

ApplicGate Exchange ActiveSync (EAS)

1 Motivation

Microsoft Exchange is a widely-used email server.

Many smartphones and mobile devices access these servers via the Internet.

But:

- **The only authentication option is username and password!**
Do you really think that username/password is sufficient to access Exchange mailboxes by any device from everywhere in the Internet?
- **Any user can change the mail client and the mobile device!**
Would you like to resume control over the mobile devices (smartphones, tablets etc.) accessing your Exchange mail server?

If you would like that:

- Only identified devices are allowed to access the mail server.
- The users cannot change the client hardware and software without central permission.
- An additional authentication option by certificates can be enabled on a device basis.
- Additional monitoring is available.

Install ApplicGate EAS!

It is easy to operate:

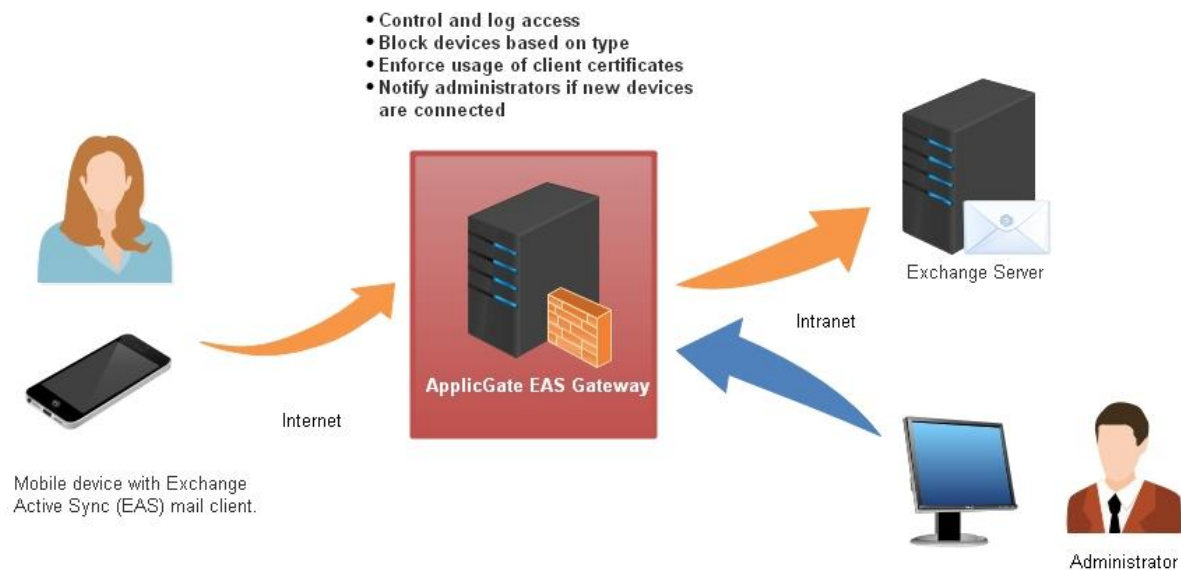
- **You do not need an expensive and complicate Mobile Device Management (MDM)!**
- No change at client software and hardware necessary!
- No change at the Exchange server necessary!

2 How does this work?

- Mobile devices communicate with the Exchange server using the Exchange ActiveSync protocol. You can find an introduction in the Wikipedia article [Exchange ActiveSync](#).
- ApplicGate EAS intercepts and monitors the communication between the mail client on the mobile device and the Exchange server.
- User names (sAMAccountName, userPrincipalName) are checked against the Active Directory.
- ApplicGate EAS does not change the data flow between the mail client and the Exchange server.
- At initial logon at the Exchange server a unique Device ID will be generated for each new device. This ensures that new devices and new mail clients are detected.

- The administrator can allow a specified number of mobile devices (different Device IDs) per user mailbox.
- Administration of mobile devices can be delegated to different persons according to the location of user objects in the Active Directory
- **Connection attempts of additional devices are blocked and the responsible administrator will be notified!**

3 Network Schema



Remark:

The “ApplicGate EAS” role can be installed at the Exchange Server. So there is no need for an additional server.

