TouchDown for Android

Manage Corporate Exchange Email While Keeping Company Data Safe

SECURITY FIRST

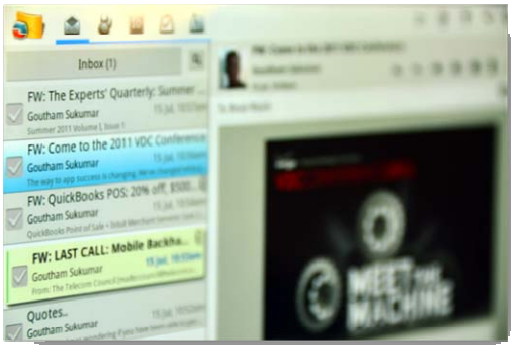
TouchDown runs on the Android platform and extends the security model of the platform to cover Microsoft® Exchange data that is stored on the device by TouchDown.

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 TDKILL:

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.

TouchDown™
With Exchange ActiveSync®

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. Regardless of the Android version, administrators don't have to worry about uniformity with the program.

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
2800 156th Ave. SE, Suite 200
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
Limitations with native email client	Provides more powerful and seamless corporate email experience

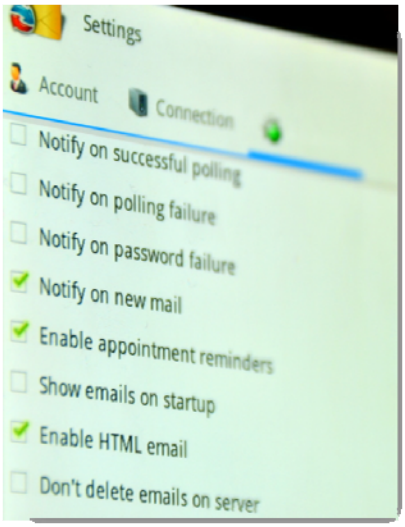
Corporate Configuration

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.



TouchDown™
With Exchange ActiveSync®

TouchDown for iOS

TouchDown Secures and Partitions Your Enterprise's Mobile Exchange Data

BENEFITS

- Comprehensive support for BYOD programs
- AES-256 encryption for an added layer of security
- Full support of Exchange ActiveSync Policies
- Seamless integration with leading MDM solutions
- Information Rights Management and DLP policy support
- Email features users need and want
- User friendly interface speeds adoption rates
- Cost- effective, streamlined architecture provides almost immediate ROI

TOUCHDOWN FOR iOS INTEGRATES WITH MOST LEADING MDM SOLUTIONS

- AirWatch
- Notify Technologies
- Symantec

For more information, please visit www.nitrodesk.com.

INTRODUCING TOUCHDOWN FOR iOS

Regardless of industry or company size, the need to secure corporate data on iOS devices is a mission-critical imperative for corporate IT. The challenge is finding a truly secure, cost-effective, and easy-to-use solution that can support the most robust bring your own device (BYOD) programs, provide seamless integration to all leading MDM solutions as well as have the email features users want and need.

NitroDesk meets this challenge head-on with **TouchDown for iOS**. This cost-effective solution provides a highly secure container for all corporate data so IT can successfully separate and partition its enterprise data from personal, ensuring that BYOD programs are not only secure, but also flexible.

TouchDown provides comprehensive support for all Exchange, Information Rights Management (IRM) and Data Loss Protection policies. The solution uses AES-256 encryption, which adds an extra layer of security, and offers more than 80% of Outlook functionality. A robust stand-alone solution, TouchDown also provides seamless integration to a wide array of leading Mobile Device Management solutions.

SEAMLESS MDM INTEGRATION

TouchDown for iOS integrates seamlessly with all leading MDM providers, extending administrative controls to the email subsystem. This integration provides IT with:

- Reliable end-user configuration
- Policy Enforcement
- Data Loss Prevention
- Compliance Monitoring
- License Management

COMPREHENSIVE SUPPORT FOR BYOD

TouchDown for iOS ensures that even the most robust BYOD programs are not only secure, but also flexible. Even for those industries with strict privacy and compliance requirements. TouchDown's comprehensive BYOD support helps reduce IT's capital investments as well as its carrier costs. The solution works by providing a highly secure container for all corporate Exchange data with the user only needing one log on to access their Email, Calendar, Contacts, Tasks and Notes.

