Smart Security Innovation!

A good partner for smart devices security solutions

ExTrus
Extreme Trust

Instroduction of Exafe MDM

ExTrus
Extreme Trust

Contents

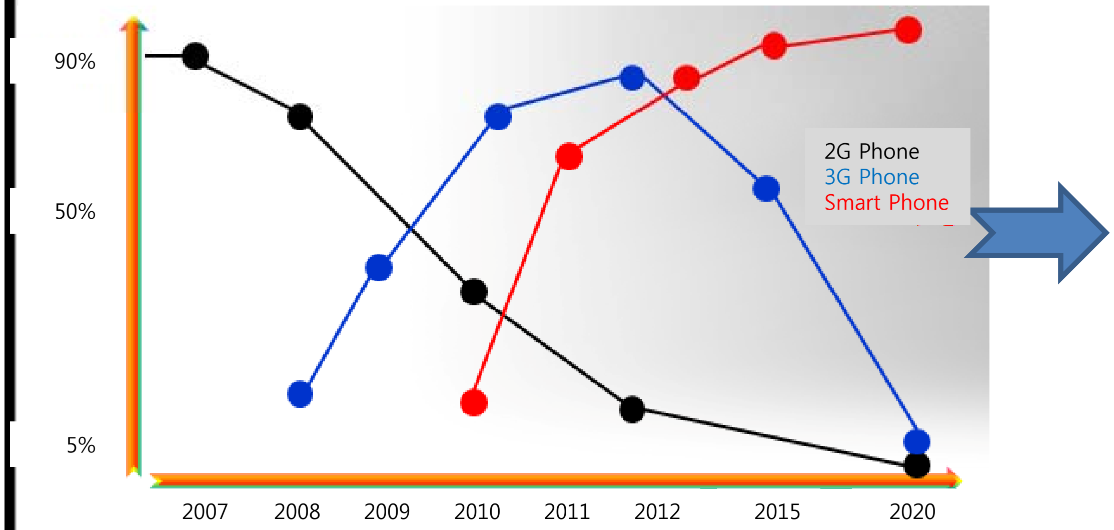
Contents

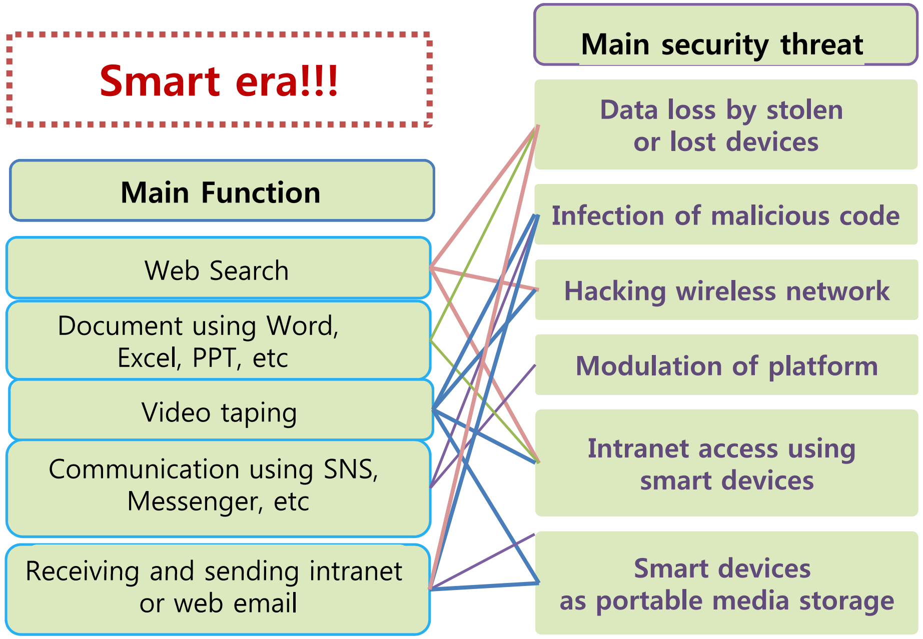
01 Proposal background

ExTrus
Extreme Trust

Smart ear VS Increasing risk factor

Coming era of 20 million people using Smartphones





Smart era!!!

Main Function
Web Search
Document using Word, Excel, PPT, etc
Video taping
Communication using SNS, Messenger, etc
Receiving and sending intranet or web email

Main security threat
Data loss by stolen or lost devices
Infection of malicious code
Hacking wireless network
Modulation of platform
Intranet access using smart devices
Smart devices as portable media storage

Issues of smart devices

Important data loss by stolen or lost smart devices

- Business or personal data loss from smart devices
- Data loss by accessing to business sites
- Non-reusable by personal data loss

Business data loss by insider using smart devices

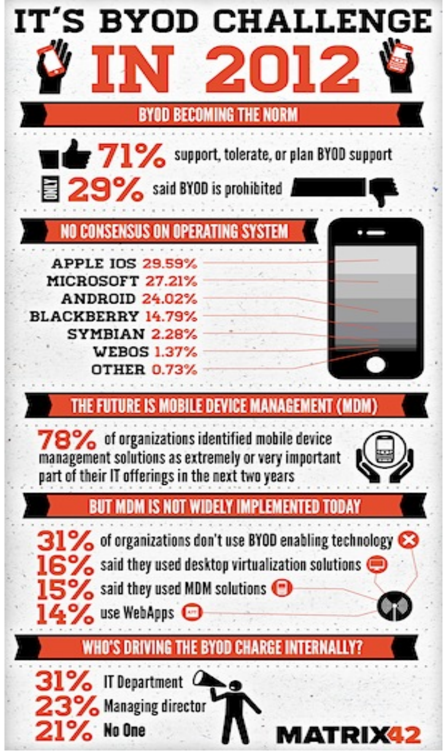
- Vulnerability and security threat of smart devices to increase dangerousness
- Wireless communication, tethering, and portable media storage
- Screen capture, camera, voice recording to steal information

01 Proposal background

ExTrus
Extreme Trust

Smart ear VS Increasing risk factor

Present situation of BYOD(Bring your Own Device)



IT'S BYOD CHALLENGE IN 2012

BYOD BECOMING THE NORM

71% support, tolerate, or plan BYOD support

ONLY 29% said BYOD is prohibited

NO CONSENSUS ON OPERATING SYSTEM

APPLE IOS	29.59%
MICROSOFT	27.21%
ANDROID	24.02%
BLACKBERRY	14.79%
SYMBIAN	2.28%
WEBOS	1.37%
OTHER	0.73%

THE FUTURE IS MOBILE DEVICE MANAGEMENT (MDM)

78% of organizations identified mobile device management solutions as extremely or very important part of their IT offerings in the next two years

BUT MDM IS NOT WIDELY IMPLEMENTED TODAY

31% of organizations don't use BYOD enabling technology

16% said they used desktop virtualization solutions

15% said they used MDM solutions

14% use WebApps

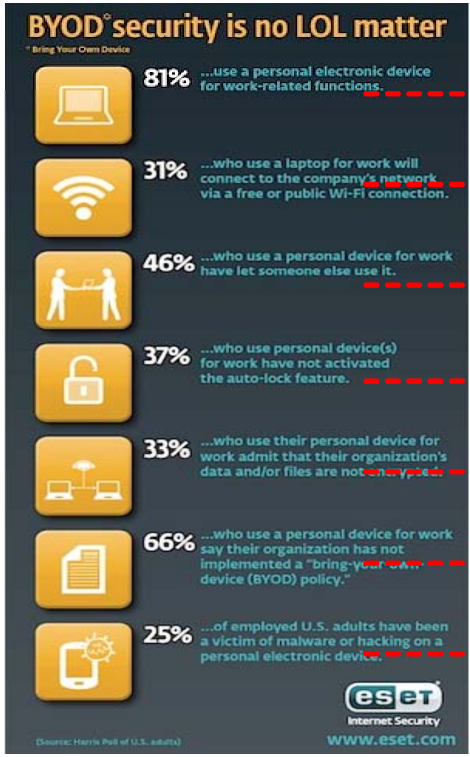
WHO'S DRIVING THE BYOD CHARGE INTERNALLY?

