

FAQ

Program name: Aloaha

1. Installation

- 1.1 Do I need to have an SMTP Server installed on the same machine as Aloaha?
- 1.2 How do I install Aloaha on a Gateway without SMTP Server?
- 1.3 Aloaha Version on our Server
- 1.4 How do I install Aloaha on the same machine as MS ISA?
- 1.5 When I start aloaha.msc all dialogs are empty except Tools and Websites.
- 1.6 Where can I download Microsoft MSDE?
- 1.7 How do I install Aloaha on the same machine as my Mailserver?

2. Configuration

2.1. *without subcategory*

- 2.1.1 Does Aloaha support different Databases other than Access/SQL/MSDE?
- 2.1.2 Bogus email addresses
- 2.1.3 Configuration does not load on NT4
- 2.1.4 Multiline greeting
- 2.1.5 Multiline Welcome
- 2.1.6 Remote SMTP Connections are not properly accepted by Aloaha
- 2.1.7 How do I change the DNS Timeout?
- 2.1.8 After the connection, nothing happens
- 2.1.9 Converting to SQL Database
- 2.1.10 Could Aloaha create an open relay?
- 2.1.11 Regular Expressions
- 2.1.12 extend body checking to header
- 2.1.13 How do I import my old keyword lists in Aloaha?

2.2. *Local User List*

- 2.2.1 How can I automatically import Exchange55 User to Aloaha?

3. Upgrading

no entries

4. General

4.1. *without subcategory*

- 4.1.1 Growing mdb file
- 4.1.2 What are the requirements for NT4?
- 4.1.3 Is there an Aloaha newsletter available?
- 4.1.4 How do I become an Aloaha reseller?
- 4.1.5 What is greylisting?
- 4.1.6 Where do I find more information about greylisting?
- 4.1.7 Remove read receipt requests
- 4.1.8 Why are you suggesting SQL/MSDE as a Database?
- 4.1.9 I read that the plugin interface is public. Where do I find the API?
- 4.1.10 Can I keep more than 20 mails in the archive
- 4.1.11 How can I start the realtime mailmonitor?
- 4.1.12 Does this product work with Groupwise 6.5 sp1? Do you offer an appliance for thi
- 4.1.13 Realtime Monitor
- 4.1.14 Simulation Mode
- 4.1.15 Where is the old Yahoo forum?
- 4.1.16 What is Channel 9?

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

- 4.1.17 How Does Aloaha work?
- 4.1.18 How does Aloaha detect if its installed on the perimeter?
- 4.1.19 How can I avoid that every incoming email is being attachment checked?
- 4.1.20 Why is Aloaha not using the .NET Framework?
- 4.1.21 I would like to get more information about your product Aloaha Archiver.
- 4.1.22 Is it possible to block an email based on the partial content of a header?
- 4.1.23 The SMTP verb QUIT does not cause the connection to be dropped.
- 4.1.24 Where can I run historical reports, if some one tells me he is missing an e-mail
- 4.1.25 What do these entries in warning.log mean?
- 4.1.26 Technicalities
- 4.1.27 Is there a German FAQ available?
- 4.1.28 Why is RFC 1925 that important?
- 4.1.29 How can I access the Aloaha News Feed (RSS)
- 4.1.30 Is it possible that Aloaha listens on multiple IPs?
- 4.1.31 Which Build Number do I need to use Greylisting?
- 4.1.32 How does Aloaha work?
- 4.1.33 Why do I not see any entries in the Monitor Section of the GUI?
- 4.1.34 Are there any security concerns regarding the realtime monitor?
- 4.1.35 I am using an old iMail on NT4. Can I protect it with Aloaha?
- 4.1.36 Is there an online Knowledge Base available?
- 4.1.37 How do I contact support?
- 4.1.38 Is there an email based discussion available?

4.2. Greylisting

- 4.2.1 How did you integrate SPF in Greylisting?

5. Scripting Engine

- 5.1 Is it possible to instruct Aloaha to archive every incoming email to disk?
- 5.2 How do I use the Script Engine?

6. logfiles

- 6.1 ProxyService.exe: regi.DeleteValue failed

7. Public API

7.1. *without subcategory*

- 7.1.1 How can I download mails from POP3 and scan them?

7.2. *SPF*

- 7.2.1 Which API do I have to use to retrieve SPF records?
- 7.2.2 How can I do a SPF check on my POP Mailbox?
- 7.2.3 Is it possible to use the SPF SDK from VB6?

