IKARUS
gateway.security

Version 3.36
Manual

IKARUS Security Software GmbH

Blechturmgasse 11

1050 Vienna

Austria

www.ikarussecurity.com

Contents

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

0
Preface

The **IKARUS gateway.security (IGS)** is a software running on a server to protect your network against several threats from external networks. It serves as a gatekeeper for different kinds of malware and spam mail and supports fine-tuned access control to your network.

IGS can work as a transparent proxy for the TCP protocols that are mostly used. Furthermore, for mail protection, it may also act as a Mail Transfer Agent (MTA).

Key Features include

- Malware detection for web and e-mail protocols
- Access control to the internal network
- Detailed access control to web resources from external networks
- Different ways of authentication including LDAP and NTLM/Kerberos
- Fully automated incremental update for all components
- Comprehensive logging of activities and security incidents
- Automated and manual reporting functionality
- RESTful API Interface for both configuring and controlling the server
- Web-based administration interface

This document is primarily intended for system administrators running and configuring an IGS server.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

1 Quick start guide

This section describes how to install the IGS software on a server and how it can be managed by the system administrator.

1.1 Preconditions

Make sure to meet the following requirements before starting the installation of IGS on a server:

- For the installation, you need administrative rights
- The system has at least 2 GB free disk space
- Other services should not listen to the TCP-Ports 443 and 15639[1]. These ports are used by GS and must not be blocked. Other ports might also be used depending on the actual configuration.
- Depending on the enabled services, the firewall must not block the TCP protocols HTTP, HTTPS, POP3, IMAP, NNTP, and SMTP from inside the system.
- The GS may be installed on the following systems:
  - Linux (RPM and DEB Packages) 64 bit
  - Microsoft Windows 32 and 64 bit

Commented [SH1]: More details

1.2 Setup

1.2.1 Installation on Microsoft Windows Systems

Installing IGS on a Microsoft Windows system is straightforward. Double-click the setup file for installation on the system and follow the instructions of the installer.

During installation, you are asked to import your license file for IGS. Alternatively, you can skip this step and activate the license later on.

1.2.2 Installation on Linux Systems

For the installation of IGS on a Linux system RPM and DEB packages are available. Each package comes as a 32-bit and 64-bit version.

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

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

The license can be imported after the installation from the command line

[1] If these ports are nevertheless needed for other services, GS can be configured to use different ports instead.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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

1.2.3 Setting up the service

1.2.3.1 Microsoft Windows

After the installation has completed, the list of services installed on the system includes the service called **securityproxy**. It can be managed like any other service using the Administrative Tools.

1.2.3.2 Linux

On a Linux system, the service is registered in the appropriate run levels. It is managed by means of a script:

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

1.3 File system structure

This image provides an overview of the IGS program folder after the installation.

```
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
```

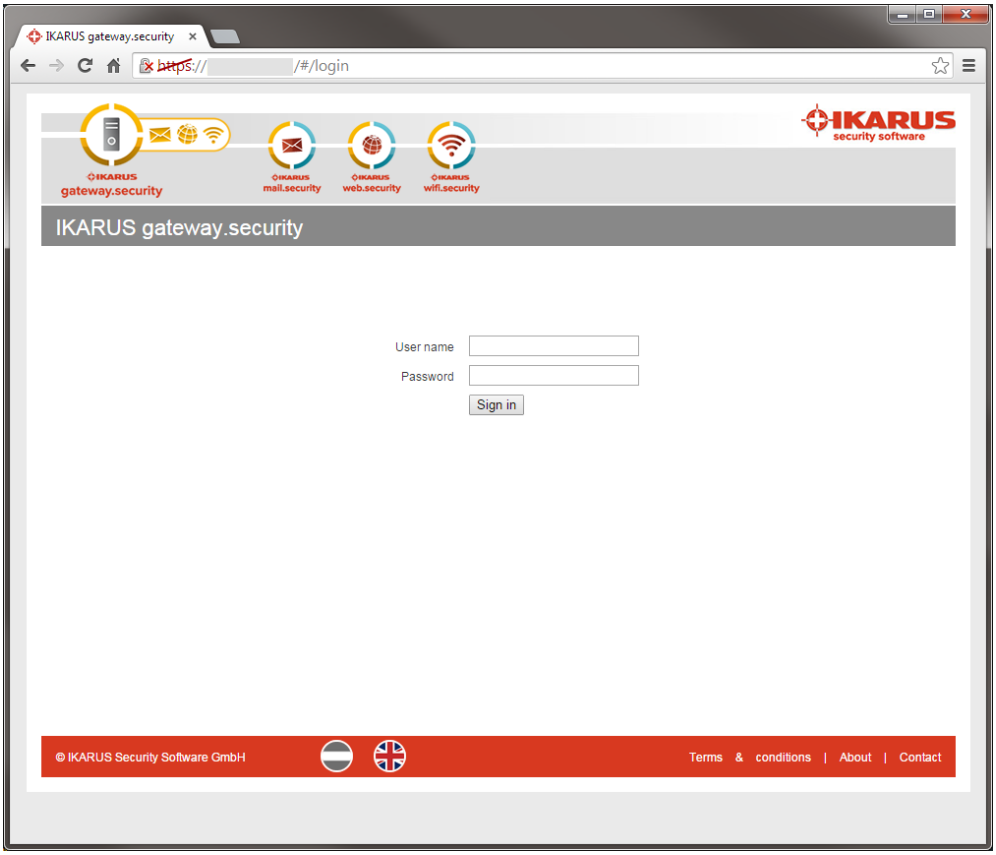
The main configuration file is named `securityproxy.conf` and can be found in the `conf` folder.

For a detailed description on the IGS configuration, see section 3.

1.4 User interface

IGS comes with a browser-based interface. By default, this interface can be accessed through HTTPS once the service is started.

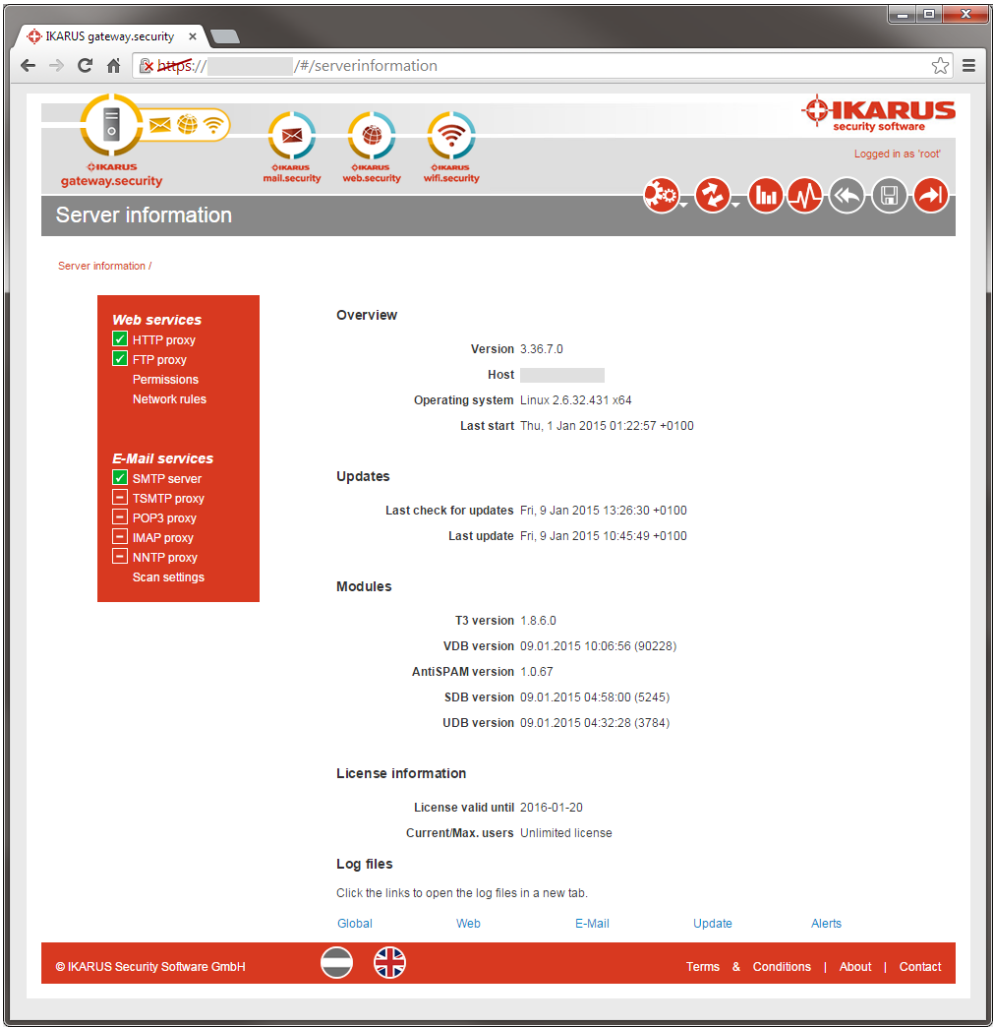
IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405