31% IT Department

23% Managing director

21% No One

MATRIX42



BYOD* security is no LOL matter

* Bring Your Own Device

81% ...use a personal electronic device for work-related functions.

31% ...who use a laptop for work will connect to the company's network via a free or public Wi-Fi connection.

46% ...who use a personal device for work have let someone else use it.

37% ...who use personal device(s) for work have not activated the auto-lock feature.

33% ...who use their personal device for work admit that their organization's data and/or files are not encrypted.

66% ...who use a personal device for work say their organization has not implemented a "bring-your-own-device (BYOD) policy."

25% ...of employed U.S. adults have been a victim of malware or hacking on a personal electronic device.

eset Internet Security

(Source: Harris Poll of U.S. adults)

www.eset.com

- Use of individual devices for business by 81%
- Suspected network access rate through WI-FI by 31%
- Use of rent business devices to others by 41%
- Non-setting password or lock-up by 37%
- Unencrypted documents or files by 33%
- Personal devices in the company that not allows BYOD by 66%
- Experience of infected by malicious or hacked code by 25%

Necessity of a maintenance system which supports and manages various mobile devices depend on company's allowance of BYOD is increased!!
Main agent: IT department, high-ranking officers, etc. <Quoted from Tech IT article on July 16, 2012>

02 Product summary

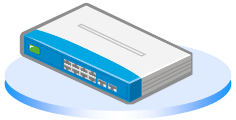
EXAFE MDM™ (Mobile Device Management)

- ✓ Management and security of mobile devices
- ✓ Distribution of essential mobile apps
  (deployment management based on OTA)
- ✓ Management of smart devices
  from robbery or loss
- ✓ Asset management of smart devices
- ✓ Support of Android, iOS
  (tablet PC, Smart phone)