4 Prerequisites

- If ApplicGate EAS should be installed at a separate server:
Any Windows or Linux (e.g. latest version of Debian or Raspbian) machine can be used.
- ApplicGate software, see www.applicgate.com
- Web server certificate (same as used at the Exchange server)
- Export of Active Directory

5 Installation and Configuration of ApplicGate EAS

5.1 Configuration Files

We need two configuration file: **routing.csv** and **groups.csv** (These examples must be adapted for local needs.)

Detailed information about ApplicGate EAS and examples for the configuration files to download can be found [here](#).

For general information see <https://help.applicgate.com> or the local help built-in ApplicGate

5.1.1 Example for Routing.csv

```
SourceIP;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Expiration;Type;UID;Comment;eMail
* ;127.0.0.1;99 ;manage ;3000 ;15 ;*;REFRH:5,TINT:5,LOG:1, GRPUPD,RTUPD, DELLOG:20, LGS, LGTIME, FLG:yes, BPRI:AboveNormal ;MGM ;Management ;
* ;* ;443 ;* ;eas.xx.com;443;*;SSL:server.pfx/passw, SSLTARGET:eas.xx.com, EAS:Block!2!Country!Site, APATH:/Microsoft-Server-ActiveSync?, NOTIFYT:A_EAS;EAS; ;
* ;* ;999 ;status ; ; ;*;SSL:server.pfx/passw, CCR:A_EAS, DEFCMD:statea$, EASACL:A_EAS ;EASmgmt;EAS Management;
```


Detailed description:

- The **first** entry defines the local **management** interface:
Local access via `http://127.0.0.1:99`
In this case DestinationIP 3000 defines the maximum number of connections allowed and DestinationPort 15 defines the default Time-To-Live (TTL) in minutes.
The keyword REFRRH sets the refresh timer for the home page to 5 seconds, TINIT defines the internal timer interval with 5 seconds, GRPUPD and RTUPD allow updates of group.csv and routing.csv via the web interface, DELLOG defines the number of days to delete old log files, LGS enables logging of sessions (one line per session with start time, duration etc.), LGTIME enables insertion of date/time in front of each log message, FLG enables logging to the general log file, BPRI sets the priority of ApplicGate.
Optional keyword: LOCATEIP:`http://www.speedguide.net/ip/%IP%` to locate the IP addresses of the mobile devices.
- The **second** entry defines the connection from the mobile devices to the Exchange Server:
Accessible via all network interfaces via TCP port 443.
DestinationIP and DestinationPort must be specified.
The Type field defines the server certificate via keyword SSL and enables TLS to the Exchange server via keyword SSLTARGET.
Following additional keywords are defined to configure the EAS role (bold keywords are required):