Because of IGS using a self-signed certificate by default, browsers normally point out that access to the site is considered unsafe. To avoid this warning, place an authorized certificate file `webapi.crt` and the corresponding private key file `webapi.key` in the folder `conf/cert`.

After logon, the user is shown an overview about the server's status.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405



In the upper right corner there is the main menu.

The buttons, from left to right, provide access to the following features:

1. Managing the IGS configuration (see section 3)

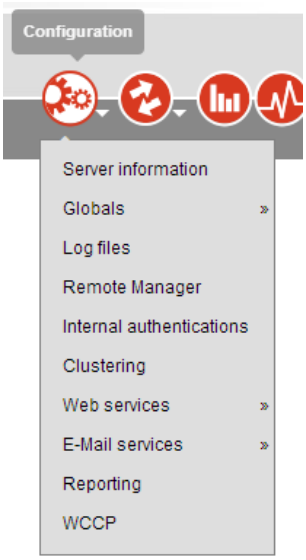
IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at | www.ikarussecurity.com | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT142011182122082100 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

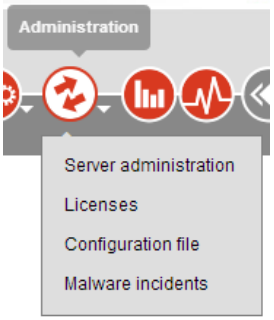
2. Managing licenses, log files, restarting the server, retrieving support info, and importing or exporting the configuration file.
3. Generating reports (see section 2.2.5)
4. Displaying the activity monitor
5. Undo changes
6. Save changes
7. Logout

On the left hand side, a quick link menu gives access to the configuration of the features that are most commonly used.

When clicking on the first two menu entries, sub-menus show up for further selection.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405





Next to most buttons and input fields, an icon can be found ( ) for displaying and hiding the documentation for the respective item.

Many section headings are preceded by an icon for collapsing and expanding the fields contained therein ( ).

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Clustering

Enable clustering

Cluster members *

Specify members of the cluster per IP address. The current instance must be included. The members must be able to reach each other on the specified addresses on TCP port 15639.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

2

Features

This section provides an overview about the features supported by IGS plus some additional background information, if necessary.

Most configuration settings are thoroughly described in section 3 or are self-explanatory, at least for system administrators. As a consequence, these feature are only mentioned briefly and the user is referred to the detailed configuration description.

2.1 How IGS works

IGS mostly works as a **security proxy** and offers security services for different kinds of TCP protocols. These proxy services can be grouped into

- 'Web services', handling HTTP and FTP connections (section 2.1.1) , and
- 'Mail services' for SMTP, IMAP, POP3, and NNTP protocols (section 2.1.2).

For mail protection, namely for SMTP traffic, the IGS can also be used as a **Mail Transfer Agent (MTA)** (section 2.1.2.2)

Depending on the server operating system, the proxy services can work in **transparent** or **non-transparent** mode. Linux operating systems support transparent proxy functionality by means of `iptables` configuration. As opposed to that, it is not possible to run a transparent proxy on Microsoft Windows Servers by default.

2.1.1 Web services

The IGS protection for web protocols is primarily defined by a set of **network rules**.

These rules define, roughly speaking, **from which network** connections are allowed or denied, and **who** is granted or denied to establish a connection (**access control**).

In addition to that, the so-called permission sets, which are referenced by the network rules, define the **restrictions imposed on the data** transferred through this connection.

2.1.1.1 Access control

When a client tries to establish a connection to the IGS, the network rules are processed by their order. Each rule has a network group, an IP address or subnet mask defined, which is checked against the client's IP address. Additionally, a rule can also contain a check for user authentication. IGS supports different kinds of user authentication.

The first rule matching the current connection source and user authentication, if applicable, is the rule which applies.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

If no network rule matches, access is denied.

If a rule yields **denied,** access is forbidden and no further checks are necessary.

2.1.1.2 Permission sets

The permission set selected by the network rules consists of a list of **permission rules**, each of which consists of several criteria and a result saying 'deny' or 'allow'.

Like the network rules, the permission rules are processed by priority, and the first matching rule applies.

If no permission rule matches, access to the resource is granted.

2.1.1.3 Selecting permission sets

Depending on the **authentication type** (see 3.3.3.12) of a network rule, placeholders might be used for selecting permission sets by means of so-called **permission set masks**.

These placeholders are replaced by current connection parameters to determine the permission set to apply. This allows for defining permissions sets based on user names or user groups.

For example, there may be a permission set `permission_user1` and a network rule having the value `permission_%u` for the permission rule. The former one applies only if the current user name is `user1`.

This works the same way for groups, if supported by the current authentication type. Internal authentication supports `%u` (user name). LDAP authentication and NTLM/Kerberos additionally support `%g`, which is replaced by the group name when evaluating the network rule.

The latter ones (LDAP or NTLM, respectively) also support the usage of SIDs (see 3.3.1.9). If configured accordingly, the SID of the user, or group, will be taken instead of the respective name for expanding the permission set name.

2.1.1.4 Blocking access

If access to a resource is granted, its content is scanned for malicious software using the **IKARUS scan.engine**.

If access is denied, the user is shown a page containing information about the reason for blocking. As mentioned above, this may happen due to

- Unauthorized access
- Access to content that is denied according to the permission rules
- The requested content proved to be malicious

These pages are called **block response pages** are highly configurable. For details see section 3.1

2.1.1.5 HTTPS and encrypted content

It is obvious that scanning encrypted content is not possible by default. This may be especially important when considering HTTPS connections.

There are third-party products available to overcome this kind of issues. If this is of interest for you, please contact IKARUS for further information.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

2.1.2 Mail services

IGS can be used either as a proxy for the protocols **SMTP**, **POP3**, **IMAP**, and **NNTP,** or as an **MTA**.

2.1.2.1 Scan rules

For checking e-mail for malicious content or SPAM, several **scan rules** can be defined.

These rules define

- what to do with malicious content detected by the IKARUS scan.engine,
- which kinds of attachments are suspicious,
- how to identify SPAM in addition to the built-in SPAM rating.

Scan rules can be assigned to each protocol service separately and define how to handle the e-mail or attachment in question.

2.1.2.2 Configuration of the proxy services

The configuration of the proxy services is the same for all four protocols POP3, IMAP, NNTP, and (transparent) SMTP.