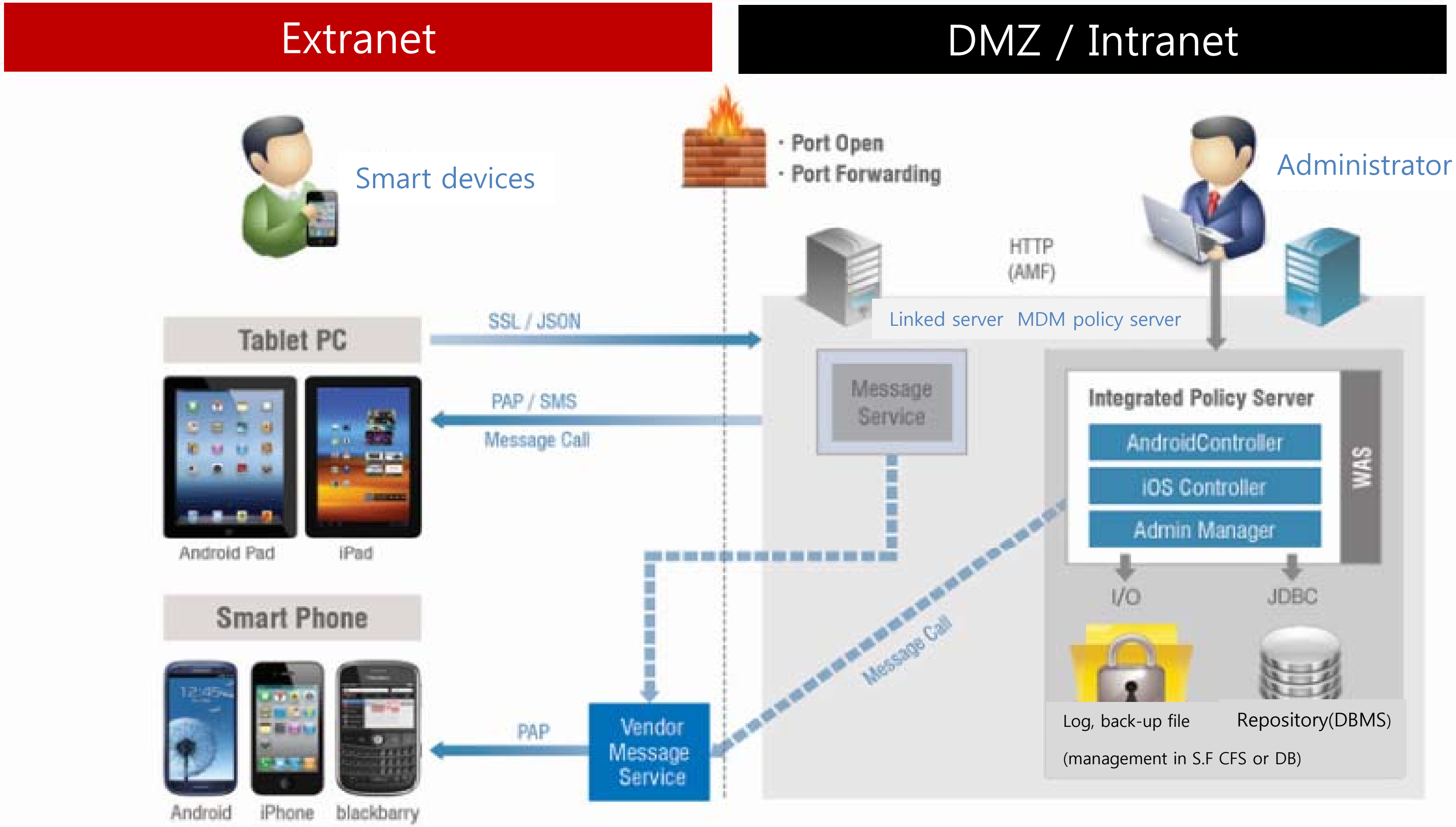
02 Product summary

ExTrus Extreme Trust

EXAFE MDM Product configuration

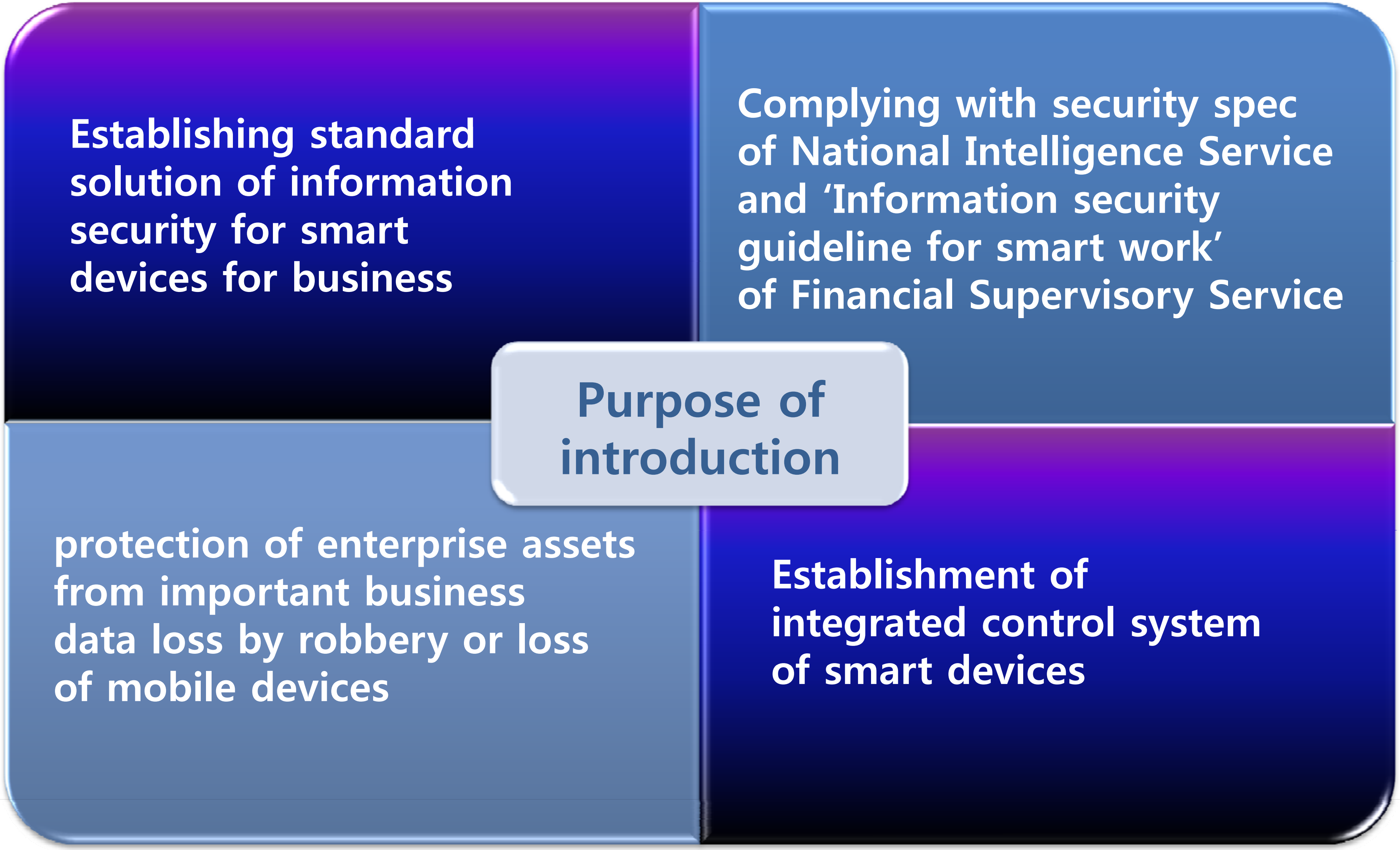
Section	Main items
 Policy server	• **Exafe MDM S/W Manager** - Device policy management for various platforms - Important information back-up and restoration for loss management - Remote command transmission and history management - Audit log management for audit - Integration of self Push and SMS Push for remote control
 Administrator console	• **Exafe MDM Admin Console** - Centralized device management - Security policy management based on group and condition - Present situation management of using smart devices - Device management by remote control (robbery and loss management, mobile office apps management) - User, group, and administrator's information management - Personalization management Service
 Smart device agent	• **Exafe MDM Agent** - Support of smart device platform(Android, iOS) - Prearranged of supporting Window Mobile - Robbery and loss management - Reception and execution of security policy - Management of mobile office apps store for enterprise - log generation and transmission

Configuration Diagram



- PAP : Push Access Protocol, AMF : ActionScript Message Format
- Diverse ways of Message Call : vendor-supported push, self-organized push and support of SMS(optional)

04 Purpose of introduction



Purpose of introduction

Establishing standard solution of information security for smart devices for business

Complying with security spec of National Intelligence Service and 'Information security guideline for smart work' of Financial Supervisory Service

protection of enterprise assets from important business data loss by robbery or loss of mobile devices

Establishment of integrated control system of smart devices

04 Purpose of introduction

Complying with information security guideline for smart work of National Intelligence Service

Section	Detailed requirements	proposal of product
Smart device security	User authentication	Notes
	❖ Execution time A. Execution of the user authentication when operate B. Execution of the user authentication when un-lock C. Logging off automatically from business server when no input within predetermined time	Exafe mPKI + Exafe KeySec
	❖ Authentication method A. Use of complicated password B. Prohibition of plain text for password C. Only security manager can un-lock when failed to authenticate several times D. Execution of authentication by password or electronic signature	
	Dealing with malicious code	Exafe Vaccine
	❖ Anti-virus A. Installing anti-virus software B. Maintaining the newest condition of the engine C. Regular inspection D. Checking whether modulated platform is used or not(jailbreak, rooting, etc.)	
	Control of data loss	Exafe MDM
	❖ Checking whether data is saved or not A. Control of saving data, policy of loss and robbery for business software ❖ Policy of loss and robbery A. Support of remote wiping function for stolen or lost smart devices B. Function of locking device constantly applied - Logging off automatically when no input within predetermined time - Use or access control when input error several times ❖ Access control of storage medium A. Access and data transmission control between smart devices and business PCs - Only storage medium permitted by security manager can only used to smart devices ❖ Access control to hardware resources A. Only permitted programs can access to hardware such as microphones, GPSs, cameras, etc B. Control of output and screen capture - Control of output and screen capture by printer, camera, etc. for business data or screen.	
	❖ Service security A. Prohibition of distribution of apps related with services through public app store (prohibition to non-permitted third-parties) B. Controlling the access to service when update is not accomplished and executing an inspection of the integrity for each important time such as distribution, installation, update, etc.	Exafe AppDefense

04 Purpose of introduction

Complying with ‘Information security guideline for smart work’ of Financial Supervisory Service

Section	Detailed requirements	Proposal of product
Smart device security	Providing protection against security threat of smart devices such as infection of malicious code, robbery/loss	notes
	❖ Prevention from malicious code infection A. Preventing from OS modulation, and maintaining newest security patch for operating system B. Installing vaccine programs, maintaining newest engine condition, and regular inspection with real-time monitoring - For installable devices, downloaded files from internet will be inspected regularly before used (Addition consideration) communication and execution of other processes will be controlled during the action of business program	Exafe Vaccine
	❖ Coping with robbery or loss A. Constantly applied locking in function for devices - Logging off automatically when no input within predetermined time - Use or access control when input error several times B. Blocking the access and remote locking of stolen or lost devices C. Remote wiping of saved program and information in stolen/lost devices ❖ Control of data loss A. Control of the information transmission through devices(including server) - Regulated targets: Bluetooth, Wi-Fi, SD card, etc B. Control of output and screen capture - Control of output and screen capture of business data/screen through printer, camera, etc. (Addition consideration) Control of camera, video/voice recorder of devices (Addition consideration) Control of installation of programs : allowing only permitted programs	Exafe MDM
	Protection from security threat such as hacking through smart work services and accessing without notice by third-parties in the area of business services	
	❖ Authentication security A. (User authentication) multiple authentication by authentication certificate other than user account (ID)/password B. (Device authentication) device authentication by certificate or unique information C. Preventing from exposure and fake/modulation when input and transmit authentication information (Addition consideration) Authentication with more than two information when authenticate devices	Exafe mPKI + Exafe KeySec
	❖ Service security A. (Distribution of business program) Prohibition of distribution of apps related with services through public app store (prohibition to non-permitted third-parties) B. (Business service protection) Controlling the access to services and executing an inspection of the integrity for each important time such as distribution, installation, update, etc. when update is not accomplished	Exafe AppDefense

05 Effect of Investment

- Management using user authentication
- Coping with newest malicious code
- Protection of important data
  - Control of storage medium
  - Prevention of screen capture
  - Measure for robbery or loss
- Protection of Mobile OS
- Resource management
  - Use of authorized programs (GPS, camera, etc)
- Installing permitted or signed S/W by institutions
- Prevention of internet connection by non-permitted devices

- Business reliability improvement by tightening security of smart work environment
- Preparation for in/outside audits by implementing mobile security system
- Reducing individual complaints caused by BYOD policy of the company
- Pro-active of possible data loss occurred by mobile devices
- Improving productivity of the company by managing business applications

06 Product's main function

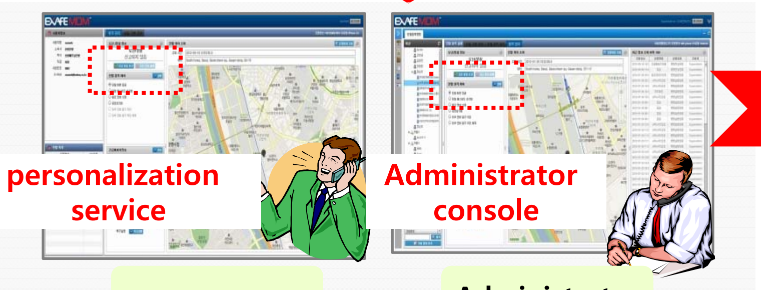
Exafe MDM can manage the asset of the company by deleting critical data or querying location information at the time of lost or stolen data caused by negligence on the business when you carry out important business of the company with company's or personal smart devices.