8. Modules

- 8.1 What are Spam URI Realtime Blocklists?

9. POP3 Connector

- 9.1 How does the Connector retrieve envelope information?
- 9.2 Can I use Exchange Journaling together with Aloaha?

10. Aloaha SINK Connector

- 10.1 Can I bind Aloaha to an event SINK as well?
- 10.2 Do I loose performance if I use the SINK Connector?

11. Regular Expressions

- 11.1 Does Aloaha support Regular Expressions?

12. SPF

12.1 Can I use SPF if Aloaha is not installed on the perimeter?

12.2 Can I use SPF if Aloaha is not installed on the perimeter?

1. Installation

1.1. Do I need to have an SMTP Server installed on the same machine as Aloaha?

Question:

Do I need to have an SMTP Server installed on the same machine as Aloaha?

Answer:

No, Aloaha does not need a SMTP Server installed on its host. The reason is due to Aloaha's innovative design. Aloaha acts like a Firewall/Proxy. It accepts datapackages and not emails. These datapackages are analysed, forwarded to the recipient or else rejected.

1.2. How do I install Aloaha on a Gateway without SMTP Server?

Question:

How do I install Aloaha on a Gateway without SMTP Server?

Answer:

During the installation of Aloaha you will see a dialog where you are asked to enter the details of the listenport and the listenip.

In the listenport you should enter the port of your SMTP Server. Usually this is 25. In the listenip you should enter the main IP of the machine.

If Aloaha is installed for example on a Microsoft ISA Machine you would have to choose the external IP and open 25 via packet rule and not via Server publishing rule.

The next dialog will ask you to enter the forwardport and the forwardip. In forward port you should enter the port of your SMTP Server. Usually 25.

In the forwardip you should enter the listenip of your SMTP Server. Usually the main IP of your mail server machine.

At this point your setup is complete. The next step is to open the Aloaha Configuration to configure the Local Domain Table and/or Local User Table.

To avoid being an open relay it is wise to set the options to accept only emails sent to Local User and/or accept only emails sent to Local Domains.

Now you can start the Aloaha Service. In about 30 seconds you can continue to receive emails - this time SPAM Free.

Of course you either have to point your MX record to the IP Number of Aloaha or if you have a NAT firewall you need to forward the mailport to Aloaha's IP instead of your Mailserver IP.

PLEASE NOTE: After a first time installation Aloaha's default is to be in Simulation mode. No emails will be rejected in Simulation mode.

To disable the Simulation mode you need to go to the General Options and deactivate it there. Please restart the Aloaha Service afterwards.

1.3. Aloaha Version on our Server

Question:

How can I check if I have the latest Aloaha's Build installed?

Answer:

You can check the Aloaha Pad file at <http://www.aloaha.com/download/aloaha.xml>

1.4. How do I install Aloaha on the same machine as MS ISA?

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

Question:

How do I install Aloaha on the same Machine as MS ISA 2000/2004?

Answer:

It is best to avoid server publishing rules for services installed on the same machine as your ISA Server. It is much better to work with packet filter and disable socket pooling of your IIS as described here:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;310155>

1.5. When I start aloaha.msc all dialogs are empty except Tools and Websites.

Question:

I installed Aloaha on my very clean and secure NT Box and downloaded the NT4 MMC from

<http://www.aloaha.com/download/aloaha.msc>

When I start aloaha.msc all dialogs are empty except Tools and Websites.

Any suggestions what is going wrong?

Answer:

Please note that some packages which are included in Windows 2000 are not included in old OSes like NT4. You need to download them from Microsoft and install/upgrade them manually. Such packages are WMI, WSH, ADO and CDO. Please click [here](#) to read more.

If you don't manage to start the MMC at all please click [here](#)

1.6. Where can I download Microsoft MSDE?

Question:

Where can I download Microsoft MSDE?

Answer:

Go to <http://www.microsoft.com/sql/msde/downloads/download.asp> to download the freeware SQL of Microsoft - called MSDE

1.7. How do I install Aloaha on the same machine as my Mailserver?

Question:

How do I install Aloaha on the same machine as my Mailserver?

Answer:

The first step is to reconfigure the listenport of your smtpserver to another unused port. For example 2525.

The second step is to start the setup. You will see a dialog where you are asked to enter the details of the listenport and of the listenip.

In the listenport you should enter the original value of your SMTP Server. Usually this is 25. In listenip you should enter the listenip of your mailserver.