TouchDown™
With Exchange ActiveSync®

TouchDown for iOS

TouchDown for iOS: A More Comprehensive, Superior Approach to Securing Enterprise Data

BENEFITS

- The user experience and support model is the same for all enterprises, regardless of size
- With unique, proprietary Enterprise Configuration Extensions, IT can control TouchDown versions without an MDM
- IT control over device configuration
  - Set and enforce corporate policies using a MDM
  - Set and enforce corporate polices without a MDM using a configuration file
- Simple licensing model and cost effective:
  - $20 per license
  - One-time license fee
  - No additional servers required

ABOUT NITRODESK

Founded in March 2008, NitroDesk is a leading provider of secure ActiveSync email solutions for the Android and iOS platforms. The company has more than 1 million licensed users from Fortune 500 companies to SMBs located across the globe and in nearly every industry vertical.

NitroDesk Headquarters
2800 156th Avenue, SE
Suite 200
Bellevue, Washington 98007
sales@nitrodesk.com

PROVIDES UNPARALLED EMAIL SECURITY

TouchDown for iOS provides comprehensive email security, including the following:

- PIN enforcement policy
- Ability to perform a remote wipe or kill
- Remote kill support for user-initiated wipe
- Settings encrypted by default using AES-256
- S/MIME signing and encryption
- HTTPS connections
- No export of calendar/email to native apps
- One-way phone book export
- End user cannot override any security policy

PROVIDES AN ELEGANT, EASY-TO-USE INTERFACE

TouchDown for iOS provides device users with a robust, easy-to-use UI that has the PIM features device users want and need. Email features include the ability to use the Global Address List within an email, search the server, sync sub folders, and customize email body styles and more. In addition, Contacts and Calendar functionality extend beyond the native app as well as the Task and Notes features, including rule-based notifications and meeting attendee availability.

Features	*Benefits*
Security	TouchDown offers Data at Rest encryption, remote wipe/kill, AES-256, S/MIME, and PIN policy
Notifications	Customize notification options, including badge on new email, appointments and tasks
Email	Edit signature line, set OOF, move and sync folders, download attachments, enable HTML, and access the GAL
Calendar	Edit, update and delete appointments, set custom views, and accept, decline and create meetings
Contacts	TouchDown allows a one-way export to native phonebook and offers the ability to search for a contact and edit multiple fields

TouchDown™
With Exchange ActiveSync®

Personal Device Data Access Agreement

I agree to the conditions set forth in Medicine Hat College's "Personal Mobile Device Use Policy" and agree to abide by all College policy in the access of college data and systems on my personally owned device. Including and in addition to college policy I agree:

- That I bear all costs associated with the purchase of any software to enable and support the access of college systems and data from my device.
- That I am responsible for any and all costs that may result from accessing college data and systems on my device, including costs associated with data transfer.
- That I understand and accept liabilities and costs with regards to the transfer of college data using my service provider.
- That MHC is not responsible for personally owned equipment, including damage, configuration, or data loss relating to its use or configuration for use on any MHC system.
- That Medicine Hat College cannot and does not guarantee connectivity, service quality and technical or use support of personal devices.
- That I commit to the use of my personal device for a two year period before I will be eligible to request a college owned device.
- That there will be no intentional access or removal of non-college data (my personal information) on my device by MHC in this process.
- That I am aware that there may be some unforeseen risk to my personal data housed on my device, including that the software and processes used may unintentionally provide MHC technical staff access to non-college information on my device, or may cause the removal of non-college data from my device. If such access is identified MHC ITS will notify me and the college will not retain any non-college owned data that may be accessed through synching of my personal device.

EMPLOYEE TO COMPLETE:

Device Information

Manufacturer and Model:

Service Provider – Carrier (TELUS, Bell, Rogers, Virgin, etc):

Phone Number (optional, only required if you are using this instead of a college allocated phone):

Employee Name (printed):

Employee Signature: _____

Date: _____

ITS TO COMPLETE:

Authorization for Connectivity **YES or NO** If no, state reason for refusal:

Signature of Director, IT or Designate: _____

Date: _____