- **EAS:Block!OUposition!ou1name!ou2name ... Activate EAS support for this routing entry**
 It is a good practice to start in learn mode, non-blocking mode, e.g. EAS:Learn!2!Country!Site
OUposition, ou1name and *ou2name* are optional. These fields define the display format and are used to define granular access rights:
 OUposition ... OU of this position (OU1) and next OU (OU2) will be shown at EAS user listing, if 0 or this parameter is missing: no OU will be shown. E.g. if there is following DN field in ADusers.csv (see description in a chapter below) and OUposition is 2:
 CN=MueLLer Max,OU=Users,OU=LNZT,OU=AT,OU=AGC,DC=abc,DC=company,DC=net
 then AT (country code in this example) and LNZT (site code in this example) will be shown in the EAS user list as OU1 and OU2
 ou1name ... name for OU1 for display, default is OU1, if blank: OU1 will not be displayed
 ou2name ... name for OU2 for display, default is OU2, if blank: OU2 will not be displayed
 - **APATH:/Microsoft-Server-ActiveSync? ... Allow EAS URLs only (and disallows Outlook Web Access)**
 - RDRA ... optional, send error message back if URL does not match the value of keyword APATH.
 - EASBLK:B_EAS ... optional, block specified devices listed in the group B_EAS
 - NOTIFYT:A_EAS ... optional, notify administrators about blocking as defined in the group (see definition below)
 - EASNDA:NumberOfDevicesAllowed ... optional, sets the initial number of devices allowed (default is 1)
 if NumberOfDevicesAllowed is 0: All devices must be unlocked manually
 - TTL:15 ... optional, set Time To Live
 - CCR, CCNRQ ... optional, request client certificate but do not terminate if the client does not send one
 ... used to request authentication by certificates for selective users
- The **third** entry is optional and is used to delegate administrative rights to selected users.
 Note: If ApplicGate is accessed via the manage entry all administrative functions are available.
 In this example this entry is accessible via all network interfaces via TCP port 999 and user authentication is done by **client certificates**.
 Also authentication via **OTP** or **TOTP** is supported as an option.
 The Type field defines the server certificate via keyword SSL to enable TLS.
 Following additional keywords are defined to configure the administrative roles (bold keywords are required):
 - **CCR:A_EAS** ... Request a client certificate for authentication (the format of the group A_EAS is described below)
 - ISS:My-Issuing-CA ... optional, allow certificates only from this issuer
 - RDR ... optional, send error message back if access by using the presented user certificate is not allowed
 - DEFCMD:statea\$... optional, Select EAS selection form as start page
 - **EASACL:A_EAS** ... Define ACL for EAS user/device list

- EASMDD:numberOfDays ... optional, minimum number of days to allow mass delete (for status routing entries), default is 60.

This is a sample view of the routing table:



The screenshot shows a web browser window with the address bar displaying '127.0.0.1:99/routtff'. The page title is 'ApplicGate EAS' with a version note '(v10.2.7737.26047 started 2021-03-08 14:40:22 on LEITNER3)'. The navigation menu includes Home, Configuration, Status, EAS_Entries, Logfiles, Test, Additional_Commands, Help, and Stop & Restart. The main content area is titled 'Routing Table' with a subtitle 'last loaded 2021-03-08 14:56:47, last written 2021-03-08 14:56:47'. Below this is a table with 12 columns: ID, Listening, Source IP, Gateway IP, Gateway Port, Gateway IP2, Destination IP, Destination Port, Expiration, Type, UID, and Comment. There are three rows of data.

ID	Listening	Source IP	Gateway IP	Gateway Port	Gateway IP2	Destination IP	Destination Port	Expiration	Type	UID	Comment
2	true	*	127.0.0.1	99	manage	3000	15	*	REFRH:5,TINT:5,LOG:1,BCK,PRM,GRPUPD,RTUPD,DELLOG:20,LGS,LGTIME,FLG:yes,BPRI:AboveNormal,LOCATEIP:"https://www.speedguide.net/ip/%IP%!"	MGM	Management
3	true	*	*	443	*	eas.xx.com	443	*	SSL:server.pfx/1, SSLTARGET:eas.xx.com,RDRA,EAS:Learn!2!Country!Site,APATH:"Microsoft-Server-ActiveSync?",NOTIFYT:A_EAS,TTL:15	EAS	Exchange
4	true	*	*	999	status	*	*	*	SSL:server.pfx/1, RDR:invalidCert.htm,CCR:A_EAS,DEFCMD:statea\$,EASACL:A_EAS	EASmgmt	EAS Management

