IKARUS
gateway.security

Version 3.46
Handbuch

IKARUS Security Software GmbH

Blechturmgasse 11

1050 Vienna

Austria

www.ikarussecurity.com

Inhalt

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

0

Vorwort

IKARUS gateway.security (IGS) ist eine Server-Lösung, die Ihr Netzwerk vor verschiedensten Bedrohungen aus dem Internet schützt. Dieser Schutz umfasst alle möglichen Formen von Schadsoftware und Spam.

IKARUS gateway.security kann als transparenter Proxy für alle geläufigen TCP Protokolle eingesetzt werden. Zum Schutz gegen Bedrohungen durch E-Mail kann IKARUS gateway.security auch als Mail Transfer Agent (MTA) eingesetzt werden.

Die wichtigsten Funktionalitäten umfassen

- Erkennung von Schadsoftware für E-Mail- oder Web-Protokolle
- Zugriffskontrolle auf das interne Netzwerk
- Differenzierte Steuerung des Zugriffs auf Netzwerk-Ressourcen für Benutzer aus dem eigenen Netzwerk
- Verschiedene Authentifizierungsmechanismen, eingeschlossen LDAP und NTLM/Kerberos
- Vollautomatische inkrementelle Aktualisierung aller Komponenten
- Ausführliche Protokollierung aller Aktivitäten und Vorfälle
- Automatisierte und manuelle Erstellung von Berichten
- RESTful API Schnittstelle zur Konfiguration und Steuerung des Servers
- Web-basiertes Administrations-Interface

Dieses Dokument richtet sich hauptsächlich an Administratoren, die einen IGS-Server konfigurieren und betreiben.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

1 Schnelleinstieg

In diesem Abschnitt wird beschrieben, wie die IKARUS gateway.security-Software auf einem Server installiert und verwaltet wird.

1.1 Voraussetzungen

Bevor Sie IGS installieren, vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind:

- Zur Installation benötigen Sie Administratorrechte.
- Das System benötigt zumindest 2 GB freien Platz auf der Festplatte.
- Es sollten keine andere Dienste die TCP-Ports 1799 und 15639 verwenden1. Dieser Ports werden von GS verwenden und dürfen nicht blockiert werden. Abhängig von der tatsächlichen Systemkonfiguration könnten auch andere Ports benötigt werden.
- Die Firewall sollte die TCP Protokolle HTTP, HTTPS, POP3, IMAP, NNTP und SMTP nicht blocken. Welche Protokolle im konkreten Fall benötigt werden, hängt von den verwendeten Diensten von GS ab.
- GS kann auf folgenden Systemen installiert werden:
    - Linux (RPM und DEB Pakete) 64 Bit
    - Microsoft Windows 32 und 64 Bit

1.2 Einrichtung

1.2.1 Installation auf Microsoft Windows Systemen

Die Installation von IGS auf einem Microsoft Windows System ist unkompliziert. Doppelklicken Sie zum Starten die Installationsdatei und folgen Sie den angezeigten Anweisungen.

Während der Installation werden Sie aufgefordert, Ihre Lizenzdatei für IKARUS gateway.security zu importierten. Wahlweise können Sie diesen Schritt auch überspringen und die Lizenz später installieren.

1.2.2 Installation auf Linux Systemen

Für die Installation von GS auf Linux Systeme stehen RPM- und DEB-Pakete zur Verfügung, jedes davon in einer 32-Bit- und einer 64-Bit-Version.

```
# rpm -ivh IKARUSSecurityProxy-<version_number>rh5.x86_64.rpm
```

[1] Werden diese Ports trotzdem für andere Zwecke benötigt, so kann GS für die Verwendung alternativer Ports konfiguriert werden.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

```
# dpkg -i IKARUSSecurityProxy-<version_number>_amd64.deb
```

Nach erfolgreicher Installation kann die Lizenz über die Kommandozeile eingespielt werden.

```
# cd /opt/securityproxy/bin
# ./securityproxy_l64 -importlicense <licensefile>
```

1.2.3 Konfiguration als Dienst

1.2.3.1 Microsoft Windows

Im Zuge der Installation wird der Dienst **securityproxy** eingerichtet. Dieser kann wie alle anderen Dienste über die Verwaltung gestoppt und gestartet werden.

1.2.3.2 Linux

Auf Linux Systemen wird der Dienst für den passenden Run-Level registriert. Stoppen und (Neu-)Starten erfolgt mithilfe von Startskripts:

```
# /etc/init.d/securityproxy stop
# /etc/init.d/securityproxy start
# /etc/init.d/securityproxy restart
```

1.3 Dateisystem

Das folgende Bild zeigt eine Übersicht über das IKAURS gateway.security Programmverzeichnis nach der Installation dar.

```
antispam/         # anti-spam plugin and database
bin/              # program files
conf/             # configuration data, licenses,
ikarust3/         # scanner and virus database
image/            # static content, default HTML templates
log/              # log files
mail/             # temporary folder for mail to be scanned
quarantine/       # quarantine for infected files
store/            # database folder
tmp/              # temporary folder
update/           # temporary update folder
```

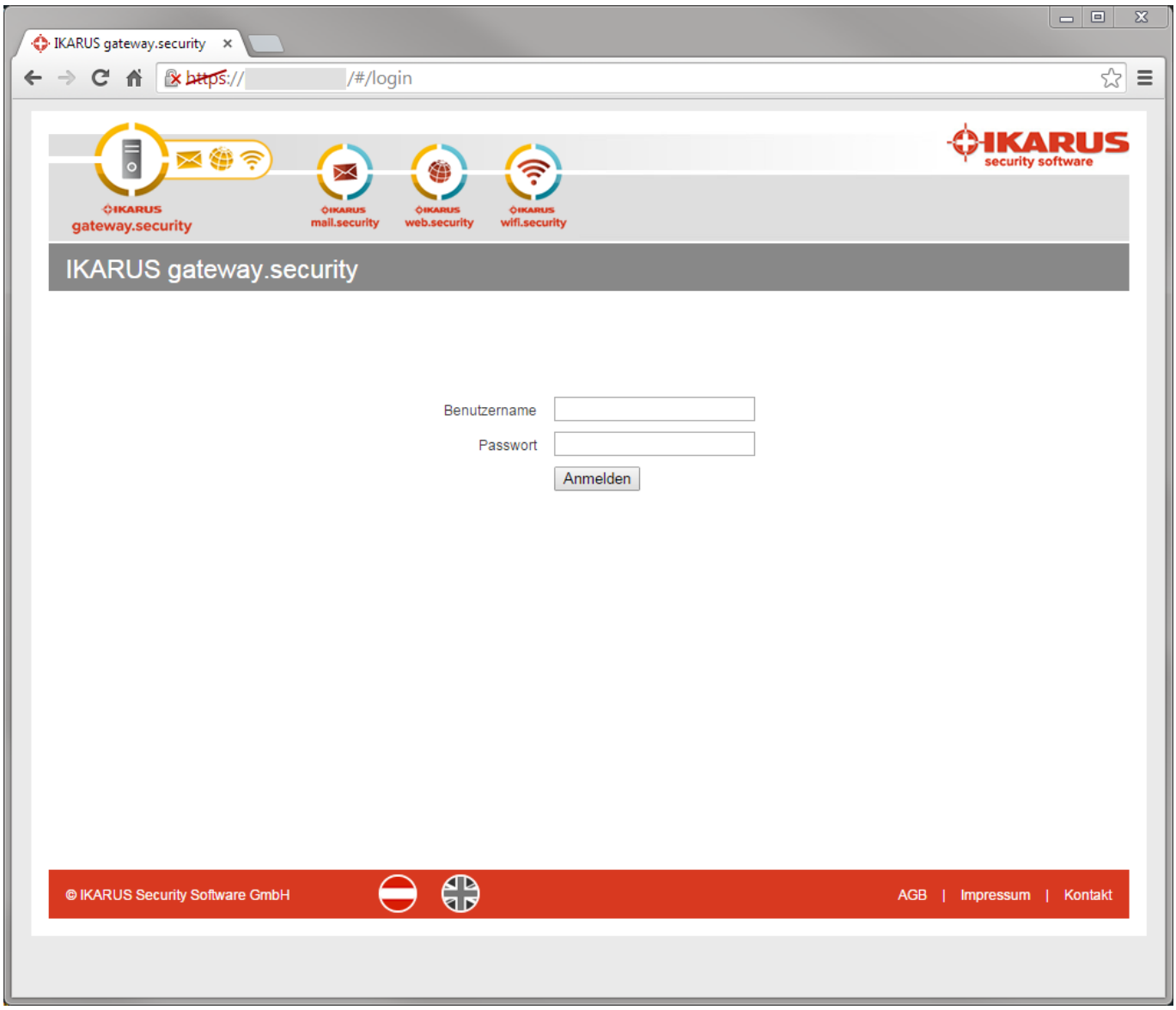
Die zentrale Konfigurationsdatei heisst `securityproxy.conf` und liegt im Verzeichnis `conf`.

Eine detaillierte Beschreibung der Konfigurationsmöglichkeiten von IGS, finden Sie in Abschnitt 3.

1.4 Benutzerschnittstelle

IGS verfügt über eine Browser-basierende Benutzeroberfläche. Standardgemäß kann diese über HTTPS angesprochen werden, sobald der Service gestartet wurde.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

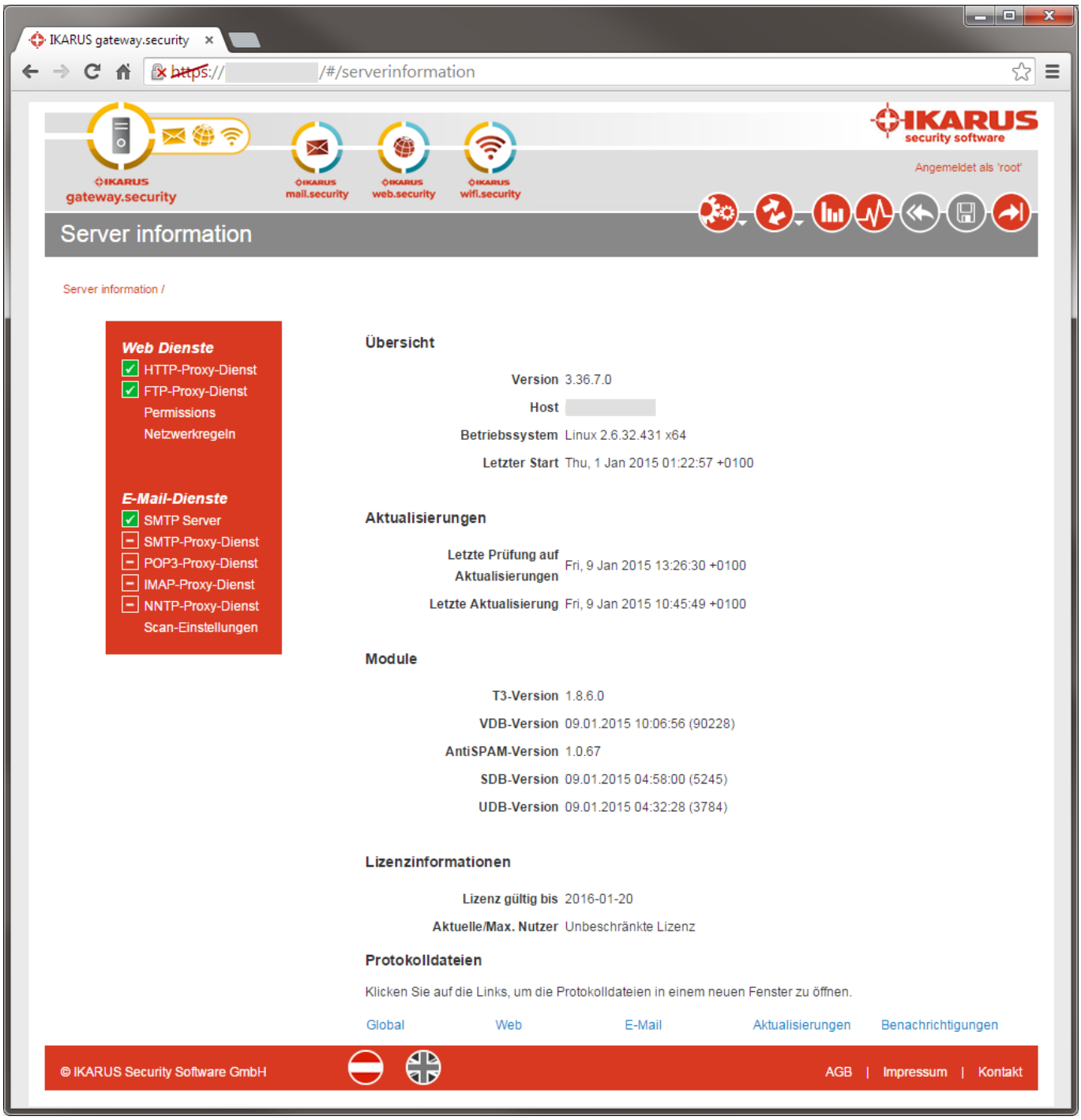


Da der gateway.security-Server im Normallfall selbstsignierte Zertifikate verwendet, weisen Browser darauf hin, dass der Zugriff auf diese Seite ein Sicherheitsrisiko darstellen kann.

Um den Zugriff ohne Einschränkung zu ermöglichen, speichern Sie ein autorisiertes Zertifikat unter `webapi.crt` und den entsprechenden privaten Schlüssel in der Datei `webapi.key` im Verzeichnis `conf/cert`.

Nach erfolgter Anmeldung wird dem Benutzer eine Seite präsentiert, die einen Überblick über den Status des Servers anzeigt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405



Oben rechts befindet sich das Hauptmenü.

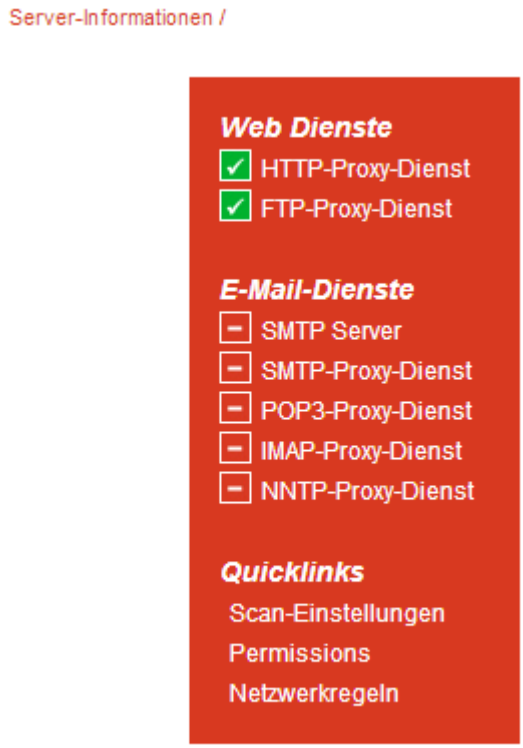
Hinter den Menüpunkten stehen, von links nach rechts gesehen, folgende Funktionen:

1. Konfiguration von IGS (siehe Abschnitt 3)

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

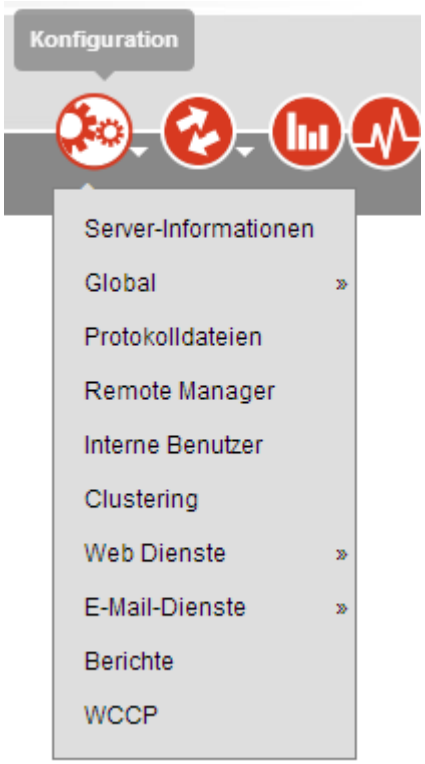
2. Lizenzverwaltung, Protokolle, Server-Neustart, Support-Informationen und Import bzw. Export der Konfigurationsdatei
3. Generieren von Berichten (siehe Abschnitt 2.2.5)
4. Anzeige des Aktivitätsmonitors
5. Änderungen rückgängig machen
6. Änderungen speichern
7. Abmelden

Auf der linken Seite findet sich ein *quick-link*-Menü für die Konfiguration der wichtigsten Funktionen.



Klickt man auf die ersten beiden Menü-Punkte, so erscheinen Untermenüs zur weiteren Auswahl.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405



Bei den meisten Buttons und Eingabefeldern befindet sich ein Icon ( ) zum Anzeigen und Ausblenden einer kurzen Dokumentation des jeweiligen Eintrages. Viele Abschnitte verfügen zusätzliche über ein Icon ( ) zum Auf- und Zuklappen der in diesem Abschnitt enthaltenen Felder.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

Clustering

Clustering aktivieren

Cluster Mitglieder *

Liste von IP Adressen der Cluster-Mitglieder. Die aktuelle Instanz von gateway.security muss in dieser Liste vorhanden sein. Die einzelnen Server müssen sich untereinander über der Remote Manager Port verbinden können.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

2

Funktionsbeschreibung

Dieser Abschnitt bietet eine Übersicht über die Funktionen von ***IGS*** sowie, falls notwendig, zusätzliche Hintergrundinformationen.