This is usually the main IP of the machine.

In the next dialog you will be asked to enter the forwardport and forwardip. In the forward port you should enter the new port of your SMTP Server. Usually 2525.

In the forwardip you will be asked to enter the listenip of your SMTP Server. Usually the main IP of your machine.

The third step includes the Configuration of Aloaha. You would have to open the configuration of Aloaha to be able to configure the Local Domain Table and/or Local User Table.

To avoid being an open relay it is wise to set the options to accept only emails sent to Local User and/or accept only emails sent to Local Domains.

At this point the installation is complete.

Now you can start the Aloaha Service. In approximately 30 seconds you will be able to receive emails - this time SPAM Free.

PLEASE NOTE: After a first time installation Aloaha's default is to be in Simulation mode. No emails will be

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

rejected in Simulation mode.

To disable the Simulation mode you need to go to the General Options and deactivate it there. Please restart the Aloaha Service afterwards.

2. Configuration

2.1. without subcategory

2.1.1. Does Aloaha support different Databases other than Access/SQL/MSDE?

Question:

Does Aloaha support different Databases other than Access/SQL/MSDE?

Answer:

Yes, you need to

1. create a file called config.udl in the aloaha directory
2. right click on it and choose properties
3. point to the database of your choice

2.1.2. Bogus email addresses

Question:

How can I reject mails which are addressed to non existent local accounts or are being spoofed with my own local addresses?

Answer:

You need to open the configuration and browse to the Local User section. There you will find a listbox and two options. In the listbox you must specify your valid local user addresses. Please note that you can import them from the Active Directory or from a file as well.

The option 'Do not accept mails sent from Local User' will reject every incoming email which has a mail from which is listed in the local user listbox.

The option 'Receive only mails addressed to Local User' will reject all mails which are not addressed to a valid Local User

2.1.3. Configuration does not load on NT4

Question:

I just installed Aloaha on NT4 but can not make the Configuration start. What am I doing wrong?

Answer:

You are doing nothing wrong. Most probably you haven't installed all required NT4 patches/upgrades. Please note that Aloaha requires the following Microsoft upgrades to work properly:

- WMI
- WSH 5.6
- ADO 2.5
- MMC

If you dont want to upgrade your MMC you could also start mmc from the "run program" and go in author mode to add the Aloaha Snapin. Like that it will work immediat without upgrading the MMC.

In case of furhter questions please contact mmc@aloaha.com

You can also download a NT4 MMC if you click [here](#)

2.1.4. Multiline greeting

Question:

Is it true that a multiline SMTP greeting can save me already lots of SPAM?

Answer:

Yes, multiline SMTP greetings can save you up to 40% SPAM since most of the SPAMMERS' scripts don't

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

support it and terminate their connections themselves.

From [BUILD 3.0.28](#) onwards it is very easy to configure such a multiline greeting.

1. Open the Aloaha configuration.
2. Browse to String Settings/SMTP Communication
3. Enter your multiline greeting in Welcome Field.

For example:

```
220-*****  
220-I am Aloaha protected  
220-Visit http://www.aloaha.com  
220 *****
```

2.1.5. Multiline Welcome

Question:

How do I configure a multiline Welcome greeting in Aloaha?

Answer:

You need [BUILD 3.0.38](#) to configure a multiline welcome greeting.

1. Open the Aloaha configuration.
2. Browse to String Settings/SMTP Communication.
3. Enter your multiline greeting in Welcome Field.

For example:

```
220-*****  
220-I am Aloaha protected  
220-Visit http://www.aloaha.com  
220 *****
```

2.1.6. Remote SMTP Connections are not properly accepted by Aloaha

Question:

Remote SMTP Connections are not properly accepted by Aloaha

Answer:

Please check if you edited the default Welcome String in String settings. It is a must according to RFC that the last line of the welcome banner starts with 220 space. For example:

```
220 Hello World
```

If you are using a multiple line welcome banner (as suggested) the other lines have to start with 220-

For example

```
220-****  
220-Hello  
220 ****
```

2.1.7. How do I change the DNS Timeout?

Question:

How do I change the DNS Timeout?

Answer:

From Version 3.0.64 onwards the DNS Timeout can be changed. The default value is 1000 ms which should be good enough in most cases.