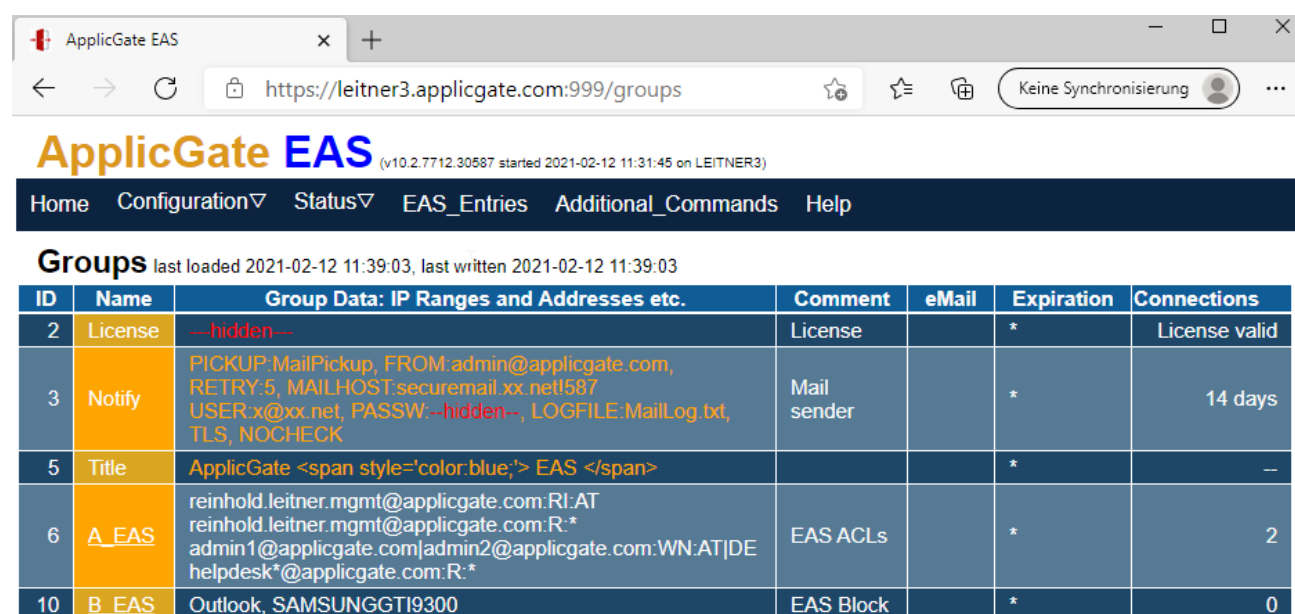
5.1.2 Example for groups.csv

```
GroupName;IPranges;Comment;eMail;Expiration
License;* COMPUTER1 My_Company-My_Name 0K0lb...8UjCsaNTu;License;;
Notify;PICKUP:MailPickup, FROM:admin@applicgate.com, RETRY:5;Mail sender;;
;MAILHOST:securemail.xx.net!587;;;
;USER:x@xx.net, PASSW:xxxx, LOGFILE:MailLog.txt, TLS, NOCHECK;;;
Title;ApplicGateEAS;EAS;EAS;EAS
A_EAS;admin0@mycomp.com:WN:*;admin1@mycomp.com|admin2@mycomp.com:WN:AT|DE;;
;helpdesk*@mycomp.com:R:*;;
B_EAS;Outlook,SAMUNGGTI9300;Outlook,SAMUNGGTI9300;Outlook,SAMUNGGTI9300
```

Detailed description:

- The license entry defines the license which can be obtained via www.applicgate.com.
- Notify holds the configuration to send notification emails.
- Title defines the title for the management interface.
- A_EAS contains access control lists (ACLs) with following format:
This group is used to delegate administrative rights to manage mobile devices: lock, unlock, delete etc.
 - Format:
email addresses (separated by |) : accessType : OU names (separated by |)
 - email addresses may contain one or more * for wildcard, e.g. *@aon.at, ab*x@mycompany.com, *.mgmt.*@x.com
 - accessType may contain W (write access), R (read access), I (display IP address and number of current sessions) and N (notification)
 - OU name: if * is specified, any entry can be accessed
 - In the example below:
 - reinhold.leitner.mgmt@applicgate.com has write access to the configuration of all mobile devices and is notified if any mobile device is blocked.
 - admin1@applicgate.com and admin2@applicgate.com have write access and are notified for all mobile devices in OU AT and OU DE.
 - helpdesk*@applicgate.com has read access for all mobile devices
- The optional group B_EAS contains a list of devices that will be blocked

This is a sample view of the groups table:



The screenshot shows a web browser window with the URL <https://leitner3.applicgate.com:999/groups>. The page title is "ApplicGate EAS" with a version number (v10.2.7712.30587) and a start time (2021-02-12 11:31:45 on LEITNER3). The navigation bar includes links for Home, Configuration, Status, EAS_Entries, Additional_Commands, and Help. The main content area is titled "Groups" and shows a table with 5 groups. The table has columns for ID, Name, Group Data, Comment, eMail, Expiration, and Connections.

