# OMTP

## ANTI-VIRUS CLIENT REQUIREMENTS FOR DEVICE MANAGEMENT



| | |
|---|---|
| **VERSION:** | Version 1_0 |
| **STATUS:** | Approved for publication |
| **DATE OF PUBLICATION:** | 23rd January 2008 |
| **OWNER:** | OMTP Limited |

# CONTENTS

# 1 INTRODUCTION

## 1.1 DOCUMENT PURPOSE

This document defines the requirements for anti-virus clients on mobile network communications Terminals that can be remotely managed by a mobile network operator's device management authority.

The Terminal itself needs to allow such an anti-virus client to be remotely managed. Therefore, a Terminal needs to fulfil a basic set of requirements for this type of remote application management.

As an anti-virus client will use a Terminal's remote management features and does not need to implement a complete remote application management solution, this document concentrates on the features that an anti-virus client needs to support.

It is assumed that an anti-virus client is a trusted application as defined in OMTP ASF [1].

This document is split into the following chapters:

Chapter 2 describes two use cases. They are examples for the use of an anti-virus client that is remotely managed by a mobile network operator's customer service agent on behalf of a customer.

Chapter 3 contains the requirements for an anti-virus client that can be the remotely managed via OMA Device Management (DM) v1.2.

Chapter 4 defines the requirements for an anti-virus client that can be remotely managed via OMA DM v1.2 and OMA Software Component Management Object (SCOMO).

Chapter 5 and 6 list the terms and abbreviations respectively used in this document.

Chapter 7 contains the documents that are referenced in this document.

## 1.2 PROFILES

Anti-virus clients fulfilling the remote management requirements defined in this document are likely to be deployed on Terminals with a variety of capabilities in terms of their processing power, memory, or remote management support. It is highly likely that not all Terminals will support OMA DM and OMA SCOMO in the future. However, an OMA DM enabled Terminal provides features that are well suited to remotely manage the specific settings of an anti-virus client.

Additional management features are supported by Terminals that offer advanced DM capabilities like OMA SCOMO or remote process management. An anti-virus client on such a Terminal allows more sophisticated features for the software management like the remotely initialised installation or execution.

Due to these different capabilities, the requirements are defined as part of two profiles. These profiles encompass requirements that are outlined in the next sub-sections.

### 1.2.1 ADMAV BASIC PROFILE

This profile encompasses a set of requirements in order to allow the remote anti-virus client configuration using OMA DM v1.2 [3]. The requirements in Chapter 3 apply to this profile.

ADMAV basic profile implementations will typically reside on a Terminal that supports OMA DM only. However, an anti-virus client fulfilling the ADMAV basic profile could also run on a Terminal offering OMA SCOMO or remote process management capabilities. In this case, the anti-virus client does not benefit from the Terminal's enhanced OMA SCOMO capabilities.

### 1.2.2 ADMAV FULL PROFILE

This profile adds a set of enhanced requirements to the ADMAV basic profile in order to allow the remote settings management through OMA DM, remote software management using OMA SCOMO and remote process management through OMA DM. The requirements in both chapters 3 and 4 apply to this profile.

ADMAV full profile implementations will typically reside on a Terminal that supports OMA DM and OMA SCOMO. However, an anti-virus client fulfilling the ADMAV full profile could also be used in an OMA DM enabled Terminal. In this case, OMA DM will only be able to manage the anti-virus client's settings.

## 1.3 BUSINESS RATIONALE

A mobile network operator (MNO) does not usually have influence on the anti-virus client products that their customers install onto their Terminals. Depending on the Terminal model and its operating system, various anti-virus client products are available on the market. The software is provided for downloading on servers in the Internet, on CD-ROM or on removable memory cards for instance.

Once the software is downloaded to the Terminal, the user manually installs it. The user is the only person who has access to the software configuration and the log files with scanning results. If the user needs support or observes a malware issue, an MNO's customer service is unlikely to be able to fully resolve the issue.

An MNO that wants to provide Terminal-based protection against malware, may provide Terminals with open operating systems that have a pre-loaded anti-virus client which the user installs., The MNO customer service agent would not have access to the software's configuration or log files.

Customers may buy their Terminals from other sources and such Terminals may not be provided with a pre-installed anti-virus client. An MNO that wants to provide a Terminal-based protection against malware may also want to provide a solution for these customers.

Therefore, MNOs are interested in the remote management of anti-virus clients. The remote management shall enable an MNO for instance:

- to remotely initiate the delivery of an anti-virus client to a Terminal that was sold without it,
- to remotely initiate the installation of an anti-virus client,
- to retrieve the current status of an installed anti-virus client, e.g. the software is running, a malware was detected and quarantined, the latest software update was not installed, yet.

Some enterprises are also likely to be interested in the remote management of anti-virus clients.

