability to manage Android OS updates.

In embracing Android Enterprise on the ProDVX APPC-10SLBe, businesses gain heightened control, improved security, and enhanced productivity. The integration of efficient enrollment methods aligns with Android Enterprise's commitment to providing diverse options for secure device setup, contributing to a robust and tailored approach to device management and security in an enterprise environment.

IEEE 802.1X

The ProDVX APPC-10SLBe places a strong emphasis on network security, integrating seamlessly with IEEE 802.1X for protection against unauthorized access. This security protocol is effectively employed over Wi-Fi and LAN, enhancing network connections with robust authentication mechanisms.

Aligned with the IEEE 802.1X standard, the APPC-10SLBe enforces stringent access controls, requiring users to authenticate their identity before gaining network access. This proactive security measure is pivotal in safeguarding sensitive data and mitigating the risks associated with unauthorized network intrusion. The APPC-10SLBe provides users with a comprehensive and adaptable network security solution for current and future connectivity scenarios.