# Administrationshandbuch

Version

1.0

AVMail

ANTIVIRUS MAIL SECURITY

Avira

PROTECTED

Handbuch Version 1.0-1
AV Mail Version 1.0
Stand: 03. März 2016


Untertürkheimer Straße 24
66117 Saarbrücken
Deutschland
www.iku-systems.de

# Inhaltsverzeichnis

# 1 AV Mail

Herzlichen Glückwunsch, dass Sie sich für AV Mail entschieden haben. Dieses Qualitätsprodukt garantiert höchste Sicherheit für Ihre E-Mailversorgung. AV Mail ist das ideale Mittel, um die ständige Verfügbarkeit von E-Mails sicherzustellen und gleichzeitig mit Malware infizierte Nachrichten abzuwehren. AV Mail ist sehr einfach zu installieren und zu benutzen. Da AV Mail aber auch eine Fülle von Möglichkeiten bietet, sollten Sie dieses Handbuch aufmerksam lesen, damit dem erfolgreichen Einsatz von AV Mail nichts mehr im Wege steht.

## 1.1 Funktionsweise

AV Mail integriert sich in die Mail Services des Univention Corporate Server (UCS). Wenn es aktiviert ist, prüft AV Mail alle transportierten Mails auf Malware. Dies geschieht durch Integration in den SMTP-Transport der beteiligten UCS Systeme.

**Achtung:** Der Einsatz von AV Mail setzt zwingend eine funktionierende E-Mail Umgebung voraus!

Bei einer Neuinstallation Ihres Mail-Systems sollten Sie zunächst das Mail-System vollständig konfigurieren und danach AV Mail auf den entsprechenden Systemen installieren. AV Mail kann auch als standalone-Server zum Scannen des zentralen E-Mail Verkehrs eingesetzt werden. Dazu muss er lediglich in die bestehende SMTP-Infrastruktur integriert werden.

AV Mail kann ausschließlich auf UCS als Plattform genutzt werden. Grundsätzlich sollten die beteiligten UCS Systeme immer in der aktuellsten Version sein. Die Installation erfolgt einfach über das Univention App Center. Nach der Installation ist der Virenscanner sofort einsatzbereit. Er wird mit einer 31-Tage Testlizenz ausgeliefert, die über diesen Zeitraum die volle Funktionalität inkl. aktuellster Viren-Pattern zur Verfügung stellt. Soll das Produkt dann weiter genutzt werden, so kann es - nach Bezug einer Lizenz - einfach per Lizenzschlüssel für den entsprechenden Zeitraum frei geschaltet werden.

Die Konfiguration von AV Mail ist sehr einfach, da sie sich in die Standard-Konfiguration des UCS-Servers integriert. So werden zur Konfiguration ausschließlich UCR-Variablen verwendet, die sich sowohl über die Univention Management Console (UMC) als auch per Befehlszeile einstellen lassen.

# 2 Schnelleinstieg

AV Mail ist bewusst einfach gehalten, um Konfigurationsfehler zu vermeiden sowie einen schnellen und einfachen Einsatz zu gewährleisten. Für die meisten Umgebungen ist keine weitere Konfiguration nötig. Der Schnelleinstieg beschreibt, wie Sie in wenigen Schritten zu einem voll funktionsfähigen System kommen.

## 2.1 Voraussetzungen

Stellen Sie sicher, dass der Mail-Transport Ihrer UCS Systeme eingerichtet ist und funktioniert. AV Mail wird auf dem System installiert, das alle Mails (ein- und ausgehende) transportiert. Sollten mehrere Systeme am Mail-Transport beteiligt sein, so sollte auch AV Mail auf jedem dieser Systeme installiert werden.

Bringen Sie die beteiligten UCS Systeme auf den neusten Stand. Nur so kann gewährleistet werden, dass AV Mail einwandfrei funktioniert.

Während der Installation muss gewährleistet sein, dass die entsprechenden Systeme über einen Internetzugang für https-Downloads verfügen. Dies kann entweder ein direkter Internetzugang sein oder eine Anbindung über http-Proxy. Weitere Informationen hierzu finden Sie im UCS-Handbuch:

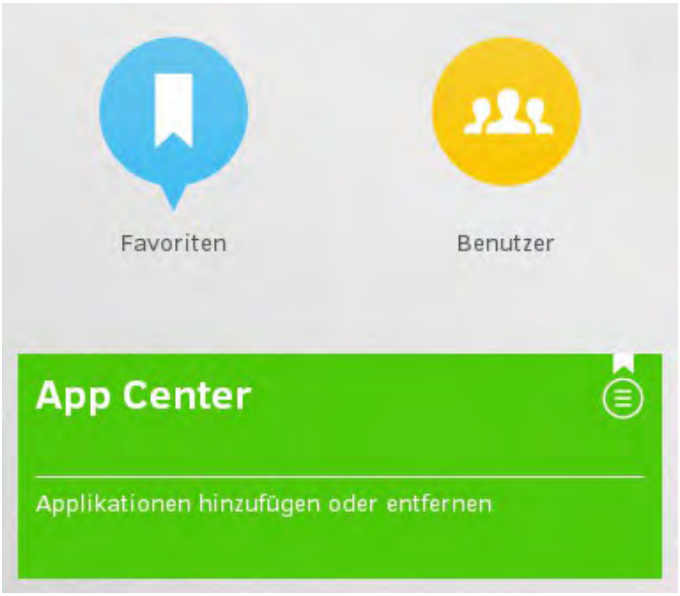
**Tipp:** https://docs.software-univention.de/handbuch-4.1.html#computers:Konfiguration_des_Proxyzugriffs

## 2.2 Installation im Univention App Center

Melden Sie sich an der Univention Management Console ('UMC') des entsprechenden Servers an, z.B.:

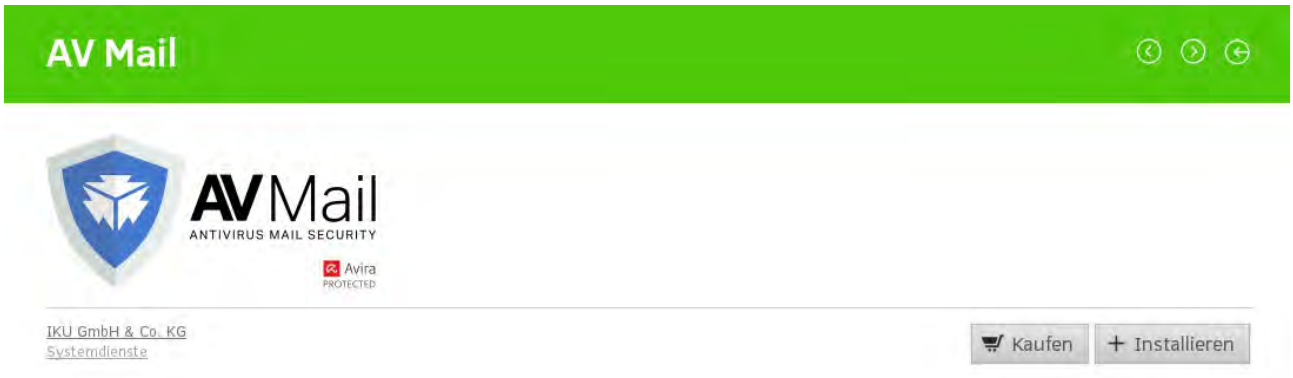
https://ucs-mail/univention-management-console/

Wählen Sie dort die Komponente 'App Center:'

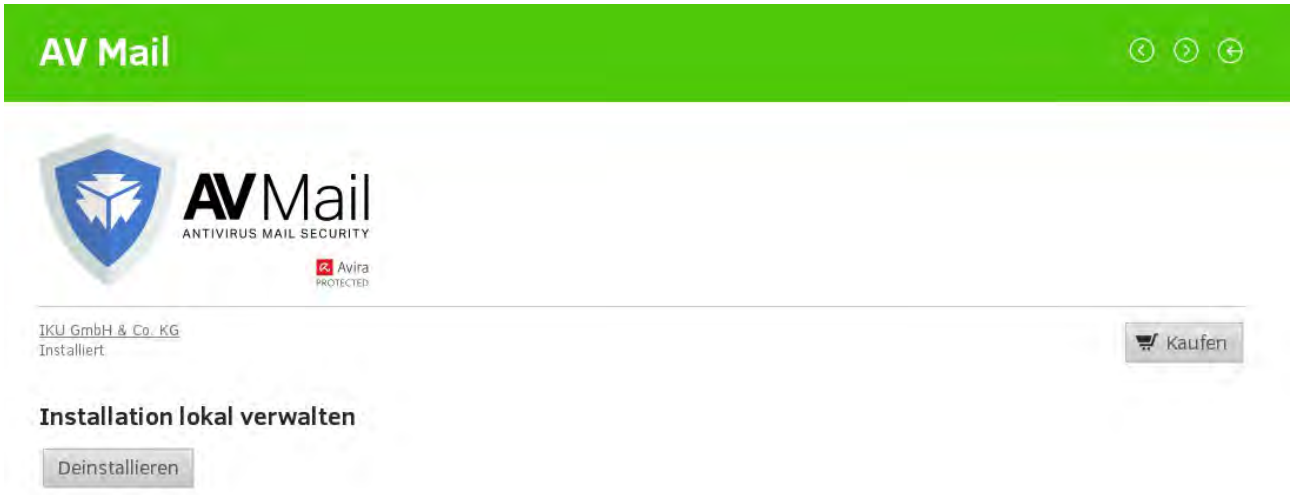


Im App Center wählen Sie die App 'AV Mail':

Installieren Sie das Produkt 'AV Mail':




Nach erfolgreicher Installation wird wieder die Produktseite angezeigt. Sie erkennen an dem Button 'Deinstallieren', dass die Installation erfolgreich abgeschlossen wurde:




An dieser Stelle können Sie das Produkt zu einen späteren Zeitpunkt wieder deinstallieren, wenn Sie es nicht mehr benötigen.

Nach der Installation ist das Produkt sofort aktiv und einsatzbereit. Während der Installation aktualisiert der Virenscanner bereits seine Virendefinitionsdatenbank und ggf. die Scan-Engine. Auch das regelmäßige, automatische Update dieser Komponenten ist aktiviert.

Auf dem System werden nun alle ein- und ausgehenden Mails, die über SMTP transportiert werden, auf Malware geprüft. Hierbei gelten folgende Standardeinstellungen, die vom Administrator angepasst werden können. Nach der Installation ist AV Mail wie folgt konfiguriert:

- Eventuell bereits eingerichtete, andere Virenscanner sind deaktiviert.
- Es wird eine Test-Lizenz verwendet, die ab dem Zeitpunkt der Installation für 31 Tage die volle Funktionalität bereit stellt.