Client configuration of POP3 and IMAP services

In case of a running a non-transparent proxy, the mail clients have to be configured using the IGS server as (POP3 or IMAP) mail server, instead of the mail provider's actual mail server.

For passing the target mail server to the proxy and thus being able to use multiple target mail servers, the mail user name can have the name of the target server added using '#' as separator.

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

This tells the IGS server to forward the mail as user `<mail-username>` to the mail server `<mail-server--name>`. The port is optional.

2.1.2.3 IGS as Mail Transfer Agent (MTA)

To detect and prevent possible threats caused by **incoming e-mail**, IGS must be used as one MTA hop before the internal mail server or as a Mail Exchange (MX) gateway. This requires changing the MX entry of the domain to point at the IGS server.

All mail traffic must be routed through IGS servers to ensure full protection.

For cleansing of **outgoing e-mail**, IGS can also act as a **relay server**.

Mail routing

The mail routes define how to forward incoming or outgoing mail and which scan rules apply. This is done based on several criteria like the sender's source IP address or subnet, or destination mailboxes.

SPAM filtering

In addition to the SPAM protection defined through the scan rules, IGS in MTA mode also supports the following methods

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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

Sender Policy Framework

SPF uses the TXT record for the domain of the sending e-mail address. This TXT record is returned by the name server and contains a list of IP addresses or subnets that are allowed to send e-mails for this domain. If the sender IP address is not in the list of the given domain, the e-mail is rejected. For domains without such a TXT record, the default behavior of accepting e-mails is used.

Greylisting

The term greylisting denotes a method for detecting mail transfer agents who are delivering SPAM mail. Mail traffic is only forwarded, if the MTA passes the greylisting check.

If an MTA can be regarded as trustworthy, it can optionally be added to a **temporary whitelist**.

Besides that there also exists a **permanent whitelist**. Traffic from MTAs listed therein is forwarded without any greylisting check.

Early Talker Rejection

According to the RFC for SMTP[4], a sender should wait for the greeting message before sending any commands. Well-behaving mail clients and servers usually wait, whereas spam bots not always do. By using this feature, IGS waits a user-defined period before sending the greeting banner. Any attempt of sending SMTP commands or data before the banner results in a rejected mail.

2.2 Common features

2.2.1 Logging

IGS writes log files of different types. For each of them, the user may define size and location.

- Global log: Stores information about the server, including status, critical errors and many more.
- Web log: Keeps information about HTTP and FTP connections.
- Mail log: Contains information for SMTP, IMAP, POP3, and NNTP protocols.
- Alert log: Holds information about IGS events such as malware incidents or updated modules.
- Debug log: Diagnostic information. Debug logging is disabled by default and must be activated if needed.

Debug logging may result in huge amounts of data to be stored on the disk.

A log file of the **update history** is always created. Its properties cannot be configured.

[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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

2.2.2 Update

IGS has an automated update support for

- the program executable
- the updater executable
- plugin libraries
- the virus database (VDB)
- the SPAM database (SDB)
- the URL filter database (UDB)

The program checks for updates of these components every 10 minutes. In case there are any updates available, they are downloaded and installed. The service is restarted automatically if needed.

2.2.3 User management

For authenticating access to IGS, pairs of usernames and passwords can be defined. They can be thought of as some sort of users, although there is no real user management associated with.

In this sense, two kinds of 'users' can be defined:

- Remote Manager Users, which are needed to authenticate for the management interfaces.
- Internal Users, which are only used for defining authentication for the network rules. Remote Manager Users can be used the same way like Internal Users, but not vice versa.

When IGS is freshly installed, the default user ROOT has the password "root". Change the password immediately after the installation!

2.2.4 Alerts

Alerting is a means for informing the administrator about infrequent or exceptional events like updates of the databases, or the detection of malware incidents.

2.2.5 Reporting

If this feature is enabled, connection data is stored in a database. Based on these data, diagrams and tables can be defined to gain overview about, for example, which kind of traffic has been blocked within a certain time range, or which are the top target domains addressed.

2.2.6 WCCP

IGS supports the WCCP[5] protocol.

2.2.7 IGS clustering

IGS supports the synchronization of configuration files among different servers. This feature is referred to as **clustering**.

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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

2.2.8 Management interfaces

2.2.8.1 Remote Manager

The Remote Manager is an interface of the IGS using TCP connections, by default running on port 15639. It is used for communication with the following clients:

- Administration plug-in for ISA/TMG server
- Other instances of IGS running on different servers, e.g. for synchronization of proxies within a cluster.
- Configuration Center (Window Desktop-Client), which is now substituted by the browser interface.

2.2.8.2 REST API

Besides the Remote Manager, IGS also provides access through a REST API (see section 5), which is used by the browser-based interface that comes with IGS.

The API provides a convenient way to integrate the IGS management into any other environment.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

3 Configuration

3.1 Block response pages

IGS displays different web pages for user authentication, information about blocked access, license errors, and much more. The respective HTML templates can be found in `image/messages`. Additional resources like style sheets, images, or scripts, reside on `image/htdocs`.

As a consequence, requests to the URL `http://proxy.ikarus.at/htdocs/` are redirected to `images/htdocs`. Access to the folder must be ensured by proper web server configuration.

After installation, the following default template files can be found in `image/messages`:

Filename	Description
`404.html`	„file not found“, is shown when accessing a resource in the `htdocs` directory that is missing
`destcontinent.html`	request was blocked due to server being in a blacklisted continent
`destcountry.html`	request was blocked due to server being in a blacklisted country
`fileblocked.html`	file was blocked because of a blacklisted filename or content type
`ftp.html`	not actually a block page, it’s the template for displaying a webpage for an FTP directory when using FTP over HTTP
`generic.html`	a generic block page, for example when no network rule was defined for this user
`infected.html`	a malicious file was blocked
`license.html`	request was blocked due to the proxy license being invalid or expired
`lockpage.html`	a landing page that is shown as long as the user has not accepted the terms of use
`networkerror.html`	destination server could not be reached
`nouser.html`	no valid permission set for this user (i.e. failed authentication)
`transferlimit.html`	user has already exceeded the transfer limit
`urlblocked.html`	request was blocked due to a blacklisted URL

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

urlcategory.html	request was blocked due to the URL being in a blacklisted category

3.1.1 Configuring block response pages

Since the files in the image folder of the proxy installation are default files, they should not be edited.

Instead, templates and files to override the default appearance can be created in conf/messages and conf/htdocs folder. Each file in the two folders overrides the corresponding file in the image folder and its sub-folders.

If a template is needed, it is first looked up in conf/messages. If it is not found there, the default version in image/messages is used instead.

3.1.1.1 Template parameters

The HTML files can contain keywords that are replaced before returning the response. These so-called 'template parameters' are enclosed in percent signs (%). As a consequence, this character must not be used in the HTML templates, or must be replaced by the numbered entity % .

Template parameter	Description
catnames	Comma-separated list of UDB categories matching the request
countryname	Country of the requested URL
continentname	Continent of the requested URL
proto	Protocol used
permission	Name of the permission set matching the request
client_ip	Client IP address
target_host	Target host name
target_port	Target port
target_path	Resource path
vdbsigname	VDB signature causing the blocking
errmsg	HTTP response headers

The link to http://proxy.ikarus.at/welcomeack is used by lockpage.html to tell the server that the user accepted the terms of use. Neither remove nor change this link.

For the templates are full HTTP responses, one must not alter the first three lines, including the newline.

3.1.2 Brandings

By means of brandings, it is possible to define several sets of web pages that apply to different networks.

The HTML templates for the different brandings are placed in subfolders of conf named after the respective brandings.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

```
conf/
    messages/
      subsidiary1/
        lockpage.html
      subsidiary2/
       lockpage.html
...
```

When assigning a branding to a network rule, the corresponding files are searched for in the branding's subfolders. As with the unbranded templates, the `image` folder is searched for a template if it is not supplied for the chosen branding.