Asset management by copying with robbery, loss

Acquirement of smart device information

H/W information	.Basic information of devices Resource information of devices
Query of state information	.Communication capacity information .Heartbeat state

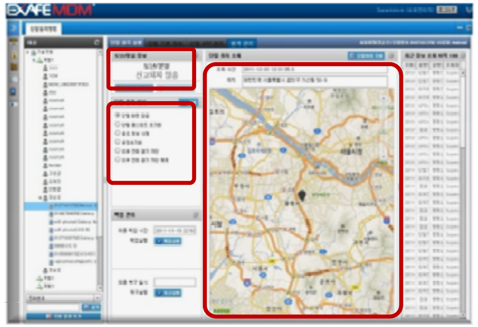
stolen or lost state registration

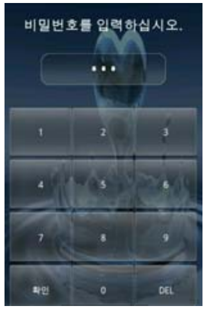


user

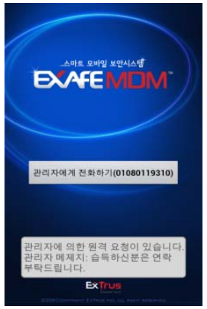
Administrator

Remote control command and location search for smart devices





Remote locking in smart devices



관리자에게 전화하기(01080119310)

관리자에 의한 원격 요청이 있습니다. 관리자 메제지: 습득하신분은 연락 부탁드립니다.

Administrator's emergency call

Locking in device → (limited functions)

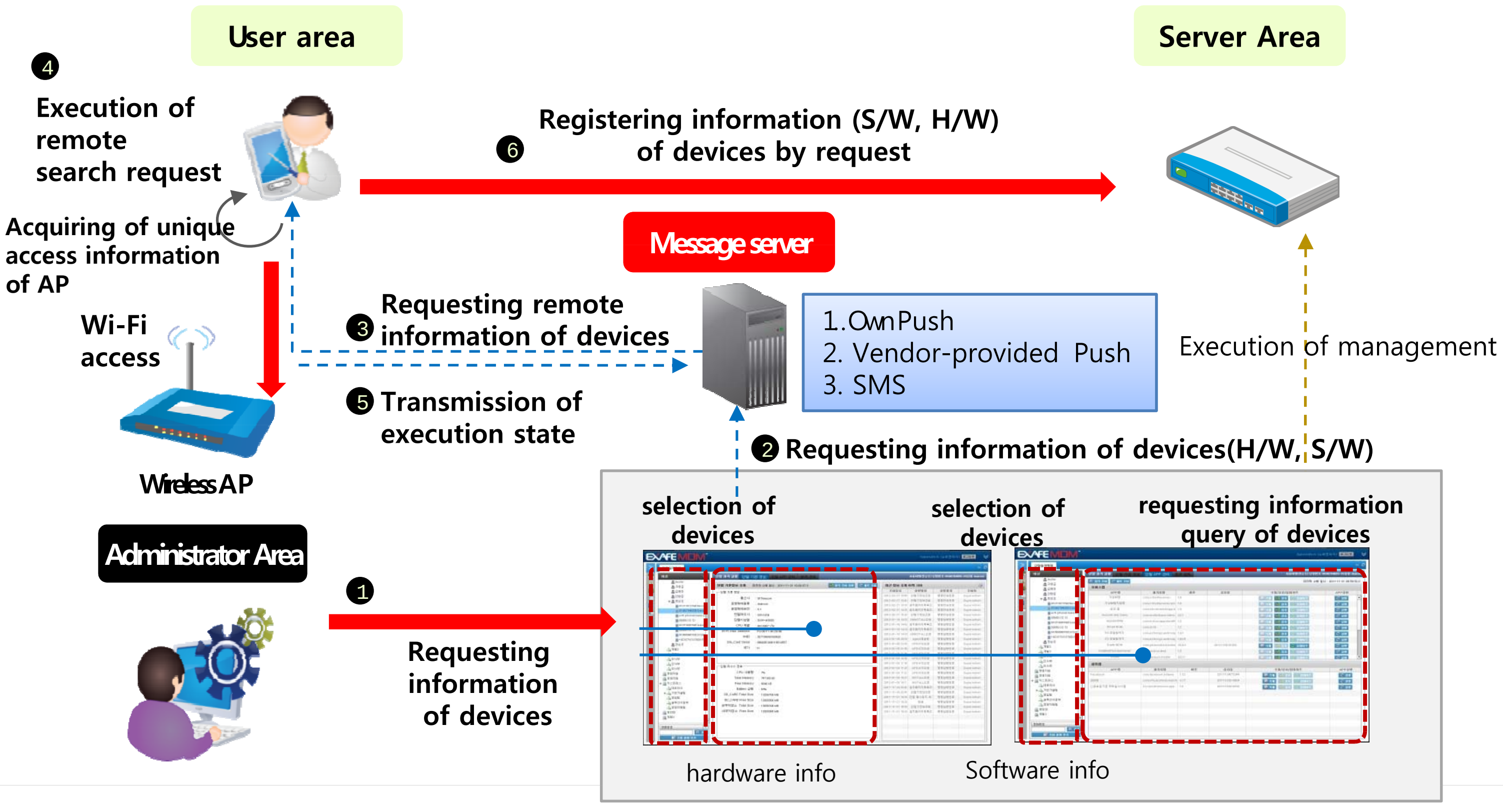
Management of stolen or lost data
Locking in devices
Factory default
Remote wiping important information
Control of phone call
Searching device location information
Backup/ Restoration
Important information back-up of devices] (address book or call log
Important information restoration of devices (address book/call log)
Help desk
Remote control history of each device
Identifying previous state through the previous and remote control history

Impossible key manipulation, data extraction

06 Product's main function

Exafe MDM regularly manages by checking smart devices' state information when register the company's or individual smart devices. Various information (OS, memory, CPU, model, platform, etc.) of smart devices can be monitored or queried remotely. Also, various search functions can be implemented such as querying of data traffic through the cooperation with the telecommunication companies.

