

TouchDown for Android

Manage Corporate Exchange Email While Keeping Company Data Safe

SECURITY FIRST

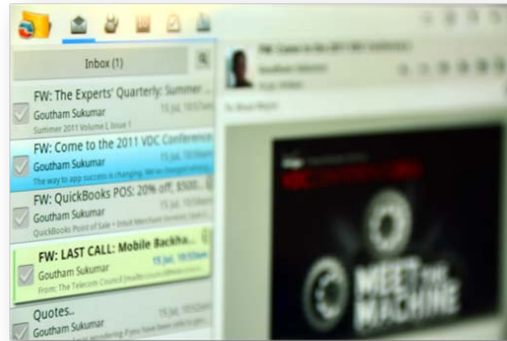
TouchDown runs on the Android platform and extends the security model of the platform to cover Microsoft® Exchange data that is stored on the device by TouchDown.

Over-the-air transmissions and enterprise data at rest on the devices are secured with industry-leading AES-256 encryption.

CORPORATE DATA SECURELY CONTAINED

The administrator can request data to be encrypted on the device. TouchDown encrypts data fields on a field-by-field basis when writing to the database. This provides a level of Data at Rest encryption, preventing the database from being analyzed.

Employees access corporate email, contacts, and calendar, just as they access Outlook on desktop computers at the office.



PIN Policy

TouchDown prompts the user to enter the password in order to access the application.

Remote Wipe

In the event of theft or loss of a device, the administrator (or end user if using Microsoft® Exchange 2007 or 2010) can issue a remote wipe command. This command removes all internal databases where email, contacts, calendar and task information is stored.

TouchDown also deletes any attachments downloaded to the SD card and any contacts copied to the device's phone book. An additional user configurable option for full SD wipe is also provided.

Email Initiated Data Wipe

TouchDown allows an end user to perform a remote wipe by sending an email with a user-specified Kill Code in the subject of the email. The user can specify the Kill Code in the settings. Once a Kill Code is set, TouchDown will perform a remote wipe on receipt of the email that contains the Kill Code in the subject line, prefixed by TKILL:

S/MIME Support

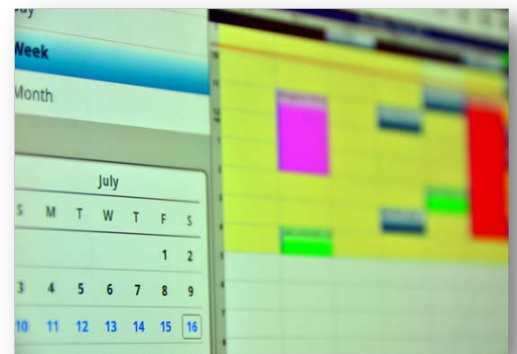
TouchDown supports sending and receiving S/MIME signed and encrypted emails, enabling authentication, non-repudiation and data tampering prevention. Administrators can choose to enable signing on all outgoing emails, check to see if the status of the certificate is set to revoked and prompt user for private key before looking up certificate.

SD Card

Administrators can request to disable the SD card so that TouchDown prevents users from downloading attachments to the SD card. Alternatively, TouchDown can encrypt downloaded attachments before storing to the SD card. This prevents users or other applications from browsing the SD card for corporate attachments. These attachments can only be opened from within TouchDown.

Remote Wipe SMS Confirmation

When a remote wipe is performed, TouchDown can send an SMS message with a confirmation to a predefined SMS number.



Security Features and Benefits

CONTROL

TouchDown provides administrators with multiple ways to enforce security of the data on the device. It enforces policies that are relevant to the product, and enables the administrator to manage those policies from the server.

TECHNICAL SUPPORT

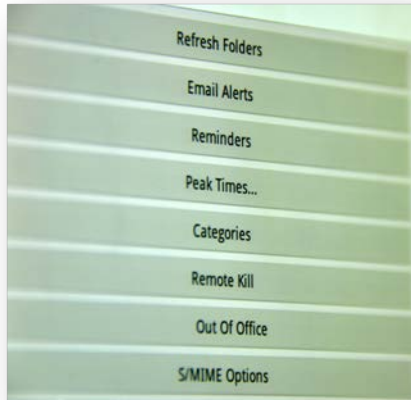
We respond to support emails within 24 hours on weekdays. Please email support@nitrodesk.com

ABOUT NITRODESK

Founded in March 2008, NitroDesk has been providing Secure Corporate Data access on Android since November 2008.

For more information on any of our products or services, please visit us on the Web at www.nitrodesk.com

NitroDesk Headquarters
3380 SE 146th PL Suite 320
Bellevue, WA. 98007
sales@nitrodesk.com



Top Issues	TouchDown's Solution
Open S/MIME emails	TouchDown supports sending and receiving S/MIME signed and encrypted emails
Set and enforce policies	Corporate controlled policies using a MDM, PCF file, or configuration file
Authenticate users	Application level PIN enforcement
Protect data store on the device	Corporate data encryption on the device and SD card
Secure data if the device is lost or stolen	Remote wipe support for administrator or user-initiated wipe
Rely on users for security	End user cannot override any security policy

Corporate Configuration

CONFIGURATION FILE

Administrators can use the NitroDesk Server Side Configuration feature to set security policies and application preferences for TouchDown when users connect to a Microsoft Exchange server. Administrators can control how TouchDown performs when connected to the server by creating a TouchDown folder on the Internet Information Services (IIS) server that hosts Microsoft ActiveSync and placing the TDPreferences.xml file in that folder.

PCF FILE

Administrators can take a successfully configured device containing initial configuration settings and suppressions and export the settings on that device to a preferences configuration file (pcf) to send to end users to configure their device.

