Administrationshandbuch

Version 1.0-1

AVProxy

ANTIVIRUS BROWSER SECURITY

Avira PROTECTED

Handbuch Version 1.0-1
AV Proxy Version 1.0-5
Stand: 03. September 2017

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

Inhaltsverzeichnis

1 AV Proxy

Herzlichen Glückwunsch, dass Sie sich für AV Proxy entschieden haben. Dieses Qualitätsprodukt garantiert höchste Sicherheit für Ihre Internetverbindung. AV Proxy ist das ideale Mittel, um den Zugriff auf normale Webseiten sicherzustellen und gleichzeitig mit Malware infizierte Seiten zu blockieren. AV Proxy ist sehr einfach zu installieren und zu benutzen. Da AV Proxy aber auch eine Fülle von Möglichkeiten bietet, sollten Sie dieses Handbuch aufmerksam lesen, damit dem erfolgreichen Einsatz von AV Proxy nichts mehr im Wege steht.

1.1 Funktionsweise

AV Proxy schützt zentral Ihre Arbeitsplätze vor Viren und anderer Schadsoftware. Es lässt sich transparent in bestehende Umgebungen integrieren und unterstützt die Protokolle ftp, http und sogar https durch modernste SSL-Technik. Durch Definition von Ausnahmen vom SSL-Scan (z.B. zur Authentisierung oder Online-Banking) ist weiterhin die Sicherheit von SSL gewährt. Der Einsatz des AV Proxy ist vielseitig: Er lässt sich auch als transparent- oder reverse-Proxy verwenden.

AV Proxy 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 AV Proxy 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.

Um AV Proxy verwenden zu können, muss dieser entweder am Client (z.B. Webbrowser) eingestellt oder als transparenter Proxy zentral in den Datenstrom eingebunden werden. AV Proxy verhält sich hier weitestgehend wie der mit UCS standardmäßig ausgelieferte Squid. Daher können die meisten Einstellungen wie im UCS-Handbuch beschrieben vorgenommen wetden:

https://docs.software-univention.de/handbuch-4.2.html#ip-config:Web-Proxy_fuer_Caching_und_Policy_Management_Virenscan

Bitte beachten Sie, dass der im UCS Handbuch beschriebene Scanner 'DansGuardian' nicht in Kombination mit AV Proxy verwendet werden kann.

Die Konfiguration von AV Proxy 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 Proxy 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

AV Proxy benötigt in einer Standardumgebung auf der einen Seite die Möglichkeit, Verbindungen ins Internet aufzubauen - dies ist auch über ein NAT Netzwerk möglich. Auf der anderen Seite muss er auf seinem HTTP-Port aus dem internen Netz erreichbar sein.

Für Nicht-Standard-Umgebungen - wie z.B. Squid als *Reverse-* oder *Tansparent-Proxy* - gelten evtl. andere/weitere Voraussetzungen.

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:

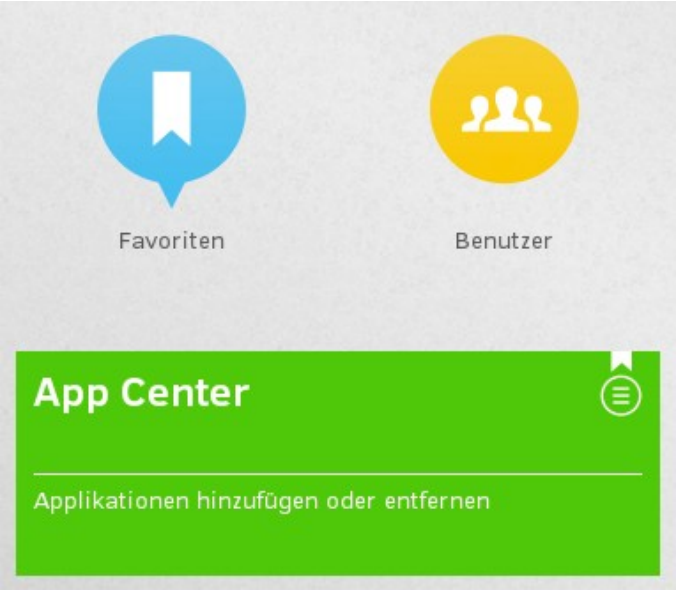
https://docs.software-univention.de/handbuch-4.1.html#computers:Konfiguration_des_Proxyzugriffs