Viele der Einstellungsmöglichkeiten sind ausführlich in Abschnitt 3 beschrieben, oder aus Sicht eines Systemadministrators selbsterklärend. Die entsprechenden Funktionen werden daher nur kurz beschrieben. Der Benutzer wird auf die Detailbeschreibung im erwähnten Abschnitt verwiesen.

2.1 Wie IGS arbeitet

IGS kann als ein **Security Proxy** eingesetzt werden und bietet Dienste für verschiedene TCP-Protokolle an. Diese Proxy-Dienste werden eingeteilt in

- **Web Dienste** zur Sicherung von HTTP und FTP Verbindungen (Abschnitt 2.1.1) , und
- **E-Mail-Dienste** für SMTP, IMAP, POP3 und NNTP Verbindungen (Abschnitt 2.1.2).

Für die Sicherung des E-Mail-Verkehrs, insbesondere von SMTP, kann GS auch als **Mail Transfer Agent (MTA)** eingerichtet werden (Abschnitt 2.1.2.2)

Je nach Betriebssystem des Servers können die Proxy-Dienste im transparenten oder nicht-transparenten Modus arbeiten. Linux-Betriebssysteme unterstützen transparente Proxys durch die Konfigurationsmöglichkeiten von *iptables*. Transparenter Proxy-Betrieb ist auf einem Microsoft Windows Servers standardgemäß nicht möglich.

2.1.1 Web-Dienste

Ausgangspunkt für die Konfiguration der Web Dienste des IGS sind die **Netzwerkregeln.**

Diese Regeln legen, vereinfacht gesagt, fest, **von welchen Netzwerken aus** Verbindungen über IGS erlaubt oder verboten sind, und **wer** Verbindungen herstellen darf oder nicht darf (Zugriffskontrolle).

Daneben gibt es die sogenannten **Permission-Sets**, die in den Netzwerkregeln referenziert werden. Diese Permission-Sets bestehen aus einem Satz von Regeln, welche Beschränkungen **basierend auf der Art der angeforderten Netzwerk-Ressourcen** definieren.

2.1.1.1 Zugriffskontrolle

Baut ein Client eine Verbindung mit IGS auf, so werden die Netzwerkregeln der Reihe nach ausgewertet. Für jede Regel ist ein **Netzwerk,** eine IP-Adresse oder eine Subnetz-Maske definiert, die mit der Client-IP-Adresse verglichen wird.

Die erste passende Netzwerkregel wird angewandt und liefert als Ergebnis, ob die Verbindung zulässig ist oder nicht.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Existiert keine passende Netzwerkregel, so wird der Zugang verweigert.

Wird aufgrund der Regel der Zugriff verweigert, so werden keine weiteren Überprüfungen mehr durchgeführt.

2.1.1.2 Permission-Sets

Das über die Netzwerkregel ausgewählte Permission-Set besteht aus einer Liste von Permission-Regeln. Jede dieser Regeln besteht aus einem oder mehreren Kriterien und liefert als Ergebnis, ob der Zugriff erlaubt oder verboten ist.

Ebenso wie die Netzwerkregeln werden auch die Permission-Sets nach ihrer Priorität abgearbeitet und die erste zutreffende Regel wird angewandt.

Trifft keine Permission-Regel zu, so ist der Zugriff gestattet.

2.1.1.3 Permission-Set-Auswahl

Abhängig vom **Authentifizierungstyp** (siehe 3.3.3.12) einer Netzwerkregel können Platzhalter verwendet werden, um Permission-Sets mit Hilfe sogenannter **Permission-Set-Masken** zu selektieren.

Diese Platzhalter werden durch aktuelle Verbindungsparameter ersetzt, um das Permission-Set zu ermitteln, das letztendlich zur Anwendung kommt. Somit können Permission-Sets pro Benutzer oder Benutzergruppen definiert werden.

Zum Beispiel könnte ein Permission-Set `permission_user1` definiert sein und eine Netzwerkregel den Wert `permission_%u` als Permission-Set eingetragen haben. Ersteres wird nur angewandt, wenn der aktuelle Benutzername `user1` ist.

Das funktioniert analog für Gruppen, sofern diese vom jeweiligen Authentifizierungstyp unterstützt werden. Die interne Authentifizierung unterstützt die Verwendung von `%u` (Benutzername). LDAP und NTLM/Kerberos erlauben zusätzlich den Platzhaltern `%g`, der bei Auswertung der Netzwerkregel durch den Gruppennamen ersetzt wird.

Die letztgenannten zwei Authentifizierungstypen (LDAP und NTLM/Kerberos) ermöglichen in der Windows-Domäne auch die Verwendung von SIDs (siehe 3.3.1.9). Ist IGS dementsprechend konfiguriert, so werden die jeweiligen Platzhalter durch die SID anstatt des Namens des Benutzers oder der Gruppe ersetzt.

2.1.1.4 Zugriff verweigern

Wird Zugriff auf die angeforderte Ressource gewährt, so wird der übertragene Inhalt mittels der IKARUS scan.engine auf Schadsoftware durchleuchtet. Sollte der Zugriff blockiert werden, wird dem Benutzer eine Seite für den Grund der Blockierung angezeigt. Mögliche Gründe sind

- Fehlende Autorisierung
- Zugriff auf den Inhalt wird aufgrund einer Permission-Regel verweigert
- Der angeforderte Inhalt stellt sich als Schadsoftware heraus.

Diese sogenannten *block-response*-Seiten sind konfigurierbar. Details finden Sie unter 3.1

2.1.1.5 HTTPS und verschlüsselte Inhalte

Es ist offensichtlich, dass verschlüsselte Inhalte normalerweise nicht gescannt werden können. Das ist besonders im Hinblick auf HTTPS-Verbindungen zu bemerken.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Es existieren Produkte von Drittanbietern, um diese Probleme zu umgehen. Sollte dies für Sie von Interesse sein, kontaktieren Sie bitte IKARUS bezüglich weiterer Informationen.

2.1.2 E-Mail-Dienste

IGS kann entweder als Security-Proxy für die Protokolle **SMTP**, **POP3**, **IMAP** und **NNTP** verwendet werden, oder aber als ***Mail Transfer Agent (MTA)*.**

2.1.2.1 Scan-Regeln

Zur Überprüfung von E-Mails auf bösartige Inhalte können verschiedene **Scan-**Regeln definiert werden.

Diese legen fest

- was mit bösartigen Inhalten geschieht, wenn diese von der IKARUS scan.engine erkannt werden
- welche Arten von Dateianhängen verdächtig sind
- woran SPAM erkannt werden kann, zusätzlich zur eingebauten SPAM-Erkennung

Scan-Regeln können den einzelnen Protokollen zugewiesen werden und legen die Behandlung betroffener E-Mail-Inhalte oder Dateianhänge fest.

2.1.2.2 Konfiguration der Proxy-Dienste

Die Konfiguration der Proxy-Dienste ist identisch für die vier Protokolle POP3, IMAP, NNTP und (transparentes) SMTP.

Client-Einstellungen für POP3 und IMAP

Im Falle eines nicht-transparenten Betriebs, muss der Security-Proxy als (POP3 oder IMAP) E-Mail-Server anstelle des tatsächlichen Mail-Servers des Providers eingetragen werden.

Um in so einem Fall dem Proxy den echten Ziel-Server bekannt zu geben, kann dieser an den Benutzernamen, durch '#' getrennt, angehängt werden.

```
<mail-username>#<mail-server-name>[:<mail-server-port>]
```

In diesem Fall werden E-Mails als Benutzer `<mail-username>` an den Mail-Server `<mail-server-name>`. Die Angabe des Ports ist optional.

2.1.2.3 Verwendung von IGS als Mail Transfer Agent (MTA)

Um potentielle Bedrohungen durch **eingehende E-Mails** zu erkennen und abzuwehren, muss IGS als MTA vor den internen Mail-Server oder als *Mail Exchange (MX) gateway* verwendet werden. Das erfordert, dass der MX Eintrag der Domäne auf den IGS-Server zeigt.

Für umfassenden Schutz muss sämtlicher E-Mail-Verkehr über den IGS-Server geleitet werden.

Zur Überprüfung **ausgehender E-Mails** muss IGS als *Mail Relay Server* konfiguriert werden.

Mail-Weiterleitung

Die E-Mail-Routen legen fest, wie eingehende oder ausgehende E-Mails weitergeleitet werden und welche Scan-Regeln anzuwenden sind. Diese Entscheidung wird anhand verschiedener Kriterien konfiguriert, wie z.B. der IP-Adresse oder Sub-Netz des Absenders oder der Ziel-Mailbox.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

SPAM Filterung

Zusätzlich zur SPAM-Erkennung mittels Scan-Regeln unterstützt IGS im MTA-Modus auch

- Sender Policy Framework (SPF)[2]
- Greylisting[3]
- Early Talker Rejection

für eingehende E-Mails.

Sender Policy Framework

SPF überprüft den TXT-Eintrag der Absender-Domäne. Dieser Eintrag wird vom *name server* retournierte und enthält eine Liste von IP-Adressen oder Subnetzen, aus denen E-Mails dieser Domäne versendet werden dürfen. Ist die IP Adresse des Absenders nicht in dieser Liste enthalten, so wird die E-Mail-Verbindung verweigert. Von Domänen ohne TXT-Eintrag müssen E-Mails standardgemäß angenommen werden.

Greylisting

Greylisting bezeichnet eine Methode zur Erkennung von MTAs, die SPAM-Mails versenden. Mail-Verkehr wird nur weitergeleitet, wenn der versendende MTA den *Greylisting*-Test besteht.

MTAs, die diesbezüglich als vertrauenswürdig erkannt worden sind, können optional in eine **temporäre *Whitelist*** eingetragen werden.

Zusätzlich existiert eine permanente Whitelist. E-Mails von MTAs in dieser Liste wird ohne *Greylisting*-Test weitergeleitet.

Early Talker Rejection

Gemäß des RFC für SMTP[4] muss der Sender auf die Begrüßungsnachricht des Empfängers warten, bevor irgendein Kommando gesendet wird. Konforme E-Mail-Clients und Server warten dies, im Gegensatz zu SPAM-Bots, normalerweise ab. Ist diese Funktion aktiviert, so wartet IGS ein gewisse, zu konfigurierende Zeitspanne, bevor das *greeting banner* gesendet wird. Jeder Versuch der Gegenseite, davor ein SMTP-Kommando zu senden, führt zu einer Ablehnung der gesendeten Nachricht.

2.2 Allgemeine Funktionen

2.2.1 Protokollierung

IGS erzeugt verschiedene Typen von Protokolldateien. Für jede dieser Dateien können maximale Größe und Speicherort festgelegt werden.

- Global: Globale Informationen wie z.B. Serverstatus oder kritische Fehler.
- Web: Informationen über HTTP- und FTP-Verbindungen.
- E-Mail log: Information über SMTP-, IMAP-, POP3- und NNTP-Verbindungen.

[2] http://www.openspf.org/

[3] http://tools.ietf.org/html/rfc6647

[4] http://tools.ietf.org/html/rfc5321#section-4.3.1

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

- Benachrichtigungen: Gesonderte Hinweise über bestimmte Ereignisse wie z.B. die Aktualisierung von Modulen. Siehe 2.2.4 für weitere Details.
- Debug: Diagnose-Informationen. Das Debug-Protokoll ist standardgemäß deaktiviert und muss bei Bedarf aktiviert werden.

Debug-Protokollierung kann dazu führen, dass große Datenmengen auf der Festplatte gespeichert werden.

Eine Protokolldatei mit der Aktualisierungs-Historie wird automatisch angelegt und kann nicht konfiguriert werden.

2.2.2 Aktualisierungen

IGS unterstützt die automatische Aktualisierung folgender Komponenten

- Programmdateien
- Aktualisierungsprogramm (*updater*)
- *plugin*-Bibliotheken
- Virendatenbank (VDB)
- SPAM-Datenbank (SDB)
- URL-Filter-Datenbank (UDB)

Der Dienst überprüft alle 10 Minuten, ob für eine der Komponenten Aktualisierungen vorhanden sind. Ist diese der Fall, werden sich heruntergeladen und installiert. Der Dienst wird bei Bedarf automatisch neu gestartet.

2.2.3 Benutzerverwaltung

Für den authentifizierten Zugriff auf IGS können Benutzernamen zusammen mit Passwörtern definiert werden. Diese kann man sich als eine Art Benutzer vorstellen, auch wenn damit keine richtige Benutzerverwaltung verbunden ist.

In diesem Sinn wird zwischen zwei Arten von 'Benutzern' unterschieden:

- Remote-Manager-Benutzer für einen autorisierten Zugriff auf die Verwaltungsoberfläche und –schnittstellen.
- Interne Benutzer, die ausschließlich zur Authentifizierung im Rahmen von Netzwerk-Regeln dienen. Remote-Manager-Benutzer können dafür ebenfalls verwendet werden, interne Benutzer aber nicht für einen Zugriff auf den Remote-Manager.

Nach der Neuinstallation von IGS ist bereits der Standard-Benutzer ROOT mit dem Passwort "root" angelegt. Ändern Sie dieses Passwort unmittelbar nach der Installation!

2.2.4 Benachrichtigungen

Benachrichtigungen dienen dazu, Systemadministratoren über unregelmäßig auftretende oder außergewöhnliche Ereignisse zu informieren, wie z.B. die Aktualisierung der Datenbanken oder die Detektion von Schadsoftware.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

2.2.5 Berichte

Wenn diese Funktion aktiviert ist, werden Verbindungsdaten in einer Datenbank gespeichert. Basierend darauf können Diagramme oder Tabellen definiert werden um z.B. eine Übersicht zu erhalten, welche Art von Zugriffen innerhalb eines bestimmten Zeitraums blockiert wurden, oder welche Domänen von den Benutzern hauptsächlich besucht werden.

2.2.6 WCCP

IGS unterstützt das WCCP-Protokoll[5].

2.2.7 IGS Clustering

IGS erlaubt die Synchronisierung der Konfigurationsdateien zwischen verschiedenen Servern. Diese Funktion wird als ***Clustering*** bezeichnet.

2.2.8 Verwaltungsschnittstellen

2.2.8.1 Remote Manager

Der *Remote Manager* ist eine TCP-Schnittstelle, die standardgemäß über Port 15639 läuft. Sie wird u.A. für folgende Zwecke genutzt:

- Verwaltungs-Plugin für ISA/TMG Server
- Kommunikation mit anderen IGS-Servern im Rahmen des Clusterings.
- Verbindung mit dem Windows Desktop-Client *Configuration Center,* welches inzwischen von der Browser-Schnittstelle abgelöst wurde.

2.2.8.2 REST API

Zusätzlich zum *Remote Manager* verfügt IGS auch über eine REST-API (Siehe Abschnitt 5). Diese läuft über HTTPS und wird von der integrierten Browser-Benutzerschnittstelle verwendet.

Die API stellt eine Möglichkeit dar, die Verwaltung von IGS in verschiedene Umgebungen zu integrieren.

[5] http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3 Konfiguration

3.1 *Block response* Seiten

IGS ermöglicht die Anzeige verschiedener Seiten zur Benutzerauthentifizierung, für Informationen über blockierte Zugriffe, Lizenz-Fehler und vieles mehr. Die entsprechenden HTML-Vorlagen liegen in dem Verzeichnis `image/messages`. Zusätzliche Ressourcen wie *style sheets*, Grafiken oder Skripte liegen in `image/htdocs`.

Zugriffe auf die URL `http://proxy.ikarus.at/htdocs/` werden nach umgeleitet `images/htdocs`. Zugriff auf dieses Verzeichnis muss durch entsprechende Konfiguration des Web-Servers sicherstellt werden.

Nach der Installation befinden sich die folgenden Standard-Vorlagen im Ordner `image/messages`:

Dateiname	Beschreibung
`404.html`	*File not found* - wird angezeigt, wenn die angeforderte Ressource nicht im Verzeichnis `htdocs` gefunden wird
`destcontinent.html`	Zugriff für den Kontinent des Ziel-Servers ist gesperrt
`destcountry.html`	Zugriff für das Land des Ziel-Servers ist gesperrt
`fileblocked.html`	Entweder der Name oder der *content type* der Datei ist gesperrt.
`ftp.html`	Anzeigeseite für FTP-Zugriffe über HTTP
`generic.html`	Generische Seite. Wird z.B. angezeigt, wenn für den aktuellen Benutzer keine Netzwerkregel definiert wurde
`infected.html`	Eine infizierte Datei wurde blockiert
`license.html`	Zugriff wurde aufgrund einer abgelaufenen oder ungültigen Lizenz gesperrt
`lockpage.html`	Eine *landing page,* die angezeigt wird, solange der Benutzer den Benutzungsbedingungen nicht zugestimmt hat
`networkerror.html`	Ziel-Server konnte nicht erreicht werden.
`nouser.html`	Kein gültiges Permission-Set für diesen Benutzer vorhanden (fehlgeschlagene Authentifizierung)
`transferlimit.html`	Benutzer hat das Transferlimit überschritten
`urlblocked.html`	Die angefragte URL ist auf der *black list*

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

`urlcategory.html`	Die Kategorie der angefragten URL ist auf einer *black list*

3.1.1 Konfiguration der Seiten

Da es sich bei den Dateien im Ordner `image` um Standard-Vorlagen handelt, sollten diese nicht geändert werden.