- Die Virendefinitionsdatenbank wird alle 20 Minuten geprüft und ggf. aktualisiert.
- Die Virenscanner Engine wird alle 2 Stunden geprüft und ggf. aktualisiert.
- Die Sprache der Benachrichtigungsmails ist Deutsch, wenn der UCS mit Deutsch als Standardsprache installiert wurde. In allen anderen Fällen ist die Sprache der Benachrichtigungsmails Englisch.
- Verwendete E-Mail Adressen (FQDN = Host- und Domainname des UCS-Systems):
  - Informationen über Virenfunde (Virus Admin): systemmail@<FQDN>
  - Benachrichtigungen über Fehler: systemmail@<FQDN>
  - Absendeadresse für Benachrichtigungen an Benutzer: systemmail@<FQDN>
- Bei Virenfund werden **niemals** Benachrichtigungen an externe E-Mail Adressen gesendet.
- Bei Virenfund wird der Sender bzw. Empfänger benachrichtigt, sofern es sich um eine interne E-Mail Adresse handelt.
- Eine als infiziert erkannte Mail wird nicht zum ursprünglichen Empfänger ausgeliefert, sondern an: systemmail@<FQDN>
- **Nach Ablauf der Lizenz werden E-Mails aus Sicherheitsgründen nicht mehr transportiert, sondern in eine lokale Warteschlange gestellt.**

**Achtung:** Wichtig: Führen Sie diese Installation auf allen am SMTP-Transport beteiligten UCS-System durch!

# 3 Konfiguration

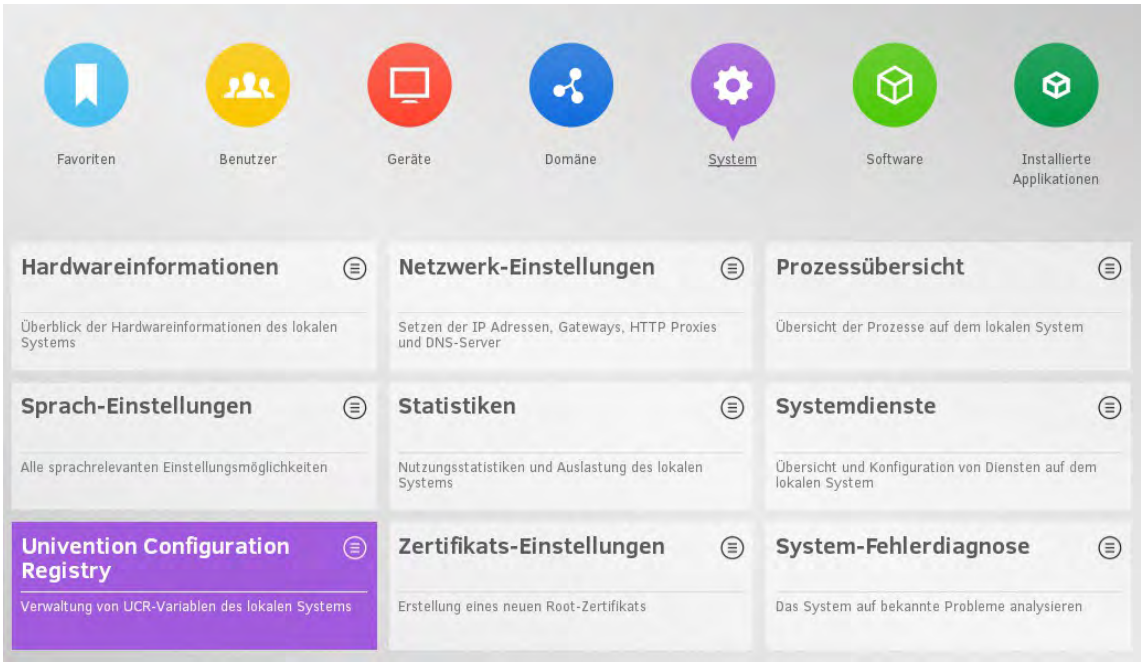
## 3.1 Konfiguration allgemein

Die Konfiguration von AV Mail erfolgt - genau wie bei vielen anderen Diensten auf UCS - über UCR-Variablen. Diese können vom Administrator geändert (und ggf. erzeugt) werden und bewirken eine Änderung der Konfiguration, ohne dass eine Konfigurationsdatei bearbeitet werden muss.

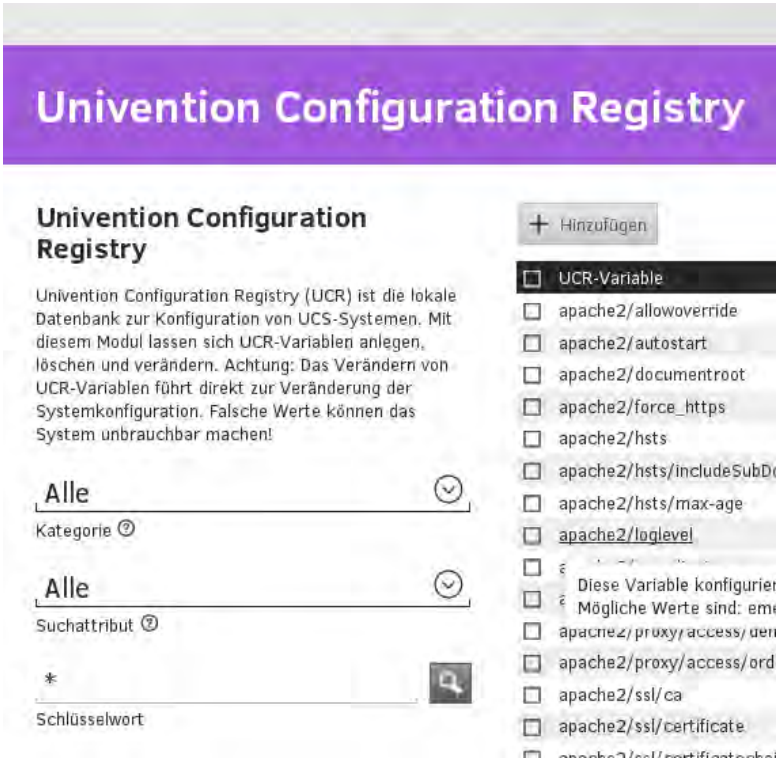
Sie finden weiter unten Tabellen zu den entsprechenden UCR-Variablen mit den relevanten Konfigurationsmöglichkeiten, den zugehörigen Variablen, Syntax und Beschreibung. Um diese zu bearbeiten, stehen Ihnen unter UCS zwei Möglichkeiten zur Verfügung:

### 3.1.1 UMC (Univention Management Konsole)

Melden Sie sich an der UCS Management Console (UMC) an:

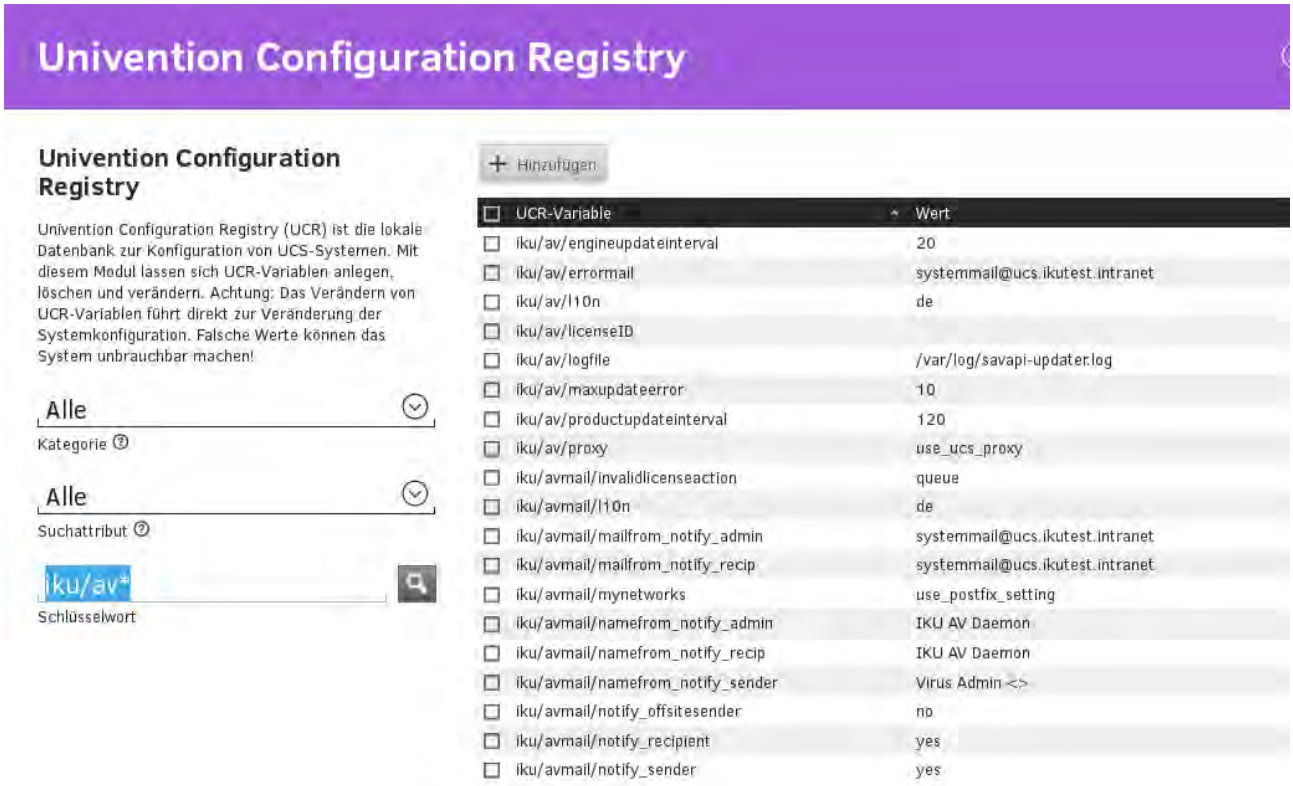


Wählen Sie dort den Bereich 'System' und dort 'Univention Config Registry':



### 3.1.1.1 Suchen

Tragen Sie im Feld 'Schlüsselwort' die entsprechende UCR-Variable ein oder einen allgemeineren Suchbegriff. Beispiel:



#### 3.1.1.2 Ändern einer Einstellungen

Um eine UCR-Variable zu ändern, klicken Sie einfach auf die Variable in der Liste rechts und ändern Sie dort den Wert:


### 3.1.2 Befehl 'ucr' in der Befehlszeile (Shell) des UCS-Systems

#### 3.1.2.1 Suchen

```
#> ucr search iku/av
iku/av/engineupdateinterval: 20
 update interval for savapi engine [minutes]
iku/av/errormail: systemmail@ox-dovecot.ox-experten.de
 mailaddress for update notifications
iku/av/l10n: de
 Language of the notifications
iku/av/licenseID: <empty>
 License ID for AVMail
iku/av/logfile: /var/log/savapi-updater.log
 logfile for savapi engine
iku/av/maxupdateerror: 10
 subsequent error count until notification
iku/av/productupdateinterval: 120
 update interval for savapi patterns [minutes]
iku/av/proxy: use_ucs_proxy
 http proxy for savapi
```

```
iku/avmail/invalidlicenseaction: queue
 Describes the action which is taken after the valid license expires
iku/avmail/l10n: de
 Language of the notifications
iku/avmail/mailfrom_notify_admin: systemmail@ox-dovecot.ox-experten.de
 Email from address for notifying admin
iku/avmail/mailfrom_notify_recip: systemmail@ox-dovecot.ox-experten.de
 Email from address for notifying recipient
iku/avmail/mynetworks: use_postfix_setting
 Local networks
iku/avmail/namefrom_notify_admin: IKU AV Daemon
 Email sender name for notifying admin (not supported yet)
iku/avmail/namefrom_notify_recip: IKU AV Daemon
 Email sender name for notifying recipient (not supported yet)
iku/avmail/namefrom_notify_sender: Virus Admin <>
 Email sender name for notifying sender (not supported yet)
iku/avmail/notify_offsitesender: no
 Notify non-local sender too
iku/avmail/notify_recipient:0,00cm yes
 Notify recipient
iku/avmail/notify_sender: yes
 Notify sender
```