## 1.4 INTENDED AUDIENCE

There are two main audiences for this requirements document:

- Mobile network operators
- Anti-virus client vendors

## 1.5 CONVENTIONS

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [2].

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

The requirements within this document are uniquely identified using the following format:

ADMAV-####, where:

- ADMAV stands for Advanced Device Management Anti-virus
- #### is a 4 digit number uniquely identifying the requirement

# 2 USE CASES

## 2.1 REMOTE CONFIGURATION

Jim has a Terminal with an anti-virus client that can be remotely configured by his MNO. He often uses his Bluetooth headset especially when he waits for the train in the morning and evening. He is often annoyed by connection requests from unknown peers. However, he is confident that his Terminal is protected by the anti-virus client and sometimes accepts the requests because of funny texts. He receives a funny game and some surprising videos. The anti-virus client has never alerted him about the detection of any known malware.

He then notices on his phone bill that there have been many premium rate calls to offshore numbers. He calls his MNO's customer service for clarification. Jim agrees that the customer service agent can remotely check the anti-virus client. The customer service agent finds out that the automatic updates are switched off. Jim remembers that he switched it off during his vacation three months ago to avoid roaming costs.

The customer service agent switches automatic updates on and Jim manually starts the update. After the successful update of the client including the latest virus definitions database, Jim initiates a scan of the Terminal's full file system. The scanner detects a well known game which is in fact a trojan that was first observed two weeks earlier. The anti-virus client asks Jim to either quarantine or delete it. Jim chooses the delete function.

## 2.2 REMOTE INSTALLATION

Jo owns a Terminal and her friend sends her a game over Bluetooth. Jo installs the game even though a warning indicates that it is from an unknown source and might be untrusted. Jo plays the game and enjoys being able to send her high score to a website which shows that she is the 5th best player this month. When Jo checks her pre-pay balance she discovers that it has dropped by €45 below what she expects. She calls her mobile network operator's customer service who informs her that calls and photo messages were sent by her to several numbers including some at a premium rate. It looks like the actions of a new malware that was observed a few weeks ago in another country.

The customer service agent asks Jo whether she needs assistance in the disinfection of this malware and wants to be protected against malware in the future. Upon agreement, the agent remotely installs an anti-virus client on the Terminal which scans all applications installed and executing on Jo’s device. The anti-virus client detects the game as the known malware which is in fact a recognised trojan which can initiate hidden calls in this way. The anti-virus client asks Jo to de-install the game, which she does.

# 3 SETTINGS MANAGEMENT AND LOGGING

In order to remotely configure an ant-virus client's settings on an OMA DM enabled Terminal, an anti-virus client shall be integrated with the Terminal's OMA Device Management v1.2 features (see [3]).

Specifically, this means that the anti-virus client extends the OMA Device Management Tree (DM Tree) with the needed branch during the anti-virus client installation process.

## *3.1 GENERAL REQUIREMENTS*

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0010** | The anti-virus client SHALL be manageable via OMA DM v1.2 [3]. |

## *3.2 SETTINGS MANAGEMENT REQUIREMENTS*

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0020** | The management objects' changes in the DM Tree SHALL take effect as soon as practical after they were initiated via OMA DM to the anti-virus client and were updated in the DM Tree. |

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0030** | The anti-virus client SHALL expose in the DM Tree the information about:<br>– Vendor<br>– Product name<br>– Release number<br>– Build version<br>Name conventions:<br>- Vendor: Legal company name or developer's full name.<br>Example: "AVvendor Ltd."<br>- Product name: The software product's name.<br>Example: "SuperAV Mobile".<br>- Release number: A code of any format used by the Vendor to identify a software release. Often a major release number and a minor release number separated by a point are used.<br>Example: "3.2".<br>- Build version: A code of any format may be used by the Vendor to uniquely identify a software release by a so-called build version to differentiate releases for different markets for instance. Then, the software product may have the same Release number but a different Build version.<br>Example: "1303" |
| **ADMAV-0040** | The anti-virus client SHALL expose in the DM Tree the information about the virus definitions databases:<br>- Version number of each database<br>- Date and time of the last database update in the format YYYY-MM-DD hh:mm:ss |
| **ADMAV-0050** | The anti-virus client SHALL expose in the DM Tree the information about the scan engine(s) that are integrated in the anti-virus client:<br>- Number of scan engines<br>- Version number of each scan engine<br>- Build version of each scan engine |