2.2 Installation im Univention App Center

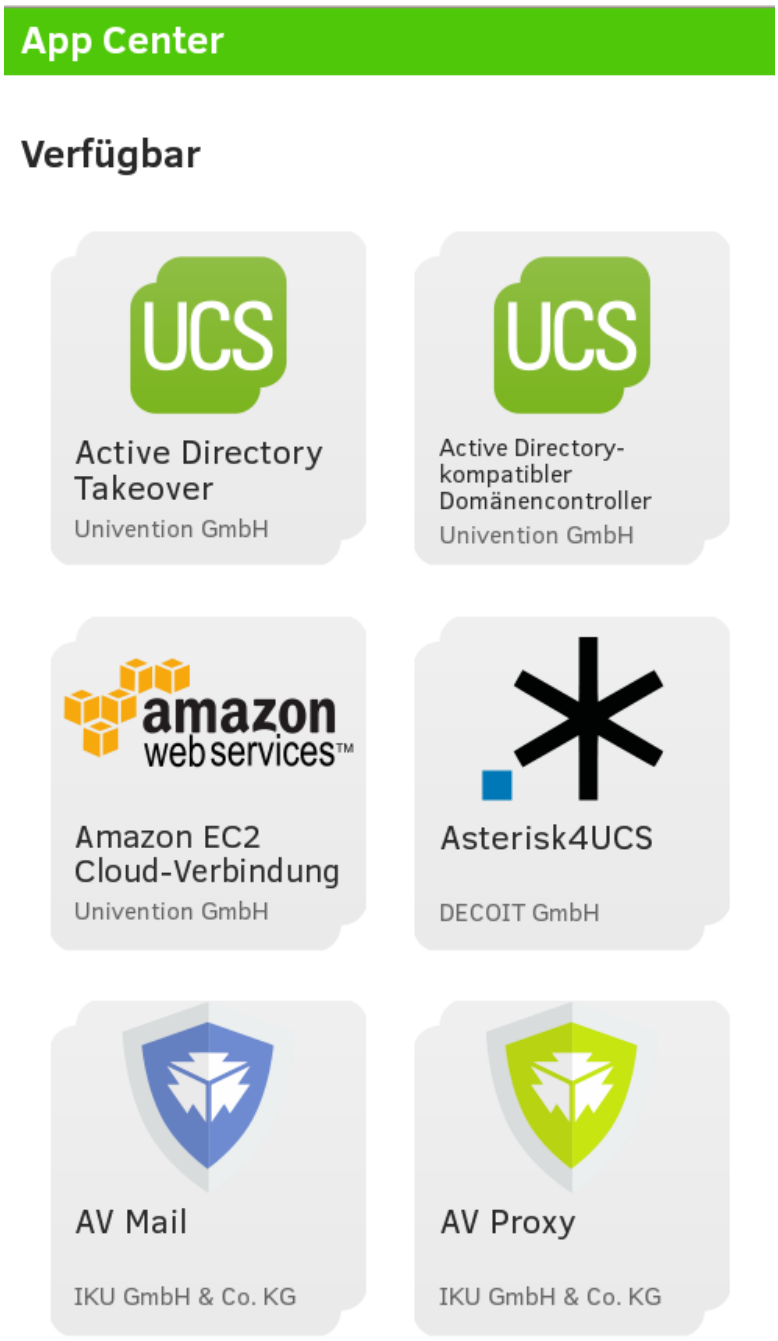
Melden Sie sich an der Univention Management Console ('UMC') des entsprechenden Servers an, z.B.:

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

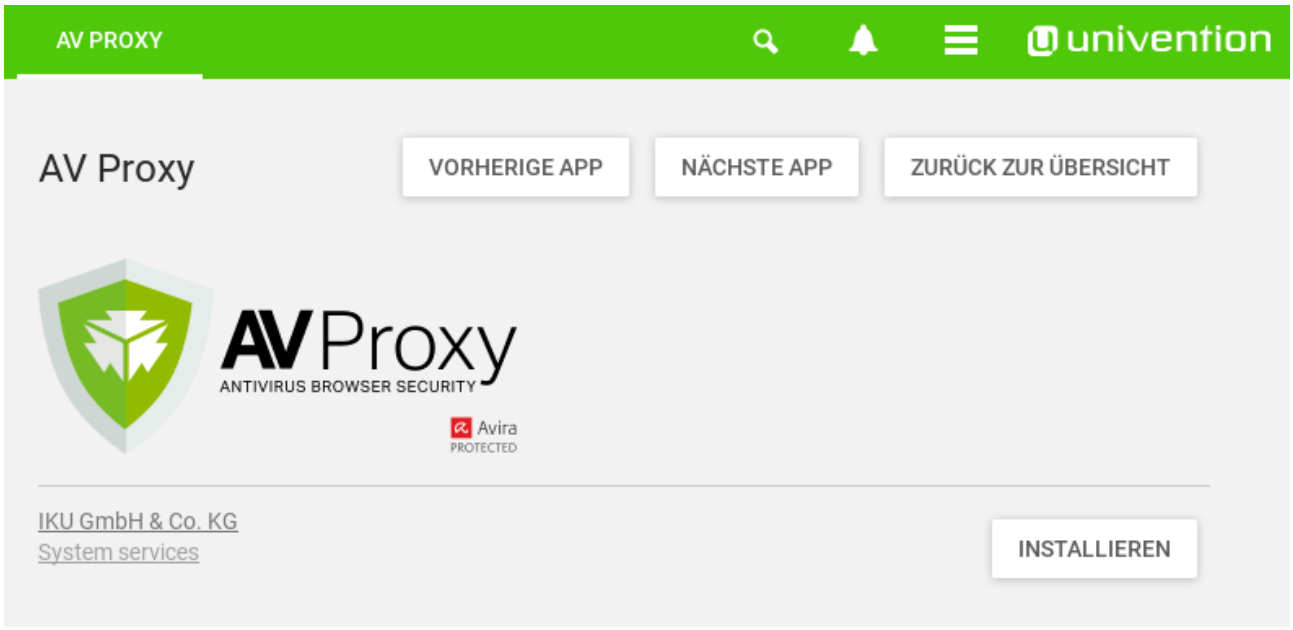
Wählen Sie dort die Komponente 'App Center':