#### 3.1.2.2 Ändern einer Einstellungen

Die Einstellungen können ebenfalls mit dem Befehl 'ucr' geändert und geprüft werden:

```
ucr set <UCR-Variable>=<Wert>
```

Beispiel:

```
#> ucr set iku/av/l10n="en"
```

Prüfen:

```
#> ucr get  iku/av/l10n
```

## 3.2 Lizenz installieren

### 3.2.1 Lizenz beziehen

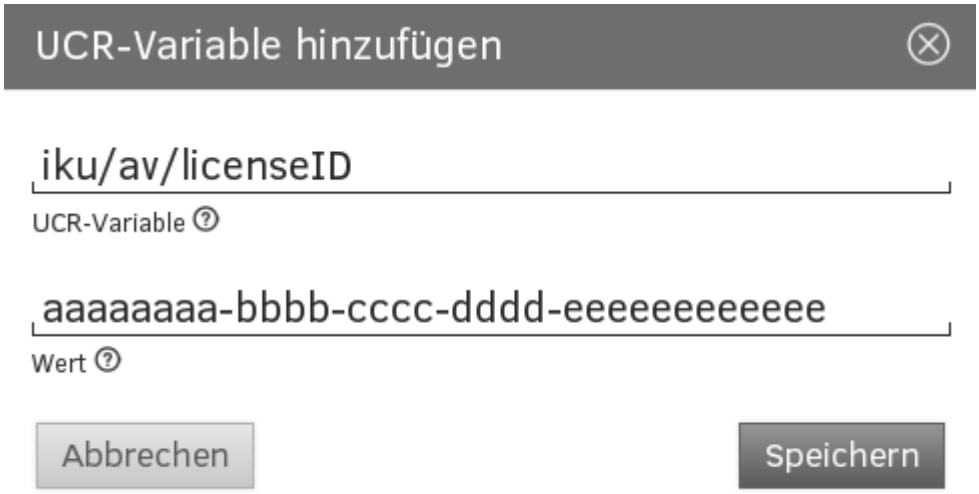
Um AV Mail nach Ablauf der Testlizenz weiter nutzen zu können, benötigen Sie eine entsprechende Lizenz. Diese erhalten Sie über folgende Wege:

- IKU Systems & Services
- Partner

### 3.2.2 Lizenz installieren

Sie erhalten mit der Lizenz eine Lizenz-ID. Um die Lizenz zu aktivieren, führen Sie bitte auf allen beteiligten UCS-Systemen folgende Schritte durch:

- Melden Sie sich wie oben beschrieben an der UCS Management Console (UMC) an und wählen Sie dort den Bereich 'System' und dort 'Univention Config Registry'.
- Wählen Sie rechts den Button 'Hinzufügen':




- Tragen Sie im Feld 'UCR-Variable' den Text 'iku/av/licenseID' ein. Bitte achten Sie exakt auf die Schreibweise inkl. Groß-/Kleinschreibung.
- Im Feld 'Wert' tragen Sie die Lizenz-ID ein, die Sie mit Ihrer Lizenz erhalten haben.

Mit 'Speichern' aktivieren Sie die neue Lizenz. Wie bei allen Änderungen zur Lizenz erhält der Virus-Admin eine Information der Mail. Diese Mail beinhaltet einen Text mit genauen Informationen zur Lizenz, wie Anzahl der Benutzer oder Laufzeit.

