Data Protection with Always-On VPN and Lockdown Mode

Highlights

- Keep corporate data safe and secure with simplified end user experience.
- Prevent end users from circumventing secure connections.
- Navigate captive portals while ensuring data protection.
- Maintain data visibility
- to adhere to compliance standards.
- Supported on Windows, and macOS.

Industry and compliance

- Healthcare L HIPAA, HITECH
- Financial: GLBA, FFIEC, PCI-DSS
- Federal: FIPS, DoDIN APL, NDcPP
- General: OSHA, SOX, GDPR

Overview

Industries such as financial services, health care and pharmaceuticals need solid security to ensure data safety and industry compliance. Ensuring the security of corporate data on laptops is key, as workforces become increasingly mobile. Not complying with industry regulations, like PCI-DSS and HIPAA, can cause setbacks like fines, lengthened product and service timelines or legal liability.

Ivanti Secure offers Always-On VPN and Lockdown Mode for compliance-focused businesses. These features protect all network traffic; from your team's laptops at home to your corporate network, Ivanti helps reduce the possibility of data loss or leakage.

Always-On VPN

When an end user logs into their laptop using our Always-On VPN, our desktop client automatically makes a secure connection to the Ivanti Connect Secure gateway. Once connected, all traffic from the laptop is sent via a protected tunnel. Furthermore, the end user will remain constantly connected to the tunnel, ensuring that data-in-motion remains secure.

Lockdown mode

Network administrators can configure the desktop client to protect profiles from end user changes, such as disconnecting from gateway or modifying any settings. Lockdown mode secures data, making sure it does not leave an end user's laptop unprotected. This is especially important for teams embracing the Everywhere Workplace.

With lockdown mode, data can only be sent or received when the device is connected to the Connect Secure gateway. (If a connection to Connect Secure is unavailable, data will remain safely on the end user's device until one is.) When Always-On is enabled, your

sure it does not leave an end user's laptop unprotected. This is especially important for teams embracing the Everywhere Workplace.

With lockdown mode, data can only be sent or received when the device is connected to the Connect Secure gateway. (If a connection to Connect Secure is unavailable, data will remain safely on the end user's device until one is.) When Always-On is enabled, your team remains constantly connected to the VPN tunnel, keeping sensitive data-in-motion secure.

User experience

When lockdown mode is enabled, users are required to connect to a VPN to access the internet. Our desktop client has the intelligence to recognize a captive portal and enables the user to enter the necessary information so a secure internet connection can be established.

User credentials can also be saved, or certificate-authentication can be used, to get your team connected faster. Both multi-factor authentication and machined-based authentication are supported to allow system updates on individual devices prior to users logging in.

ivanti.com
1 800 982 2130
sales@ivanti.com