ID	Name	Group Data: IP Ranges and Addresses etc.	Comment	eMail	Expiration	Connections
2	License	---hidden---	License		*	License valid
3	Notify	PICKUP:MailPickup, FROM:admin@applicgate.com, RETRY:5, MAILHOST:securemail.xx.net!587 USER:x@xx.net, PASSW:---hidden---, LOGFILE:MailLog.txt, TLS, NOCHECK	Mail sender		*	14 days
5	Title	ApplicGate EAS 			*	—
6	A_EAS	reinhold.leitner.mgmt@applicgate.com:RI:AT reinhold.leitner.mgmt@applicgate.com:R:* admin1@applicgate.com admin2@applicgate.com:WN:AT DE helpdesk*@applicgate.com:R:*	EAS ACLs		*	2
10	B_EAS	Outlook, SAMSUNG GTI9300	EAS Block		*	0

Number of groups: 5

5.2 Active Directory Import

To map sAMAccountName to UserPrincipalName an extract of the Active Directory is required. This extract must be stored into the file **ADusers.csv** located in the default directory of ApplicGate.

The header of ADusers.csv must be

"DN,sAMAccountName,userPrincipalName" or "DN,userPrincipalName,sAMAccountName".

This AD export can be generated by the Windows program csvde.exe.

Start the .bat file below on a machine that is a Windows domain member and copy ADusers.csv to the default directory of ApplicGate:

```
rem Select Global Catalog (optional):
rem set LS=-s dcl.applicgate.com
rem Define Root:
set root="CN=users,DC=applicgate,DC=com"
rem -----
set attr="sAMAccountName,userPrincipalName"
csvde -f ADusers.csv -l %attr% -d %root% -p Subtree -r (objectCategory=person) %LS%
```

ADusers.csv will be loaded during start of ApplicGate.

Additionally loading of this file can be triggered via command loadad.

This can be done manually or via program HttpGet.exe, e.g.

```
httpget http://127.0.0.1:99/loadad
```

5.2.1 Uploading of ADusers.csv by HttpPost.exe

Especially if ApplicGate EAS is located in a DMZ secure uploading of ADusers.csv may be difficult.

In this case you can use the program HttpPost.exe (provided by ApplicGate) as follows.

Add a command like below to the .bat file above and execute it within a scheduled task periodically:

```
Httppost.exe ADusers.csv https://myserver.mycomp.com:442/ADusers.csv -c mycertificate.cer
```

The switch -c is optional and used for authentication at the target via client certificates.

If this switch is not specified the sender IP address (SourceIP) must be specified in the routing entry below.

Example for routing entry at the ApplicGate EAS to receive the file:

```
SourceIP;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Expiration;Type      ;UID      ;Comment  ;eMail
*          ;*          ;442          ;web      ;          ;          ;*          ;see below ;Web      ;web      ;
```

Type field with following keywords:

SSL:server.pfx/passw

... TLS encryption

CCR:email

... authentication by user certificate (optional)

if not specified: Specify SourceIP (IP address of the sender)

POST:C:\ApplicGate\ADusers.csv ... accept posts and store to the specified file

START:loadad

... load ADusers.csv after successful upload

5.3 Installation of ApplicGate EAS

Before you start the installation you have to copy the files routing.csv, groups.csv and ADusers.csv to the installation directory.