You can change the timeout if you add in the registry hive
HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha
the following STRING value
DNSTimeout=timeout in ms

2.1.8. After the connection, nothing happens

Question:

After the connection, nothing happens.

```
listen(1): Connection request from x.x.x.x accepted
```

and then nothing

If I telnet to the port I get a blank page (and from the log I can see it connected) but no banner. Then I type "ehlo" and I get the banner, shouldn't the banner come first? It seems like the external servers as connecting and waiting for the banner.

Also it does not seem to clear the connection when QUIT is issued.

Chris

Answer:

Hi Chris,

The first time you connect with telnet it will take some seconds (up to 30) until you get the banner since the plugins will read their data from the database.

Kind Regards
Frank Hellmann

2.1.9. Converting to SQL Database

Question:

Converting to SQL Database

When converting to a SQL database, what exactly do I have to do? I have tried to connect it but it does not seem to work. I have a copy of a SQL database running (from another program).

Here is the command line in the " MSSQLDBCreator.exe"
Provider='sqloledb';Data Source='laptop';Initial
Catalog='Aloaha';User ID='sa';Password=''

Suggestions?

Answer:

There are several ways to connect Aloaha to SQL. You can do it either via the registry key sqldaprovider or a file called config.udl. Furthermore it is wise to import the access database into your SQL database before you connect

Aloaha. Like that you will keep all your settings.

Below the 2 possibilities:

1. sqldaprovider

Create a key sqldaprovider in HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha containing the connectionstring to

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

your

Database. sqldataprovider will actually override the default dataprovider string.

An example for an SQL connection string would be:

```
Provider='sqloledb';Data Source='mysqlserver';Initial Catalog='aloaha';User ID='sa';Password='blabla123'
```

2. config.udl

Place an empty file config.udl into the Aloaha directory. Right click on that file, choose properties and connect it to your SQL Database. Once you are ready you might want to open the config.udl and check if your user credentials have been saved properly. Furthermore you can create the connectionstring you find as a template for choice 1 above.

After you did these changes please restart Aloaha. Thats all.

When choosing the user credentials please note that Aloaha is running as localsystem account. So its easier to avoid windows authentication.

2.1.10. Could Aloaha create an open relay?

Question:

Could Aloaha create an open relay?

Answer:

Yes,

if you allow in your virtual SMTP server settings relay from the Aloaha IP it is possible that you create an open relay.

For example you install Aloaha on the same machine as Exchange and allow 127.0.0.1 to relay mails.

To avoid creating an open relay please configure Aloaha that it accepts only emails sent to local domains/user.

2.1.11. Regular Expressions

Question:

How do I use the new Regular Expression Engine you mention in "[New Regular Expression Engine included](#)"?

Answer:

It is quite easy. You can use the regular expression engine in wordlists and domainlists.

Just write your entry like regex[yourexpression] and yourexpression will be treated as a regular expression.

For example the use of regex[(.*)sex(.*)] entered in domain blacklist will block all domains containing the word sex somewhere.

2.1.12. extend body checking to header

Question:

What does "extend body checking to header" mean?

Answer:

If you enable this option you instruct Aloaha to extend the wordcheck to the Mime Header of the email.

2.1.13. How do I import my old keyword lists in Aloaha?

Question:

How do I import my old keyword lists in Aloaha?

Answer:

Every Dialog in Aloaha contains a button called Import/Export. Here you can import or export plain text lists.

2.2. Local User List

2.2.1. How can I automatically import Exchange55 User to Aloaha?

Question:

How can I automatically import Exchange55 User to Aloaha?

Answer:

There are different ways. The easiest is to create a textfile add.txt containing all your local user emails and place it in \user\

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

Like this it will automatically be imported.

Of course if you are able to script vbs you could also write a script to automate your task.

Please note that you need to have the Option Pack or ADSI2.5 installed. For further help please contact scripting@aloaha.com

```
Set FileSystem = WScript.CreateObject("Scripting.FileSystemObject")
Set OutPutFile = FileSystem.CreateTextFile("c:\program files\aloaha\user\add.txt", True)
set con = CreateObject("ADODB.Connection")
set com = CreateObject("ADODB.Command")
con.Provider = "ADsDSOObject"
con.Open
set Com.ActiveConnection = con
Com.CommandText = ";" & "(objectClass=*);mail,rfc822Mailbox,OtherMailbox;subTree"
set rs = Com.Execute
Do Until rs.EOF
sResultText1 = sResultText1 & rs.Fields("mail") & vbCrLf
sResultText2 = sResultText2 & rs.Fields("rfc822Mailbox") &
vbCrLf
'sResultText3 = sResultText3 & rs.Fields("OtherMailbox") &
vbCrLf
rs.MoveNext
Loop
OutPutFile.WriteLine sResultText1
OutPutFile.WriteLine sResultText2
'OutPutFile.WriteLine sResultText3
```

3. Upgrading

no entries

4. General

4.1. without subcategory

4.1.1. Growing mdb file

Question:

Why is the config.mdb always growing - even if I delete my emails from the mail archive?