In the same way, subfolders of `conf/htdocs` can be used for other resources needed for the different brandings. It is recommended to use the `<base>` HTML element to easily access the resources without having to adapt too many template file.

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

3.2 Configuration basics

All configuration settings that can be changed by the user (except for the HTML templates) are stored in the Apache[6]-style configuration file `conf/securityproxy.conf`[7].

This file consists of key-value-pairs (configuration items), which are grouped together in sections similar to XML. As a consequence, a *path expression* can be given to address each item in the file, which is used to link it to the documentation below.

There are several ways to modify the configuration

1. Editing the file manually. This requires file system access.
2. Through the IGS web interface.
3. Through the REST API (see section 5.) This API is used by the web interface to read and write the configuration. In addition to this, the API provides all features necessary to manage the IGS.

3.3 Configuration data

This is a full description of all configuration items of IGS. Every item can be located within the configuration file by means of the given path expression.
Mandatory items are marked with an asterisk (∗);

Additionally, for each section, there is also the corresponding REST API path given. Path elements within angular brackets ('<>') correspond to named objects.
They can be created and given distinct names by the user, like, for example, a permission set.

Following below, a list of the data types and enumerations used can be found.

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

[7] For the application's file system structure, see section 1.3

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

3.3.1 Configuration items

3.3.1.1 Configuration data

API path: `/config`

Configuration file location: /

Configuration data for IKARUS gateway.security

3.3.1.2 Web services

API path: `/config/access`

Configuration file location: `/ACCESS`

Settings for web services, which handle HTTP and FTP connections

Attribute	Name	Description	Type
`browser_lists`	Browser list	Named list(s) of web browsers	`Array(String)`
`contenttype_lists`	Content type list	List of content types	`Array(ContentType)`
`file_lists`	File list	List of named lists of file name masks. File lists can be used as permission rule criterion	`Array(File)`
`url_lists`	URL list	Named lists of URLs	`Array(URL)`

3.3.1.3 Landing page

API path: `/config/access/lockpage`

Configuration file location: `/ACCESS/LOCKPAGE`

Settings for landing pages

Attribute	Name	Description	Type
`session_timeout`	Session Timeout	Duration of landing page session	`Integer`

3.3.1.4 Data collector

API path: `/config/access/lockpage/datacollector`

Configuration file location: `/ACCESS/LOCKPAGE/DATACOLLECTOR`

Settings for landing pages that support data collector forms

Attribute	Name	Description	Type
`confirm_timeout`	Confirm Timeout	Time for user to click confirmation link [sec]	`Integer`
`confirm_tries`	Confirm Tries	Maximum tries for the user to fill out the form within the session if the user did not confirm	`Integer`

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

3.3.1.5 Form

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

Configuration file location: `/ACCESS/LOCKPAGE/DATACOLLECTOR/FORMS/<data_collector_form_name>`

Input form for the data collector. Each form has a unique name

Attribute	Name	Description	Type
`label_email`	Label Mail	The text to appear as label for the email	`String`
`mail_subject`	Mail Subject	Subject for the email containing the confirmation link	`String`

3.3.1.6 Additional form field

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

Configuration file location: `/ACCESS/LOCKPAGE/DATACOLLECTOR/FORMS/<data_collector_form_name>/FIELDS/<data_collector_form_field_name>`

Additional input fields for data collector form. The field "email" is always generated automatically and cannot be added

Attribute	Name	Description	Type
`key`	Key	Unique name for the input field	`DatacollectorFormFieldKey`
`label`	Label	Text to appear next to the input field	`String`
`mandatory`	Mandatory	Indicates whether data for this input field are mandatory	`Flag`

3.3.1.7 Network rules

API path: `/config/access/networks`

Configuration file location: `/ACCESS/NETWORKS`

Network rules used for access control settings

Attribute	Name	Description	Type
`groups`	Networks	Network groups. Used to group several networks together for applying access control setting for all at once	`Array(IpAddress)`

3.3.1.8 Priority list

API path: `/config/access/networks/group_priority/<group_priority_name>`

Configuration file location: `/ACCESS/NETWORKS/GROUP_PRIORITY/<group_priority_name>`

Group priority list to be applied for the network rule

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Attribute	Name	Description	Type
name	SID/LDAP group	Unique name of the Priority list	String

3.3.1.9 Network rules

API path: /config/access/networks/rules/<network_rule_name>

Configuration file location: /ACCESS/NETWORKS/<network_rule_name>

This is a list of rules that return whether access is allowed or denied based on several criteria

Attribute	Name	Description	Type
auth_result	Permission-Set per mask	Mask for selecting a permission set	PermissionSetMask
auth_type	Authentication method	The authentication type to be used for the selected network/IP address	NetworkAuthenticationType
branding	Branding	Defines the branding used for the selected network	Branding
form	Form	Form to be used for authentication	
group_priority	Priority list	Priority list to apply to the network rule. Only needed for authentication through LDAP or NTLM/Kerberos	
network_group	Network group	Network group for which the rule applies	
network_rule_type	Type	Indicates whether the rule applies for a subnet, or a network group	
permission_set	Permission set	Permission set to be applied	
redirecturl	Redirect to	URL to redirect the end user after having authenticated	String
result	Allow/Deny	Specifies whether access is allowed or denied as a result of this rule	Enum(RuleResult)
router	Router	IP address of GRE router	IpAddress
subnet	Subnet	IP subnet for which the rule applies	Subnet

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

use_sid	Use SID instead of name	Use the SID of users or groups instead of names	Flag

3.3.1.10Permissions

API path: /config/access/permissions

Configuration file location: /ACCESS/PERMISSIONS

Permission settings

3.3.1.11Permission set

API path: /config/access/permissions/permission_sets/<permission_set_name>

Configuration file location: /ACCESS/PERMISSIONS/<permission_set_name>

A permission set consists of rules to match a requested web resource. If the rules match, the permission set yields the result whether the resource may be accessed or blocked

Attribute	Name	Description	Type
encryptedfilebad	Treat encrypted files as malware	Tells whether an encrypted file should be treated as malware by default	Enum(FlagInherited)
extends	Based on permission set	Other permission set where this permission can inherit settings from	
mz_filebad	Treat executable files as malware	Tells whether an executable file should be treated as malware by default	Enum(FlagInherited)
transferlimit	Transfer limit	Limit amount of data [MB] allowed to get transferred by client. Only works in combination with a lock page	DataSizeWithUnit

3.3.1.12Permission rules

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

Configuration file location: /ACCESS/PERMISSIONS/<permission_set_name>/URLS/<permission_rule_name>

Ordered list of rules consisting of multiple selection criteria. The entries of the list are processed in the given order i.e. the selection criteria are checked against the current connection. The first rule that matches applies, and access to the requested network resource is either allowed or denied, based on the selected rule

Attribute	Name	Description	Type
alternating_id	Criterion type	Various selection criteria according to which properties the individual rules should be filtered	
browser_list	Browser list	Use a browser list as selection criterion	

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

contenttypelist	Content type list	Use a content type list as selection criterion	
continent	Continent code	Select by continent	
country	Country code	Select by country	
days	Weekdays	Define days on which this selection applies	Enum(DaysOfWeek)
file	File/Extension	Select by file name	FileExtension
filelist	File list	Use a file list for selecting	
result	Allow	The result used if this selection matches	Enum(RuleResult)
time	Period of time	Defines the time range at which the selection applies (format 'hh:mm-hh:mm')	Timespan
time_control	Time control	Defines whether the given time value is a weekday, or a time intervall	
url	URL	Select for a given URL	URL
urlfiltercat	URL filter category	Select for an URL filter category	
urllist	URL list	Use an URL list for selecting	