Managing information of smart devices



User area

Server Area

4 Execution of remote search request

Acquiring of unique access information of AP

Wi-Fi access

Wireless AP

Administrator Area

6 Registering information (S/W, H/W) of devices by request

Message server

3 Requesting remote information of devices

5 Transmission of execution state

1. Own Push
2. Vendor-provided Push
3. SMS

Execution of management

2 Requesting information of devices(H/W, S/W)

1 Requesting information of devices

selection of devices

selection of devices

requesting information query of devices

hardware info

Software info

Management of devices' setting

- Time setting for lock-up of screen
- Management of wireless AP for access

H/W resource management

- H/W specification query by remote request
- CPU,M/M,HDD,MAC,OS,etc
- Summary of used amount of session or traffic
- Querying to AP information to access data through WIFI

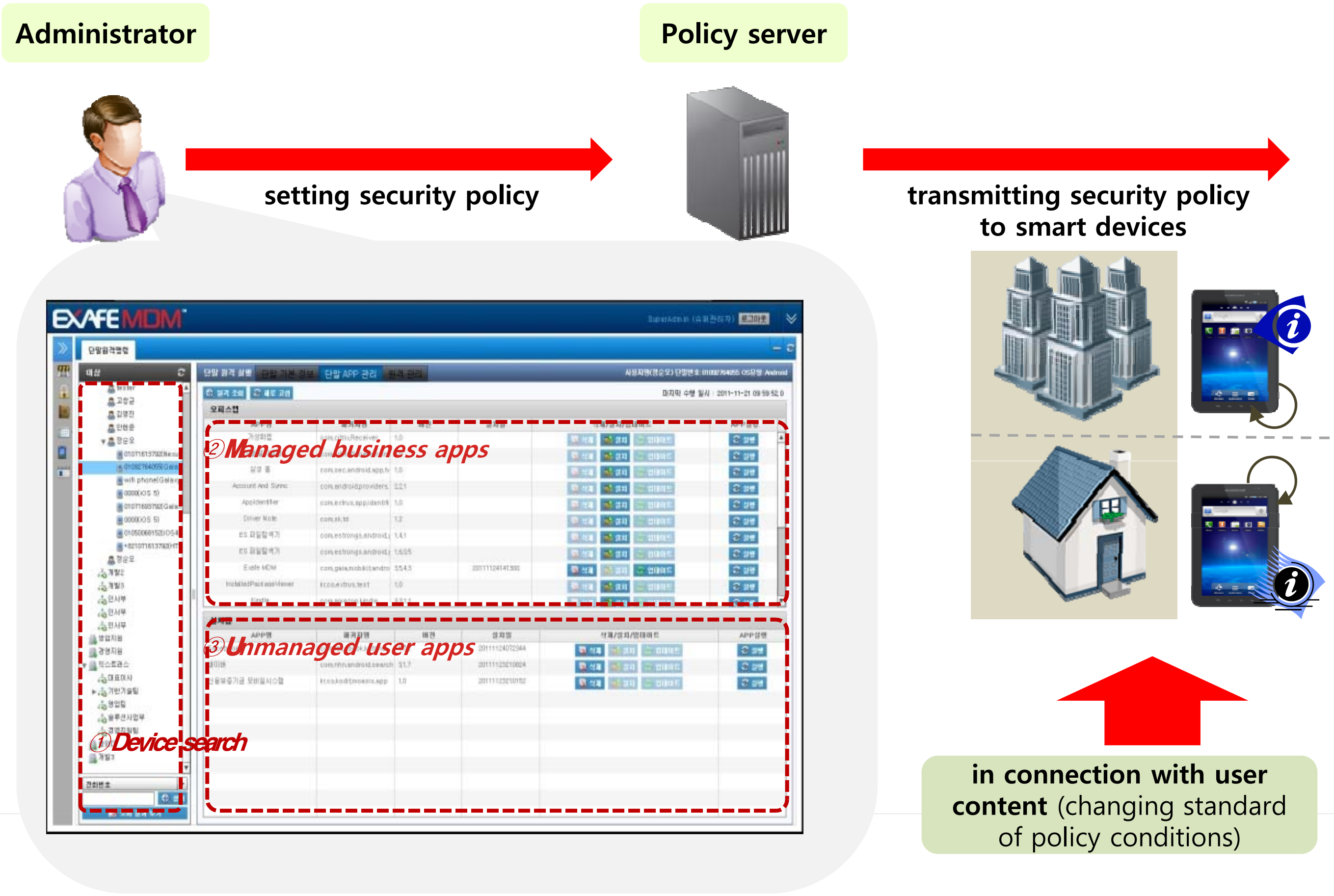
S/W resource management

- Querying list of installed and executed apps
- Leading essential apps to update
- Leading apps to install, update, delete

06 Product's main function

Exafe MDM can improve work efficiency by managing policy of apps in addition to the business when you carry out important business with smart devices of the companies or individuals.

Improving work efficiency by managing business apps



Administrator

Policy server

setting security policy

transmitting security policy to smart devices

in connection with user content (changing standard of policy conditions)

Condition #1	Security policy used inside the company

Applying to security policy (policy condition #1)

Policy item	Set value
stock apps	block
kakaotalk	block
internet apps	block
camera/recorder	block
business apps	permit

Condition #2	Security policy used outside the company

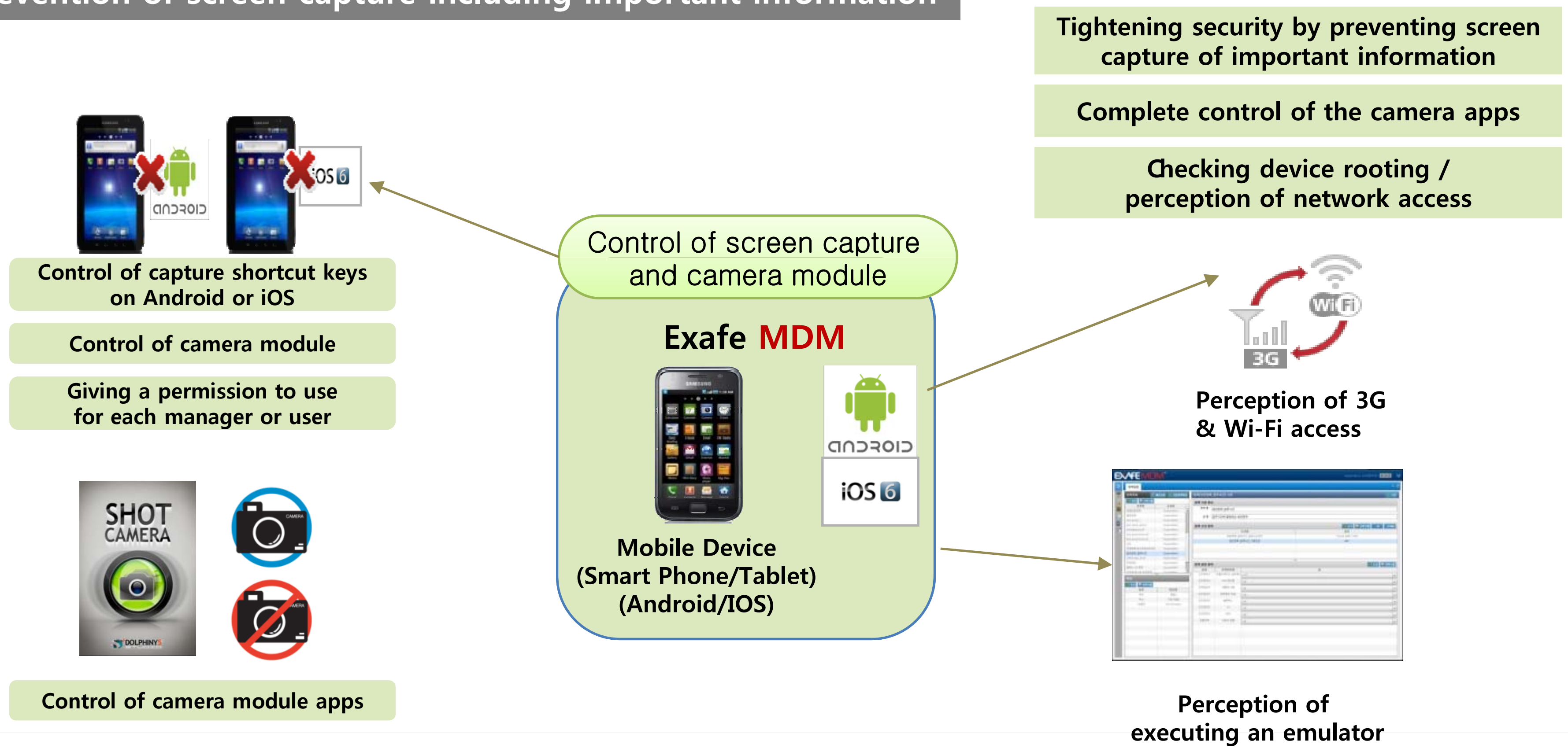
Applying to security policy (policy condition #2)