Stattdessen können Vorlagen, Bilder und andere Dateien in den Verzeichnissen `conf/messages` und `conf/htdocs` angelegt werden, um das Erscheinungsbild anzupassen. Jede Datei in den genannten zwei Ordnern überschreibt die entsprechende Datei in `image` und dessen Unterverzeichnissen.

Wird eine Vorlage für eine *block response*-Seite benötigt, so wird sie zuerst in `conf/messages` gesucht. Ist sie dort nicht vorhanden, so wird stattdessen die Standardversion aus `image/messages` verwendet.

3.1.1.1 Template-Parameter

Die HTML-Vorlagen können Schlüsselwort enthalten, die ersetzt werden, bevor die Seite als Antwort retourniert wird. Diese sogenannten Template-Parameter werden von Prozent-Zeichen (`%`) eingeschlossen. Dieses Zeichen darf daher in den Vorlagen nicht verwendet werden oder muss durch die HTML-Entität `&#37;` ersetzt werden.

Template-Parameter	Beschreibung
`catnames`	Komma-getrennte Liste der UDB-Kategorien, die auf die angeforderte Seite zutreffen
`countryname`	Land der angeforderten Seite
`continentname`	Kontinent der angeforderten Seite
`proto`	Verwendetes TCP-Protokoll
`permission`	Name des Permission-Sets, das auf die Abfrage zutrifft
`client_ip`	IP-Adresse des Client
`target_host`	Name des Zielserver
`target_port`	Port des Zielservers
`target_path`	Pfad der angeforderten Ressource
`vdbsigname`	VDB-Signatur, aufgrund derer der Zugriff blockiert wurde
`errmsg`	HTTP Response-Header

Der Link `http://proxy.ikarus.at/welcomeack` wird von `lockpage.html` verwendet, um dem Server mitzuteilen, dass der Benutzer die Benutzungsbedingungen akzeptiert hat. Dieser Link darf weder entfernt noch modifiziert werden.

Da die Vorlagen direkt in die HTTP-Response übernommen werden, müssen die ersten 3 Zeilen unverändert von den Vorlagen übernommen werden.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.1.2 Brandings

Mit Hilfe sogenannter *Brandings* ist er möglich, unterschiedliche Sätze von *block repsonse*-Vorlagen sowie den dazu gehörigen Grafiken etc. zu definieren. Diese Brandings können dann für verschiedene Netzwerke angewandt werden sollen.

Die HTML-Vorlagen für die verschiedenen Brandings liegen in Unterverzeichnissen von `conf`, die entsprechend dem jeweiligen Branding benannt sind.

```
conf/
    messages/
      Filial1/
        lockpage.html
      Filiale2/
       lockpage.html
...
```

Wird ein Branding über eine Netzwerkregel zugewiesen, so werden die entsprechenden Verzeichnisse nach HTML-Vorlagen durchsucht. Ebenso wie bei den Vorlagen ohne Branding wird in letzter Instanz das `image` Verzeichnis nach Vorlagen durchsucht, sollten sie im Branding-Ordner nicht vorhanden sein.

In derselben Art und Weise werden die Unterverzeichnisse von `conf/htdocs` nach anderen Ressourcen durchsucht, die für das jeweilige Branding benötigt werden. Es wird empfohlen, das HTML-Element `<base>` zu verwenden, um den Zugriff auf Ressourcen über relative Pfade zu ermöglichen. Somit kann der Aufwand für Anpassungen verringert werden.

```
<base href="http://proxy.ikarus.at/htdocs/subsidiary1" />
```

3.2 Grundlegendes zur Konfiguration

Alle Konfigurationseinstellungen (mit Ausnehme der oben beschriebenen HTML-Vorlagen), die vom Systemadministrator geändert werden können, werden in einer Konfigurationsdatei namens `conf/securityproxy.conf`[6] gespeichert. Dieser Datei verwendet im Wesentlichen dasselbe Format, wie es für die Konfiguration von Apache[7]-Webservern verwendet wird.

Diese Datei besteht aus Schlüssel-Wert-Paaren (Konfigurationsitems), welche in Gruppen, ähnlich einer XML-Datei, zusammengefasst sind. Daher kann für jedes dieser Items ein *Pfad* angegeben werden, um es in der Datei zu finden und in der nachfolgenden Dokumentation nachzuschlagen.

Es bestehen folgende Möglichkeiten, die Konfiguration zu ändern:

1. Manuelles Editieren der Konfigurationsdatei. Das erfordert Zugriff auf das Dateisystem.
2. Über die IGS Browser-Oberfläche (siehe 1.4).
3. Mittels der REST API (siehe Abschnitt 5). Diese API wird von der Browser-Oberfläche zum Lesen und Schreiben der Konfigurationsdaten verwendet und zur Verwaltung des Servers verwendet.

[6] Für die Verzeichnisstruktur des Programms siehe Abschnitt 1.3

[7] http://httpd.apache.org/

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3 Konfigurationsdaten

Dies ist eine vollständige Beschreibung aller Konfigurationseinträge von IGS. Wo ein Eintrag in der Konfigurationsdatei zu finden ist, wird mittels eines Pfades angegeben.
Pflichtfelder sind mit einem Stern markiert (∗);

Für jeden Abschnitt ist ebenso der Pfad angegeben, über den er mittels der REST-API bearbeitet werden kann. Pfad-Element, die in spitzen Klammern ('<>') stehen, entsprechen benannten Objekten.
Diese können vom Benutzer selbst angelegt und benannt werden, wie z.B. die Permission Sets.

Im Anschluss daran findet sich eine Aufstellung der verwendeten Datentypen und Enumerationen.

3.3.1 Konfigurationseinträge

3.3.1.1 Konfiguration

API-Pfad: `/config`

Pfad in der Konfigurationsdatei: `/`

Konfiguration von IKARUS gateway.security

3.3.1.2 Web Dienste

API-Pfad: `/config/access`

Pfad in der Konfigurationsdatei: `/ACCESS`

Zugriffskontrolle für HTTP Verbindungen

Attribut	Name	Beschreibung	Typ
`browser_lists`	Browser-Liste	Benannte Liste von Webbrowsern	`Array(String)`
`contenttype_lists`	Content-Type-Liste	Liste von Content Types	`Array(ContentType)`
`file_lists`	Datei-Liste	Benannte Listen von Dateimasken. Diese Listen können als Kriterien für Permission-Regeln verwendet werden	`Array(File)`
`url_lists`	URL-Liste	Benannte URL-Listen	`Array(URL)`

3.3.1.3 Landingpage

API-Pfad: `/config/access/lockpage`

Pfad in der Konfigurationsdatei: `/ACCESS/LOCKPAGE`

Einstellungen für gateway.security Landing Pages

Attribut	Name	Beschreibung	Typ
`session_timeout`	Session Timeout	Dauer der Landing-Page-Session	`Integer`

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

3.3.1.4 Data Collector

API-Pfad: `/config/access/lockpage/datacollector`

Pfad in der Konfigurationsdatei: `/ACCESS/LOCKPAGE/DATACOLLECTOR`

Einstellungen für Anmeldeseiten, die den Datacollector verwenden

Attribut	Name	Beschreibung	Typ
`confirm_timeout`	Bestätigungs-Timeout	Zeit (in Sekunden), die der Benutzer hat, um den Bestätigungslink zu klicken	`Integer`
`confirm_tries`	Anmeldeversuche	Maximale Anzahl der Versuche, das Formular erneut zu versenden	`Integer`

3.3.1.5 Formularname

API-Pfad: `/config/access/lockpage/datacollector/forms/<data_collector_form_name>`

Pfad in der Konfigurationsdatei: `/ACCESS/LOCKPAGE/DATACOLLECTOR/FORMS/<data_collector_form_name>`

Eine Liste mehrerer Formulare, die für den Datacollector verwendet werden. Jedes Formular benötigt einen eindeutigen Namen. Somit kann es bei den Netzwerkregeln referenziert werden, wenn Authentifizierung mittels Datacollector erforderlich ist

Attribut	Name	Beschreibung	Typ
`label_email`	E-Mail Anzeigetext	Beschriftungstext für das Eingabefeld der E-Mail-Adresse	`String`
`mail_subject`	E-Mail-Betreff	Betreffzeile für die E-Mail mit dem Bestätigungslink	`String`

3.3.1.6 Zusätzliche Felder

API-Pfad: `/config/access/lockpage/datacollector/forms/<data_collector_form_name>/fields/<data_collector_form_field_name>`

Pfad in der Konfigurationsdatei: `/ACCESS/LOCKPAGE/DATACOLLECTOR/FORMS/<data_collector_form_name>/FIELDS/<data_collector_form_field_name>`

Eingabefelder des Formulars für den Datacollector. Das Feld "email" wird immer automatisch erzeugt und kann daher nicht hinzugefügt werden

Attribut	Name	Beschreibung	Typ
`key`	Schlüssel	Eindeutiger Bezeichner für das Eingabefeld. Dieser Bezeichner wird für das HTML-Formular des Datacollectors verwendet	`DatacollectorFormFieldKey`
`label`	Beschriftung	Beschriftungstext vor dem Eingabefeld	`String`

mandatory	Pflichtfeld	Gibt an, ob die Eingabe von Daten für dieses Feld verpflichtend ist	Flag

3.3.1.7 Netzwerkregeln

API-Pfad: /config/access/networks

Pfad in der Konfigurationsdatei: /ACCESS/NETWORKS

Netzwerkregeln für die Zugangskontrolle

Attribut	Name	Beschreibung	Typ
groups	Netzwerke	Netzwerkgruppen dienen zur Zusammenfassung verschiedener Netzwerke. Die Zugriffskontrolle kann damit für viele Netzwerke über eine Regel gesteuert werden	Array(IpAddress)

3.3.1.8 Prioritätsliste

API-Pfad: /config/access/networks/group_priority/<group_priority_name>

Pfad in der Konfigurationsdatei: /ACCESS/NETWORKS/GROUP_PRIORITY/<group_priority_name>

Gruppen-Prioritätsliste, welche für die Netzwerkregel angewandt wird

Attribut	Name	Beschreibung	Typ
name	SID/LDAP Gruppe	Eindeutiger Name der Gruppen-Prioritätsliste	String

3.3.1.9 Netzwerk Regeln

API-Pfad: /config/access/networks/rules/<network_rule_name>

Pfad in der Konfigurationsdatei: /ACCESS/NETWORKS/<network_rule_name>

Mittels dieser Liste von Regeln wird anhand verschiedener Kriterien ermittelt, ob der Zugang gestattet wird oder nicht

Attribut	Name	Beschreibung	Typ
auth_result	Permission-Set pro Maske	Either 'deny' or 'allow' as result if the network rule matches the current connection	PermissionSetMask
auth_type	Authentifizierungsmethode	Authentifizierungtyp für das ausgewählte Netzwerk	NetworkAuthenticationType
branding	Branding	Legt das Branding fest, welches für das ausgewählte Netzwerk anzuwenden ist	Branding

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

form	Formular	Data Collector Formular, das zur Authentifizierung verwendet wird	
group_priority	Prioritätsliste	Gruppen-Prioriätsliste, die für die Netzwerkregel anzuwenden ist. Wird nur im Zusammenhang mit der Authentifizierung mittels LDAP oder NTLM/Kerberos benötigt	
network_group	Netzwerkgruppe	Netzwerkgruppe, auf welche die Netzwerkregel anzuwenden ist	
network_rule_type	Typ	Zeigt an ob die Netzwerkregel für ein Subnetz oder eine Netzwerkgruppe gilt	
permission_set	Permission-Set	Das Permission-Set, das für das Netzwerk angewandt wird	
redirecturl	Weiterleiten nach	URL, an die der Endbenutzer nach erfolgter Authentifizierung wietergeleitet wird	String
result	Zulassen/verbieten	Legt fest, ob als Ergebnis dieser Netzwerkregel der Zugriff erlaubt oder blockiert wird	Enum(RuleResult)
router	Router	IP Adresse des GRE Routers	IpAddress
subnet	Subnetz	IP Subnetz, auf das die Regel angewandt wird	Subnet

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

use_sid	SID statt Namen verwenden	Verwende SID der Benutzer oder Gruppen statt Namen	Flag

3.3.1.10 Permissions

API-Pfad: /config/access/permissions

Pfad in der Konfigurationsdatei: /ACCESS/PERMISSIONS

Permission Sets

3.3.1.11 Permission-Set

API-Pfad: /config/access/permissions/permission_sets/<permission_set_name>

Pfad in der Konfigurationsdatei: /ACCESS/PERMISSIONS/<permission_set_name>

Ein Permission-Set besteht aus einem Satz von Regeln, um Netzwerkressourcen zuzuordnen. Passt eine Regel auf eine angeforderte Ressource, so bestimmt diese Regel, ob der Zugriff erlaubt wird oder nicht

Attribut	Name	Beschreibung	Typ
encryptedfilebad	Verschlüsselte Dateien als Malware behandeln	Legt fest, ob verschlüsselte Dateien grundsätzlich als Malware eingestuft werden sollen	Enum(FlagInherited)
extends	Basiert auf Permission-Set	Es kann ein Permission-Set angegeben werden, um von diesem Einstellungen zu übernehmen	
mz_filebad	Ausführbare Dateien als Malware behandeln	Legt fest, ob ausführbare Dateien grundsätzlich als Malware eingestuft werden sollen	Enum(FlagInherited)
transferlimit	Datenlimit	Beschreibt die Datenmenge in MB, die übertragen werden darf (nur in Kombination mit Lockpage)	DataSizeWithUnit

3.3.1.12 Content-Regeln

API-Pfad: /config/access/permissions/permission_sets/<permission_set_name>/urls/<permission_rule_name>

Pfad in der Konfigurationsdatei: /ACCESS/PERMISSIONS/<permission_set_name>/URLS/<permission_rule_name>

Geordnete Liste von Regeln, bestehend aus mehreren Auswahlkriterien. Die Einträge der Liste werden der Reihe nach durchgegangen und die Kriterien mit der aktuellen Verbindung verglichen. Die erste passende Regel wird angewandt und legt fest, ob Zugriff auf die angeforderte Ressource gewährt oder verweigert wird

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Attribut	Name	Beschreibung	Typ
alternating_id	Criterion type	Verschiedenste Auswahlkriterien, nach welchen Eigenschaften die einzelnen Regeln gefiltert werden sollen	
browser_list	Browser-Liste	Browser-Liste, die als Kriterium angewandt wird	
contenttypelist	Content-Type-Liste	Als Kriterium wird eine Content-Type-Liste verwendet	
continent	Kontinentcode	Als Kriterium wird der Kontinent der Ziel-IP-Adresse verwendet	
country	Ländercode	Als Kriterium wird das Land der Ziel-IP-Adresse verwendet	
days	Wochentage	Legt die Wochentage fest, für die das Permission-Set gilt	Enum(DaysOfWeek)
file	Datei/Dateiendung	Als Kriterium wird der Dateiname der angeforderten Ressource verwendet	FileExtension
filelist	Dateiliste	Eine Dateiliste, die als Kriterium verwendet wird	
result	Erlauben	Das Ergebnis, wenn die Regel zutrifft	Enum(RuleResult)
time	Zeitraum	Legt die Zeitspanne fest, in der dieser Regel angewandt wird (Format: 'hh:mm-hh:mm')	Timespan
time_control	Zeitsteuerung	Legt fest, ob es sich bei dem Wert um einen Wochentag, oder um ein Zeitintervall handelt	
url	URL	Eine URL als Kriterium verwenden	URL
urlfiltercat	URL-Filterkategorie	URL-Filter-Kategorie als Kriterium verwenden	
urllist	URL Liste	URL-Liste als Kriterium verwenden	

3.3.1.13 Automatisches Update

API-Pfad: /config/autoupdate

Pfad in der Konfigurationsdatei: /AUTOUPDATE

Einstellungen für automatische Updates. Sind diese aktiviert, so prüft gateway.security alle 10 Minuten, ob neue Programm- oder Datenbank-Updates verfügbar sind

Attribut	Name	Beschreibung	Typ

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

enableautoupdate	Automatisches Update aktivieren	Aktivieren/deaktivieren automatischer Updates	Flag

3.3.1.14 Clustering

API-Pfad: /config/cluster

Pfad in der Konfigurationsdatei: /CLUSTER

Einstellungen für einen gateway.security Cluster. Mehrere Instanzen von gateway.security können zu einem solchen Cluster zusammengefasst werden, um die Konfigurationseinstellungen zwischen diesen Instanzen zu synchronisieren