Answer:

That is a limitation in access databases. They cannot be compressed while accessed by any processes. Still so Aloaha tries to compress the config.mdb at every service start.

We also recommend to use Microsoft SQL/MSDE Databases since they are much more performant and even allow Aloaha to work in a Network Load Balancing environment.

4.1.2. What are the requirements for NT4?

Question:

What requirements are needed for Aloaha to work properly on NT4

Answer:

Aloaha needs always ADO2.5, WSH5.6, CDO and WMI installed. As from Windows 2000 onwards these packages are installed by default. For NT4 you would need to download these packages manual from Microsoft and install them.

4.1.3. Is there an Aloaha newsletter available?

Question:

Is there an Aloaha newsletter available?

Answer:

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

Yes, just send a blank email to: newsletter-subscribe@aloaha.com

4.1.4. **How do I become an Aloaha reseller?**

Question:

How do I become an Aloaha reseller?

Answer:

Please refer to [this](#) KB article.

4.1.5. **What is greylisting?**

Question:

What is greylisting?

Answer:

Greylisting is a very advanced feature of Aloaha. Most probably Aloaha is even the first windows solution which supports this technology. More information you find it if you click [here](#)

4.1.6. **Where do I find more information about greylisting?**

Question:

Where do I find more information about greylisting?

Answer:

Check <http://projects.puremagic.com/greylisting/>.

There you will find lots of more information.

4.1.7. **Remove read receipt requests**

Question:

What does the General Option "Remove receipts of incoming emails if not whitelisted" mean?

Answer:

Basidly Aloaha removes all kind of delivery and read receipt requests from emails such as esmtp verbs and mime header lines. The result is that incoming emails don't generate any kind of receipts anymore. Not even if a mail fails.

4.1.8. **Why are you suggesting SQL/MSDE as a Database?**

Question:

Why are you suggesting SQL/MSDE as a Database?

Answer:

The default access database inherited a lot of access limitations such as speed and others. It is much more efficient to use a professional database such as SQL/MSDE. Furthermore if you use a SQL/MSDE Database you can install several Aloaha instances to use the same database. An example would be a Network Load Balancing Cluster.

4.1.9. **I read that the plugin interface is public. Where do I find the API?**

Question:

I read that the plugin interface is public. Where do I find the API?

Answer:

The API hasn't been published on the homepage.

You will need to send an email to api@aloaha.com

4.1.10. **Can I keep more than 20 mails in the archive**

Question:

Can I keep more than 20 mails in the archive?

Answer:

Yes, for more information click [here](#).

But please note that this is only suggested if you use a professional database such as SQL/MSDE.

4.1.11. **How can I start the realtime mailmonitor?**

Question:

This PDF Document was generated for free by the Aloaha PDF Suite
If you want to learn how to make your own PDF Documents visit:
<http://www.aloaha.com>

How can I start the realtime mailmonitor?

Answer:

You need to call telnet localhost 25602 from the Aloaha Machine and you will see all your SMTP traffic in realtime.

4.1.12. **Does this product work with Groupwise 6.5 sp1? Do you offer an appliance for thi**

Question:

Does this product work with Groupwise 6.5 sp1? Do you offer an appliance for this product?

Answer:

Yes, Aloaha is designed to work together with all RFC conform SMTP Server. It doesn't matter how many SPAM or Virus Filter are already installed on that Server since Aloaha does not depend on technologies like Microsoft Event Sinks. Aloaha can be installed on Windows2k/Windows2k3 and Windows XP.

In case of multiple SPAM and/or Virusfilter it is advised to install Aloaha as the first line of defense.

For your Case with Groupwise I suggest to install Aloaha on the same machine as Groupwise.

Before you install Aloaha on the same machine as your Groupwise please reconfigure your system to accept emails on a different port than 25. Then call the Aloaha Setup.

During the Setup you will be asked for Listenport/IP.