정책 아이템	설정 값
stock apps	permit
kakaotalk	permit
internet apps	permit
camera/recorder	permit
business apps	block

06 Product’s main function

Exafe MDM cuts off the path revealing the confidential information using screen capture and a camera when you carry out important business with smart devices of the companies or individuals

Prevention of screen capture including important information



Control of capture shortcut keys on Android or iOS

Control of camera module

Giving a permission to use for each manager or user

Control of camera module apps

Control of screen capture and camera module

Exafe MDM

Mobile Device (Smart Phone/Tablet) (Android/IOS)

Tightening security by preventing screen capture of important information

Complete control of the camera apps

Checking device rooting / perception of network access

Perception of 3G & Wi-Fi access

Perception of executing an emulator

06 Product's main function

Exafe MDM reduces communication cost by managing devices against the threats that can be occurred on the communication(3G, Wi-Fi, Bluetooth, etc) and providing through a variety of security policies according to the characteristics of the company when you carry out important business with smart devices of the companies or individuals.

Control of network devices

Security threat on mobile wireless communication

Security threat by using wireless LAN

- **Packet sniffing on wireless LAN**
- **Smart phones attack by unauthorized AP**

Security threat by using Wibro

- **Attack through wireless signal Jamming**
- **Attack by managing message modulation**

Security threat by using Bluetooth

- **Vulnerability of directory search using Bluetooth**
- **Rebooting attack by using Bluetooth**

Control needed

block of smart phone devices

3G **Bluetooth** **Wi-Fi** **USB Tethering**

dud	PB	RM	Branch Manager	Branch Employee	IT department
Camera / Capture	X	X	X	X	X
Bluetooth	X	X	X	X	O
Wi-Fi	O	O	X	X	O
3G	O	O	X	O	X
USB Tethering	O	O	X	X	X
Call	O	[illegible]	[illegible]	X	O
GPS	O	O	[illegible]	[illegible]	[illegible]

Demonstration

Policy setting based lon location

3G ☑
Wi-Fi ☑
Bluetooth □
Tethering □

3G ☑
Wi-Fi ☑
Bluetooth ☑
Tethering ☑

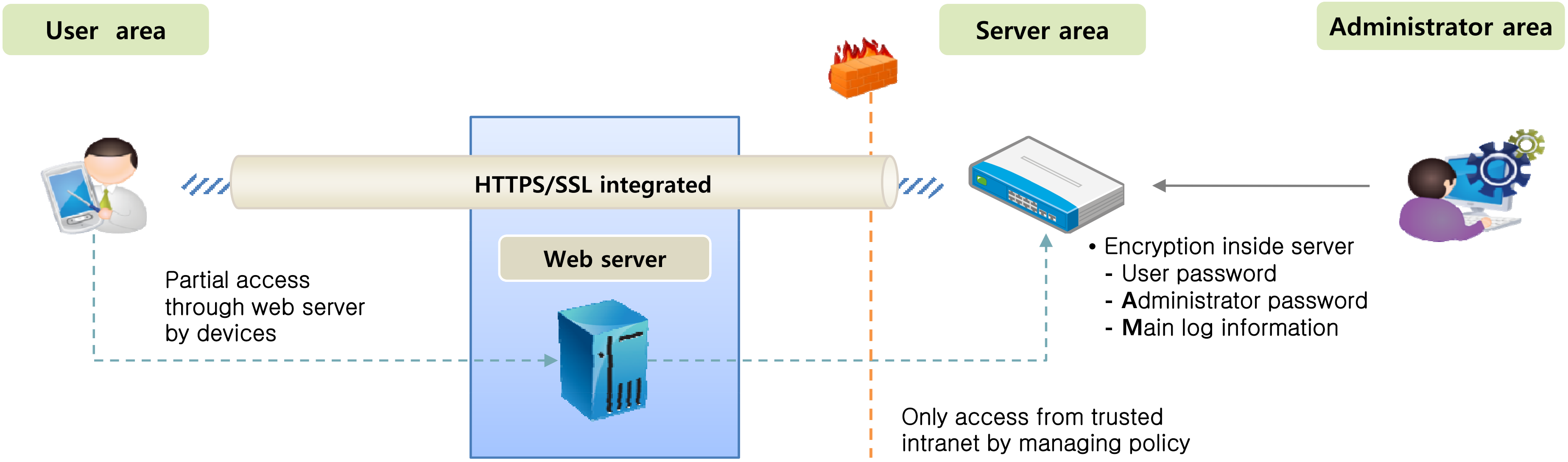
3G ☑
Wi-Fi □
Bluetooth □
Tethering □

06 Product's main function

Exafe MDM runs the security through encryption of important information saved in networks, servers or d evices through cooperation with SSL when you carry out important business with smart devices of the co mpanies or individuals

Encryption of communication network

Management of security policy - encryption of sending and receiving data or Push service



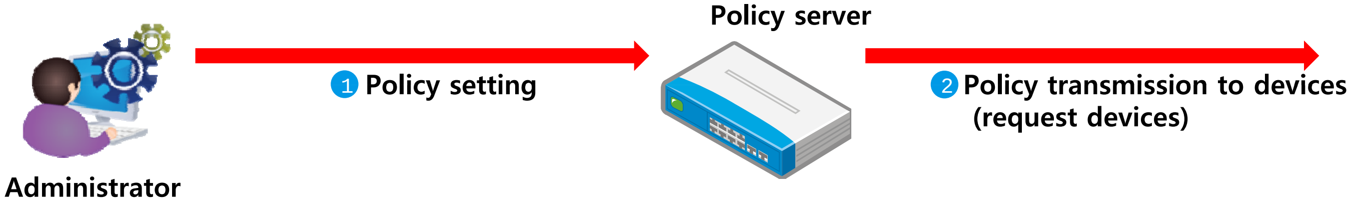
- Encryption inside server
  - User password
  - Administrator password
  - Main log information

Only access from trusted intranet by managing policy

06 Product's main function

Exafe MDM can manage the asset by registering policies (GPS/ WPS, Cell ID, access control integration, business hours, WhiteList) when you carry out important business with smart devices of the companies or individuals.

Policy management base on condition



Company	Policy condition #1 :Company

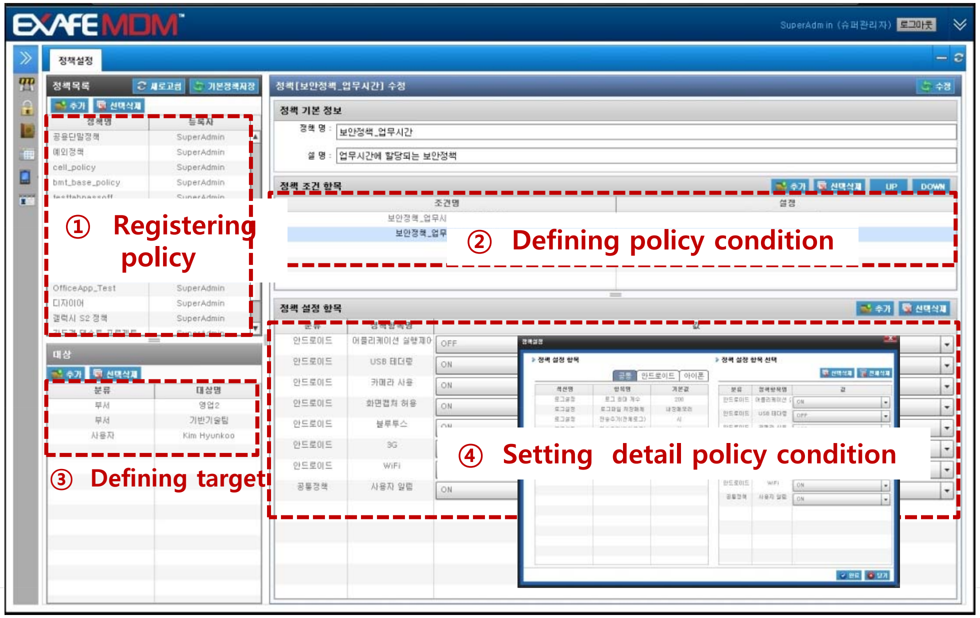
Policy item	Set value
using camera	block
screen capture	block
W ii – F i / AP	restriction of registered AP
3G	block
Bluetooth	block