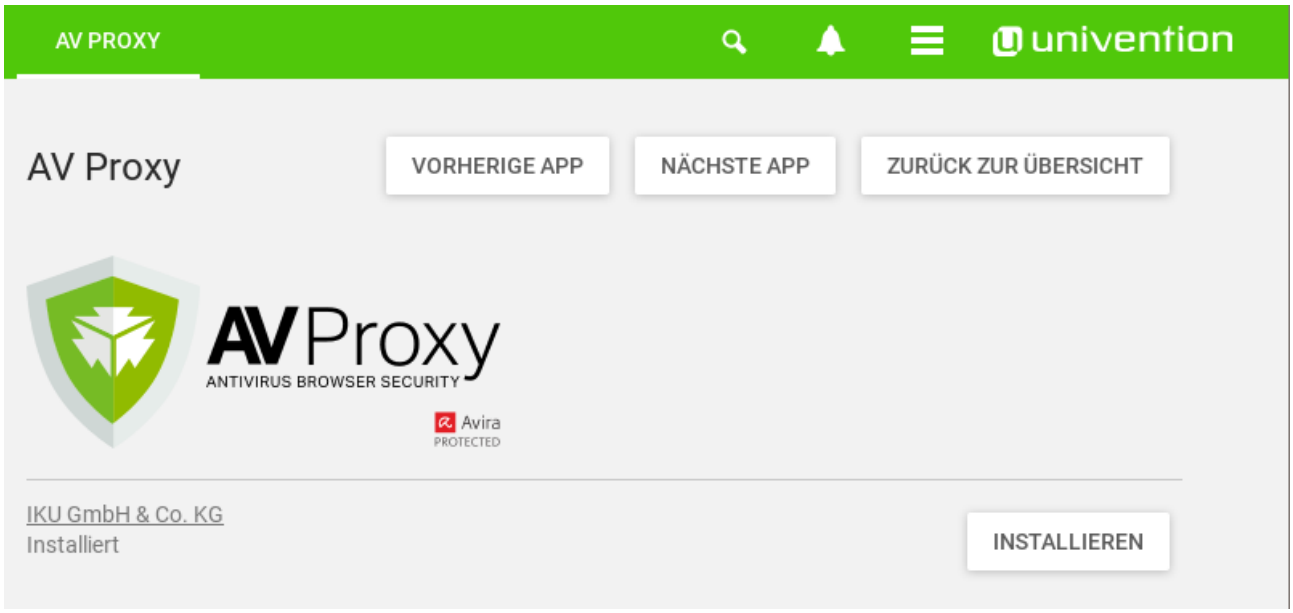
Im App Center wählen Sie die App 'AV Proxy':



Installieren Sie das Produkt 'AV Proxy':



Nach erfolgreicher Installation wird wieder die Produktseite angezeigt. Sie erkennen am Infotext '***Installiert***' **unten links**, 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.

Hierbei gelten folgende Standardeinstellungen, die vom Administrator angepasst werden können. Nach der Installation ist AV Proxy wie folgt konfiguriert:

- Eventuell bereits eingerichtete, andere Virenscanner für squid 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 Benachrichtigungen ist Deutsch, wenn der UCS mit Deutsch als Standardsprache installiert wurde. In allen anderen Fällen ist die Sprache der Benachrichtigungen Englisch.
- Verwendete E-Mail Adressen (FQDN = Host- und Domainname des UCS-Systems):
  - Benachrichtigungen über Fehler: systemmail@<FQDN>
- Es wird kein Scan von SSL-Verbindungen durchgeführt. Die Anfragen werden ungefiltert durchgereicht.
- Zugriffe sind nur aus lokalen Netzen (ohne Router-Übergang) und von localhost erlaubt.
- Es findet keine Benutzer-Authentisierung statt
- Squid lauscht auf allen Interfaces auf Port 3128/TCP
- **Nach Ablauf der Lizenz werden HTTP-Anfragen aus Sicherheitsgründen generell blockiert.**

An dieser Stelle ist AV Proxy bereits einsatzfähig. Sie können ihn direkt aus dem internen Netz verwenden, indem Sie am Client für HTTP-Verbindungen *http://<FQDN>:3128* als Proxy einstellen.