Please enter as listenport 25 and ListenIP the major IP of your Machine. In the next Dialog you will be asked for the forwardport and IP. Here you enter the new Port of your Groupwise System and the major IP of your machine.

You can also refer to FAQ Article Number 22. <http://www.aloaha.com/mmc/faq/faq.php?lang=en&display=faq&onlynewfaq=0&catnr=1&faqnr=22&prog=aloaha>

4.1.13. **Realtime Monitor**

Question:

What is the Realtime Monitor

Answer:

You can start the realtime monitor if you execute the following command on your aloaha machine:

```
telnet localhost 25602
```

(please note that this is not a security risk since you can only call it locally from the same machine)

In the realtime monitor you will see all the incoming emails in realtime like in a Network Monitor.

4.1.14. **Simulation Mode**

Question:

Why is Aloaha not rejecting any connections?

Answer:

By default Aloaha is in Simulation mode. It only logs potential rejections but actually does not reject at all.

You can disable Simulation Mode in Aloaha's general settings

4.1.15. **Where is the old Yahoo forum?**

Question:

Where is the old Yahoo forum?

Answer:

The old Yahoo Forum still exists. It is now reachable via <http://groups.yahoo.com/group/aloaha/>

Post message: aloaha@yahoogroups.com

Subscribe: aloaha-subscribe@yahoogroups.com

Unsubscribe: aloaha-unsubscribe@yahoogroups.com

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

List owner: aloaha-owner@yahoogroups.com

Please note if you need an invitation that you just send to send us an email and we will send you the invitation.

4.1.16. What is Channel 9?

Question:

What is Channel 9?

Answer:

You might know that if you ever travelled in US by plane.

Anyway - try telnet localhost 25602 and you will see all traffic passing through the Proxy in realtime.

Please note that this is not a security whole since only the localhost has access.

If you need access to Channel 9 from remote hosts please let us know. We can implement that in a couple of minutes.

4.1.17. How Does Aloaha work?

Question:

How Does Aloaha work?

Answer:

How Does Aloaha work?

Aloaha's innovative secret is that it works as a transparent SMTP proxy. That means that it accepts the SMTP Datastream on Port 25 and forwards it UNMODIFIED to the port 25 of the backend mailserver. Aloaha does not contain any SMTP MTA.

Between the listen Winsock and forward winsock there are a couple of plugins/filters which analyse the datastream in realtime.

In case a filter classifies this stream as HAM the stream will skip the following plugins/filter. If the datastream is classified as SPAM Aloaha will send a 5xX Error to the sending Server and will send a quit to the receiving mailserver. Then it will drop the connection.

This architecture has the huge advantage that it works not only on machines which have a microsoft SMTP Server (IIS) installed and it enables Aloaha to reject emails before they are 100% transmitted.

A bit different it is the SINK input. It is possible to register the Aloaha Plugins/Filter into the IIS Event SINKS. That is only suggested if for some reasons somebody does not want to use the rejecting features of the Proxy but would prefer just to TAG their emails as SPAM.

If Aloaha is registered into the SINK it always retrieves the full email and starts scanning after retrieving it. From that point onwards it does not make

sense to reject a mail since that would mean additional traffic and jammed queues.
In case Aloaha is registered into the SINK it can TAG the emails in the Header and Subject as SPAM/HAM. Furthermore it is possible to move detected SPAM into a SPAM Mailbox.

The optional POP3 Connector works similar as the SINK. The full email gets downloaded from the POP3 Mailbox, scanned and TAGGED/forwarded.

Please contact support at support@aloaha.com if you are not sure which input type to choose.

Please note that the suggested type is the Proxy type. It is possible to use all 3 Input types parallel for extra protection.

4.1.18. How does Aloaha detect if its installed on the perimeter?

Question:

How does Aloaha detect if it is installed on the perimeter?

Answer:

As soon Aloaha gets a connection request it checks if the IP is a private IP or listed in the Local IP Table. If that check is true that means for Aloaha that it is NOT installed on the perimeter and it will postpone IP checks until it retrieves the mime header so it can parse that header for the right IP.

4.1.19. How can I avoid that every incoming email is being attachment checked?

Question:

How can I avoid that every incoming email is being attachment checked?

Answer:

Hi,
it is for your own security that EVERY inbound mail is being attachment checked - even whitelisted ones. That's why we decided to plug the attachment checking module into the Aloaha Antivirus Interface.
But due to the flexible structure of Aloaha it is quite easy to change that behavior (even if not suggested).