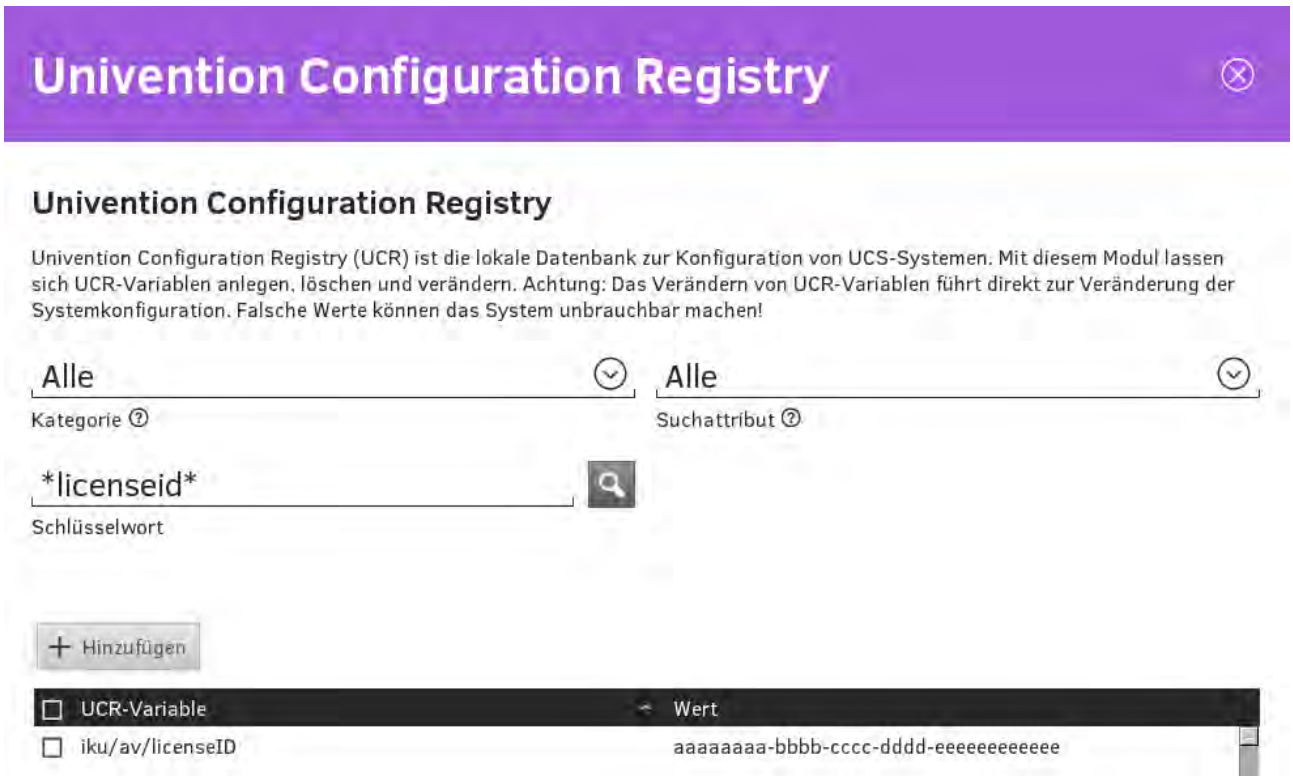
### 3.2.3 Lizenz prüfen

Sie können die Gültigkeit der Lizenz auch in der Befehlszeile des UCS prüfen:

```
/usr/lib/iku-av/bin/license-tool -l
```

### 3.2.4 Lizenz ändern

Da die UCR-Variable bereits beim ersten Einspielen der Lizenz-ID erstellt wurde, ist diese beim Ändern nicht mehr neu zu erstellen. Sie können die Variable entsprechend im Feld links suchen und dann ändern, indem Sie auf die gefundene UCR-Variable klicken:




Wie bei allen Änderungen zur Lizenz erhält der Virus-Admin eine Information der Mail. Diese Mail beinhaltet einen Text mit genauen Informationen zur Lizenz, wie Anzahl der Benutzer oder Laufzeit.

### 3.2.5 Einstellungen zur Lizenz ändern

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| iku/avmail/invalidlicenseaction | 'queue' | 'pass' oder 'queue' | 'queue': Der Virenscanner wird aus Sicherheits-gründen deaktiviert, Mails werden nicht mehr transportiert.<br>'pass': Der Virenscanner wird deaktiviert und Mails werden ohne Prüfung transportiert |

## 3.3 Updates

### 3.3.1 Produktupdates AV Mail

Updates für AV Mail selbst werden über die üblichen Mechanismen des UCS durchgeführt. Weitere Informationen finden Sie im UCS-Handbuch unter:

**Tipp:** https://docs.software-univention.de/handbuch-4.1.html#software::ucs-updates

### 3.3.2 Produktupdates Virenscanner

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| iku/av/proxy | 'use_ucs_proxy' | 'use_ucs_proxy'<br>Proxy-URL, z.B.:<br>http://myproxy:3128<br><leer> | HTTP-Proxy, der für Updates des Virenscanners verwendet werden soll.<br>'use_ucs_proxy': Es wird die Proxy-Einstellung verwendet, die auch das UCS-System für Updates verwendet.<br>Proxy-URL: Dieser Proxy wird verwendet.<br><leer>: Es wird kein Proxy verwendet |
| iku/av/errormail | systemmail@<FQDN> | E-Mail Adresse | E-Mail Adresse, an die Update-Fehler gemeldet werden.<br>Dieser Empfänger erhält auch Informationen zu Lizenz-Änderung und -Ablauf. |
| iku/av/maxupdateerror | 10 | Ganzzahl >= 1 | Wenn ein Fehler beim Update auftritt, wird dieser per Mail berichtet.<br>Der Wert der Variable gibt an, wie oft ein Update in Folge fehlschlagen darf, bis eine Mail versandt wird. |
| iku/av/l10n | 'de' oder 'en' | 'de' oder 'en' | Sprache der E-Mail bei Update-Fehler |
| iku/av/logfile | /var/log/savapi-updater.log | Dateipfad | Pfad zum Logfile für Updates des Virenscanners |

#### 3.3.2.1 Produktupdates Virenscanner Engine

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| iku/av/engineupdateinterval | 20 | Ganzzahl >= 1 | Zeitspanne in Minuten zwischen zwei Updates der Virendefinitions-datenbank |

#### 3.3.2.2 Produktupdates Virendefinitionsdatenbank

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| iku/av/productupdateinterval | 120 | Ganzzahl >= 1 | Zeitspanne in Minuten zwischen zwei Updates der AntiVir Engine |

### 3.3.3 Benachrichtigungen

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| iku/avmail/l10n | 'de' oder 'en'<br>(Abhängig von der Sprache des UCS) | 'de' oder 'en' | Sprache der Benachrichtigungs-E-Mails |
| iku/avmail/mailfrom_notify_admin | systemmail@<FQDN> | E-Mail Adresse | Absenderadresse von Benachrichtigungs-E-Mails an den Virus Admin |
| iku/avmail/notify_recipient | 'yes' | 'yes' oder 'no' | Soll der ursprüngliche Empfänger einer infizierten E-Mail benachrichtigt werden? |
| iku/avmail/mailfrom_notify_recip | systemmail@<FQDN> | E-Mail Adresse | Absenderadresse von Benachrichtigungs-E-Mails an den Empfänger |
| iku/avmail/notify_sender | 'yes' | 'yes' oder 'no' | Soll der Sender einer infizierten E-Mail benachrichtigt werden? |

| UCR-Variable | Default | Mögliche Werte | Beschreibung |
|---|---|---|---|
| iku/avmail/mynetworks | 'use_postfix_setting' | Liste von Netzwerken, durch Komma getrennt, z.B.:<br>127.0.0.0/8, 192.168.0.0/16<br>Oder:<br>'use_postfix_setting' | Es werden nur Benachrichtigungen an Empfänger gesendet, die aus diesen Netzen E-Mails versenden. Hierduch wird entchieden, ob eine (infizierte) E-Mail von Extern oder Intern versandt wurde. Es werden niemals Benachrichtigungen an E-Mail Adressen versandt, die als extern gelten.<br>'use_postfix_setting': Die Einstellungen des mit UCS mitgelieferten SMTP-Servers postfix werden verwendet. Diese werden über folgende UCR-Variable eingestellt:<br>mail/postfix/mynetworks |