Attribut	Name	Beschreibung	Typ
enable	Clustering aktivieren	De/aktivieren der Cluster-Funktionalität	Flag
members	Cluster Mitglieder	Liste von IP Adressen der Cluster-Mitglieder. Die aktuelle Instanz von gateway.security muss in dieser Liste vorhanden sein. Die einzelnen Server müssen sich untereinander über der Remote Manager Port verbinden können	Array(IpOrHostname)

3.3.1.15 Global

API-Pfad: /config/global

Pfad in der Konfigurationsdatei: /

Globale Einstellungen für gateway.security

3.3.1.16 Benachrichtigungen

API-Pfad: /config/global/alerts

Pfad in der Konfigurationsdatei: /

Beim Eintreten bestimmter Ereignisse kann der Server Benachrichtigungen erzeugen. Diese können als Einträge in einer Protokolldatei erfolgen, oder durch das Versenden einer E-Mail an eine vordefinierte Adresse

3.3.1.17 Benachrichtigung

API-Pfad: /config/global/alerts/alerts/<alert_name>

Pfad in der Konfigurationsdatei: /ALERTS/<alert_name>

Beim Eintreten bestimmter Ereignisse kann der Server Benachrichtigungen erzeugen. Diese können als Einträge in einer Protokolldatei erfolgen, oder durch das Versenden einer E-Mail an eine vordefinierte Adresse

Attribut	Name	Beschreibung	Typ
email	E-Mail-Adresse	Empfänger der E-Mail-Benachrichtigung	EmailAddress

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

event	Ereignisse	Ein Liste von Ereignissen, für die eine Benachrichtigung erzeugt wird	Enum(AlertEventFlags)
path	Protokolldatei	Relativer Pfad der Protokolldatei für die Benachrichtigung	Path
type	Benachrichtigungstyp	Gibt an, in welcher Form die Benachrichtigung erfolgen soll (Protokollierung oder E-Mail)	

3.3.1.18 LDAP

API-Pfad: /config/global/ldap

Pfad in der Konfigurationsdatei: /ACCESS/NETWORKS/LDAP/

Einstellungen zur Benutzerauthentifizierung mittels LDAP

Attribut	Name	Beschreibung	Typ
authldapbinddn	DN des Benutzers	Legt den DN Namen für die LDAP-Authentifizierung fest	String
authldapbindpassword	Passwort	Passwort zur LDAP Authentifizierung	Password
authldapurl	LDAP URL	Die LDAP URL gemäß RFC 2255	String

3.3.1.19Automatisierte E-Mails

API-Pfad: /config/global/messenger

Pfad in der Konfigurationsdatei: /MESSENGER

Einstellungen für den Versand von E-Mails durch IKARUS gateway.security

Attribut	Name	Beschreibung	Typ
smtpserver	Mail Server	Mailserver für den E-Mail-Versand	String
systemadmin	E-Mail-Adresse des Absender	Absender für E-Mails, die von IKARUS gateway.security versandt werden	EmailAddress

3.3.1.20Verzeichnisse

API-Pfad: /config/global/paths

Pfad in der Konfigurationsdatei: /

Globale Einstellungen für gateway.security

Attribut	Name	Beschreibung	Typ
quarantinepath	Quarantäne-Verzeichnis	Verzeichnis zum Speichern von gefährlichen E-Mail-Dateianhängen	Path

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

storepath	Verzeichnis für Datenbank-Dateien	Verzeichnis für Datenbank-Dateien	Path
tmppath	Temporäres Verzeichnis	Verzeichnis für temporäre Dateien	Path

3.3.1.21 Next-Proxy

API-Pfad: /config/internet

Pfad in der Konfigurationsdatei: /PROXY

Einstellungen für die Verwendung eines Proxy-Servers durch gateway.security

Attribut	Name	Beschreibung	Typ
auth_pass	Passwort	Passwort für Proxy-Server	Password
auth_user	Benutzername	Benutzername für Proxy-Server	String
excludedomains	Ausgenommene Domains	Liste von Domänen, für die kein Proxy verwendet wird	Array(String)
ftp_host	FTP	Proxy-Server für FTP-Verbindungen	String
ftp_port	Port	Proxy-Server-Port fpr FTP Verbindungen	Port
http_host	HTTP	Proxy-Server für HTTP-Verbindungen	String
http_port	Port	Proxy-Server-Port für HTTP-Verbindungen	Port
https_host	HTTPS	Proxy-Server für HTTPS-Verbindungen	String
https_port	Port	Proxy-Server-Port für HTTPS-Verbindungen	Port

3.3.1.22 Protokolldateien

API-Pfad: /config/logging

Pfad in der Konfigurationsdatei: /LOGGING

Einstellungen für Protokolldateien

3.3.1.23 Debug

API-Pfad: /config/logging/log_debug

Pfad in der Konfigurationsdatei: /LOG/LOG_DEBUG

Einstellungen für Debug Protokolldateien

Attribut	Name	Beschreibung	Typ
enable	Debug Protokoll aktivieren	Diese Option ermöglicht Debug-Protokollierungen. Aktivieren Sie diese Option nur temporär, um Fehlerquellen effizienter	Flag

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

		aufzufinden, da dies zu Einbrüchen in der Performanz führen kann	
maxdirsize	Maximale Größe (insgesamt)	Maximale Größe aller Debug-Protokolldateien in dem Verzeichnis. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
maxsize	Maximale Größe	Maximale Größe einer Debug-Protokolldatei. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
path	Verzeichnis für Protokolldateien	Verzeichnis für Debug-Protokolldateien	Path

3.3.1.24Global

API-Pfad: /config/logging/log_global

Pfad in der Konfigurationsdatei: /LOG/LOG_GLOBAL

Einstellungen für gateway.security Protokoll

Attribut	Name	Beschreibung	Typ
maxdirsize	Maximale Größe (insgesamt)	Maximale Größe aller globalen Protokolldateien in dem Verzeichnis. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
maxsize	Maximale Größe	Maximale Größe einer globalen Protokolldatei. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
path	Verzeichnis für Protokolldateien	Verzeichnis für globale Protokolldateien	Path
timespan	Neue Datei anlegen	Zeitspanne, nach der eine neuen Protokolldatei angelegt wird	Enum(LogInterval)

3.3.1.25E-Mail

API-Pfad: /config/logging/log_mail

Pfad in der Konfigurationsdatei: /LOG/LOG_MAIL

Protokolleinstellungen für E-Mail-Dienste

Attribut	Name	Beschreibung	Typ

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

maxdirsize	Maximale Größe (insgesamt)	Maximale Größe aller Protokolldateien in dem Verzeichnis. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
maxsize	Maximale Größe	Maximale Größe einer E-Mail-Protokolldatei. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
path	Verzeichnis für Protokolldateien	Verzeichnis für Protokolldateien	Path
timespan	Neue Datei anlegen	Zeitspanne, nach der eine neuen Protokolldatei angelegt wird	Enum(LogInterval)

3.3.1.26Web

API-Pfad: /config/logging/log_proxy

Pfad in der Konfigurationsdatei: /LOG/LOG_PROXY

Protokolleinstellungen für Web Dienste

Attribut	Name	Beschreibung	Typ
maxdirsize	Maximale Größe (insgesamt)	Maximale Größe aller Proxy-Protokolldateien in dem Verzeichnis. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
maxsize	Maximale Größe	Maximale Größe einer Proxy-Protokolldatei. Benutzen Sie bitte das Postfix 'K', 'M' oder 'G' (ohne Leerzeichen) als Maßeinheit	DataSizeWithUnit
path	Verzeichnis für Protokolldateien	Verzeichnis für HTTP-Protokolldateien	Path
timespan	Neue Datei anlegen	Zeitspanne, nach der eine neuen Protokolldatei angelegt wird	Enum(LogInterval)

3.3.1.27Remote Manager

API-Pfad: /config/remotemanager

Pfad in der Konfigurationsdatei: /REMOTEMANAGER

Einstellungen für den IKARUS gateway.security Remote Manager

Attribut	Name	Beschreibung	Typ
allowip	IP Adresse/Netzwerk	IP Adresse oder Netzwerk, von dem aus Verbindungen mit	Array(Subnet)

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

		dem Remote Manager erlaubt sind	
auth_mode	Authentifizierungsmodus	Legt fest, ob sich der Remote-Manager-Benutzer mittels Passwort oder über LDAP authentifiziert	Enum(RemoteManagerAuthMode)
ip	Remoteverwaltung	Bind Adresse für den Remote Manager Service. Falls nicht angegeben, wird an alle Adressen gebunden	IpAddress
port	Port für Remote Manager	Listener Port des Remote Managers	Port

3.3.1.28 Benutzer

API-Pfad: /config/remotemanager/users/<remote_manager_user_name>

Pfad in der Konfigurationsdatei: /REMOTEMANAGER/<remote_manager_user_name>

Einstellungen für Remote-Manager-Benutzer

Attribut	Name	Beschreibung	Typ
allowip	Erlaubte IPs	Host/Netzwerk, von dem aus der Remote Manager Verbindungen akzeptiert	Array(Subnet)
rights	Benutzerberechtigungen	Legt fest, ob der Benutzer die Konfiguration ändern oder nur lesen darf	

3.3.1.29 Web API Server

API-Pfad: /config/remotemanager/webapiserver

Pfad in der Konfigurationsdatei: /WEBAPI_SERVER

Einstellungen für die REST Schnittstelle

Attribut	Name	Beschreibung	Typ
listen	Listener	Port und optionale lokale IP-Adresse, die für Verbindungen zur REST API und zum Web Interface verwendet werden	Array(IpWithPort)

3.3.1.30 Berichte

API-Pfad: /config/reports

Pfad in der Konfigurationsdatei: /REPORTS

Einstellungen für Berichte. Wenn die Funktion nicht aktiviert ist, werden keine Verbindungsdaten aufgezeichnet. Infolgedessen stehen keine Daten aus dem Zeitraum zur Verfügung, wo diese Funktion deaktiviert war

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Attribut	Name	Beschreibung	Typ
enable	Berichte aktivieren	Aktiviert/deaktiviert das Protokollieren von Verbindungsdaten zum Erstellen von Berichten. Ist diese Funktion deaktiviert, so werden keine Verbindungsdaten protokolliert und stehen auch nachträglich nicht für Berichte zur Verfügung	Flag
maxsize	Maximale Größe	Beschränkt die Größe der Verbindungsdatenbank auf der Festplatte. Wenn diese Größe überschritten wird, dann werden die ältesten 5% der aufgezeichneten Verbindungen gelöscht. "Älteste" bezieht sich in diesem Fall auf das Datum, zu dem der Eintrag erstellt wurde, und nicht, für welchen Zeitraum der Eintrag gilt. Das kann zur Folge haben, dass nachträglich importierte Verbindungsdaten später gelöscht werden als erwartet und dadurch Lücken in der Zeitreihe entstehen können	DataSizeWithUnit

3.3.1.31 Automatische Berichte

API-Pfad: `/config/reports/autoreporting/<autoreporting_name>`

Pfad in der Konfigurationsdatei: `/AUTOREPORTING/<autoreporting_name>`

Automatische Erstellung von Berichten

Attribut	Name	Beschreibung	Typ
days_month	Tage des Monats	Automatischer Bericht wird an der angegebenen Liste von Tagen im Monat versandt. Tage des Monats beginnen mit 1	Array(DaysOfMonth)
days_week	Wochentage	Automatischer Bericht wird an der angegebenen Liste von Wochentagen versandt. Wochentage beginnen mit 1	Enum(DaysOfWeek)
email	E-Mail	Liste von E-Mail Adressen, an die die automatisch generierten Berichteverschickt werden	Array(EmailAddress)
http_reports	HTTP Berichte	Liste von HTTP Berichten, die automatisch erstellt werden	Array(HttpReport)
period	Periode	Bericht wird an den angegebenen Wochentagen oder Tagen des Monats erzeugt	
smtp_reports	SMTP Berichte	Liste von SMTP Berichten, die automatisch erstellt werden	Array(SmtpReport)
time	Uhrzeit	Tageszeit, zu welcher der Bericht an den ausgewählten Tagen versandt wird	Time

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.1.32 HTTP Berichte

API-Pfad: `/config/reports/http_reports/<http_report_name>`

Pfad in der Konfigurationsdatei: `/REPORTS/<http_report_name>`

Liste aller HTTP Berichte

Attribut	Name	Beschreibung	Typ
`chart`	Diagrammart	Legt fest, ob der Bericht als Tabelle oder als ein bestimmter Diagrammtyp ausgegeben werden soll	
`height`	Pixel	Höhe des Diagramms in Pixel	`Integer`
`httpreportfilter`	Filter	Vordefinierte Kriterien zum Selektieren der Daten für den Bericht	
`shape_bar`	Balkendiagramm	Art des Balkendiagramms	`Enum(ReportShapeBar)`
`shape_pie`	Tortendiagramm	Art des Tortendigramms	`Enum(ReportShapePie)`
`text_bottom`	Beschriftungstext unterhalb	Zusatztext, der unterhalb des Diagramms angedruckt wird	`String`
`text_top`	Beschriftungstext oberhalb	Zusatztext, der oberhalb des Diagramms angedruckt wird	`String`
`title`	Reporttitel	Titel des Berichts	`String`
`width`	Breite	Breite des Diagramms in Pixel	`Integer`

3.3.1.33 SMTP Berichte

API-Pfad: `/config/reports/smtp_reports/<smtp_report_name>`

Pfad in der Konfigurationsdatei: `/REPORTS/<smtp_report_name>`

Liste aller SMTP Berichte

Attribut	Name	Beschreibung	Typ
`chart`	Diagrammtyp	Legt fest, ob der Bericht als Tabelle oder als ein bestimmter Diagrammtyp ausgegeben werden soll	
`height`	Pixel	Höhe des Diagramms in Pixel	`Integer`
`shape_bar`	Balkendiagramm	Art des Balkendiagramms	`Enum(ReportShapeBar)`
`shape_pie`	Tortendiagramm	Art des Tortendiagramms	`Enum(ReportShapePie)`

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

smtpreportfilter	Filter	Vordefinierte Kriterien zum Selektieren der Daten für den Bericht	
text_bottom	Beschriftungstext unterhalb	Zusatztext, der unterhalb des Diagramms angedruckt wird	String
text_top	Beschriftungstext oberhalb	Zusatztext, der oberhalb des Diagramms angedruckt wird	String
title	Titel des Berichts	Titel des Berichts	String
width	Pixel	Breite des Diagramms in Pixel	Integer

3.3.1.34 E-Mail-Dienste

API-Pfad: /config/services

Pfad in der Konfigurationsdatei: /

IKARUS gateway.security bietet Dienste für verschiedene TCP-Protokolle an. Diese können in 'Web-Dienste' und 'E-Mail-Dienste' eingeteilt werden. Erstere behandeln HTTP- und FTP-Anfragen, letztere sind für die Protokolle SMTP, IMAP, POP3 und NNTP zuständig

3.3.1.35 FTP-Proxy-Dienst

API-Pfad: /config/services/ftpproxy

Pfad in der Konfigurationsdatei: /FTP_PROXY

Der FTP-Proxy-Dienst

Attribut	Name	Beschreibung	Typ
anonymous_password	Anonymes Passwort	Passwort für anonyme FTP-Verbindungen	Password
enable	Aktivieren	Aktivieren/deaktivieren des FTP-Proxy-Dienstes	Flag
listen	Listener	Port und optionale lokale IP Adresse, auf der der FTP-Proxy-Dienst auf Anfragen wartet	Array(IpWithPort)
use_outgoing_passive	Passiven Modus verwenden	Wird benötigt, wenn IKARUS gateway.security aufgrund von Firewall-Einstellungen keine aktiven Verbindungen aufbauen darf. In diesem Fall kann die Option gesetzt werden, um Verbindungen im passiven Modus zu verwenden	Flag

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.1.36HTTP-Proxy-Dienst

API-Pfad: `/config/services/httpproxy`

Pfad in der Konfigurationsdatei: `/HTTP_PROXY`

Der HTTP-Proxy-Dienst

Attribut	Name	Beschreibung	Typ
`enable`	Aktivieren	Aktivieren/Deaktivieren des HTTP-Proxy-Dienstes	`Flag`
`listen`	Listener	Port und optionale lokale IP-Adresse, auf der der HTTP-Proxy-Dienst auf Anfragen wartet	`Array(IpWithPort)`

3.3.1.37IMAP-Proxy-Dienst

API-Pfad: `/config/services/imapproxy`

Pfad in der Konfigurationsdatei: `/IMAP_PROXY`

Der IMAP-Proxy-Dienst

Attribut	Name	Beschreibung	Typ
`enable`	Aktivieren	Aktivieren/deaktivieren des IMAP-Proxy-Dienstes	`Flag`
`imap_server`	Standard Ziel-Server	Standard-IMAP-Server. Wird verwendet, wenn der Benutzername keine Informationen über den Ziel-IMAP-Server enthält	`IpOrHostname`
`imap_server_port`	Standard Ziel-Server-Port	Port für der Standard-IMAP-Server	`Port`
`listen`	Listener	Port und optionale lokale IP-Adresse, auf der der IMAP-Proxy-Dienst auf Anfragen wartet	`Array(IpWithPort)`
`scanner_rule`	Scan-Regel	Vom IMAP-Proxy-Dienst verwendete Scan-Regel	