3 Konfiguration

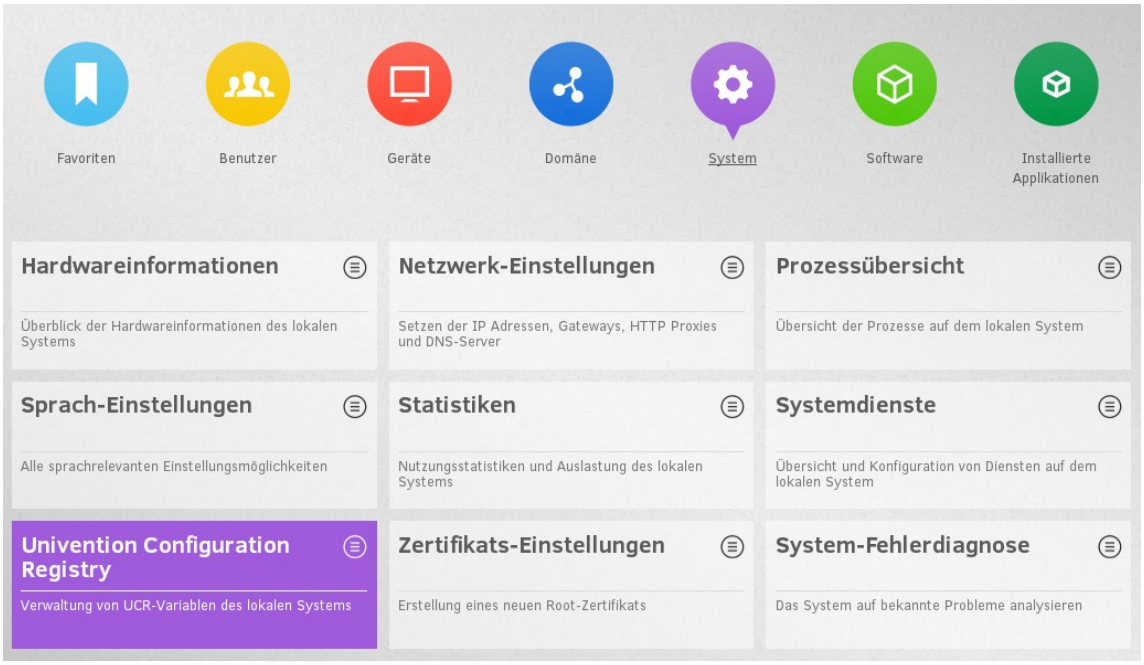
3.1 Konfiguration allgemein

Die Konfiguration von AV Proxy 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.

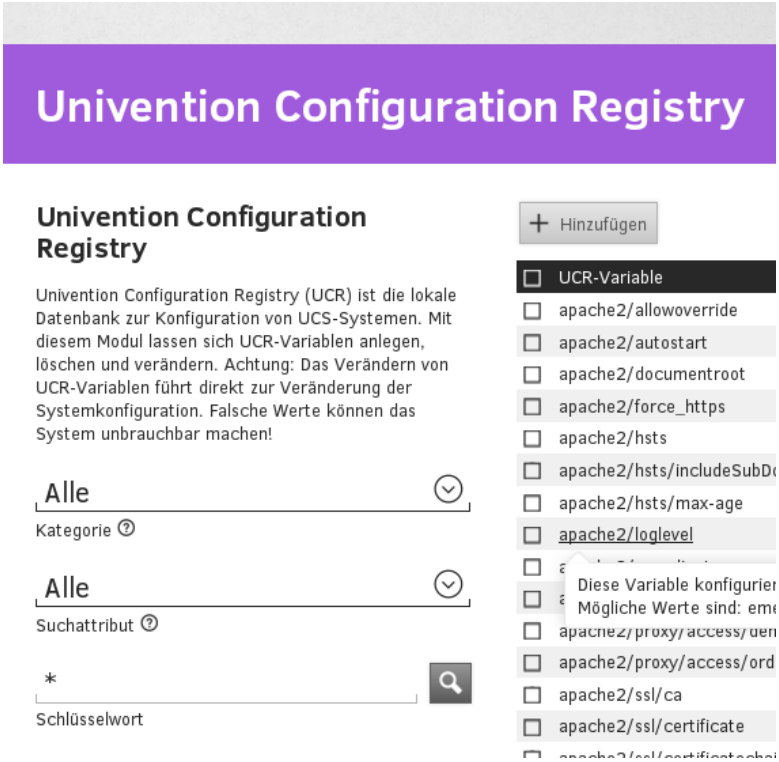
Sie finden weiter unten Tabellen zu den entsprechenden UCR-Variablen mit den relevanten Konfigurationsmöglichkeiten, den zugehörigen Variablen, Syntax und Beschreibung. Um diese zu bearbeiten, stehen Ihnen unter UCS zwei Möglichkeiten zur Verfügung:

3.1.1 UMC (Univention Management Konsole)

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

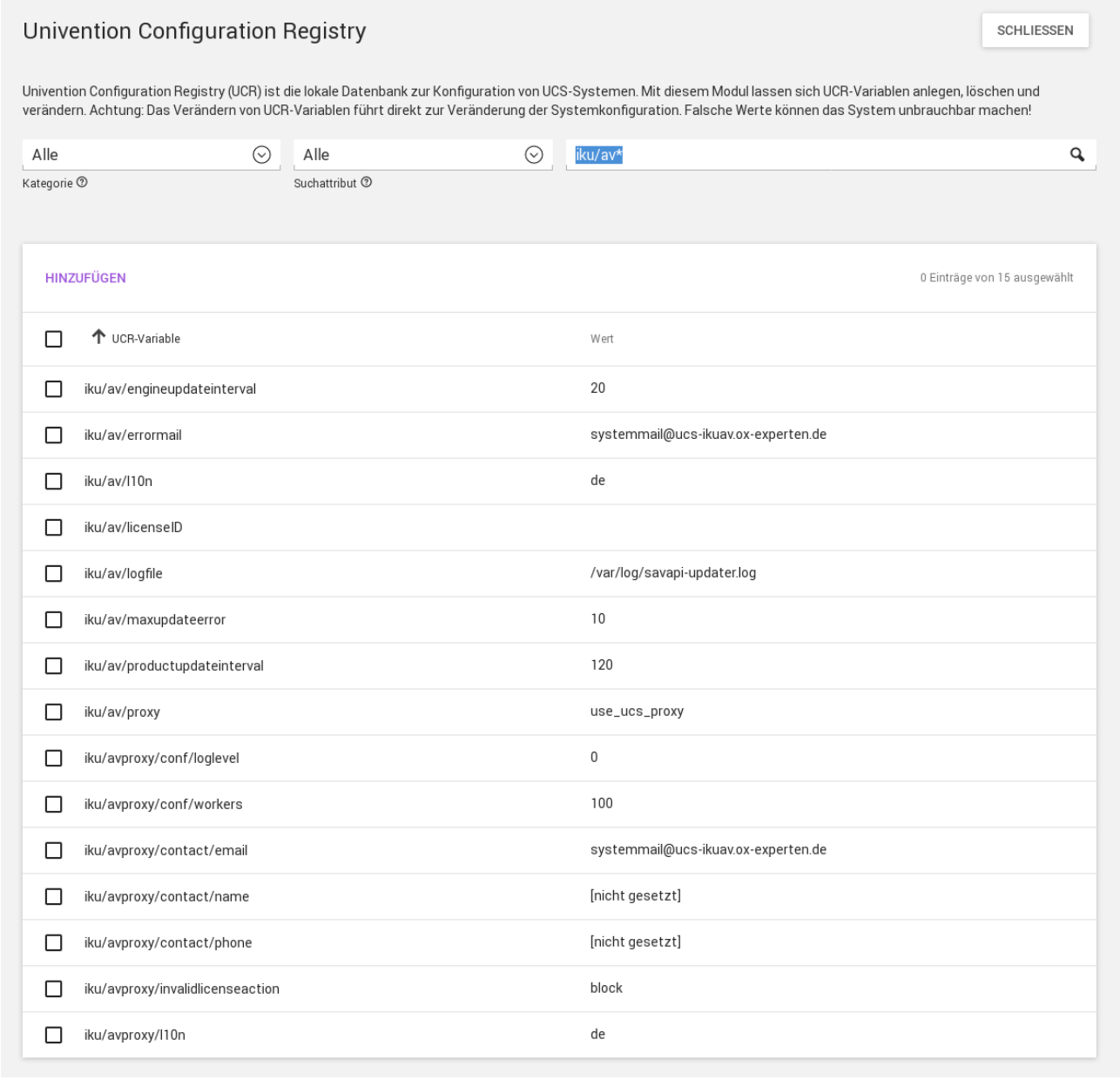


Wählen Sie dort den Bereich 'System' und dort 'Univention Config Registry':



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 von Einstellungen über UMC

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@ucs-ikuav.ox-experten.de
 mailaddress for update notifications
iku/av/l10n: de
 Language of the notifications
iku/av/licenseID: <empty>
 License ID for IKU AV Products
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/avproxy/conf/loglevel: 0
 icap loglevel
iku/avproxy/conf/workers: 100
 Maximum number of icap worker threads
```