### 3.3.4 Behandlung infizierter Mails

| UCR-Variable | Default | Mögliche Werte | Beschreibung |
|---|---|---|---|
| mail/antivir/quarantine_to | systemmail@<FQDN> | E-Mail Adresse<br>oder:<br>'virus-quarantine'<br>oder:<br><leer> | E-Mail Adresse: Infizierte Mails werden an diese E-Mail Adresse ausgeliefert<br>'virus-quarantine': Infizierte Mails werden auf dem Server in eine besondere Warteschlange (Quarantaine) gestellt.<br><leer>: Infizierte Mails werden verworfen und nicht gespeichert. |

#### 3.3.4.1 Ausliefern infizierter Mails bzw. Anhänge

Der einfachste Weg, infizierte Mails zu verwalten, ist es, diese an einen E-Mail Empfänger auszuliefern. Dieses Postfach kann dann einem Administrator zur Verfügung gestellt werden. Interne Empfänger erhalten standardmäßig eine Benachrichtigung bei einem Virenfund. Sollte der Empfänger vermuten, dass es sich um eine Fehlinterpretation des Virenscanners ('False positive') handelt, so kann der den Virus-Administrator kontaktieren. Dieser kann die entsprechende E-Mail dann nochmal gesondert prüfen und ggf. dann die Mail weiter leiten.

Es ist auch möglich, infizierte Mails in eine spezielle Warteschlange des (Postfix-) Mailservers zu stellen. Diese können dann durch folgende Schritte ausgeliefert werden:

Der ursprüngliche Empfänger erhält in der Benachrichtigungs-E-Mail eine eindeutige Nummer, die 'Queue-ID'.

Anhand dieser kann ein Administrator diese Mail frei geben:

**Achtung:** Nachteile der Einstellung 'virus-quarantine':

- Der Virus-Administrator benötigt root-Zugriff per Konsole auf den entsprechenden Mail-Server.
- Es ist aufwendiger, die Mail nochmal gesondert auf Malware zu prüfen, bevor sie zugestellt wird.
- Die Mail kann nicht ohne Weiteres an eine andere Adresse weiter geleitet werden.

Wird die Variable leer gelassen oder ist sie gar nicht gesetzt, so werden die als infiziert erkannte Mails verworfen. Ein nachträgliches Zustellen ist dann nicht mehr möglich.

### 3.3.5 Allgemeine Einstellungen

| *UCR-Variable* | *Default* | *Mögliche Werte* | *Beschreibung* |
|---|---|---|---|
| mail/antivir/scanner | 'iku-av' | Liste von Virenscannern, durch Leerzeichen getrennt, z.B.:<br>'iku-av clamav' | Liste von UCS-unterstützten Virenscannern. Weitere Informationen finden Sie im UCS Handbuch. |
| mail/antivir | 'yes' | 'yes' oder 'no' | Virenscanner aktivieren. Achtung: 'no' bewirkt, dass E-Mails ungefiltert transportiert werden. |

### 3.3.6 Vorlagen für E-Mails

Für den Versand von Benachrichtigungs-E-Mails werden z.Zt. die Sprachen Deutsch und Englisch unterstützt. Die Vorlagen finden Sie auf den beteiligten UCS-Systemen unter:

- /etc/amavis/iku_DE
- /etc/amavis/iku_EN

Dort befinden sich jeweils drei Textdateien, die als Template für generierte E-Mails verwendet werden:

- template-virus-recipient.txt
- template-virus-sender.txt
- template-virus-admin.txt

Es ist sinnvoll, in die Templates für Sender und Empänger (Recipient) die Kontaktdaten des Virus-Admins einzutragen.

# 4 Tests

Nach der Produktinstallation und Konfiguration sollte dessen Funktionalität geprüft werden. Es wird hier davon ausgegangen, dass der Mail-Transport bereits vor der Installation von AV Mail korrekt eingerichtet war und somit auch getestet werden kann. Folgende Tests sollten nach der Installation durchgeführt werden:

- Transport nicht infizierter E-Mails: Diese sollten genau so transportiert und ausgeliefert werden, wie vor der Installation von AV Mail.
- Transport infizierter E-Mails (mit EICAR Test Pattern als Anlage):
  - Diese sollten gemäß der oben beschriebenen Regeln verworfen, in Quarantäne gestellt oder an den Virus-Admin per E-Mail ausgeliefert werden.
  - Wenn Benachrichtigungen aktiviert sind, sollten diese auch geprüft werden - aber insbesondere auch, dass keine Benachrichtigungen an externe Empfänger versandt werden.
- Überprüfen der Protokolldateien: Es sollte bei den o.g. Tests jeweils das entsprechende Protokoll geprüft werden, diese sind:
  - /var/log/mail.log
  - /var/log/maill.err
  - /var/log/savapi-updater.log

**Tipp:** Das EICAR Test-Pattern finden Sie unter:
http://www.eicar.org/85-0-Download.html

# 5 Spam-Abwehr

AV Mail verfügt nicht über eine eigene Spam-Abwehr. Vielmehr wird das System zur Spam-Abwehr, das mit UCS mitgeliefert wird verwendet. Die Konfiguration erfolgt analog zu den von Univention beschriebenen Verfahren. Der folgende Text ist dem UCS-Handbuch entnommen.