3.3.1.38 NNTP-Proxy-Dienst

API-Pfad: `/config/services/nntpproxy`

Pfad in der Konfigurationsdatei: `/NNTP_PROXY`

Der NNTP-Proxy-Dienst

Attribut	Name	Beschreibung	Typ
`enable`	Aktivieren	Aktivieren/deaktivieren des NNTP-Proxy-Dienstes	`Flag`

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

listen	Listener	Port und optionale IP Adresse, an welcher der NNTP-Proxy-Dienst auf Anfragen wartet	Array(IpWithPort)
nntp_server	Standard Ziel-Server	NNTP Ziel-Server	IpOrHostname
nntp_server_port	Standard Ziel-Server-Port	Port für den Ziel-NNTP-Server	Port
scanner_rule	Scan-Regel	Vom NNTP-Proxy-Dienst verwendete Scan-Regel	

3.3.1.39 POP3-Proxy-Dienst

API-Pfad: /config/services/pop3proxy

Pfad in der Konfigurationsdatei: /POP3_PROXY

Der POP3-Proxy-Dienst

Attribut	Name	Beschreibung	Typ
enable	Aktivieren	Aktivieren/deaktivieren des POP3-Proxy-Dienstes	Flag
listen	Listener	Port und optionale lokale IP-Adresse, auf der der POP3-Proxy-Dienst auf Anfragen wartet	Array(IpWithPort)
pop3_server	Standard Ziel-Server	Standard-POP3-Server. Wird verwendet, wenn der Benutzername keine Informationen über den Ziel-POP3-Server enthält	IpOrHostname
pop3_server_port	Standard Ziel-Server-Port	Port für Standard-POP3-Server	Port
scanner_rule	Scan-Regel	Vom POP3-Proxy-Dienst verwendete Scan-Regel	

3.3.1.40 SMTP Server

API-Pfad: /config/services/smtp

Pfad in der Konfigurationsdatei: /SMTP

Einstellungen für den SMTP-MTA-Dienst

Attribut	Name	Beschreibung	Typ
enable	Aktivieren	Aktivieren/deaktivieren des SMTP MTA Dienstes	Flag
path	Temporäres Verzeichnis für E-Mails	Verzeichnis zum temporären Speichern von E-Mails	Path

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.1.41 Einstellungen für eingehende E-Mails

API-Pfad: `/config/services/smtp/receive`

Pfad in der Konfigurationsdatei: `/SMTP/RECEIVE`

Einstellungen für eingehende E-Mails

Attribut	Name	Beschreibung	Typ
`banner_delay`	Verzögerung für Early Talker Rejection	Zeit in Sekunden, die der SMTP-Dienst wartet, bevor er das SMTP-Banner sendet. Das Banner signalisiert dem sendenden MTA, dass der Empfänger bereit für die Übertragung ist. Viele SPAM-Bots, die das Banner nicht abwarten, können somit blockiert werden	`Integer`
`ip`	Listen-on-Adresse	IP Adresse für eingehende E-Mails	`IpAddress`
`max_connections`	Max. eingehende Verbindungen	Maximale Anzahl von eingehenden SMTP-Verbindungen. Wird diese Anzahl überschritten, so wird ein temporärer Fehler als Antwort retourniert (SMTP Error 421)	`MaxConnections`
`port`	Port	Listener-Port für das SMTP-Protokoll	`Port`

3.3.1.42 Greylisting

API-Pfad: `/config/services/smtp/receive/greylist`

Pfad in der Konfigurationsdatei: `/SMTP/RECEIVE/GREYLIST`

Einstellungen für das Greylisting

Attribut	Name	Beschreibung	Typ
`ignore`	Permanente Whitelist	Eine Liste von Netzwerken oder Absendern, für die kein Greylisting angewandt wird	`IgnoreRule`
`minlastseen`	Verzögerung	Zeitintervall (in Sekunden), das vor dem erneuten Versenden mindestens verstreichen muss, um den Greylisting-Test zu bestehen	`Integer`
`timeout`	Timeout	Zeitintervall (in Sekunden), innerhalb dessen eine E-Mail nach ihrem ersten Eintreffen erkannt wird. Nach Verstreichen dieser Zeit wird der Greylisting-Test für die E-Mail zurückgesetzt	`Integer`
`ttlwhitelist`	Zeitdauer für temporäres Whitelisting	Zeitdauer (in Sekunden), für die der Sender der E-Mail nach bestandenem Greylisting-Test auf der temporären Whitelist bleibt. Ist kein Wert angegeben, wird kein temporäres Whitelisting angewandt	`Integer`

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.1.43 Routen

API-Pfad: `/config/services/smtp/routes/<route_name>`

Pfad in der Konfigurationsdatei: `/SMTP/ROUTES/<route_name>`

SMTP Routen werden definiert, um bestimmte Aktionen auf ein- oder ausgehende SMTP-Verbindungen anzuwenden. Die Routen werden in der angegebenen Reihenfolge mit der bestehenden Verbindung verglichen. Die erste zutreffende Route wird verwendet und die zugeordneten Einstellungen werden auf die Verbindung angewandt

Attribut	Name	Beschreibung	Typ
`client_ip`	Client IP Adressmaske	Client-IP-Adresse oder -Netzwerkmaske	`Subnet`
`direction`	Richtung	Legt fest, ob die Routen-Einstellungen für eingehenden oder ausgehenden E-Mail-Verkehr angewendet werden. Die Einstellung 'Standard' existiert aus Kompatibilitätsgründen und sollte möglichst nicht verwendet werden	
`forwarding`	Aktion	Legt fest, wie E-Mails weitergeleitet werden	
`greylist`	Greylisting	Greylisting aktivieren/deaktivieren	`Flag`
`host_forward`	Host	Wenn die Weiterleitung statisch definiert ist, so werden E-Mails an diesen Server weitergeleitet	`String`
`ldap`	LDAP	Die Mailbox wird über LDAP identifiziert	`String`
`mailbox_file`	Mailbox-Datei	Datei mit einer Liste von Domänen oder E-Mail-Adressen. Der Dateipfad kann entweder absolut oder relativ zum Programmverzeichnis angegeben werden	`Path`
`scan_rule`	Scan	Scan-Regeln ermöglichen es auf detaillierte Art und Weise, Malware oder SPAM zu identifizieren und E-Mails entsprechend zu kennzeichnen	
`spf1`	SPF1	Sender Policy Framework (SPF) aktivieren/deaktivieren	`Flag`
`target_domain`	Ziel-Domäne/E-Mail	Domäne oder E-Mail-Adresse des Empfängers	`Array(DomainOrMail)`
`type`	Typ	Legt fest, auf welche Art die Route definiert wird	

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.1.44 Scan-Einstellungen

API-Pfad: `/config/services/smtp/scansettings`

Pfad in der Konfigurationsdatei: `/SMTP/SCANSETTINGS`

Scan-Einstellungen

3.3.1.45 Scan-Regeln

API-Pfad: `/config/services/smtp/scansettings/scansettings/<scan_setting_name>`

Pfad in der Konfigurationsdatei: `/SMTP/SCANSETTINGS/<scan_setting_name>`

Scan-Einstellungen

Attribut	Name	Beschreibung	Typ
`attachmentfilter`	Anhangfilterung	Einstellungen zum Filtern von E-Mail-Anhängen basierend auf dem Namen der Datei	
`spamfilter`	SPAM Filter	Einstellungen für den IKARUS SPAM-Filter. Dieser bewertet E-Mails anhand ihres Betreffs, Inhalt, Dateianhängen etc. und vergibt umso mehr Punkt, je wahrscheinlicher es sich um SPAM handelt. Durch Festlegen der unteren Grenzwerte für "Potentiellen SPAM" und "SPAM" kann je nach Beurteilung der E-Mail unterschiedlich vorgegangen werden	
`virusfilter`	Malware-Erkennung	Einstellungen für das Klassifizieren und Erkennen von Malware. Bei E-Mails werden sowohl der Nachrichteninhalt als auch Dateianhänge gescannt	

3.3.1.46 Einstellungen für ausgehende E-Mails

API-Pfad: `/config/services/smtp/send`

Pfad in der Konfigurationsdatei: `/SMTP/SEND`

Einstellungen für das Weiterleiten von E-Mails

Attribut	Name	Beschreibung	Typ
`max_connections`	Max. ausgehende Verbindungen	Maximale Anzahl der gleichzeitig ausgehenden Verbindungen	`MaxConnections`

3.3.1.47 SMTP-Proxy-Dienst

API-Pfad: `/config/services/smtpproxy`

Pfad in der Konfigurationsdatei: `/SMTP_PROXY`

Der SMTP-Proxy-Dienst

Attribut	Name	Beschreibung	Typ

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

enable	Aktivieren	Aktivieren/deaktivieren des SMTP-Proxy-Dienstes	Flag
listen	Listener	Port und optionale lokale IP-Adresse, auf der der SMTP-Proxy-Dienst auf Anfragen wartet	Array(IpWithPort)
scanner_rule	Scan Regel	Scan-Regeln für den SMTP Proxy	
smtp_server	Standard Ziel-Server	Standard SMTP Server. Dieser wird verwendet, wenn der Benutzername keine Informationen über den Ziel-Server enthält	IpOrHostname
smtp_server_port	Standard Ziel-Server-Port	Port für den Standard SMTP Server	Port

3.3.1.48 WCCP

API-Pfad: `/config/wccp`

Pfad in der Konfigurationsdatei: `/WCCP`

Einstellungen für WCCP

Attribut	Name	Beschreibung	Typ
designated	Designated Web-Cache	Kennzeichnet diese Instanz von IKARUS gateway.security als Designated Web Cache	Flag
enable	WCCP aktiviert	Aktivieren/deaktivieren der WCCP Funktionalität	Flag
ip_address	WCCP-IP Adresse des Proxy	IP Adresse des gateway.security Servers für die WCCP Router	IpAddress
redirection_type	Art der Weiterleitung	Die anzuwendende Um- oder Weiterleitungsmethode	Enum(WccpRedirectionType)
routers	Liste der WCCP Router	Einer oder mehrere Router, zu denen eine WCCP-Verbindung hergestellt wird	Array(IpAddress)

3.3.2 Datentypen

Typ	Beschreibung
Branding	Branding
ContentType	Content-Type

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

DataSizeWithUnit	Mengenangabe für Datenvolumina. Besteht aus einer positiven, ganzen Zahl, gefolgt von einem Postfix für die Mengeneinheit. Gültige Werte sind 'K','M' oder 'G' für Kilobyte, Megabyte oder Gigabyte. Zwischen der Zahl und der Einheit darf kein Leerzeichen stehen
Date	Datum
Domain	Gültiger Ausdruck für eine Domäne oder Subdomäne
DomainOrMail	Domäne oder E-Mail-Adresse
EmailAddress	Eine gültige E-Mail-Adresse
File	Dateinname
FileName	Dateiname
Flag	Boolscher Wert
HttpReport	Referenz auf einen HTTP-Bericht
IgnoreRule	
Integer	Eine ganze Zahl
IpAddress	Eine IPv4 Adresse
IpWithPort	Eine IP Adresse, gefolgt von einem Doppelpunkt (':') und einer Port-Nummer
Password	Ein Passswort
Path	Ein gültiger Ausdruck für einen Dateipfad. Als Trennzeichnen kann sowohl Backslash ('\') als auch Slash ('/') verwendet werden
PermissionSetMask	Permission-Set-Maske
Port	Port
SmtpReport	Referenz auf einen SMTP-Bericht
SpamLevel	Eine Dezimalzahl zwischen 0.0 und 10.0
String	Eine Zeichenkette
Subnet	Ein Sub-Netz
Time	Zeit
Timespan	Zeitintervall
URL	URL

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

3.3.3 Enumerationen

3.3.3.1 AlertEventFlags

Ereignis

Literal	Beschreibung
`error`	Fehler
`license`	Die Lizenz läuft demnächst ab.
`lowdiskspace`	Auf der Festplatte ist wenig Platz.
`update`	VDB/UDB/SDB Datenbank wurde aktualisiert.
`vdbupdate`	UDB-Aktualisierung
`virusfound`	Malware wurde gefunden.

3.3.3.2 AlertType

Definiert die Art, wie die Benutzer benachrichtigt werden

Literal	Beschreibung
`email`	Benachrichtigungen erfolgen per E-Mail
`logfile`	Benachrichtigungen erfolgen nur über Einträge in der Protokolldatei.

3.3.3.3 AttachmentFilterListPriority

Literal	Beschreibung
`black`	Zuerst Dateien der Blacklist berücksichtigen
`white`	Zuerst Dateien der Whitelist berücksichtigen.

3.3.3.4 AutoReportingPeriod

Intervall

Literal	Beschreibung
`month`	Monatlich
`week`	Wöchentlich

3.3.3.5 ContenttypeSource

Content-Typ

Literal	Beschreibung
`custom`	Individuell

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

predefined	Vordefiniert

3.3.3.6 Contenttypes

Content-Type

Literal	Beschreibung
all	Alle
archive	Archivdatei
audio	Audio
excel	MS Excel
executeable	Ausführbare Datei
office	MS Office
pdf	PDF
powerpoint	MS PowerPoint
video	Video
visio	MS Visio
word	MS Word

3.3.3.7 DataSizePostfix

Einheit

Literal	Beschreibung
g	Gigabyte
k	Kilobyte
m	Megabyte

3.3.3.8 DaysOfWeek

Wochentag

Literal	Beschreibung
1	Montag
2	Dienstag
3	Mittwoch
4	Donnerstag

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

5	Freitag
6	Samstag
7	Sonntag

3.3.3.9 FlagInherited

Inherited flag

Literal	Beschreibung
inherit	Vererbt
no	Nein
yes	Ja

3.3.3.10 GreylistIgnoreType

Permanente Whitelist Typ

Literal	Beschreibung
domain	Domäne
ipmask	IP-Maske
mail	E-Mail

3.3.3.11 LogInterval

Log interval

Literal	Beschreibung
day	Täglich
week	Wöchentlich

3.3.3.12 NetworkAuthenticationType

Authentifizierungstyp

Literal	Beschreibung
datacollector	Funktioniert ähnlich wie die Landingpage Authentifizierung. Die Benutzerin wird auf eine Seite mit einem Formular weitergeleitet. Nach Abschicken der Formulardaten erhält sie eine E-Mail mit einem Link zur Freischaltung des Internetzugangs.
ldap	Die Benutzer-Zugangsdaten werden mittels LDAP verifiziert.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

lockpage	Beim ersten Zugriff auf das Netzwerk wird die Benutzerin auf eine Seite mit einem Link zum Freischalten weitergeleitet. Nach Betätigen des Links wird für die aktuelle IP Adresse Zugriff auf das Netzwerk gewährt.
negotiate	Die Benutzerin identifiziert sich durch ihre Domänen-Konto. Die Authentifizierungsdaten werden in der HTTP Anfrage übertragen.
proxy	IKARUS gateway.security erlaubt die Definition von Zugangsdaten mittels Benutzernamen und Passwort. Wenn eine Benutzerin Zugang zum Netzwerk benötigt, wird sie nach den Zugangsdaten gefragt.
set	Die Authentifizierung wird nicht geprüft.

3.3.3.13 NetworkRuleType

Regel-Typ

Literal	Beschreibung
network_group	Netzwerkgruppe
subnet	Subnetz

3.3.3.14 PermissionCriterionType

Kriterium

Literal	Beschreibung
all	Alle
contenttypelist	Content-Type-Liste
continent	Kontinente
country	Länder
file	Datei/Dateiendung
filelist	Dateiliste
url	URL
urlfiltercat	URL-Filterkategorien
urllist	URL-Liste

3.3.3.15 RemoteManagerAuthMode

Authentication type

Literal	Beschreibung
internal_user	Benutzerauthentifizierung erfolgt mittels der Remote Manager Zugangsdaten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

ldap_group	Benutzerauthentifizierung erfolgt über eine LDAP Anfrage.