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0060** | The anti-virus client SHALL expose the auto-protect mode (e.g. "on" or "off" for real-time scanning of all incoming and outgoing data) in the DM Tree. |
| **ADMAV-0070** | The anti-virus client SHALL expose the scanning level (e.g. quick, full) in the DM Tree. |
| **ADMAV-0080** | The anti-virus client SHALL expose the default action to be performed with a detected file (e.g. delete, quarantine, ignore, repair) in the DM Tree. |
| **ADMAV-0090** | The anti-virus client SHALL expose the types of files to be scanned (e.g. all file types, list of selected file types, ignore list of selected file types). |
| **ADMAV-0100** | The anti-virus client SHALL expose the directories to be scanned (e.g. all directories, list of selected directories, ignore list of selected directories) in the DM Tree. |
| **ADMAV-0110** | The anti-virus client SHALL expose the maximum size of the anti-virus client log file (e.g. file size in KBytes or number of logged events) in the DM Tree. |
| **ADMAV-0120** | The anti-virus client SHALL expose the maximum size of the scan log file (e.g. file size in KBytes or number of logged events) in the DM Tree. |
| **ADMAV-0130** | The anti-virus client SHALL expose the automatic software update interval policy (e.g. daily, bi-daily, weekly, bi-weekly, or in minutes) in the DM Tree. |
| **ADMAV-0140** | The anti-virus client SHALL expose in the DM Tree the configuration parameter that determines that it must be automatically executed during or just after Terminal boot-up (e.g. yes, no). |
| **ADMAV-0150** | The anti-virus client SHALL expose in the DM Tree a configuration parameter that allows the initiation of the virus definitions databases update. |
| **ADMAV-0160** | The anti-virus client SHALL expose in the DM Tree a configuration parameter that allows the initiation of a scan. |
| **ADMAV-0170** | The anti-virus client SHALL monitor changes to its settings in the DM Tree and implement any changes. |

## 3.3 LOGGING REQUIREMENTS

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0180** | The anti-virus client SHALL expose in the DM Tree the anti-virus client log file that contains information about the recent process events. |
| **ADMAV-0190** | The anti-virus client log file SHALL contain the following fields per event:<br>1. Time stamp in the format YYYY-MM-DD hh:mm:ss<br>2. Process event (e.g. executed, terminated, error)<br>3. Error code in case of an error |
| **ADMAV-0200** | The anti-virus client SHALL expose in the DM Tree scan engine(s) scan log file containing the recent scan results. |
| **ADMAV-0210** | The scan log file SHALL have the following fields per event:<br>1. Time stamp in the format YYYY-MM-DD hh:mm:ss<br>2. Name of the detected malware or exploit<br>3. Action (e.g. deleted, quarantined, ignored, released) |

# 4 SOFTWARE AND PROCESS MANAGEMENT

In order to remotely manage an anti-virus client on an OMA SCOMO enabled Terminal, it needs to be manageable via OMA SCOMO to install and remove it for instance.

## *4.1 SOFTWARE MANAGEMENT REQUIREMENTS*

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0220** | OMA SCOMO [4] SHALL allow the installation and removal of the anti-virus client. |

## *4.2 PROCESS MANAGEMENT REQUIREMENTS*

| REQ. ID | REQUIREMENT |
|---|---|
| **ADMAV-0230** | It SHALL be possible to initialise the execution of the anti-virus client through OMA DM. |
| **ADMAV-0240** | It SHOULD be possible to terminate the execution of the anti-virus client through OMA DM. |
| **ADMAV-0250** | It SHALL be possible to retrieve information about the anti-virus client's current execution status (e.g. running, not executed, error) through OMA DM. |

# 5 DEFINITION OF TERMS

| TERM | DESCRIPTION |
|---|---|
| **DM TREE** | The mechanism by which an OMA device management client interacts with the Terminal, e.g. by storing and retrieving values from it and by manipulating the properties of it. It is called “management tree” in the OMA DM [3] specification. The DM Tree organizes all available management objects in the Terminal. |
| **TERMINAL** | Used as an alternative term for a cellular telephone, handset or device. |

# 6 ABBREVIATIONS

| ABBREVIATION | DESCRIPTION |
|---|---|
| **ADM** | Advanced Device Management |
| **ADMAV** | Advanced Device Management for Anti-Virus clients |
| **DM** | Device Management |
| **MNO** | Mobile Network Operator |
| **OMA** | Open Mobile Alliance |
| **OMTP** | Open Mobile Terminal Platform |
| **SCOMO** | Software Component Management Object |

# 7 REFERENCED DOCUMENTS

| NO. | DOCUMENT | AUTHOR | DATE |
|---|---|---|---|
| 1 | OMTP Application Security Framework v2.1<br><br>http://www.omtp.org/pdf/recommendation_papers/OMTP_Application_Security_Framework_v2_1.pdf | OMTP | Sept 2007 |
| 2 | RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels<br><br>http://www.ietf.org/rfc/rfc2119.txt | IETF | March 1997 |
| 3 | OMA Device Management v1.2<br><br>http://www.openmobilealliance.org/release_program/dm_v1_2A.html | OMA | Feb 2007 |
| 4 | OMA Software Component Management Object Requirements<br><br>http://www.openmobilealliance.org/release_program/rd.html | OMA | July 2007 |

**-------- END OF DOCUMENT --------**