3.3.1.13Auto update

API path: /config/autoupdate

Configuration file location: /AUTOUPDATE

Settings for automatic updates. If activated, gateway.security checks for available program or database updates every 10 minutes

Attribute	Name	Description	Type
enableautoupdate	Activate automatic update	Enable/disable automatic updates	Flag

3.3.1.14Clustering

API path: /config/cluster

Configuration file location: /CLUSTER

Several server can be combined to a cluster for synchonization of their configuration files. You need at least two instances of gateway.security to form a cluster

Attribute	Name	Description	Type
enable	Enable clustering	Enable/disable cluster support	Flag

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

members	Cluster members	Specify members of the cluster per IP address. The current instance must be included. The members must be able to reach each other on the specified addresses on TCP port 15639	Array(IpOrHostname)

3.3.1.15Globals

API path: /config/global

Configuration file location: /

Global settings

3.3.1.16Alerts

API path: /config/global/alerts

Configuration file location: /

To inform the administrator about certain events, messages can be created. This may be log entries or an automatically generated e-mail

3.3.1.17Alert

API path: /config/global/alerts/alerts/<alert_name>

Configuration file location: /ALERTS/<alert_name>

To inform the administrator about certain events, messages can be created. This may be log entries or an automatically generated e-mail

Attribute	Name	Description	Type
email	E-Mail address	Recipient of the e-mail alert	EmailAddress
event	Events	A comma-separated list of events that trigger the alert	Enum(AlertEventFlags)
path	Log file	Relative path of the alert log file	Path
type	Notification type	Defines the type of alert (log entry or e-mail)	

3.3.1.18LDAP

API path: /config/global/ldap

Configuration file location: /ACCESS/NETWORKS/LDAP

Settings for user authentication through LDAP

Attribute	Name	Description	Type
authldapbinddn	DN for user	Specifies the DN name to be used for authentication	String
authldapbindpassword	Password	The password for LDAP authentication	Password

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

authldapurl	LDAP URL	The LDAP URL as defined by RFC 2255	String

3.3.1.19Automated e-mails

API path: /config/global/messenger

Configuration file location: /MESSENGER

If gateway.security has to send e-mails (e.g. for alerting), this section contains settings for mail delivery

Attribute	Name	Description	Type
smtpserver	Mail server	Mail server to be used	String
systemadmin	Sender address	Sender address used for automatic e-mails	EmailAddress

3.3.1.20Paths

API path: /config/global/paths

Configuration file location: /

Global settings for gateway.security

Attribute	Name	Description	Type
quarantinepath	Quarantine path	Folder to store malicious mail attachments or SPAM mail	Path
storepath	DB files path	Folder for storing database files	Path
tmppath	Temporary folder	Temporary files folder	Path

3.3.1.21Next proxy

API path: /config/internet

Configuration file location: /INTERNET/PROXY

Settings for using a proxy server for gateway.security

Attribute	Name	Description	Type
auth_pass	Password	Password for proxy server	Password
auth_user	User name	User name for proxy server	String
excludedomains	Excluded domains	List of domains for which no proxy is used	Array(String)
ftp_host	FTP Server	Proxy server to be used for FTP traffic	String
ftp_port	FTP Port	Proxy server port for FTP traffic	Port
http_host	HTTP Server	Proxy server to be used for HTTP traffic	String
http_port	HTTP Port	Proxy server port for HTTP traffic	Port
https_host	HTTPS Server	Proxy server to be used for HTTPS traffic	String

https_port	HTTPS Port	Proxy server port for HTTPS traffic	Port

3.3.1.22Log files

API path: /config/logging

Configuration file location: /LOG

Settings for log files

3.3.1.23Debug

API path: /config/logging/log_debug

Configuration file location: /LOG/LOG_DEBUG

Settings for debug logging

Attribute	Name	Description	Type
enable	Enable debug logging	Enables/disables debug logging. Only enable this option temporarily if you want to trace execution in highest detail to solve problems. Program execution can be slowed down considerably	Flag
maxdirsize	Maximum size (all)	Maximum size of all debug log files in the directory.Use the postfix 'K', 'M', or 'G' (without blank) as unit	DataSizeWithUnit
maxsize	Maximum size	Maximum size of debug log file. Use the postfix 'K', 'M', or 'G' (without blank) as unit	DataSizeWithUnit
path	Log files folder	Location for debug log files. The path is taken relative to the program folder	Path

3.3.1.24Global

API path: /config/logging/log_global

Configuration file location: /LOG/LOG_GLOBAL

Settings for gateway.security log file

Attribute	Name	Description	Type
maxdirsize	Maximum size (all)	Maximum size of all global log files in the directory.Use the postfix 'K', 'M', or 'G' (without blank) as unit	DataSizeWithUnit
maxsize	Maximum size	Maximum size of global log file. Use the postfix 'K', 'M', or 'G' (without blank) as unit	DataSizeWithUnit
path	Log files folder	Location for global log files. The path is taken relative to the program folder	Path
timespan	Split interval	Interval for creating a new log file	Enum(LogInterval)

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

3.3.1.25E-Mail

API path: `/config/logging/log_mail`

Configuration file location: `/LOG/LOG_MAIL`

Log file settings for mail services

Attribute	Name	Description	Type
`maxdirsize`	Maximum size (all)	Maximum size of all mail log files in the directory.Use the postfix 'K', 'M', or 'G' (without blank) as unit	`DataSizeWithUnit`
`maxsize`	Maximum size	Maximum size of mail log file. Use the postfix 'K', 'M', or 'G' (without blank) as unit	`DataSizeWithUnit`
`path`	Log files folder	Location for mail log files. The path is taken relative to the program folder	`Path`
`timespan`	Split interval	Interval for creating a new log file	`Enum(LogInterval)`

3.3.1.26Web

API path: `/config/logging/log_proxy`

Configuration file location: `/LOG/LOG_PROXY`

Log file settings for web services

Attribute	Name	Description	Type
`maxdirsize`	Maximum size (all)	Maximum size of all proxy log files in the directory.Use the postfix 'K', 'M', or 'G' (without blank) as unit	`DataSizeWithUnit`
`maxsize`	Maximum size	Maximum size of proxy log file. Use the postfix 'K', 'M', or 'G' (without blank) as unit	`DataSizeWithUnit`
`path`	Log files folder	Location for http log files. The path is taken relative to the program folder	`Path`
`timespan`	Split interval	Interval for creating a new log file	`Enum(LogInterval)`

3.3.1.27Remote Manager

API path: `/config/remotemanager`

Configuration file location: `/REMOTEMANAGER`

Settings for the IKARUS gateway.security Remote Manager

Attribute	Name	Description	Type
`allowip`	IP address/network	Host/networks allowed to connect to the Remote Manager	`Array(Subnet)`

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

auth_mode	Authentication mode	Specifies if the Remote Manager user authenticates by Remote Manager credentials, or LDAP	Enum(RemoteManagerAuthMode)
ip	Listen-on-address	Bind address for the Remote Manager. If not specified, binds to all IP addresses	IpAddress
port	Remote manager port	Port used by the Remote Manager	Port

3.3.1.28User

API path: /config/remotemanager/users/<remote_manager_user_name>

Configuration file location: /REMOTEMANAGER/<remote_manager_user_name>

Settings for Remote Manager users

Attribute	Name	Description	Type
allowip	Allowed IPs	Host/Networks from which the Remote Manager can be connected	Array(Subnet)
rights	User permissions	Specifies whether the user has the permission to modify the configuration, or only is granted read-only access	

3.3.1.29Web API server

API path: /config/remotemanager/webapiserver

Configuration file location: /WEBAPI_SERVER

Settings for the REST Interface and the Web GUI

Attribute	Name	Description	Type
listen	Listener	Listener for the REST API and the Web Interface. By default, Port 443 is used	Array(IpWithPort)