3.3.3.16 ReportChart

Diagrammtyp

Literal	Beschreibung
bar	Balken
line	Linie
pie	Torte
table	Tabelle

3.3.3.17 ReportFilterBlocked

Blocked

Literal	Beschreibung
blocked	Geblockt
notblocked	Nicht geblockt

3.3.3.18 ReportFilterInfected

Infected

Literal	Beschreibung
infected	Infiziert
notinfected	Nicht infiziert

3.3.3.19 ReportHttpFilterDetail

Detail

Literal	Beschreibung
contenttype	Geblockte Contenttypen
continent	Geblockte Kontinente
country	Geblockte Länder
infected	Geblockte Infektionen
notinfected	Nicht geblockt
permissionset	Geblockte Permissionsets
transferlimit	Geblockt wg. Transferlimit

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

url	Geblockte URLs
urlcat	Geblockte URL-Kategorien

3.3.3.20 ReportHttpFilterFlagGroup

Filter

Literal	Beschreibung
all	Alles
blocked	Geblockt
details	Details

3.3.3.21 ReportHttpFilterGroup

Eine Liste vordefinierter HTTP-Berichte

Literal	Beschreibung
all	Bericht über das gesamte Datenvolumen.
all_customers_nwgroup_param	Kunden in Netzwerkgruppe
all_customers_subnet_param	Bericht gruppiert nach Kunden des angegebenen Subnetzes.
all_domain_param	Bericht für die angegebene Domäne.
all_nwgroup_param	Bericht über die angegebene Netzwerkgruppe
all_permissionset_param	Bericht über die angegebenen Permission Sets
all_srcip_param	Bericht für die angegebene Quell-IP-Adresse.
all_subnet_param	Bericht über das angegebene Subnetz.
all_tld_param	Bericht über die angegebene Top Level Domain.
top_domain	Bericht gruppiert nach Domänen. Die führenden Ergebnisse werden angezeigt.
top_domain_permissionset_param	Top Domänen für Permission-Set
top_domain_srcip_param	Top Domains per Source IP
top_domain_subnet_param	Top Domains für Subnetz
top_nwgroup	Bericht gruppiert nach Netzwerkgruppen.
top_permissionset	Top Permission-Set
top_srcip	Bericht gruppiert nach Quell-IP-Adressen.
top_subnet	Bericht gruppiert nach Subnetzen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

top_subnet_nwgroup_param	Top Subnetze für Netzwerkgruppe
top_tld	Bericht gruppiert nach Top Level Domains.
top_tld_nwgroup_param	Top TLDs für Netzwerkgruppe
top_tld_permissionset_param	Top TLDs pro Permission-Set
top_tld_srcip_param	Top TLDs per Source IP
top_tld_subnet_param	Top TLDs für Subnetz

3.3.3.22 ReportShapeBar

Bar

Literal	Beschreibung
hor	Horizontal
horstack	Horizontal gestapelt
vert	Vertikal
vertstack	Vertikal gestapelt

3.3.3.23 ReportShapePie

Torte

Literal	Beschreibung
empty	Leer
fill	Voll
slice	Gestückelt

3.3.3.24 ReportSmtpFilterDetail

Detail

Literal	Beschreibung
grey	Greylisted
ham	HAM
pspam	Possible SPAM
spam	SPAM
spf	SPF

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.3.25 ReportSmtpFilterDirection

Direction

Literal	Beschreibung
`all`	Ein- und ausgehend
`in`	Eingehend
`out`	Ausgehend

3.3.3.26 ReportSmtpFilterFlagGroup

Filter

Literal	Beschreibung
`all`	Alles
`blocked`	Geblockt
`details`	Details
`infected`	Infiziert

3.3.3.27 ReportSmtpFilterGroup

Berichtstyp

Literal	Beschreibung
`all`	Alle Mailboxen.
`all_mailbox_param`	Mailbox
`top_mailbox`	Zeigt die Daten nach Mailboxen gruppiert und absteigend nach Datenvolumen an.

3.3.3.28 ReportSummarizeBy

Sum up by

Literal	Beschreibung
`data_size`	Datenvolumen
`number`	Anzahl

3.3.3.29 ReportTimeUnit

Time unit

Literal	Beschreibung
`day`	Tage

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

hour	Stunden
month	Monate
quarter	Quartale
week	Wochen
year	Jahre

3.3.3.30 RuleResult

Zugriff

Literal	Beschreibung
allow	Zulassen
deny	Verbieten

3.3.3.31 SmtpRouteDirection

Richtung

Literal	Beschreibung
default	Standard
inbound	Eingehend
outbound	Ausgehend

3.3.3.32 SmtpRouteForwarding

Versand

Literal	Beschreibung
mx	MX
static	Host

3.3.3.33 SmtpRouteType

Typ

Literal	Beschreibung
client_ip	Client-IP-Adresse
ldap	LDAP
mailbox_file	Mail-Box-Datei
target_domain	Zieldomäne

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

3.3.3.34SpamFilterAction

Aktion

Literal	Beschreibung
block	E-Mail blocken
markonly	E-Mail nur kennzeichnen
redirect	E-Mail weiterleiten

3.3.3.35SpamRuleField

SMTP-Header, die als Kriterien für SPAM-Regeln zur Verfügung stehen. Manche erfordern die zusätzliche Angabe eines Wertes zur Überprüfung, ob der Header diesen Wert enthält.

Literal	Beschreibung
emptyfrom	Leerer Header 'From'
emptysubject	Leerer Header 'Subject'
emptyto	Leerer Header 'To'
envelopfrom	Absender in SMTP envelope ist gleich dem angegebenen Wert.
envelopto	Empfänger in SMTP envelope ist gleich dem angegebenen Wert.
from	Header 'From' beinhaltet <FROM>
mailtext	E-Mail- Text
nofromline	Header 'From' fehlt
notoline	'To' fehlt
novalidaddrfrom	'From' ungültig
novalidaddrto	'To' ungültig
onlyhtmltext	Nachrichtentext nur HTML
subject	'Subject' enthält
to	'To' enthält
toandfromequal	'To' und 'From' identisch

3.3.3.36SpamRuleResult

Ergebnis

Literal	Beschreibung
always	SPAM

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

never	REGULAR
possible	POSSIBLE SPAM

3.3.3.37TimeControl

Zeitsteuerung

Literal	Beschreibung
none	Keine
time_range	Zeitintervall
weekdays	Wochentage
weekdays_and_time_range	Wochentage und Zeitinterval

3.3.3.38VirusFilterEmailAction

Action

Literal	Beschreibung
deleteitem	Lösche Anhang
dropemail	Lösche E-Mail

3.3.3.39WccpRedirectionType

Type

Literal	Beschreibung
gre	Weiterleitung mittels GRE.
layer2	Weiterleitung mit Überschreiben der Ziel-MAC-Adresse.

3.4 Content Types

Dies ist eine umfassende Liste der *Content Types,* die von IGS erkannt werden.

Typ	Basistyp
Archive	
compiler/linker	
Documents	
EMail	
Executables	
Miscellaneous	
Multimedia	

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
777 Archive	Archive
7-Zip Archive	Archive
WinAce Archive	Archive
AMGC/OOP Archive	Archive
ARC Archive data, crunched	Archive
ARC Archive data, dynamic LZW	Archive
ARC Archive data, packed	Archive
ARC Archive data, squashed	Archive
ARC Archive data, squeezed	Archive
ARC Archive data, uncompressed	Archive
ARJ Archive	Archive
QuArk Compressed Archive	Archive
ARX Archive	Archive
System V ar Archive	Archive
ASD Archive	Archive
ArcFS Archive	Archive
BAG Archive	Archive
BAG Archive	Archive
BlackHole Archive	Archive
Binary II Archive	Archive
Archive	Archive
Blink Archive	Archive
BOA Archive	Archive
Bzip 2 UNIX Compressed File	Archive
BZip2 Archive	Archive
Microsoft Cabinet Archive	Archive
ChArc Archive	Archive
CKit Archive	Archive
CPIO Archive (Linux)	Archive
CPIO Archive	Archive
CRUSH Archive	Archive
DC Archive	Archive
DMS Archive	Archive
DWC archive	Archive
ELI Archive	Archive
ETCP Archive	Archive
Microsoft Compress 6.2 Archive	Archive
Microsoft Compress 5 Archive	Archive
EXP Archive	Archive
Freeze Archive	Archive
GNU TAR Archive	Archive
GZip Archive	Archive
HAP Archive	Archive
HPACK Archive	Archive
WinZip Archive	Archive
Huffman Archive	Archive
Hyper Archive	Archive
Freeze! Compressed Archive	Archive
IMP Archive	Archive
InstallShield Archive	Archive

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
InstallShield Cab Archive	Archive
JAM Archive	Archive
JARC Compressed Archive	Archive
JAR Archive	Archive
Java Archive	Archive
JRC Archive	Archive
LBR Archive	Archive
LHA Archive (compressed)	Archive
LIMIT Archive	Archive
LZA Archive	Archive
LZH Archive (compressed)	Archive
LZOP Archive	Archive
LZSH Archive	Archive
LZX Compressed File	Archive
MAR Archive	Archive
NRV Archive	Archive
NuFX Archive	Archive
Old GZip/Freeze Archive	Archive
Pack Archive	Archive
PKZIP Archive	Archive
PAKLEO Archive	Archive
PMarc archive data [pm0]	Archive
PMarc archive data [pm1]	Archive
PMarc archive data [pm2]	Archive
PopCom compressed executable (CP/M)	Archive
PMarc archive data (CP/M, DOS)	Archive
PPMd Archive	Archive
Posix Tar Archive	Archive
PowerPacker Archive	Archive
QFC Archive	Archive
Quantum Archive	Archive
Q archive	Archive
WinRAR Archive	Archive
ReSOF Archive	Archive
SAR Archive	Archive
SBC Archive	Archive
SCO LZH Compress Archive	Archive
Semone Archive	Archive
Symbian Software Installation Script	Archive
StuffIt Compressed Archive	Archive
StuffIt Compressed Archive	Archive
SQSH Archive	Archive
SQueezed Archive	Archive
SQWEZ Archive	Archive
Squeeze Compressed file archive for UNIX and MS-DOS	Archive
SWAG Archive	Archive
SZIP Archive	Archive
Tape Archive	Archive
TNEF Archive (winmail.dat)	Archive

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
TSComp Archive	Archive
UC2 Compressed Archive	Archive
UltraCrypt2 Archive	Archive
UFA Archive	Archive
UHArc Archive	Archive
Make Upgrade Archive	Archive
Wraptor Archive	Archive
XPK Archive	Archive
YAC Archive	Archive
YC Archive	Archive
YBS Archive	Archive
ZET Archive	Archive
TurboZip Archive	Archive
ZOO Archive	Archive
ZZip Archive	Archive
Z Compressed Archive	Archive
InstallShield Data Archive	Archive
7 Zip SFX	Archive
Windows Selfextracting .ace	Archive
Windows Selfextracting .arj	Archive
LZH SFX	Archive
NSIS Installer	Archive
Windows Selfextracting pklite	Archive
Windows Selfextracting .rar	Archive
Windows Selfextracting .zip	Archive
Selfextracting WinAce File	Archive
Office 2010	Archive
Adlib Sound	Audio
CD Audio Track	Audio
Extended MOD Sound Data	Audio
Farandoyle Tracker Music Module	Audio
Interchangeable File Format	Audio
Impulse Tracker Music Module	Audio
MIDI Sound	Audio
MPEG Layer 2 Sound File	Audio
L.A.M.E. encoded MP3 Audiofile	Audio
MPEG Layer 3 Sound	Audio
MPEG Layer 4 Sound	Audio
Sound Advanced Audio Coding (ACC)	Audio
MPEG Layer 1 Sound File	Audio
MutliTracker Music Module	Audio
RealAudio Sound File	Audio
RealAudio Sound File	Audio
RMI MIDI File	Audio
ScreamTracker v3 Sound File	Audio
ScreamTracker v2 Sound File	Audio
Sun/NeXT Audio Data	Audio
UltraTracker Music Module	Audio
Creative Voice File	Audio
WAV Sound	Audio

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
Microsoft Visual FoxPro File	compiler/linker
Microsoft Visual C++ File	compiler/linker
Microsoft ClassWizard	compiler/linker
Visual Basic Active Designer Cache	compiler/linker
Delphi Compiled Unit	compiler/linker
MS Developer Intermediate MDPX File	compiler/linker
Borland Project	compiler/linker
Program Library Common Object File Format (COFF)	compiler/linker
Microsoft Visual FoxPro Menu	compiler/linker
Microsoft PreCompiled Header File	compiler/linker
MS Visual C++ Debugging Info	compiler/linker
MS Visual C++ Debugging Info	compiler/linker
Python Compiler Script	compiler/linker
Microsoft Visual Studio Resource	compiler/linker
Watcom C Project	compiler/linker
MS Office	Documents
Textfile	Documents
WordPerfect	Documents
Leading doctype document	Documents
Adobe Acrobat Forms Document	Documents
HTML document	Documents
OLE Document	Documents
Adobe Acrobat Document	Documents
Richtext Document	Documents
MS Works Spreatsheet	Documents
Email - Plain Text	EMail
UPX Converted Executable	ExePacker
Archive	Executables
ExePacker	Executables
Amiga Executable	Executables
Android Dalvik executable file	Executables
Symbian executable file (OS version > 9)	Executables
ELF binary	Executables
Windows 16 bit DLL	Executables
PE DLL	Executables
LE executable	Executables
DOS executable	Executables
NE executable	Executables
PE+ executable	Executables
PE+ 64 bit opcode	Executables
PE+ DLL	Executables
PE+ Itanium executable	Executables
PE+ System File	Executables
PE 64 bit opcode	Executables
PE corrupt file	Executables
PE Itanium executable	Executables
PE executable	Executables
PE System File	Executables
Visual Basic program - native code	Executables

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

Typ	Basistyp
Visual Basic program - p-code	Executables
VxD driver	Executables
MZ Executable, corrupt?	Executables
Mach O executable file	Executables
Novell NetWare Executable	Executables
Win2k Loader Executable	Executables
x86 opcode	Executables
GERMAN ASCII - Plain Text	GERMAN - ASCII
Image	Graphic
AnimatedImage	Image
3D Studio Max Scene (OLE Document)	Image
3D Studio Max Image	Image
3DX Image File	Image
Computer Graphics Metafile	Image
Blender 3D Image	Image
Bitmap Image	Image
Corel Draw Image	Image
ComputerEyes Raw Image	Image
Continous Edge Graphic Image	Image
Autodesk Animator Graphic	Image
ColoRIX Image	Image
Autodesk Animator Color Map	Image
Corel Texture Image	Image
Microsoft Windows Cursor	Image
Microsoft Paintprush Image	Image
Device Independent Bitmap Graphic	Image
DPX Image	Image
AutoCAD Drawing Database	Image
AutoCAD Drawing Interchange Image	Image
Enhanced Windows Meta File Image	Image
Adobe Encapsulated PostScript	Image
Fractal Image	Image
FIG Image File	Image
Flexible Image Transport System	Image
FlashPix Bitmap	Image
GIMP Image	Image
Prassi CD Image	Image
GIMP Image	Image
Handmade Software JPEG Image	Image
Imagic Film Image	Image
Windows Icon	Image
Netware Printing	Image
Img Software Set Bitmap	Image
Img Software Set Image	Image
Amiga Icon	Image
JFIFF Image	Image
JPEG-LS Image	Image
JPEG Network Graphic Bitmap	Image
JPEG Image	Image
LBM Image	Image

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
Lotus PIC Image	Image
MacPaint Bitmap Graphic	Image
Magick Image File Format	Image
Microsoft Paint Image	Image
PAT GIMP Image	Image
Unix Portable Bitmap Graphic	Image
PCX Image	Image
GIMP Image	Image
Unix Portable GrayMap Graphic	Image
PC Paint Bitmap Graphic File	Image
Autodesk Animator Pro Graphic	Image
Autodesk Animator Graphic	Image
Japan PI Image	Image
Autodesk Animator Polygon File	Image
PM Image	Image
Portable (Public) Network Graphic	Image
GIMP Image	Image
Unix Portable PixelMap Graphic	Image
Adobe Photoshop File	Image
Quick Link II Fax Image	Image
CALS Image	Image
WaveFront RLA Image	Image
Utah Raster Toolkit Bitmap Image	Image
Standard Archive Format Image	Image
AutoCAD Shape Entities	Image
SPIFF Image	Image
Sun Icon	Image
Sun Raster Image	Image
TrueVision Image (256 Colors)	Image
Tagged Image Format	Image
Autodesk Animator Tween Data	Image
VICAR2 Image	Image
XCF GIMP Image	Image
X PixMap Image	Image
X Window Dump Image	Image
Animated Cursor	AnimatedImage
Digital Video File Format	AnimatedImage
Shockwave File	AnimatedImage
GIF Image	AnimatedImage
Multiple Network Graphics Video	AnimatedImage
Silicon Graphics Movie	AnimatedImage
Apple QuickTime Movie	AnimatedImage
MPEG 2.0 Video data	AnimatedImage
Microsoft Access 2000/2002 Document	MS Access
Microsoft Access 2.0 Document	MS Access
Microsoft Access 97 Document	MS Access
MS Excel 2.0 Document	MS Excel
MS Excel 3.0 Document	MS Excel
MS Excel 4.0 Document	MS Excel
MS Excel 5.0 or 7.0 (Excel 95) Document	MS Excel