```
iku/avproxy/contact/email: systemmail@ucs-ikuav.ox-experten.de
 the e-mail address which is to be displayed in the contact details section of
the alert screen
iku/avproxy/contact/name: [nicht gesetzt]
 the name which is to be displayed in the contact details section of the alert
screen
iku/avproxy/contact/phone: [nicht gesetzt]
 the phone number which is to be displayed in the contact details section of
the alert screen
iku/avproxy/invalidlicenseaction: block
 Describes the action which is taken after the valid license expires
iku/avproxy/l10n: de
 Lokalisierung der alert, content_filtered und error templates
```

3.1.2.2 Ändern von Einstellungen in der Befehlszeile

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 Konfiguration des AV Proxy

3.2.1 Allgemeine Einstellungen

UCR-Variable	*Default*	*Mögliche Werte*	*Beschreibung*
iku/avproxy/conf/loglevel	0	0-5	Loglevel des Scanner-Prozesses (ICAP)
iku/avproxy/conf/workers	100	<Ganzzahl>	Maximale Anzahl von Threads für den Scanner-Prozess
iku/avproxy/contact/email	systemmail@<FQHN>	<E-Mail>	E-Mail Adresse des Virenscanner-Admins, die bei Virenfund angezeigt wird.
iku/avproxy/contact/name	-		Name des Virenscanner-Admins (optional)
iku/avproxy/contact/phone	-		Telefonnummer des Virenscanner-Admins (optional)
iku/avproxy/l10n	'de' oder 'en'		Sprache der Benachrichtigungsseiten bei Virenfund bzw. Fehlern

UCR-Variable	*Default*	*Mögliche Werte*	*Beschreibung*
iku/squid/icap/use	'yes'	'yes' oder 'no'	Virenscanner Ein-/Ausschalten. **Achtung: Steht diese Einstellung nicht auf 'yes', werden keine Inhalte gescannt.**

3.2.2 SSL

AV Proxy bietet die Möglichkeit, auch SSL-Verbindungen zu scannen. Dies erfordert allerdings ein 'Aufbrechen' der Verbindung ('*bump*'). SSL-Scan ist standardmäßig deaktiviert, da es einiger Schritte bedarf, diesen einzurichten.

3.2.2.1 Konfiguration des AV Proxy

Zertifikat (CA)

Mit der Installation wird eine automatisch generierte CA erzeugt, die Sie für Testzwecke nutzen können, jedoch für den Produktivbetrieb durch eine selbst erzeugte CA ersetzen sollten. Die CA befindet sich nach der Installation in /etc/squid3/ssl/squidCA.crt. Weitere Informationen - insbesondere wie ein Zertifikat erzeugt wird, finden Sie hier:

https://wiki.squid-cache.org/ConfigExamples/Intercept/SslBumpExplicit

Ersetzen Sie dann das vorinstallierte Zertifikat durch Ihr eigenes. Wichtig ist hierbei, dass die Datei sowohl den privaten Schlüssel als auch das Zertifikat enthält. Die Datei ist dann folgendermaßen aufgebaut:

```
-----BEGIN PRIVATE KEY-----
...
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Beachten Sie, dass die Datei nur für den Benutzer root lesbar sein darf! Dies können Sie z.B. erreichen durch den Befehl:

```
#> chmod 600 /etc/squid3/ssl/squidCA.crt
```

Ausnahmen vom SSL-Scan können Sie (durch Leerzeichen getrennt) über folgende UCR-Variable definieren (Beispiel):

```
#> ucr set iku/squid/ssl/exceptions="www.sparkasse.de www.postbank.de"
```

Danach aktivieren Sie den SSL-Scan:

```
#> ucr set iku/squid/ssl/bump=yes
#> service squid3 restart
```

3.2.2.2 Konfiguration des Browsers

Installieren Sie anschließend das Zertifikat (ohne Schlüssel) auf den zugreifenden Clients (Browsern) als vertrauenswürdige Zertifizierungsstelle. Nach erfolgreichen Tests an einigen Browsern kann das Zertifikat z.B. in Windows-Domänen auch per Gruppenrichtlinie verteilt werden.

3.2.2.3 UCR Variablen

UCR-Variable	*Default*	*Mögliche Werte*	*Beschreibung*
iku/squid/ssl/bump	'no'	'yes' oder 'no'	Scan von SSL-Verbindungen aktivieren.
iku/squid/ssl/cert	/etc/squid3/ssl/squidCA.crt		Zertifikats-CA für das on-the-fly Erzeugen von Zeritifikaten. Diese CA muss im Browser (Proxy-Client) als vertrauenswürdige CA installiert sein.
iku/squid/ssl/exceptions	-		Liste von URLs, die vom SSL-Scan ausgenommen sind, separiert durch Leerzeichen.
iku/squid/ssl/ignorecerterror	-		Sollte es Zertifikatsfehler in der Verbindung zwischen AV Proxy und dem Zielsystem geben, so werden diese ignoriert.