3.3.1.30Reporting

API path: /config/reports

Configuration file location: /REPORTS

Settings for reporting features. If reporting is not enabled, no information is logged. As a consequence, no data is available from the time on when the reporting was disabled

Attribute	Name	Description	Type
enable	Enable reporting	Enables/disables reporting	Flag

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

maxsize	Maximum size	Sets the database size on the disk. Use the postfix 'K', 'M', or 'G' (without blank) as unit. Whenever this amount is exceeded, the oldest 5 percent of data gets deleted. "Oldest" here refers to the insertion date rather than the recording date. Therefore, imported data might be the last one to be deleted, and gaps may occur in the timeline	DataSizeWithUnit

3.3.1.31Auto report

API path: /config/reports/autoreporting/<autoreporting_name>

Configuration file location: /AUTOREPORTING/<autoreporting_name>

Automatic report generation

Attribute	Name	Description	Type
days_month	Days of month	Report is sent on the given list of days of month. Days of month start with 1	Array(DaysOfMonth)
days_week	Days of week	Report is sent on the given list of weekdays. Days of week start with 1	Enum(DaysOfWeek)
email	E-Mail	List of e-mail addresses that receive the automated report	Array(EmailAddress)
http_reports	HTTP Reports	List of HTTP reports to be automatically generated	Array(HttpReport)
period	Period	Report is sent on selected days every month or week (month, week)	
smtp_reports	SMTP reports	List of SMTP reports to be automatically generated	Array(SmtpReport)
time	Time	Time to send the report on the selected days (format 24h-based HH:MM)	Time

3.3.1.32HTTP report

API path: /config/reports/http_reports/<http_report_name>

Configuration file location: /REPORTS/<http_report_name>

List containing all HTTP reports

Attribute	Name	Description	Type
chart	Chart type	Chart type or table	
height	Height	Height of diagram	Integer
httpreportfilter	Filter	Set of criteria to determine which data, and how they should be reported. Filter groups	

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

		allow for narrowing selected data for analysis. The total of all flags within a filter group is always 100 %	
shape_bar	Bar	Style of bar chart	Enum(ReportShapeBar)
shape_pie	Pie	Style of pie chart	Enum(ReportShapePie)
text_bottom	Lower label	Explanatory text to be displayed below the report	String
text_top	Upper label	Explanatory text to be displayed above the report	String
title	Report title	Report title	String
width	Width	Width of diagram	Integer

3.3.1.33SMTP report

API path: /config/reports/smtp_reports/<smtp_report_name>

Configuration file location: /REPORTS/<smtp_report_name>

List containing all SMTP reports

Attribute	Name	Description	Type
chart	Chart type	Chart type or table	
height	Height	Height of diagram	Integer
shape_bar	Bar	Style of bar chart	Enum(ReportShapeBar)
shape_pie	Pie	Style of pie chart	Enum(ReportShapePie)
smtpreportfilter	Filter	Set of criteria to determine which data, and how they should be reported	
text_bottom	Text at bottom	Explanatory text to be displayed below the report	String
text_top	Text at top	Explanatory text to be displayed above the report	String
title	Report title	Report title	String
width	Width	Width of diagram	Integer

3.3.1.34E-Mail services

API path: /config/services

Configuration file location: /

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

IKARUS gateway.security offers services for different kinds of TCP protocols. They can be grouped into 'Web services', handling HTTP(S) and FTP requests, and 'Mail services' which handle SMTP, IMAP, POP3, and NNTP protocols

3.3.1.35FTP proxy

API path: `/config/services/ftpproxy`

Configuration file location: `/FTP_PROXY`

The FTP service

Attribute	Name	Description	Type
`anonymous_password`	Anonymous password	Password used for anonymous FTP connections	`Password`
`enable`	Enable	Enable/disable the FTP proxy service	`Flag`
`listen`	Listener	The port, and optional local IP, where the FTP proxy service listens for client requests	`Array(IpWithPort)`
`use_outgoing_passive`	Use outgoing passive	If your firewall blocks active FTP connections (which requires the server to open a connection to the proxy), then turn on this option to use passive mode	`Flag`

3.3.1.36HTTP proxy

API path: `/config/services/httpproxy`

Configuration file location: `/HTTP_PROXY`

The HTTP service

Attribute	Name	Description	Type
`enable`	Enable	Enable/disable the HTTP proxy service	`Flag`
`listen`	Listener	The port, and optional local IP, where the HTTP proxy service listens for client requests	`Array(IpWithPort)`

3.3.1.37IMAP proxy

API path: `/config/services/imapproxy`

Configuration file location: `/IMAP_PROXY`

The IMAP service

Attribute	Name	Description	Type
`enable`	Enable	Enable/disable the IMAP proxy service	`Flag`

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

imap_server	Default target server	Default IMAP server. Is used if when the user name does not include information about the target IMAP server	IpOrHostname
imap_server_port	Default target server port	Port for default IMAP server	Port
listen	Listener	The port, and optional local IP, where the IMAP proxy service listens for client requests	Array(IpWithPort)
scanner_rule	Scan setting	Scan rule to be applied by the IMAP proxy	

3.3.1.38NNTP proxy

API path: /config/services/nntpproxy

Configuration file location: /NNTP_PROXY

The NNTP service

Attribute	Name	Description	Type
enable	Enable	Enable/disable the NNTP proxy service	Flag
listen	Listener	The port, and optional local IP, where the NNTP proxy service listens for client requests	Array(IpWithPort)
nntp_server	Default target server	Default NNTP server. Is used when the user name does not include information about the target NNTP server	IpOrHostname
nntp_server_port	Default target server port	Port for default NNTP server	Port
scanner_rule	Scan setting	Scan rule to be applied by the NNTP proxy	

3.3.1.39POP3 proxy

API path: /config/services/pop3proxy

Configuration file location: /POP3_PROXY

The POP3 service

Attribute	Name	Description	Type
enable	Enable	Enable/disable the POP3 proxy service	Flag
listen	Listener	The port, and optional local IP, where the POP3 proxy service listens for client requests	Array(IpWithPort)

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

pop3_server	Default target server	Default POP3 server. Is used when the user name does not include information about the target POP3 server	IpOrHostname
pop3_server_port	Default target server port	Port for default POP3 server	Port
scanner_rule	Scan setting	Scan rule to be applied by the POP3 proxy	

3.3.1.40SMTP server

API path: /config/services/smtp

Configuration file location: /SMTP

Settings for the SMTP service. These settings apply when using the SMTP MTA service

Attribute	Name	Description	Type
enable	Enable	Enable/disable the SMTP MTA service	Flag
path	Queuing path	Path for storing mails	Path

3.3.1.41Settings for incoming emails

API path: /config/services/smtp/receive

Configuration file location: /SMTP/RECEIVE

Settings for incoming mail

Attribute	Name	Description	Type
banner_delay	Early talker rejection delay	The number of seconds that the SMTP service waits before sending the SMTP banner. With this feature, SPAM bots can be blocked that send data in a non-compliant way, without waiting for the banner that signals the server being ready	Integer
ip	Listen-on address	IP address to listen for incoming mail	IpAddress
max_connections	Max. incoming connections	Maximum number of open connections for receiving e-mails	MaxConnections
port	Port	Port to listen for mails	Port

3.3.1.42Greylisting

API path: /config/services/smtp/receive/greylist

Configuration file location: /SMTP/RECEIVE/GREYLIST

Settings for greylisting

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Attribute	Name	Description	Type
ignore	Permanent whitelist	List client-subnets or sender-addresses/-domains for which greylisting are never applied	IgnoreRule
minlastseen	Delay	Minimum time interval (in sec) to be elapsed for passing greylisting test	Integer
timeout	Timeout	Amount of time a mail is recognized after having been first encountered. After this interval has elapsed, the greylisting check for this mail is reset	Integer
ttlwhitelist	Timespan for temporary whitelisting	Amount of time (sec) the mail sender remains whitelisted after passing the greylisting check. If not set, no temporary whitelisting is applied	Integer