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
MS Excel XP Document	MS Excel
Microsoft Excel Document	MS Excel
Archive	MS Office
MS Access	MS Office
MS Excel	MS Office
MS PowerPoint	MS Office
MS Visio	MS Office
MS Word	MS Office
Microsoft Office Design File	MS Office
OEL compound file	MS Office
MS Write Document	MS Office
Microsoft PowerPoint 4.0 Document	MS PowerPoint
Microsoft Visio 4.x Document	MS Visio
Microsoft Visio 6.x Document	MS Visio
MS Office Document	MS Word
Microsoft PowerPoint 97 - 2002 Document	MS Word
Microsoft Word 2000/2002 Document	MS Word
Microsoft Word 2.0 Document	MS Word
Microsoft Word 6.0 or 7.0 Document (95)	MS Word
Microsoft Word 97/98 Document	MS Word
NetWare Unicode Rule Table	Miscellaneous
3D Studio Max Matlib File (OLE Document)	Miscellaneous
3D Studio Max Plugin	Miscellaneous
3D Studio Max Project	Miscellaneous
Microsoft Agent Character	Miscellaneous
Kaspersky Antivirus File	Miscellaneous
Winamp Advanced Visualization Studio	Miscellaneous
Microsoft Answer Wizard	Miscellaneous
Microsoft Visual Basic Module	Miscellaneous
Babylon Dictionary	Miscellaneous
Microsoft Publisher Border	Miscellaneous
Device Driver For Pascal	Miscellaneous
Device driver for C/C++	Miscellaneous
Babylon Glossary	Miscellaneous
Microsoft Backup File	Miscellaneous
Windows Calender	Miscellaneous
Microsoft Security Catalog	Miscellaneous
Internet Security Certificate	Miscellaneous
Compiled HTML - Header File	Miscellaneous
Java Class	Miscellaneous
Microsoft Visual Basic Class Module	Miscellaneous
Help File Contents	Miscellaneous
Microsoft FaxCover	Miscellaneous
Windows Helpfile	Miscellaneous
Cygwin Info	Miscellaneous
Microsoft Internet Explorer Cache File	Miscellaneous
Cygwin File	Miscellaneous
Microsoft Visual FoxPro Database Container	Miscellaneous
dBase III PLUS Database	Miscellaneous

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
Microsoft Outlook Express E-Mail Folder	Miscellaneous
Microsoft Visual FoxPro Database Container	Miscellaneous
Data Interchange File	Miscellaneous
AIL Sound Driver	Miscellaneous
Microsoft Visual Basic Active Designer Binary	Miscellaneous
TeX Device Independent Document	Miscellaneous
Rational Rose 98 Compiled Script	Miscellaneous
eMacs Lisp Byte-compiled Source Code	Miscellaneous
UUENCODE Encoded	Miscellaneous
FORTRAN Interface	Miscellaneous
FLC Animation Format	Miscellaneous
FLI Animation Format	Miscellaneous
Saved Search	Miscellaneous
Windows Font	Miscellaneous
Microsoft Visual FoxPro File	Miscellaneous
Microsoft Visual FoxPro Table	Miscellaneous
Visual Basic Binary Form	Miscellaneous
Windows Help Full-Text Search Index	Miscellaneous
Microsoft Visual FoxPro Compiled Program	Miscellaneous
Windows Program Manager Group	Miscellaneous
Compressed PC-Library Hierarchy	Miscellaneous
Windows Helpfile	Miscellaneous
HTML Help File	Miscellaneous
HyperTterminal Data	Miscellaneous
ICC Profile	Miscellaneous
MIDI Instruments Definition File	Miscellaneous
Java Tracking File	Miscellaneous
Watcom Help File	Miscellaneous
Intel IPhone Compatible File	Miscellaneous
Microsoft Linker Database	Miscellaneous
ISO Image	Miscellaneous
InstallShield Unistall Script	Miscellaneous
Internet Document Set	Miscellaneous
Kaspersky Antivirus Key	Miscellaneous
Reflection X Keymap	Miscellaneous
MS-SQL Server Transaction Log File	Miscellaneous
MSPaper Language	Miscellaneous
Windows Shortcut	Miscellaneous
Microsoft Access Module Link File	Miscellaneous
Winamp3 Compiled Script	Miscellaneous
Maple Libraray	Miscellaneous
Microsoft Access Report Link File	Miscellaneous
MS-SQL Master Database	Miscellaneous
Rational Rose Object Design Model	Miscellaneous
Microsoft Developer Studio Project	Miscellaneous
AIL Midi Driver	Miscellaneous
MMF File	Miscellaneous
Cygwin Messages	Miscellaneous

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
Oracle 7 Data	Miscellaneous
Oracle 7 Datafile	Miscellaneous
Microsoft Installer Patch	Miscellaneous
Microsoft Installer	Miscellaneous
Winamp3 Table	Miscellaneous
Winamp3 Index	Miscellaneous
Oracle 7 Data File	Miscellaneous
Lotus Notes Database Template File	Miscellaneous
VMWare NVRam	Miscellaneous
Windows Object	Miscellaneous
OFM Font File	Miscellaneous
Developer Studio File Workspace Options	Miscellaneous
Autodesk Animator Optics Menu Settings	Miscellaneous
Cygwin/Adobe Font	Miscellaneous
Microsoft Profiler Binary Input	Miscellaneous
Reflection X Font	Miscellaneous
X.509 Certificate	Miscellaneous
Adope PostScript Type 1 Font	Miscellaneous
Printer Font	Miscellaneous
Windows Program Information	Miscellaneous
Microsoft Office Settings	Miscellaneous
Microsoft Visual FoxPro Project	Miscellaneous
Windows Precompiled Setup Information	Miscellaneous
Windows Password List	Miscellaneous
RDOFF Executable	Miscellaneous
Windows NT Registry	Miscellaneous
Windows 95/98 Registry	Miscellaneous
Oracle Resource	Miscellaneous
RedHat Package Manager File	Miscellaneous
Microsoft Foxpro Screen	Miscellaneous
Speedo Scalable Font	Miscellaneous
Ocracle SYM	Miscellaneous
Windows Keyboard Driver	Miscellaneous
T2 Temp. Signatur Datenbank	Miscellaneous
TeX Font Metric File	Miscellaneous
SPSS Type Library	Miscellaneous
Borland Pascal Unit	Miscellaneous
TrueType Font File	Miscellaneous
True Type Font File	Miscellaneous
FoxPro Class Library	Miscellaneous
Ikarus Software Virus Database	Miscellaneous
VMware Virtual Disk	Miscellaneous
Windows Meta File	Miscellaneous
Fast Tracker 2 Extended Module	Miscellaneous
XPCOM Type Library	Miscellaneous
Java Time Zone	Miscellaneous
Audio	Multimedia
Graphic	Multimedia
Audio	Multimedia
GERMAN - ASCII	Textfile

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Typ	Basistyp
US - ASCII	Textfile
Active Server Page Document	Textfile
Applixware Words Document	Textfile
DOS Batch	Textfile
Microsoft Channel Definition	Textfile
SSL Encrypted Certificate Revocation List	Textfile
HTML Document	Textfile
Java Script	Textfile
Java Network Launching Protocol File	Textfile
MHTML Document	Textfile
Perl Script	Textfile
Pretty Good Privacy Encrypted File	Textfile
UNICODE - This File is Unicode	Textfile
UUEncoded	Textfile
Visual Basic Script	Textfile
XML Document	Textfile
US ASCII - Plain Text	US - ASCII
Microsoft Advanced Streaming Format	Video
AVI Video/Sound	Video
Flash video multimedia container format	Video
MPEG Video	Video
MPEG Video Stream Data	Video
MPEG Video	Video
Macromedia Flash Format	Video
Shockwave Flash Object	Video
Video	Audio
WordPerfect Dictionary	WordPerfect
WordPerfect Document	WordPerfect
WordPerfect Display Resource(DRS)	WordPerfect
WordPerfect Overlay File (FIL)	WordPerfect
WordPerfect Help Document	WordPerfect
WordPerfect Prefix Information	WordPerfect
WordPerfect Keyboard Definition	WordPerfect
WordPerfect Macro	WordPerfect
WordPerfect Macro Resource(MRS)	WordPerfect
WordPerfect Printer Resource(ALL)	WordPerfect
WordPerfect Printer Resource(PRS)	WordPerfect
WordPerfect Setup	WordPerfect
WordPerfect Thesaurus Document	WordPerfect
WordPerfect Graphics Driver (WPD)	WordPerfect
WordPerfect Document	WordPerfect

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

4

Remote Manager (English only)

The Remote Manager (RM) is an interface of the IKARUS gateway.security (GS) using TCP connections.

As of now, the RM is used for communication with the following clients:

- Configuration Center
- Administration plug-in for ISA/TMG server
- Other instances of GS running on different servers.
- This is used for synchronization of proxies within a cluster.

4.1 Configuration

The settings needed for the RM are as follows:

Attribute	Default value	Description
PORT	15639	The remote manager's listening port.
IP	0.0.0.0	Bind address. If not specified, binds to all IP addresses.
AUTH_MODE	internal_user	Authorization mode for connecting to RM Possible values: internal_user: Use internal users (see below). ldap_group: Use LDAP.
ALLOWIP		Comma-separated list of hosts or networks which are accepted for RM connections. *Localhost* is always supported.

If access is denied, the connection will be reset without any response.

4.2 Internal users

GS supports the definition of user names and passwords.

Attribute	Default value	Description

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

NAME		Unique username.
ALLOWIP		Comma-separated list of hosts or networks from which the user is allowed to connect the RM.
AUTH	passwd	Authentication type (legacy)
PASSWD		Password
RIGHTS		User permissions: *read:* Only read configuration data. *write:* Change configuration data and restart server.

Remark: After installation, the user *root* with password *root* is defined. For security reasons, these user settings have to be changed as soon as possible.

4.3 Protocol

The RM protocol is line-base. Each line has to be terminated by <CR><LF>. With regard to standard string implementations of C, null bytes are NOT allowed.

4.4 Definition of protocol

```
<line> ::= <line-character> <LF> | <line-character> <CR> <LF>
<line-character> :: any character that is not: <NUL>, <CR>, <LF>
<NUL> ::= null-character (ASCII 0)
<CR> ::= carriage return (ASCII 13, '\r')
<LF> ::= line feed (ASCII 10, '\n')
```

4.5 Request syntax

Requests to the Remote Manager consist of commands. Each line of the request comprises a single command. Commands are case-insensitive and consist of the letters A-Z, and underscore ('_').

Depending on the actual command, additional parameters may be supported. Command and parameter(s) are separated by (one or more) spaces.

Parameter names may contain any character except whitespaces and quotes.

4.6 Definition of command lines

```
<command-line>      ::= <command> | <command><parameter-list>
<command>           ::= <a-z_> | <a-z_><command>
<parameter-list>    ::= <separator><parameter> |
<separator><parameter><parameter-list>
<separator>         ::= <sp> | <sp><separator>
<parameter>         ::= <unquoted-string> | <quote><quoted-string><quote>
<unquoted-string>   ::= <unquoted-char> | <unquoted-char><unquoted-string>
<quoted-string>     ::= <quoted-char> | <quoted-char><quoted-string>
<a-z_>              ::= any of the 26 alphabetic characters, either upper or
lowercase, and underline
<unquoted_char>     ::= any character that is not SPACE (32), QUOTE (34)
<quoted_char>       ::= any character that is not QUOTE (34)
<quote>             ::= quote character (ASCII 34, '"')
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

4.7 Response syntax

Except for the authentication status of the client, the communication with the Remote Manager is stateless. As a consequence, the RM always responds sending a single data stream.

This data stream consists of at least a single status line. Other content may follow.

4.7.1 Status response

The status line consists at least of a 3-digit status code. This may be followed by a return value list, depending on the command submitted. A comment may be appended, too. The latter one must be ignored by the client; it is just provided for readability and may be subject to changes.

Depending on the command issued, there may, or may not follow text or binary content after the first status line. The last line of the response then contains another status line describing the overall status of the transaction.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

4.7.2 Definition of Status line

```
<status-line> ::= <status-code> | <status-code><separator><comment>
<status-line-with-values> ::= <status-code><parameter-list> |
                              <status-code><parameter-list>
                               <separator><comment>
<status-code> ::= <d><d><d>
<d> ::= any one of the ten digits 0 through 9
<comment> ::= <line-character> | <line-character><comment>
```

The first digit of the status code designates the so-called status class; the second digit refers to a subclass providing more detailed information about the status, or error, respectively.

4.7.3 Status classes

Code	Description
2xx	Command was successfully executed.
3xx	Command sequence is initiated, continue sending content.
4xx	Command temporarily cannot be executed. This may be due to limited memory, exceeding the number of allowed connections, or any other error that may be resolved later.
5xx	Command cannot be executed because of wrong parameters, insufficient privileges, or because the command is unknown.

Remark: Status class 4xx is hardly ever used.

4.7.4 Status subclasses

Code	Description
x0x	Syntax - Unknown command, invalid parameters.
x1x	Just displaying information, no effects on service.
x2x	Connection status has changed.
x3x	Transaction, Read/Write

4.8 Content

4.8.1 Text content

Some commands, like reading or writing the configuration, require the transfer of text content. As mentioned above, the text content is always preceded by a class 3xx status command.

Text is transferred as 8-bit characters without quoting. Therefore, the preservation of line breaks cannot be granted. The text must not contain null bytes.

The end of the text is indicated by a line containing nothing but a dot ('.'), which is similar to the SMTP protocol.

In the following, text content in the response definitions is represented by the token DOT_ENCODED_TEXTLINES.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

4.8.2 Variable lists

As a special case of text, a list of variables may be transferred. Each line consists of the variable name, followed by whitespaces and the content. This is represented by NAME_VALUE_PAIR_LIST.

4.8.3 Binary data

When retrieving binary data, the expected size of the data is provided by the 3xx status line. There are no dot and newline at the end of the data. The closing status line follows immediately. Binary data are represented by BINARY_DATA.

4.9 Authentication

There are different *modes* for connecting to the RM. There are three anonymous connection modes where the client needs not to identify itself by providing credentials. Depending on the client's IP address, one of the following modes is selected:

- Connecting from *localhost* (mode LOCAL).
- Connecting from a cluster member. Cluster members are defined in the GS configuration (mode CLUSTER).
- Connecting from any other address. Only a very small set of commands is available (ANON).

After having connected in one of the ways described above, the RM responds with status 220 and a comment indicating which one of the three modes is active.

```
220 IKARUS security.proxy Remote-Manager for localhost
220 IKARUS security.proxy Remote-Manager for cluster member
220 IKARUS security.proxy Remote-Manager
```

The client may now identify itself as

- Configuration center (CC)
- TMG/ISA server (TMG)

4.10Commands

In this documentation, *request data* sent by the client are preceded by ►.
Response data coming from the server start with ◄.

4.10.1 Commands for all modes

```
► QUIT
```

Close the connection. No response.

```
► SNMP [<host>]
```

Return data concerning the HTTP session, similar to the SNMP protocol.
If <host> is provided, the command will be redirected to the GS running on this host.

```
◄ 332 Transmitting values
◄ <NAME_VALUE_PAIR_LIST>
◄ .
◄ 230 Transfer complete
◄ 430 Transfer aborted
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

```
◄ 530 Error connecting to Remote-Manager
```

4.10.2 Commands for anonymous connection (ANON)

► GUIVERSION <major.minor.patch>

Switch to 'configuration center mode' providing the version number of the CC used.

```
◄ 231 <major.minor.patch> is compatible
◄ 531 <major.minor.patch> required
```

► LOGIN <username> <password>

Switch to authorized mode. ***Preconditions***: The command GUIVERSION or TMGVERSION must have been sent before.

◄ 230 Logged in
◄ 530 Not logged in, authentication failed
◄ 503 Bad sequence of commands, requires: GUIVERSION, TMGVERSION

► READ GUISETUP

Get the CC setup file provided by the GS. ***Preconditions***: The command GUIVERSION must have been sent before.

◄ 330 <filesize> <suggested_filename> Transmitting binary data
<BINARY_DATA>
(connection-reset on error)
◄ 230 Transfer complete

Error codes:

◄ 530 Setup not available

► STARTTLS

Activate TLS encryption for the current connection. This works the same way as for SMTP. For more details, please refer to RFC 3207.

◄ 220 Ready to start TLS

► (initialize client-side SSL)

4.10.3 Commands for connection from localhost (LOCAL)

► LICENSE <command>

Manage license. If no <command> is provided, RM responds

◄ 501 Syntax error in parameters or arguments

► LICENSE ADD

Add a new license and reload the license store. Return the current license status.

◄ 331 Receiving text, end with <CR><LF>.<CR><LF>

► <DOT_ENCODED_TEXTLINES>
► .

◄ 230 A valid license is installed

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

Error codes:

◄ 532 <ReturnValue_GetBestLicense> is current License-Status

► LICENSE CLEAN

Remove all licenses that have already expired.

◄ 230 Cleaned outdated licenses

► LICENSE DELETE <serial>

Remove the license with the serial key provided.

◄ 230 Specified license was removed

Error codes:

◄ 501 Syntax error in parameters or arguments
◄ 530 Specified license was not found or not removed

►LICENSE LIST [ACTIVE]

Provide a list of all installed licenses, or the active license only.

◄ 331 Transmitting text
◄ LICENSE_DATA
◄ .
◄ 230 Transfer complete

► PASSWD <command>

Manage passwords. If no <command> is provided, RM responds with status 501.

► PASSWD LIST

List all names that have a password assigned.

◄ 331 Transmitting text
◄ USERNAMES
◄ .
◄ 230 Transfer complete

► PASSWD SET <username> [<new password>]

Set the password for the given user. If password is omitted, the user password will be deleted.