3.2.3 Weitere Squid-Einstellungen

Zu den oben genannten - AV Proxy spezifischen - Einstellung kommen noch weitere Einstellungsmöglichkeiten, des Standard-UCS Systems. Weitere Infos finden Sie auch hier im UCS-Handbuch:

https://docs.software-univention.de/handbuch-4.2.html#ip-config:Web-Proxy_fuer_Caching_und_Policy_Management_Virenscan

Folgende UCR-Variablen können noch zur Squid-Konfiguration verwendet werden:

```
squid/allowfrom: <empty>
squid/append_domain: <empty>
squid/auth/allowed_groups: <empty>
squid/basicauth/children: <empty>
squid/basicauth: <empty>
squid/cache: yes
squid/contentscan: <empty>
squid/debug/level: ALL,1
squid/forwardedfor: off
squid/httpport: 3128
squid/krb5auth/children: <empty>
squid/krb5auth/keepalive: <empty>
squid/krb5auth/tool: <empty>
squid/krb5auth: <empty>
squid/ntlmauth/children: <empty>
squid/ntlmauth/keepalive: <empty>
squid/ntlmauth/tool: <empty>
squid/ntlmauth: <empty>
squid/parent/directnetworks: <empty>
squid/parent/host: <empty>
squid/parent/options: <empty>
squid/parent/port: <empty>
squid/redirect: <empty>
squid/transparentproxy: false
squid/virusscan: <empty>
squid/webports: <empty>
```

3.3 Lizenz installieren

3.3.1 Lizenz beziehen

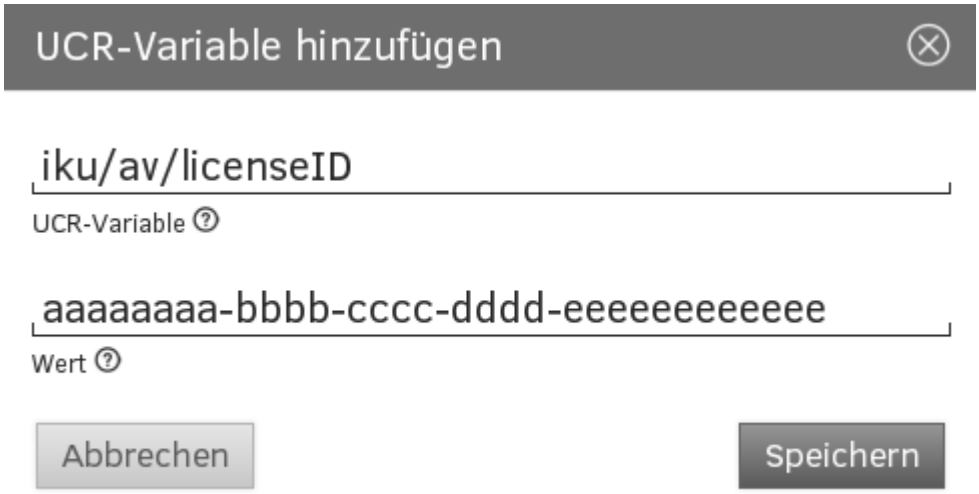
Um AV Proxy nach Ablauf der Testlizenz weiter nutzen zu können, benötigen Sie eine entsprechende Lizenz. Diese erhalten Sie über folgende Wege:

- IKU Systems & Services
- Partner

3.3.2 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.