3.3.1.43Routes

API path: /config/services/smtp/routes/<route_name>

Configuration file location: /SMTP/ROUTES/<route_name>

Routes are used to apply certain actions on traffic coming in from , or going out to a defined network. They are checked in order against the current connection. The first matching route is used and its settings are applied for the connection

Attribute	Name	Description	Type
client_ip	Client IP mask	Client IP address, or mask	Subnet
direction	Direction	Makes a Route inbound, outbound or standard (bidirectional)	
forwarding	Action	Determines how e-mail is routed	
greylist	Greylisting	Activate/deactivate greylisting	Flag
host_forward	Host	E-mail is forwarded to this host if forwarding is 'static'	String
ldap	LDAP	Identify mailbox to be routed by an LDAP string	String
mailbox_file	Mailbox-File	File containing a list of domains or e-mail addresses. The path can be either absolute or relative to the application folder	Path
scan_rule	Scan setting	Scan rules allow for handling mail content in an elaborate way to identify, mark, and handle malicious mail content or SPAM	
spf1	SPF1	Enable/disable Sender Policy Framework	Flag

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

target_domain	Target domain/E-mail address	Domain, or mail address, of recipient	Array(DomainOrMail)
type	Type	Select how to define this route	

3.3.1.44Scan settings

API path: /config/services/smtp/scansettings

Configuration file location: /SMTP/SCANSETTINGS

Scan settings

3.3.1.45Scan rules

API path: /config/services/smtp/scansettings/scansettings/<scan_setting_name>

Configuration file location: /SMTP/SCANSETTINGS/<scan_setting_name>

Scan settings

Attribute	Name	Description	Type
attachmentfilter	Attachment scanning	Settings for filtering e-mail attachments based on the attachments' filenames	
spamfilter	SPAM filter	Settings for SPAM filter. The IKARUS SPAM filter assigns a score to e-mails depending on the subject, content, etc. By defining the levels for "SPAM" and "Possible SPAM", different actions can be performed depending on the score	
virusfilter	Malware detection	Settings for classification and detection of malware. For e-mails, both content and attachments are scanned	

3.3.1.46Settings for outgoing emails

API path: /config/services/smtp/send

Configuration file location: /SMTP/SEND

Settings for sending e-mail

Attribute	Name	Description	Type
max_connections	Max. outgoing connections	Maximum number of simultaneous outgoing connections	MaxConnections

3.3.1.47TSMTP proxy

API path: /config/services/smtpproxy

Configuration file location: /SMTP_PROXY

The TSMTP proxy service

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Attribute	Name	Description	Type
enable	Enable	Enable/disable the SMTP proxy service	Flag
listen	Listen-on	The port, and optional local IP, where the SMTP proxy service listens for client requests	Array(IpWithPort)
scanner_rule	Scan setting	Scan rule to be applied by the SMTP proxy	
smtp_server	Default target server	Default SMTP server. Is used when the user name does not include information about the target SMTP server	IpOrHostname
smtp_server_port	Default target server port	Port for default SMTP server	Port

3.3.1.48WCCP

API path: /config/wccp

Configuration file location: /WCCP

Settings for WCCP

Attribute	Name	Description	Type
designated	Designated web cache	Marks this instance of the gateway.security server as the designated web-cache	Flag
enable	Enable WCCP	Enable/disable support for WCCP	Flag
ip_address	IP address of proxy for WCCP	IP address of gateway.security as seen by the WCCP routers	IpAddress
redirection_type	Redirection type	Redirection or forwarding method to apply	Enum(WccpRedirectionType)
routers	Router IP address	List of WCCP routers to be connected	Array(IpAddress)

3.3.2 Data types

Type	Description
Branding	Branding
ContentType	Content type
DataSizeWithUnit	A quantity of data size. Consists of a positive integer, followed by a postfix denoting the unit. Valid postfixes are 'K', 'M', or 'G' for kilobytes, megabytes, or gigbytes, respectively. There must be no blank between the integer and the postfix.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

`Date`	Date
`Domain`	Every valid expression for a domain, or sub-domain.
`DomainOrMail`	Either a domain name or an e-mail-address
`EmailAddress`	A valid e-mail address.
`File`	File name
`FileName`	File name
`Flag`	A boolean value.
`HttpReport`	A reference to an HTTP report.
`IgnoreRule`	
`Integer`	An arbitrary integer.
`IpAddress`	An IPv4 address
`IpWithPort`	An IP address, followed by a colon (':') and a port number.
`Password`	Password
`Path`	A valid file system path expression. Either backslash ('\') or slash ('/') may be used as separator.
`PermissionSetMask`	Permission set mask
`Port`	Port
`SmtpReport`	SMTP report
`SpamLevel`	A decimal number between 0.0 and 10.0.
`String`	A string.
`Subnet`	Subnet
`Time`	Time
`Timespan`	Timespan
`URL`	URL

3.3.3 Enumerations

3.3.3.1 AlertEventFlags

Alert event

Literal	Description
`error`	Error

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

license	License is about to expire
lowdiskspace	Disk space is low
update	VDB/UDB/SDB database is updated
vdbupdate	Update VDB
virusfound	Malware detected

3.3.3.2 AlertType

Defines the way how to inform about an alert.

Literal	Description
email	Inform about alert by email
logfile	Write alert event to log file only

3.3.3.3 AttachmentFilterListPriority

Literal	Description
black	Check for black-listed files first
white	Check for white-listed files first

3.3.3.4 AutoReportingPeriod

Interval

Literal	Description
month	Monthly
week	Per week

3.3.3.5 ContenttypeSource

Content-Type

Literal	Description
custom	Custom
predefined	Predefined

3.3.3.6 Contenttypes

Content type

Literal	Description
all	All
archive	Archive

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

audio	Audio
excel	Excel
executeable	Executable
office	Office
pdf	PDF
powerpoint	Powerpoint
video	Video
visio	Visio
word	Word

3.3.3.7 DataSizePostfix

Unit

Literal	Description
g	Gigabytes
k	Kilobytes
m	Megabytes

3.3.3.8 DaysOfWeek

Weekday

Literal	Description
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday
7	Sunday

3.3.3.9 FlagInherited

Inherited flag

Literal	Description
inherit	Inherit

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

no	No
yes	Yes

3.3.3.10GreylistIgnoreType

Permanent whitelist Type

Literal	Description
domain	Domain
ipmask	IP mask
mail	E-mail

3.3.3.11LogInterval

Log interval

Literal	Description
day	Daily
week	Weekly

3.3.3.12NetworkAuthenticationType

Authentication type

Literal	Description
datacollector	Works similar to landing page authentication. The user is redirected to a web form. After submission, she receives an email containing a confirmation link for unlocking web access.
ldap	The user is prompted for her credentials which are verified through an LDAP request.
lockpage	At the first attempt to access the network, the user is redirected to a page containing a link to grant access for the source IP address of the current connection.
negotiate	The user authenticates through her domain account. The authentication data are provided through the HTTP request.
proxy	IKARUS gateway.security allows for defining its own user credentials consisting of user name and password. Once the user tries to access the network, she is prompted for her credentials.
set	No authentication is checked

3.3.3.13NetworkRuleType

Rule type

Literal	Description
network_group	Network group

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

subnet	Subnet

3.3.3.14PermissionCriterionType

Criterion type

Literal	Description
all	All
contenttypelist	Content type list
continent	Continents
country	Countries
file	File/Extension
filelist	File list
url	URL
urlfiltercat	URL filter categories
urllist	URL list

3.3.3.15RemoteManagerAuthMode

Authentication type

Literal	Description
internal_user	The user authenticates through internal authentication, consisting of a name and a password.
ldap_group	The user is authenticated through an LDAP request.