Just open the registry editor and browse to:
HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha\modules\checkattachments

You will find there the property Type with the value AV. Just change that value to BODY and you are done. Whitelisted mails will not be checked anymore.

4.1.20. Why is Aloaha not using the .NET Framework?

Question:

Why is Aloaha not using the .NET Framework?

Answer:

Since the average Aloaha users are "Powerusers" it is assumed that they would never dare to install the .NET Framework on such an import server as their inbound SMTP Server.

If we would base Aloaha on the .NET Framework we would loose these important customers.

If you have further questions please contact dotnet@aloaha.com

4.1.21. **I would like to get more information about your product Aloaha Archiver.**

Question:

I saw your company featured on MSD2D.COM and would like to get more information about your product Aloaha Archiver.

Answer:

Basically Aloaha is an AntiSPAM Solution/Framework which supports different inputtypes. These inputtypes are transparent SMTP Proxy, IIS/Exchange SINK and POP3 Connector. Additional inputtypes can be created since the Aloaha APIs are public declared.

The Core of the Aloaha Framework is a database. This is by default an Access Database but can be switched to MSDE/SQL and others.

Every email which passed through any of the above input types is being archived in the database. By default that are the last 1000 mails. But that value can be changed.

To archive inbound mails I suggest to use the transparent proxy since that has the best AntiSPAM Results. The proxy is able to reject SPAM so it does not even enter your system and degrades system performance.

If you want to archive inbound and outbound mails I suggest to register the SINK Input. This can be done additional to the proxy.

In case you want to archive additional internal emails you need to enable message journaling in your exchange server. Then you use the POP3 Connector to download these mails into a local folder. Like that you will have all your emails dumped to a local folder AND you will have them archived to the Database.

4.1.22. **Is it possible to block an email based on the partial content of a header?**

Question:

Is it possible to block an email based on the partial content of a header?

Answer:

Yes, of course it is possible. You can extend the keyword checks in Subject-/Bodyrules with enabling the checkbox extend Bodychecking to Mail Header. You are even able to use Regular Expressions.

4.1.23. **The SMTP verb QUIT does not cause the connection to be dropped.**

Question:

The SMTP verb QUIT does not cause the connection to be dropped. If you telnet to any other SMTP server, issue a HELO command followed by the QUIT command, the SMTP server disconnects. Aloaha Version 3.0.64 does not. Is this by design or what?

Answer:

Yes,
that is by design and proven to be the most efficient way.
Thanks

4.1.24. **Where can I run historical reports, if some one tells me he is missing an e-mail**

Question:

Where can I run historical reports, if some one tells me he is missing an e-mail

Answer:

Regarding the historical reports you need to open the Monitoring section in the configuration. You will find Mail Monitor, IP Logging, Header Logging, Keyword Logging and Attachment Logging. Mails which did not trigger any filter you will find in Mail Monitor, Blacklisted IPs you will find in IP Logging, lots of other Filters you find in Header Logging, Keywords and URI in Keyword Logging and last but not least

blocked attachments in Attachment Logging.

Please note that you need to enable logging to Database in general settings to have the full logging enabled.

4.1.25. **What do these entries in warning.log mean?**

Question:

What do these entries in warning.log mean? There's one for every minute for the past couple of days (we disabled Aloaha now, because a lot of mails from whitelisted sources got lost).

```
20041210121456 Aloaha.exe: problems with listensock (detected by attendant) - going to restart sockets
20041210122023 NSPAttendant.exe: do_action called from testsock_timer
20041210122514 NSPAttendant.exe: do_action called from testsock_e
20041210122514 NSPAttendant.exe: could not connect to NSP (212.203.75.8) - actioncounter: 3
20041210122614 NSPAttendant.exe: do_action called from testsock_timer
```

Answer:

Hi Rene,
entries in warning.log should be always an indication to contact support@aloaha.com.
Please zipi your *.log and *.mdb files and attach them to your email. Our technical support will follow your issue up.
Since you are using NT4 please check if WMI, WSH5.6 and ADO are properly installed.
Kind Regards
Frank Hellmann

4.1.26. **Technicalities**

Question:

Technicalities!

Answer:

A helicopter was flying around above Seattle when an electrical malfunction disabled all of the aircraft's electronic navigation and communications equipment.