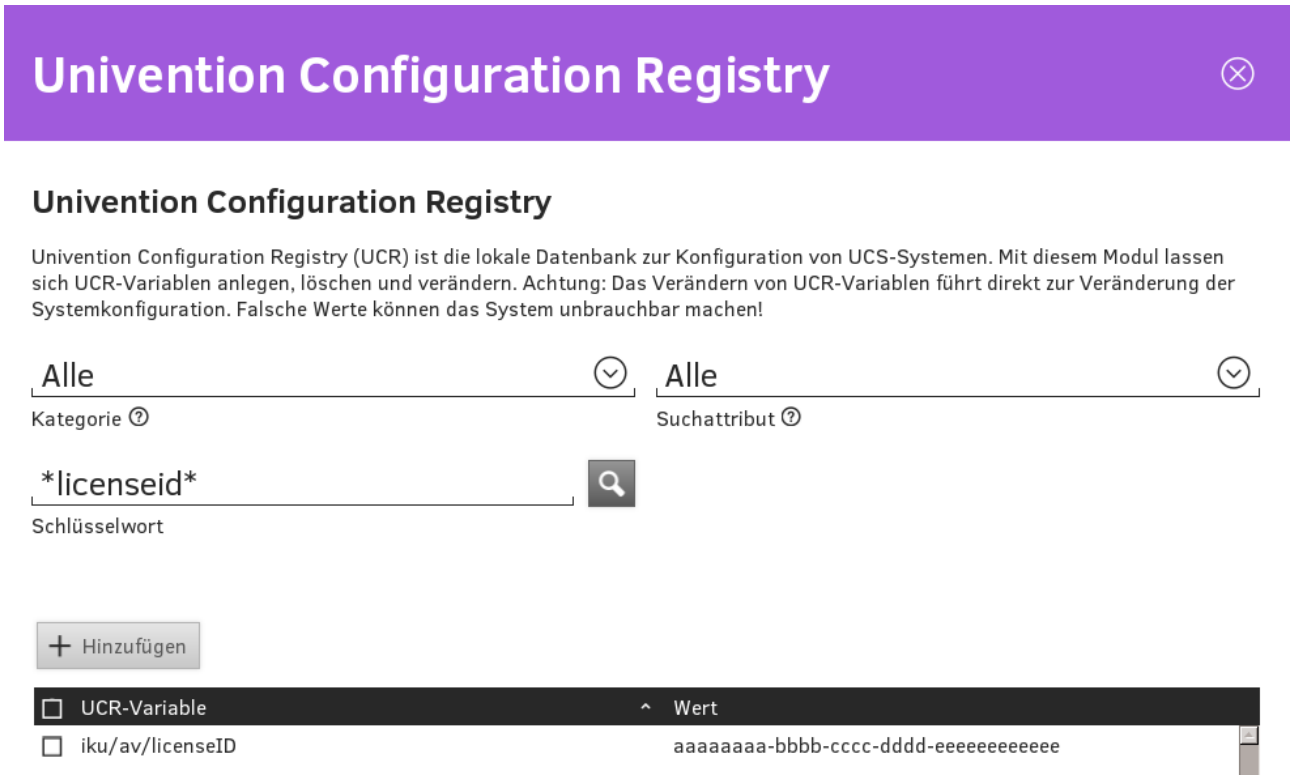
3.3.3 Lizenz prüfen

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

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

3.3.4 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.

3.3.5 Einstellungen zur Lizenz ändern

UCR-Variable	*Default*	*Mögliche Werte*	*Beschreibung*
iku/avproxy/invalidlicenseaction	'block'	'pass' oder 'block'	'block': Der Virenscanner wird aus Sicherheits-gründen deaktiviert, alle HTTP-Anfragen werden blockiert. 'pass': Der Virenscanner wird deaktiviert und alle Proxy-Anfragen werden ohne Prüfung weitergeleitet.

3.4 Updates

3.4.1 Produktupdates AV Proxy

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

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

3.4.2 Produktupdates Virenscanner

UCR-Variable	*Default*	*Mögliche Werte*	*Beschreibung*
iku/av/proxy	'use_ucs_proxy'	'use_ucs_proxy' Proxy-URL, z.B.: http://myproxy:3128 <leer>	HTTP-Proxy, der für Updates des Virenscanners verwendet werden soll. 'use_ucs_proxy': Es wird die Proxy-Einstellung verwendet, die auch das UCS-System für Updates verwendet. Proxy-URL: Dieser Proxy wird verwendet. <leer>: Es wird kein Proxy verwendet
iku/av/errormail	systemmail@<FQDN>	E-Mail Adresse	E-Mail Adresse, an die Update-Fehler gemeldet werden. 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. 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

3.4.2.1 Produktupdates Virenscanner Engine

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

3.4.2.2 Produktupdates Virendefinitionsdatenbank

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

4 Tests

Nach der Produktinstallation und Konfiguration sollte dessen Funktionalität geprüft werden.

Verwenden Sie einen HTTP-Client (hier im Beispiel firefox Browser) und stellen Sie dort AV Proxy als Proxy-Server für alle Verbindungen ein:

Besuchen Sie dann mit diesem Browser folgende Seite:

http://www.eicar.org/85-0-Download.html

Versuchen Sie, eine der (oder alle) Dateien 'eicar.* über standard HTTP-Protokoll (nicht SSL) herunter zu laden. Dieser Download muss mit folgender Meldung blockiert werden:

Versuchen Sie anschließend, eine der (oder alle) Dateien 'eicar.* über HTTPS-Protokoll (SSL) herunter zu laden. Dieser Download sollte erfolgreich sein. Die herunter geladene Datei ist lediglich ein Test-Pattern für Virenscanner und stellt keine Gefahr für Ihr Netz dar.

Um auch SSL-Scan zu testen, ändern Sie folgende UCR-Variable (über Befehlszeile oder über das Univention Management Center):

```
#> ucr set iku/squid/ssl/bump=yes
```

Starten Sie anschließend den Squid-Proxy neu:

```
#> /etc/init.d/squid3 restart
```

Versuchen Sie anschließend, eine der (oder alle) Dateien 'eicar.* über HTTPS-Protokoll (SSL) herunter zu laden. Der Browser wird zunächst einen Zertifikatsfehler melden, da er der auf AV Proxy installierten CA (noch) nicht vertraut. Ignorieren Sie diese Meldung im Browser.

Anschließend müssen Sie auch beim Download über SSL eine entsprechende Fehlermeldung des AV Proxy erhalten.

AV Proxy ist nun voll einsatzbereit.