3.3.3.16ReportChart

Chart type

Literal	Description
bar	Bar
line	Line
pie	Pie
table	Table

3.3.3.17ReportFilterBlocked

Blocked

Literal	Description

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

blocked	Blocked
notblocked	Not blocked

3.3.3.18ReportFilterInfected

Infected

Literal	Description
infected	Infected
notinfected	Not infected

3.3.3.19ReportHttpFilterDetail

Detail

Literal	Description
contenttype	Blocked Contenttypes
continent	Blocked Continents
country	Blocked Countries
infected	Blocked Infections
notinfected	Not blocked
permissionset	Blocked Permission sets
transferlimit	Blocked transfer limit
url	Blocked URLs
urlcat	Blocked URL categories

3.3.3.20ReportHttpFilterFlagGroup

Filter

Literal	Description
all	All
blocked	Blocked
details	Details

3.3.3.21ReportHttpFilterGroup

Parameter to select predefined queries for reporting HTTP traffic.

Literal	Description
all	Report the overall amount of traffic.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

all_customers_nwgroup_param	Customers in network group
all_customers_subnet_param	Report traffic grouped by customers of the subnet passed as parameter.
all_domain_param	Report traffic for domain passed as parameter.
all_nwgroup_param	Report the traffic for network group passed as parameter.
all_permissionset_param	Report the traffic for permission set passed as parameter.
all_srcip_param	Report the traffic for the source IP address passed as parameter.
all_subnet_param	Report the traffic for subnet passed as parameter.
all_tld_param	Report traffic for the top level domain passed as parameter.
top_domain	Report the traffic grouped by domains. Display the top results only.
top_domain_permissionset_param	Top domains for permission set
top_domain_srcip_param	Top domains per source IP
top_domain_subnet_param	Top domains for subnet
top_nwgroup	Report the traffic grouped by network groups.
top_permissionset	Top permission set
top_srcip	Report the traffic grouped by source IP.
top_subnet	Report the traffic grouped by subnet.
top_subnet_nwgroup_param	Top subnets for network group
top_tld	Report the traffic grouped by top level domains.
top_tld_nwgroup_param	Top TLDs for network group
top_tld_permissionset_param	Top TLDs per permission set
top_tld_srcip_param	Top TLDs per source IP
top_tld_subnet_param	Top TLDs for subnet

3.3.3.22ReportShapeBar

Bar

Literal	Description
hor	Horizontal
horstack	Horizontally stacked
vert	Vertical
vertstack	Vertically stacked

3.3.3.23ReportShapePie

Pie

Literal	Description
`empty`	Empty
`fill`	Filled
`slice`	Sliced

3.3.3.24ReportSmtpFilterDetail

Detail

Literal	Description
`grey`	Greylisted
`ham`	HAM
`pspam`	Possible SPAM
`spam`	SPAM
`spf`	SPF

3.3.3.25ReportSmtpFilterDirection

Direction

Literal	Description
`all`	In- and outbound
`in`	Inbound
`out`	Outbound

3.3.3.26ReportSmtpFilterFlagGroup

Filter

Literal	Description
`all`	All
`blocked`	Blocked
`details`	Details
`infected`	Infected

3.3.3.27ReportSmtpFilterGroup

Report type

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Literal	Description
all	Display non-grouped data.
all_mailbox_param	Display data grouped by mailboxes.
top_mailbox	Display data grouped by mailboxes and ordered descending by amount of data.

3.3.3.28ReportSummarizeBy

Sum up by

Literal	Description
data_size	Data size
number	Number

3.3.3.29ReportTimeUnit

Time unit

Literal	Description
day	Days
hour	Hours
month	Months
quarter	Quarter
week	Weeks
year	Years

3.3.3.30RuleResult

Result

Literal	Description
allow	Allow
deny	Deny

3.3.3.31SmtpRouteDirection

Direction

Literal	Description
default	Default
inbound	Inbound
outbound	Outbound

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

3.3.3.32SmtpRouteForwarding

Forwarding

Literal	Description
mx	MX
static	Host

3.3.3.33SmtpRouteType

Type

Literal	Description
client_ip	Client IP
ldap	LDAP
mailbox_file	Mailbox file
target_domain	Target domain

3.3.3.34SpamFilterAction

Action

Literal	Description
block	Block E-Mail
markonly	Only mark E-Mail
redirect	Redirect E-Mail

3.3.3.35SpamRuleField

Fields that are available as SPAM rule criteria. Some require a value for checking whether an SMTP header contains a certain value.

Literal	Description
emptyfrom	Header 'From' is empty.
emptysubject	Header 'Subject' is empty.
emptyto	Header 'To' is emtpy.
envelopfrom	SMTP envelope sender is <FROM>
envelopto	SMTP envelope recipient is <TO>
from	From header item includes <FROM>
mailtext	Mail text
nofromline	From header item does not exist

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

notoline	Missing 'To' header
novalidaddrfrom	Invalid 'From'
novalidaddrto	Invalid 'To'
onlyhtmltext	Message HTML only
subject	'Subject' contains
to	'To' contains
toandfromequal	'To' equals 'From'

3.3.3.36SpamRuleResult

Result

Literal	Description
always	SPAM
never	REGULAR
possible	POSSIBLE SPAM

3.3.3.37TimeControl

Time control

Literal	Description
none	None
time_range	Time range
weekdays	Weekdays
weekdays_and_time_range	Weekdays and time range

3.3.3.38VirusFilterEmailAction

Action

Literal	Description
deleteitem	Delete attachment
dropemail	Drop E-Mail

3.3.3.39WccpRedirectionType

Type

Literal	Description
gre	Forward packages to proxies using GRE

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

layer2	Forward by rewriting the destination MAC address

3.4 Content types

This is a comprehensive list of all content types detected by IGS.

Type	Super type
Archive	
compiler/linker	
Documents	
EMail	
Executables	
Miscellaneous	
Multimedia	
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
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
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
AIL Midi Driver	Miscellaneous
MMF File	Miscellaneous
Cygwin Messages	Miscellaneous
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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Type	Super type
Audio	Multimedia
GERMAN - ASCII	Textfile
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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

4

Remote Manager

The Remote Manager (RM) is an interface of the IGS 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 is reset without any response.

4.2 Internal users

IGS supports the definition of user names and passwords.

Attribute	Default value	Description
NAME		Unique username.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: 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.

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.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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.

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)

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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 is redirected to the IGS running on this host.

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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

► (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

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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

◄ .
◄ 230 Transfer complete

PASSWD SET <username> [<new password>]
Set the password for the given user. If password is omitted, the user password is 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.

◄ 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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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
◄ 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
```


IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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
```

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 is 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 is returned instead.

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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

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 is assumed.

Response format: Tree, DOT_ENCODED_TEXTLINES

Errors:

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

```
530 Error opening logfile
```

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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

5 REST API

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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: 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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

```
200 OK
Content-Type: application/json
{
    "username" : "root"       #current user
    "rights" : "write_locked" # 'read', 'write' or 'write_locked'
    "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 3.3.1.

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
```


IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

```
{
 "allowip":[
          "0.0.0.0/0",
          "127.0.0.1/32"
],
 "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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

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

<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
```


IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

```
Content-Type: application/json

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

IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Request

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

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
```


IKARUS Security Software GmbH | Blechturmgasse 11 |A-1050 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405

Response(s)

```
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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: 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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: 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 Vienna/Austria | 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 | Commercial Register: FN 64708i | Place of jurisdiction: Vienna |
VAT ID: ATU15191405