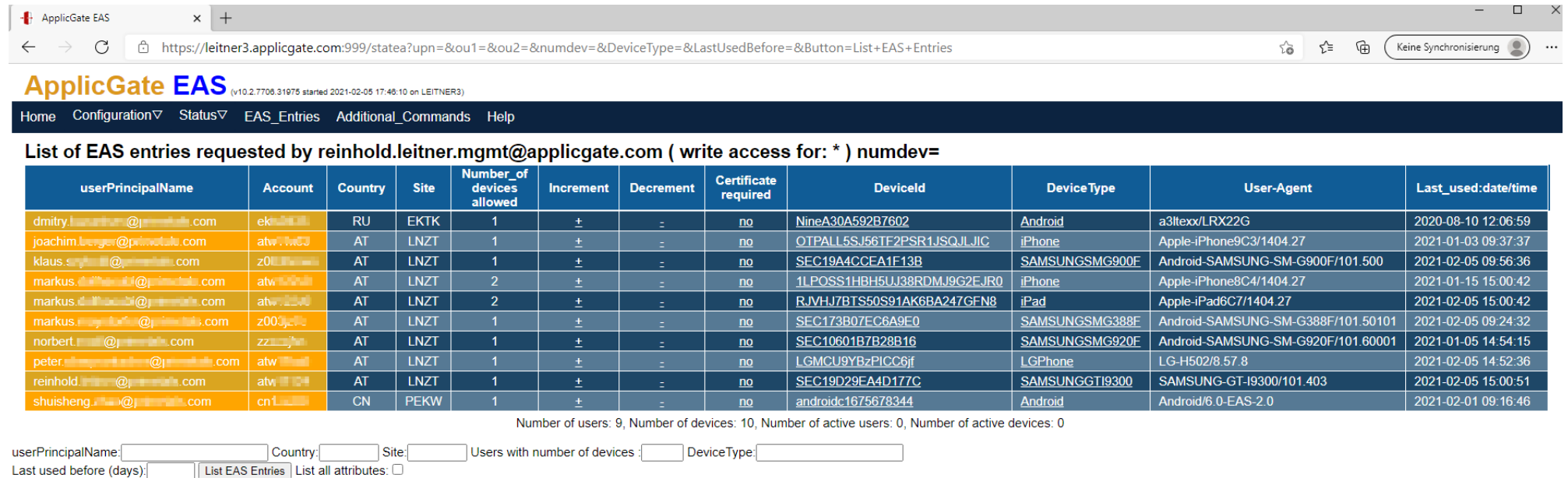
Or you use the switch /install:EAS during install to generate the files routing.csv and groups.csv like the examples in this document.

For installation on Windows see: <https://help.applicgate.com/helpmeST.htm>

For installation on Linux see: <https://help.applicgate.com/helpmeSX.htm>

6 Manage Mobile Devices

Via the command **statea** you can manage the mobile devices:



The screenshot shows the ApplicGate EAS web interface. The browser address bar displays the URL: `https://leitner3.applicgate.com:999/statea?upn=&ou1=&ou2=&numdev=&DeviceType=&LastUsedBefore=&Button=List+EAS+Entries`. The page title is "ApplicGate EAS (v10.2.7708.31975 started 2021-02-05 17:48:10 on LEITNER3)". The navigation menu includes: Home, Configuration, Status, EAS_Entries, Additional_Commands, and Help.

The main content area displays the title: "List of EAS entries requested by reinhold.leitner.mgmt@applicgate.com (write access for: *) numdev=". Below this is a table with the following columns: userPrincipalName, Account, Country, Site, Number of devices allowed, Increment, Decrement, Certificate required, DeviceId, Device Type, User-Agent, and Last_used:date/time.