◄ 230 Password changed
◄ 231 Password cleared

Error codes:

◄ 530 Error updating password-store
◄ 501 Syntax error in parameters or arguments

► SERVICE RELOAD <module name>

Inform the service about the update of a module.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

◄ 230 <module name> Reload initiated
◄ 530 <module name> is unknown

► SERVICE RELOAD LICENSESTORE

Reload license list.

◄ 230 LICENSESTORE Reload initiated

► SUPPORTZIP [PROXYLOG] [MAILLOG] [UPDATELOG]

Create a zip archive of the given log files and return it as binary content.

◄ 330 <filesize> Transmitting binary data
◄ BINARY_DATA (connection reset on error)
◄ Transfer complete

Error codes:

◄ 530 Support-ZIP not available
◄ 501 Syntax error in parameters or arguments

► TMGVERSION <major.minor.patch>

Switch to TMG mode for the administration plugin for ISA servers.

◄ 231 <major.minor.patch> is compatible
◄ 531 <major.minor.patch> required

► SERVICE RUNSTATE <timeout>

Request a shutdown of the server. If used within a 'cluster', the shutdown request is only accepted if the minimum number of host required stays up and running.

◄ 330 RUNSTATE shutdown in progress
◄ RUNSTATE shutdown
◄ RUNSTATE denied

4.10.4 Anonymous access for cluster members

► SERVICE RUNSTATE

Return the state of the cluster member

► WRITE CONFIG

Send the currently active configuration.

◄ 333 Receiving tree, end with <CR><LF>.<CR><LF>

► DOT_ENCODED_TEXTLINES
► .

◄ 231 Configuration fully active
◄ 232 Configuration not fully active, restart required

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

◄ 530 Configuration not applied
◄ 430 Error creating temporary file

4.10.5 Authorized access for configuration center

► LDAP <command>

Issue a LDAP command

Command definition

<command> ::= <ldap_url>
<ldap_url> ::= ldap://<ldap_host_parameter>/<ldap_query_string>
<ldap_host_parameter> ::= <ldap_binddn>:<ldap_bindpassword>@<ldap_host> |

<ldap_host>

<ldap_host> ::= <hostname_or_ip> | <hostname_or_ip>:<port>

► LDAP CHECKMAILBOX <ldap_url> <mailbox>

Ask the LDAP server whether a mailbox exists or not.

◄ 230 Operation completed successfully
◄530 <status> Error returned by CheckMailBox

Status codes

1 (LDAP_OPERATIONS_ERROR) General error

4285967295 (LDAP_MAILBOX_NOTFOUND1) Mailbox not found

4285967294 (LDAP_MAILBOX_NOTFOUND2) Mailbox not found

► LICENSE <command>

See above.

► NOOP

No operation. This one is used by the client to keep the connection from timing out.

◄ 231 <infostore-change-count> OK

► PASSWD <command>

See above.

►SERVICE MANUALUPDATE

Update the manual. This is not supported for all product variants. The update is processed by *spupdate.*

◄ 230 supudate initiated
◄ 231 spupdate already running

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

►SERVICE RESTART

Restart the service.

◄ 230 Service-restart initiated.

►STATS

Return the connections' states. Deliver information for each protocol about the number of active connections. For HTTP, the number of idle connections is shown, too.

Protocols supported

http, ftp, smtp_recv, smtp_send, smtp_t, pop3, nntp, imap

►SUPPORTZIP

See above.

►WRITE CONFIG

►WRITE TEMPLATE <name>

4.10.6 READ commands

For the procedure for READ commands is nearly always the same, it is summarized here.

1. The RM responds with a 33x status indicating the type of text to be returned

◄332 Transmitting values
◄333 Transmitting tree
◄334 Transmitting message-templates

For some reasons, the data may not be determined. In this case, the status 530 is returned plus a comment describing the error.

◄530 Error reading ...

2. This is followed by the content, finished by the dot-line.
3. At the end, normally the 230 status line is printed.

◄230 Transfer complete

Some commands support a <language> parameter. In this case, the text may be returned in the given language. If omitted, or the text is missing in the given language, English will be assumed as a default.

► READ CONFIG [DEFAULTS]

Return the current configuration and information whether it is active or not. 'Active' means that the latest changes of the configuration have already been reloaded by the server.

If DEFAULTS is provided, the default configuration will be returned instead.

```
◄ 230 Configuration is default
◄ 231 Configuration fully active
◄ 232 Configuration not fully active, restart required
◄ 530 Error opening configuration file.
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

► **READ CATEGORIES [<language>]**

Return the list of categories defined by the URL filter. <language> denotes the language for the category descriptions.

Response format: Values, NAME_VALUE_PAIR_LIST

► **READ CONTINENTS [<language>]**

Return a list of continents that can be detected by the URL filter.

Response format: Values, NAME_VALUE_PAIR_LIST

► **READ COUNTRIES [<language>]**

Return a list of countries that can be detected by the URL filter.

Response format: Values, NAME_VALUE_PAIR_LIST

► **READ ENV**

Return a list of some environment variables.

Response format: Values, NAME_VALUE_PAIR_LIST

► **READ INFOSTORE [path]**

Return the info store, containing information about viruses found, updates etc. The optional path selects the section in the info store configuration tree that should be returned, by default the whole info store is returned.

Response format: Tree, DOT_ENCODED_TEXTLINES

Errors:

```
◄ 530 Error reading infostore
```

► **READ LOG <logtype>**

Return the last 8K of the given log file. Possible log types are:

Log type	Description
global	Global Service-Log, splogfile.log
proxy	Log for HTTP and FTP protocol
mail	Log for mail protocols (POP3/IMAP4/SMTP)
update	Log of the 'spupdate' program
alerts	Log file for alerts. If multiple alerts are defined, the first log in the configuration file will be assumed.

Response format: Tree, DOT_ENCODED_TEXTLINES

Errors:

```
        530 Error opening logfile
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

► READ TEMPLATES

Return all message templates. Every template is finished by a dot-line.

Response format: Message templates, DOT_ENCODED_TEXTLINES

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

5

REST API (English only)

IKARUS gateway.security offers a RESTful API for managing the server. The base path is

```
https://<server>[:<port>]/api
```

The HTTPS port 443 is used by default. This can be changed in the configuration file.

The REST API is used internally by the IGS web interface.

5.1 API Overview

The API supports the following HTTP methods:

- **GET** for requesting data. Example: Read some configuration data. Get list of licenses.
- **PUT** for creating data. Examples: Create new user. Import configuration file.
- **POST** for updating data. Example: Set configuration data. For triggering commands. Example: Restart the server.
- **DELETE** for deleting data. Example: Remove a license from the server.

5.2 Content

The content is normally sent as JSON. In turn, the requests mostly return data (if any) as JSON. For requests using different data types the *Content-Type* is specified explicitly in this document.

5.3 Status codes and error handling

The API returns the following standard codes, as defined by Hypertext Transfer Protocol (HTTP) Status Code Registry):

Code	Description
200 Ok	The request was successfully processed. Further information may be found in the content.
401 Not authorized	Login required or user credentials are not sufficient for action.
404 Not found	The resource cannot be found. **Example:** A non-existing configuration item is referenced.
405 Method Not Allowed	The given method is not supported for the URL provided. **Example:** An attempt was made to delete a configuration section.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

501 Syntax error in parameters or arguments	Request could not be parsed correctly or the input data provided are malformed.

5.3.1 Custom codes

If a requests yields a domain-specific error, the status code **432** is returned. This covers errors like validation violations, unresolved references within the configuration, or missing mandatory field.
In this case, additional information must be present in the message body to give a human-readable feedback to the end user.

```
Content-Type: application/json
{
    "msg": "error_literal",
    "params" : [
          "max_retries", "1234"
    ]
}
```

msg	Literal for error message. The corresponding message text may contain placeholders {0}, {1}, etc., which is be replaced by the parameters in the `params` array.
params	Contains the parameter substitutions in the language identifier.

It is up to the API client to provide a localizable message text for each error literal.

```
msg.api.<error literal>
```

For example:

```
{
    "msg" : "ObjectIsReferenced",
    "params" : [
        "PermissionRule"
     ]
}
```

For domain-specific errors, the return code qualifier, and the parameters, are given in this documentation. As mentioned above, in this case the HTTP status is always considered 432.

5.4 Session handling and authentication

This section describes how login and logout of a user are handled.

The API client must support cookies.

5.4.1 Login

The API access requires authentication through user credentials (username and password). For authentication, the client must support cookies. The user identifies herself through the following POST request:

```
POST /api/login Content-Type: application/x-www-form-urlencoded
username=&password=
```

The credentials of the user are returned as response

```
200 OK
Content-Type: application/json
{
    "username" : "root"       #current user
    "rights" : "write_locked" # 'read', 'write' or 'write_locked'
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

```
    "write_locked": {          # only existing if 'rights' == 'write_locked'
          "user" : "root"       # locking user
          "host" : "127.0.0.1" # IP address which locking user logged in from
     }
}
```

5.4.2 Logout

The API access deletes the value in the browser cookie and removes the entry from the internal list, once the following POST request is sent:

```
POST /api/logout
```

5.5 Configuration

This section describes *how* to read, create, update, and delete configuration data. A comprehensive reference of the configuration items can be found in section 3.

Configuration data are always returned as JSON. They are grouped into several sections similar to the configuration file `securityproxy.conf`. These section are represented by JSON objects.

5.5.1 Get data

Examples: Read global configuration data.

Request

```
GET /api/config/global
```

Response

```
200 OK
Content-Type: application/json

{
 "quarantine_path" : "quarantine/" ,
 "global_log" : {
          "max_size": "10240K",
          "max_dirsize": "2G",
          "timespan": "week"
    }
    ...
}
```

If the item is not existing within the configuration, the status **404** is returned.

5.5.2 Create data

Example: Create a new user.

Request

```
PUT /api/config/remotemanager/users/new_user
Content-Type: application/json
{
 "allowip":[
          "0.0.0.0/0",
          "127.0.0.1/32"
],
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

```
 "passwd":"jhgdh",
 "rights":[
    "write",
    "read"
],
 "auth":"passwd"
}
```

Remark: Mandatory configuration fields must be provided through the request content.

Possible error codes

```
ReferenceNotResolved
ValidationFailed
MandatoryFieldMissing
```

5.5.3 Update data

Change existing data.

Request

```
POST /api/config/global
Content-Type: application/json

{
 "quarantine_path" : "new_quarantine/" ,
 "global_log" : {
          "max_size": "2048K",
          "max_dirsize": "7G",
          "timespan": "day"
    }
    ...
}
```

Possible error codes

```
ReferenceNotResolved
ValidationFailed
MandatoryFieldMissing
```

5.5.4 Delete data

Example: Delete an existing user.

Request

```
DELETE /api/config/remotemanager/users/user_to_be_deleted
```

Possible error codes

```
ObjectIsReferenced
```

5.6 Non-configuration data and commands

5.6.1 Import license file

Request

```
POST /api/info/ikkey
Content-Type: multipart/form-data
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

```
<license file content>
```

Possible error codes

```
LicenseNotInstalled
```

5.6.2 Delete license

Request

```
DELETE /api/info/ikkey/<serial-number>
```

Possible error codes

```
LicenseNotFound
```

5.6.3 Get license list

Retrieves the list of all stored licenses. `best` set to `yes` marks the currently active license, `usercount` and `features` are optional values. If they are not set, it means unlimited users or that all features are enabled.

Request

```
GET /api/info/ikkey
```

Response(s)

```
200 OK
Content-Type: application/json

{
    "0": {
         "desc": "License for internal use only",
         "owner": "IKARUS Security Software GmbH",
         "enddate": "2014-12-31",
         "serial": "xx996644pp09",
         "isvalid": "yes",
         "best": "yes",
         "usercount": "10",
         "features": "web mail"
    },
    ...
}
```

5.6.4 Get active/best license

Retrieves the license that is currently used by gateway.security. `usercount` and `features` are optional values. If they are not set, it means unlimited users or that all features are enabled. `usercount_used` is the number of `used` users and only shows up if `usercount` is set.

Request

```
GET /api/info/ikkey/active
```

Response(s)

```
200 OK
Content-Type: application/json

{
    "desc": "License for internal use only",
    "owner": "IKARUS Security Software GmbH",
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

```
    "enddate": "2014-12-31",
    "serial": "xx996644pp09",
    "isvalid": "yes",
    "usercount": "10",
    "usercount": "5",
    "features": "web mail"
}
```

5.6.5 Export configuration file

Request

```
GET /api/info/config
```

Response(s)

```
200 OK
Content-Type: text/plain

<configuration file content>
```

5.6.6 Import configuration file

Request

```
POST /api/info/config
Content-Type: multipart/form-data

<configuration file content>
```

Possible error codes

```
ReferenceNotResolved
ValidationFailed
MandatoryFieldMissing
```

5.6.7 Import default configuration file

Sets the session configuration to the default configuration.

Request

```
POST /api/info/config/default
```

5.6.8 Commit changes to configuration file

Commits the session configuration to the backend, flushes the configuration to the hard disk and reloads the configuration.

Request

```
POST /api/info/config/commit
```

Possible error codes

```
ConfigurationNotApplied
```

5.6.9 Get users list

Returns a list of all users that have a password assigned.

Request

```
GET /api/info/password
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Response(s)

```
200 OK
Content-Type: application/json

[ "root", "guest ]
```

5.6.10 Set user password

Request

```
POST /api/info/password
Content-Type: application/json

{
  "user" : "theUserName" ,
  "password" : "veryVerySecret"
}
```

Possible error codes

```
ErrorUpdatingPasswordStore
```

5.6.11 Read countries, continents, categories

Request

```
GET /api/info/countries
GET /api/info/continents
GET /api/info/categories
```

Response(s)

```
200 OK
Content-Type: application/json

<JSON arrays of the data requested>
```

5.6.12 Get support zip file

Request

```
GET /api/info/supportzip
```

Response(s)

```
200 OK
Content-Type: application/zip

<binary content>
```

Possible error codes

```
SupportZIPNotAvailable
```

5.6.13 Get Information about server status

Request

```
GET /api/info/server
```

Response(s)

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

```
200 OK
Content-Type: application/json

{
    "global": {
        "buildos" : "WIN64",
        "os" : "Windows 7 x64 Service Pack 1 (Build 7601)",
        "version" : "3.34.17",
        "hostname" : "securityproxy.ik.local",
        "laststartdate" : "Mon, 31 Mar 2014 18:51:19 +0200",
        "modulepath" : "C:\securityproxy\w64\bin\securityproxy_w64.exe"
    }
    "modules": {
    "securityproxy" : "3.34.17.0",
    "spupdate" : "1.1.3",
    ...
    },
    "update": {
          "lastcheck" : "Fri, 14 Mar 2014 09:00:26 +0100",
          "laststatus" : 0,
          "lastupdate" : "Fri, 14 Mar 2014 09:01:37 +0100}"
    }
}
```

5.6.14 Malware information

Retrieve information about detected malware incidents.

Request

```
GET /api/info/malware
```

Response(s)

```
200 OK
Content-Type: application/json

{
    "20140113_160601_0000" :
       {
       "date":  "Mon, 13 Jan 2014 16:06:01 +0100",
       "virusname":  "EICAR-ANTIVIRUS-TESTFILE",
       "virusid":  "462103-0",
       "filename":  "eicarcom.zip==>eicar.com",
       "destination":  "0.0.0.0:0"
    },

    ...

}
```

5.6.15 Get log files

Request

```
GET /api/info/log/global
GET /api/info/log/proxy
GET /api/info/log/mail
GET /api/info/log/update
GET /api/info/log/alerts
```

Response(s)

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien |
UID-Nr.: ATU15191405

```
200 OK
Content-Type: text/plain

<log file content>
```

Possible error codes

```
ErrorOpeningLogFile
```

5.6.16 Get report

Request

```
GET /api/info/report/<report-name>
```

Response

```
200 OK
Content-Type: text/html

<HTML report content>
```

Possible error codes

```
CouldNotCreateReport
```

5.6.17 Connection status

Get information about the currently open connections.

Request

```
GET /api/info/stats
```

Response

```
200 OK
Content-Type: application/json

{
    "http_active": "1",
    "http_idle": "14",
    "ftp": "0",
    "smtp_recv": "0",
    "smtp_send": "0",
    "tsmtp": "0",
    "pop3": "0",
    "imap": "0",
    "nntp": "0"
}
```

5.7 Commands

5.7.1 No operation

```
POST /api/command/server/noop
```

5.7.2 Restart the service.

```
POST /api/command/server/restart
```

5.7.3 Initiate reloading of licenses

```
POST /api/command/ikkey/reload
```


IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

5.7.4 Clean outdated licenses

```
POST /api/command/ikkey/cleanup
```

5.7.5 Check LDAP Authentication

Request

```
POST /api/command/ldap/checkauth
Content-Type: application/json

{
 "url" : "<ldap_url>" ,
 "user" : "theUser",
 "password": "theMostAndYetUnveiledSecretPassword"
}
```

Possible error codes

```
LdapBadUrl
```

The LDAP URL is malformed.

```
WrongInputType
```

One of the credentials parameters `user` or `password` may either be malformed (e.g. a number instead of a string), or missing.

```
LdapAuthenticationFailed
```

Authentication failed.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405