(Quelle: https://docs.software-univention.de/handbuch-4.1.html#mail::spam)

Unerwünschte und nicht angeforderte E-Mails werden als Spam bezeichnet. Zur automatisierten Erkennung solcher E-Mails integriert UCS die Software SpamAssassin und Postgrey. SpamAssassin versucht anhand von Heuristiken über Herkunft, Form und Inhalt einer E-Mail zu erkennen, ob sie erwünscht ist oder nicht. Postgrey ist ein Policy Server für Postfix der "Greylisting" implementiert. Greylisting ist eine Spam-Erkennungsmethode die E-Mail beim ersten Zustellversuch eines externen Servers ablehnt. Mailserver von Spamversendern unternehmen häufig keinen zweiten Zustellversuch, während legitime Server dies tun. Die Integration erfolgt über die Pakete univention-spamassassin und univention-postgrey, die bei der Einrichtung des Mailserver-Pakets automatisch eingerichtet werden.

SpamAssassin arbeitet mit einem Punktesystem, das mit steigender Punktzahl eine höhere Wahrscheinlichkeit für Spam ausdrückt. Punkte werden nach verschiedenen Kriterien vergeben, die beispielsweise auf Schlagworte innerhalb der E-Mail oder fehlerhafte Codierungen ansprechen. In der Grundeinstellung werden nur Mails bis zu einer Größe von 300 Kilobyte geprüft. Dies kann mit der Univention Configuration Registry-Variable mail/antispam/bodysizelimit konfiguriert werden. E-Mails, die als Spam klassifiziert wurden - also eine bestimmte Anzahl Punkte überschreiten - werden bei der Auslieferung durch Dovecot nicht im Posteingang des Empfängers, sondern im darunter liegenden Ordner Spam abgelegt. Der Name des Ordners kann mit der Univention Configuration Registry-Variable mail/dovecot/folder/spam konfiguriert werden. Die Filterung erfolgt durch ein Sieve-Skript, das beim Anlegen des IMAP-Postfachs eines Benutzers automatisch generiert wird.

Der in die Sieve-Skripte eingetragene Schwellwert, ab der E-Mails als Spam deklariert werden, ist mit der Univention Configuration Registry-Variable mail/antispam/requiredhits konfigurierbar. Die Voreinstellung (5) muss in der Regel nicht angepasst werden. Je nach Erfahrung im eigenen Umfeld kann dieser Wert aber auch niedriger angesetzt werden. Es muss dann jedoch mit mehr E-Mails gerechnet werden, die fälschlich als Spam erkannt wurden. Die Änderung des Schwellwerts wirkt sich nicht auf bestehende Benutzer aus, diese können den Wert aber im Horde-Webclient selbst anpassen (siehe UCS Handbuch Abschnitt 13.10.4).

Zusätzlich gibt es die Möglichkeit, E-Mails mit einem Bayes-Klassifikator bewerten zu lassen. Dieser vergleicht eine eingehende E-Mail mit statistischen Daten, die er aus bereits verarbeiteten E-Mails gewonnen hat und kann so seine Bewertung an die Mailgewohnheiten anpassen. Die Bayes-Klassifizierung wird vom Benutzer selbst gesteuert, in dem nicht vom System aber vom Benutzer als Spam erkannte E-Mails in den Unterordner Spam verschoben und eine Auswahl legitimer Mails in den Unterordner Ham (mail/dovecot/folder/ham) kopiert werden. Diese Ordner werden täglich ausgewertet und noch nicht erfasste oder bisher falsch klassifizierte Daten in einer gemeinsamen Datenbank erfasst. Diese Auswertung ist in der Grundeinstellung aktiviert und kann mit der Univention Configuration Registry-Variable mail/antispam/learndaily konfiguriert werden.

Die Spam-Filterung kann durch Setzen der Univention Configuration Registry-Variable mail/antivir/spam auf no deaktiviert werden. Bei Änderungen an Univention Configuration Registry-Variablen, die die Spamerkennung betreffen, muss der AMaViS-Dienst und Postfix neu gestartet werden.

## 5.1 Identifikation von Spam Quellen mit DNS basierten Blackhole List (DNSBL)

Eine weitere Möglichkeit gegen Spam vorzugehen ist die Verwendung von DNS-based Blackhole List (DNSBL) bzw. Real-time Blackhole List (RBL). DNSBL sind Listen von IP Adressen, von denen der Betreiber denkt, dass sie (potentiell) Quellen von Spam sind. Die Listen werden per DNS abgefragt. Ist dem DNS-Server die IP des sendenden E-Mail-Servers bekannt, so wird die Nachricht abgelehnt. Der Check einer IP-Adresse ist schnell und vergleichsweise ressourcenschonend. Er findet vor dem Annehmen der Nachricht statt. Erst nach dem Empfang findet die aufwändige Inhaltsüberprüfung mit SpamAssassin und Anti-Virus statt. Postfix hat eine eingebaute Unterstützung für DNSBL (http://www.postfix.org/postconf.5.html#reject_rbl_client).

Im Internet existieren DNSBL von verschiedenen Projekten und Firmen. Bitte informieren Sie sich auf deren Webseiten über Konditionen und Preise.

Um DNSBL mit Postfix zu verwenden muss die Univention Configuration Registry-Variable

```
mail/postfix/smtpd/restrictions/recipient/SEQUENZ=REGEL
```

gesetzt werden. Mit ihr können Empfangsbeschränkungen über die Postfix-Option smtpd_recipient_restrictions konfiguriert werden (siehe http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions). Die Sequenznummer dient der alphanumerischen Sortierung mehrerer Regeln, über die die Reihenfolge beeinflusst werden kann.

**Tipp:** Existierende smtpd_recipient_restrictions Regeln können wie folgt aufgelistet werden:

```
ucr search --brief mail/postfix/smtpd/restrictions/recipient
```

In einer unveränderten Univention Corporate Server Postfix Installation sollten die DNSBL am Ende der smtpd_recipient_restrictions Regeln angehängt werden. Zum Beispiel so:

```
ucr set mail/postfix/smtpd/restrictions/recipient/80=
"reject_rbl_client ix.dnsbl.manitu.net"
```