③ applying to policy(policy condition #1)

③ applying to policy(policy condition #2)

Home	Policy condition #2 : Home

Policy item	Set value
using camera	permit
screen capture	permit
W ii – F i / AP	permit all
3G	permit
Bluetooth	permit



정책[보안정책_업무시간] 수정

정책 기본 정보

정책 명 : 보안정책_업무시간

설 명 : 업무시간에 할당되는 보안정책

정책명	등록자
공용단말정책	SuperAdmin
예외정책	SuperAdmin
cell_policy	SuperAdmin
bmt_base_policy	SuperAdmin
OfficeApp_Test	SuperAdmin
디자이어	SuperAdmin
갤럭시 S2 정책	SuperAdmin

① Registering policy

정책 조건 항목

조건명	설정
보안정책_업무시	
보안정책_업무	

② Defining policy condition

분류	대상명
부서	영업2
부서	기반기술팀
사용자	Kim Hyunkoo

③ Defining target

분류	정책항목명	값
안드로이드	어플리케이션 실행제어	OFF
안드로이드	USB 테더링	ON
안드로이드	카메라 사용	ON
안드로이드	화면캡처 허용	ON
안드로이드	블루투스	ON
안드로이드	3G	
안드로이드	WiFi	
공통정책	사용자 알림	ON

④ Setting detail policy condition

Integrated with UC (standard of changing policy condition)

※When policy condition changed, Android changes configuration inside devices and iOS transmits changed configuration from a server to devices.

06 Product’s main function

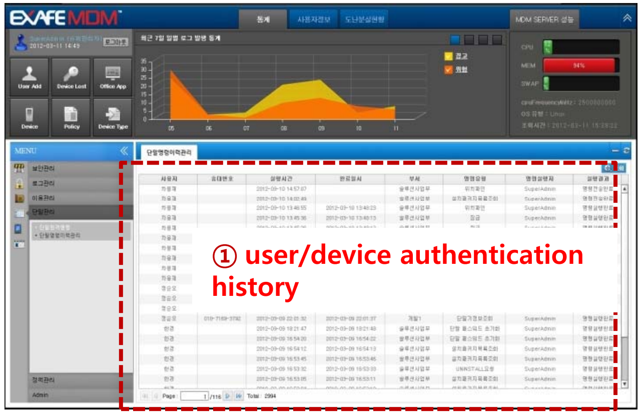
ExTrus
Extreme Trust

Exafe MDM makes you be able to use audit log by logging history of acting or reporting when you carry out important business with smart devices of the companies or individuals.

Managing log and statistic

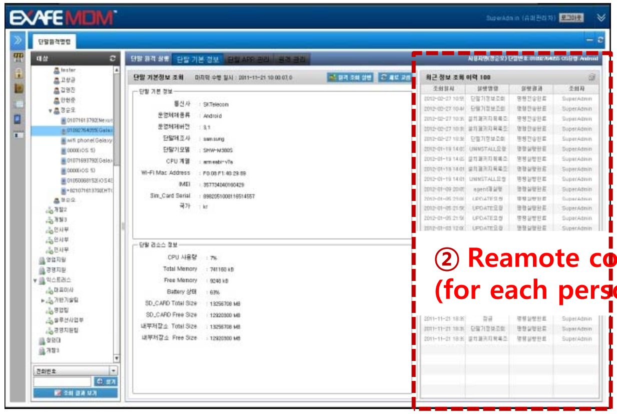
- User access time, device authenticated time, successiveness, and recent access time to update the policy
- Present state of apps installation or policy distribution for each device.
- History of administrator’s act from manager console (daily recording files)
- Present state of stolen, lost, backup, recovery, installation of client and recent log

Audit to users, devices’ authentication information



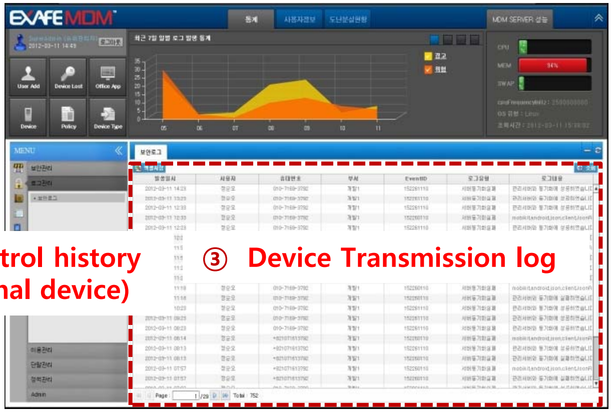
① user/device authentication history

Processed result of remote control



② Reamote control history (for each personal device)

