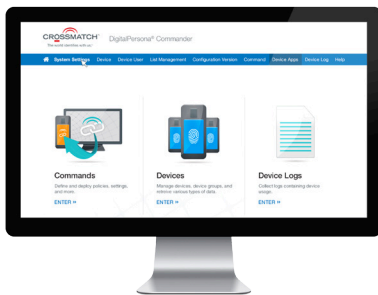


DigitalPersona[®] Commander

Mobile Device Management Application



FEATURES

- Manage base network of up to 500 devices
- Support additional devices (optional 100 device increments)
- Assign devices to management groups
- Create friendly device and group names
- Secure platform encrypts data at rest and data in motion
- Schedule software updates

OVERVIEW

DigitalPersona Commander is a multi-purpose, mobile device management application that provides IT and network system managers a secure, centralized point of access for the management and control of deployed devices. Administrators gain complete visibility and control of custom groups or individual devices and users.

Each mobile device is individually provisioned by and registered with the Commander application using a device-resident service application, Commander Link. Utilizing industry standard Public Key Infrastructure (PKI), a secure communication channel is established between Commander and Commander Link that provides encryption of data while at rest and in motion, which maximizes the safekeeping of Personally Identifiable Information (PII).

The secure channel allows Commander to communicate with networked devices in the field, such as the Crossmatch[™] Verifier[®] Sentry. Administrators can define and deploy over-the-air software or workflow updates; retrieve transaction logs for compliance reporting; and in the event of theft or loss, simply lock the device or wipe sensitive data altogether. The application provides a tiered system of user privileges with comprehensive policy control. In addition, Commander is the server-side interface for Crossmatch's Mobile ID application, which aggregates submissions from the field and responses from multiple configured AFIS, as well as synchronizes device-resident watchlists.

In today's world of proliferating devices and applications, DigitalPersona Commander provides secure administration, oversight and optimization of your networked mobile devices.

ABOUT CROSSMATCH

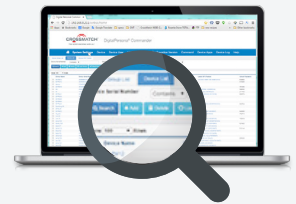
Crossmatch helps organizations solve their identity management challenges through biometrics. Our enrollment and authentication solutions are trusted to create, validate and manage identities for a wide range of government, law enforcement, financial institution, retail and commercial applications. Our solutions are designed using proven biometric technologies, flexible enrollment and strong multi-factor authentication software, and deep industry expertise. We offer an experienced professional services capability to assess, design, implement and optimize our identity management solutions for a customer's individual challenges. Our products and solutions are utilized by over 200 million people in more than 80 countries.

Learn more at www.crossmatch.com

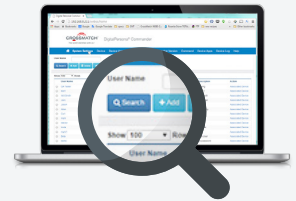
SPECIFICATIONS

Device Management	Functionality includes Add, Delete, Lock, Unlock, Wipe, Collect Lists and Logs, Clear Logs; Manage devices individually or in groups using friendly names
Device User Management	Add, Delete, Synchronize to device
List Management	IDs Found, Targeted IDs, Lists of Categories, Revocation Lists
Configuration Management	Import, Export, Delete, Update to Device
Command Management	View Queue, Delete From Queue, Command Status, Delete from Status, Schedule Commands
Application Management	Upload, Update
Log Management	Search Report Writer
AFIS Management	Submission, Responses
System Requirements (Hardware)	Dual Processors (recommended) with 2 GHz Minimum (32-bit or 64-bit), 8 GB RAM, 160 GB Hard Drive
System Requirements (Software)	Windows Server 2012 R2, IIS version 7.5 or higher, Microsoft .NET version 4.0 or higher, Active Directory — application server within same domain
<i>Data subject to change without notice</i>	

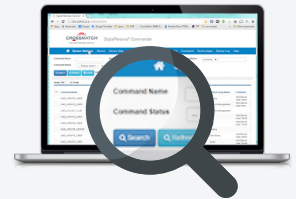
DEVICE MANAGEMENT



USER MANAGEMENT



COMMAND MANAGEMENT



Corporate Headquarters:

Crossmatch
3950 RCA Boulevard, Suite 5001
Palm Beach Gardens, FL 33410 USA

www.crossmatch.com