userPrincipalName	Account	Country	Site	Number of devices allowed	Increment	Decrement	Certificate required	DeviceId	Device Type	User-Agent	Last_used:date/time
dmitry.leitner@j...com	ekn...	RU	EKTK	1	±	-	no	NineA30A592B7602	Android	a3ltexx/LRX22G	2020-08-10 12:06:59
joachim.benger@primetale.com	atw...	AT	LNZT	1	±	-	no	OTPAL15SJ56TF2PSR1JSQJLJIC	iPhone	Apple-iPhone9C3/1404.27	2021-01-03 09:37:37
klaus.s...@j...com	z00...	AT	LNZT	1	±	-	no	SEC19A4CCEA1F13B	SAMSUNGSMG900F	Android-SAMSUNG-SM-G900F/101.500	2021-02-05 09:56:36
markus...@j...com	atw...	AT	LNZT	2	±	-	no	1LPOSS1HBBH5UJ38RDMJ9G2EJR0	iPhone	Apple-iPhone8C4/1404.27	2021-01-15 15:00:42
markus...@j...com	atw...	AT	LNZT	2	±	-	no	RJVHJ7BTS50S91AK6BA247GFN8	iPad	Apple-iPad6C7/1404.27	2021-02-05 15:00:42
markus...@j...com	z00...	AT	LNZT	1	±	-	no	SEC173B07EC8A9E0	SAMSUNGSMG388F	Android-SAMSUNG-SM-G388F/101.50101	2021-02-05 09:24:32
norbert...@j...com	zz...	AT	LNZT	1	±	-	no	SEC10601B7B28B16	SAMSUNGSMG920F	Android-SAMSUNG-SM-G920F/101.60001	2021-01-05 14:54:15
peter...@j...com	atw...	AT	LNZT	1	±	-	no	LGMCU9YBzPICC6jf	LGPhone	LG-H502/8.57.8	2021-02-05 14:52:36
reinhold...@j...com	atw...	AT	LNZT	1	±	-	no	SEC19D29FA4D177C	SAMSUNG GTI9300	SAMSUNG-GT-I9300/101.403	2021-02-05 15:00:51
shuisheng...@j...com	cn1...	CN	PEKW	1	±	-	no	androidc1675678344	Android	Android/6.0-EAS-2.0	2021-02-01 09:16:46

Below the table, the following statistics are displayed: Number of users: 9, Number of devices: 10, Number of active users: 0, Number of active devices: 0.

At the bottom, there are input fields for filtering: userPrincipalName, Country, Site, Users with number of devices, and DeviceType. There are also checkboxes for "Last used before (days)", "List EAS Entries", and "List all attributes".

Selection of list entries:

- Specify any string in the fields userPrincipalName, Country, Site, DeviceType
- Specify "Users with number of devices" to display only users with specified number or more (use *=number* for exact match)
- Enter number of days to display old entries and optionally delete all these old entries.
For security reasons this mass delete is allowed only if number of days is equal or higher than specified by keyword EASMDDD.
- If the checkbox "List all attributes" is checked following additional attributes (as far as they are transmitted by the mobile device) will be shown:
Model, IMEI, OS, OSLanguage, PhoneNumber, MobileOperator

Actions via presented links (if write access to the entry is allowed):

- Increment ... Increment number of allowed devices
- Decrement ... Decrement number of allowed devices
- Certificate required ... Start/Stop client certificate request (see below)
- DeviceID ... Remove Device (allowed only if not active) and remove user if there is no associated device
- DeviceType ... Lock/Unlock device
- IPAddress ... If is field is shown (accessType I) and if the keyword LOCATEIP is defined: Link to page to show location of IP address

6.1 Require Client Certificates for Mailbox Access

For mailboxes where high security is requested a client certificate can be configured.

A user certificate must be issued and installed at the EAS mail client in the mobile device.

The email address in the certificate must match the userPrincipalName (UPN).

If the presented client certificate is not available or if it is invalid the connection will be terminated.

This can be configured at a device basis.

As prerequisite the EAS routing entry must contain the keywords CCR and CCNRQ to instruct ApplicGate to request client certificates..

7 Table of Contents

1	Motivation.....	1
2	How does this work?.....	1
3	Network Schema.....	2
4	Prerequisites	2
5	Installation and Configuration of ApplicGate EAS	3
5.1	Configuration Files	3
5.1.1	Example for Routing.csv.....	3
5.1.2	Example for groups.csv	6
5.2	Active Directory Import	7
5.2.1	Uploading of ADusers.csv by HttpPost.exe.....	7
5.3	Installation of ApplicGate EAS.....	8
6	Manage Mobile Devices.....	9
6.1	Require Client Certificates for Mailbox Access	10
7	Table of Contents	11