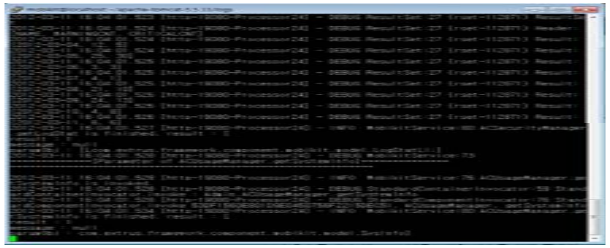
Device’s RAW log



③ Device Transmission log

Administrator’s act

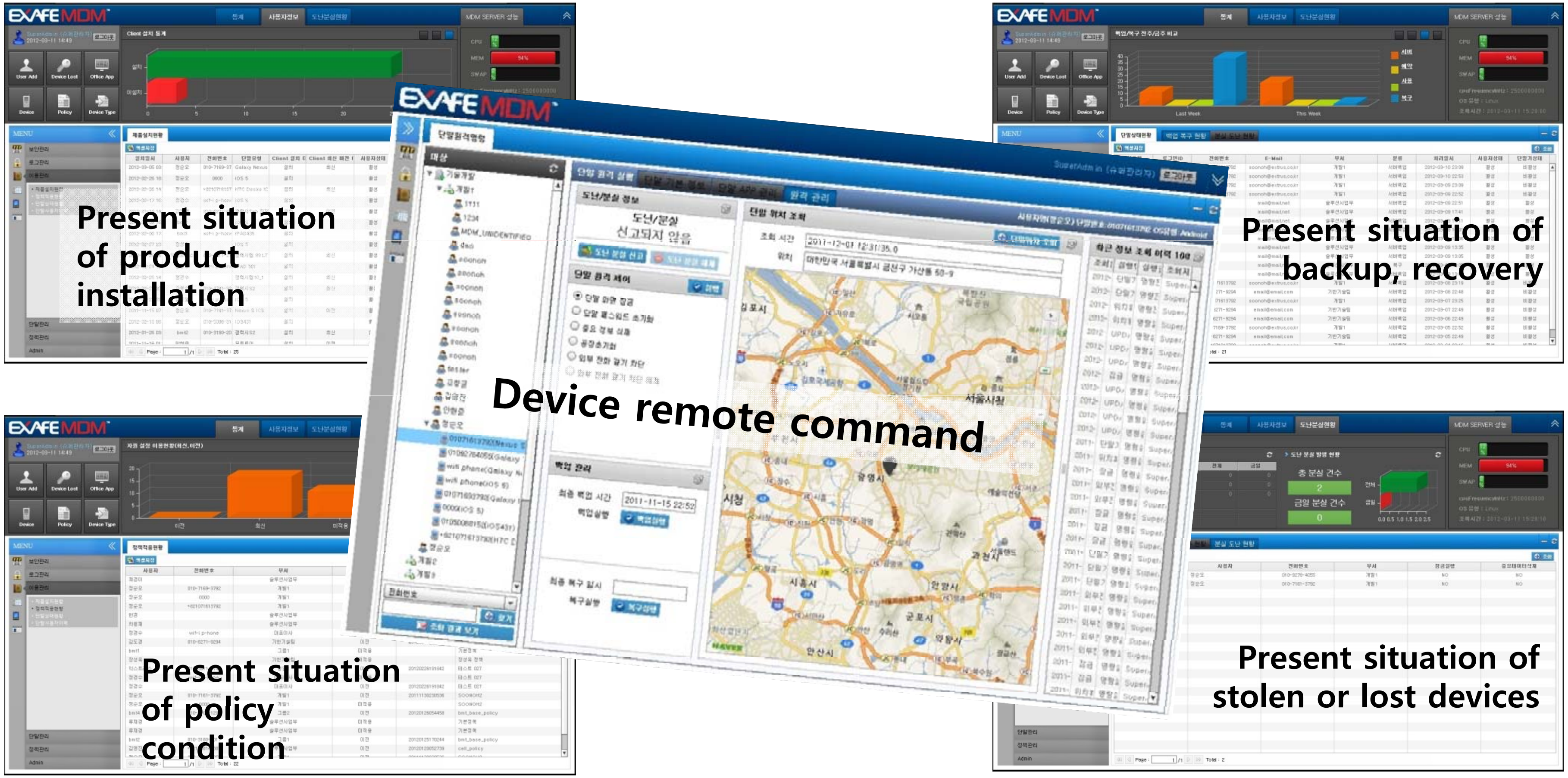
```
2011-09-16 15:27:00.910 [http-8080-Processor2] - [INFO ] AdminConsoleManager:1688 [IP:112.216.169.150, admin]
2011-09-16 15:27:05.682 [http-8080-Processor12] - [INFO ] ACPolicyManager:4066 update
```



06 Product’s main function

Exafe MDM can monitor in real time agent installation, operational state, user and group-specific policies state, application backup state, recovery state and lost or stolen reports, etc.

Monitoring smart devices



Present situation of product installation

Device remote command

Present situation of backup, recovery

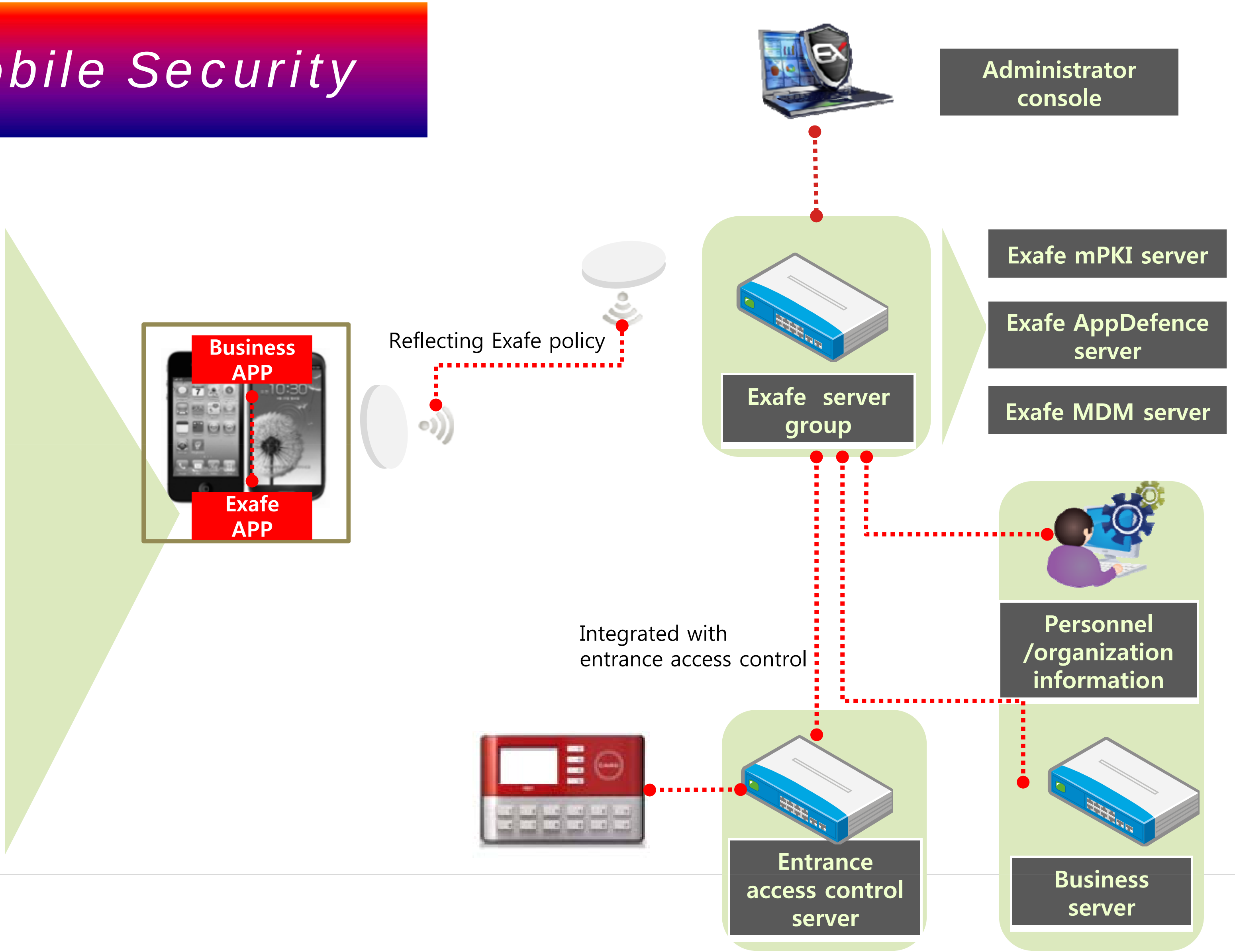
Present situation of policy condition

Present situation of stolen or lost devices

07 Guide of mobile security build-up

Smart Mobile Security

- Exafe Crypto
- Exafe MDM
- Exafe Vaccine
- Exafe mPKI
- Exafe KeySec
- Exafe AppDefence
- Exafe Wall
- Exafe RemoteCall



08 Reference

ExTrus
Extreme Trust

Public Institution

행정안전부
MINISTRY OF PUBLIC ADMINISTRATION AND SECURITY

교육과학기술부
MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

KODIT 신용보증기금
KOREA CREDIT GUARANTEE FUND

사학연금

TS
교통안전공단

KFDA
식품의약품안전청
Korea Food & Drug Administration

기상청
Korea Meteorological Administration

법무부보호관찰소

POMA
우체국시설관리단

Private Company

kt

SK C&C

S-OIL

BS 부산은행

Webcash

INICIS

AMOREPACIFIC
CORPORATION

You can trust
Extrus, Inc.
at any time.

Thanks.

[Product Inquiry] Extrus, Inc.

☎ +82-2-6959-0774 ⓔ-mail : extrus@extrus.co.kr