Due to the clouds and haze, the pilot could not determine the helicopter's position. The pilot saw a tall building, flew toward it, circled, and held up a handwritten sign that said "Where am I?" in large letters. People in the tall building quickly responded to the aircraft, drew a large sign, and held it in a building window. Their sign said "You are in a Helicopter."

The pilot smiled, waved, looked at his map, determined the course to steer to SEATAC airport, and landed safely. After they were on the ground, the co-pilot asked the pilot how he had done it.

"I knew it had to be the Microsoft Building, because they gave me a technically correct but completely useless answer."

4.1.27. **Is there a German FAQ available?**

Question:

Is there a German FAQ available?

Answer:

Yes,
just click [here](#)

4.1.28. **Why is RFC 1925 that important?**

Question:

Why is RFC 1925 that important?

Answer:

Because it tells you the

Twelve Networking Truths. When coding Aloaha
I try to stick as much as possible to RFC 1925

Please click [here](#) to download the RFC.

With sufficient thrust, pigs fly just fine. However, this is not necessarily a good idea. It is hard to be sure where they are going to land, and it could be dangerous sitting under them as they fly overhead.

4.1.29. **How can I access the Aloaha News Feed (RSS)**

Question:

How can I access the Aloaha News Feed (RSS)

Answer:

The URL to the Aloaha News Feed (RSS) is http://www.aloaha.com/mmc/rss_news.php

4.1.30. **Is it possible that Aloaha listens on multiple IPs?**

Question:

Is it possible that Aloaha listens on multiple IPs?

Answer:

Yes,
from build [3.0.35](#) onwards it is possible that Aloaha listens either on one IP or on ALL IP Numbers.

To be able to listen on ALL IP Numbers you just enter 0.0.0.0 as ListenIP.

4.1.31. **Which Build Number do I need to use Greylisting?**

Question:

Which Build Number do I need to use Greylisting?

Answer:

You need as a minimum Build Number 3.0.8 to use the new Greylisting feature.

4.1.32. **How does Aloaha work?**

Question:

How does Aloaha work?

Answer:

Please refer to: [Do I need to have an SMTP Server installed on the same machine as Aloaha?](#)

4.1.33. **Why do I not see any entries in the Monitor Section of the GUI?**

Question:

Why do I not see any entries in the Monitor Section of the GUI?

Answer:

You need to enable logging to Database in General Options.

4.1.34. **Are there any security concerns regarding the realtime monitor?**

Question:

Are there any security concerns regarding the realtime monitor?

Answer:

No,
Aloaha only accepts connections on port 25602 from localhost and forwardip.

4.1.35. **I am using an old iMail on NT4. Can I protect it with Aloaha?**

Question:

I am using an old iMail on NT4. Can I protect it with Aloaha?

Answer:

Yes, Aloaha is not using any IIS/Exchange related features like sinks. So you are able to use it together with any backend SMTP Server

4.1.36. **Is there an online Knowledge Base available?**

Question:

Is there an online Knowledge Base available?

Answer:

Yes, you can reach the Knowledgebase via <http://www.aloaha.com/mmc/faq/kb.php>

4.1.37. **How do I contact support?**

Question:

How do I contact support?

Answer:

Please refer to [this](#) KB article.

4.1.38. **Is there an email based discussion available?**

Question:

Is there an email based discussion available?

Answer:

Yes, just send a blank email to: list-subscribe@aloaha.com

4.2. *Greylisting*

4.2.1. **How did you integrate SPF in Greylisting?**

Question:

How did you integrate SPF in Greylisting?

Answer:

Since greylisting make only sense if the sending party (SPAMMER) is not using an SMTP Engine we found out that greylisting is not need if the sender is properly SPF authenticated.

In other words - emails which are originating from a domain which is publishing SPF and such emails are passing the SPF test - these emails are not being delayed by greylisting anymore.

5. Scripting Engine

5.1. **Is it possible to instruct Aloaha to archive every incoming email to disk?**

Question:

Is it possible to instruct Aloaha to archive every incoming email to disk?

Answer:

Yes, can write a script for the scripting engine to do that task. An example you find below.

1. Open Scripting Engine in MMC
2. Fill in Function Name archive
3. Choose AV as position
4. Press create new script from template
5. cut and paste my example from below into the text box
6. press ave
7. enable scripting engine
8. restart Aloaha

===

```
Function archive(input)
```

```
'This scripts helps you to archive your emails to a folder
```

```
On Error Resume Next
```

'Please set enable to true to enable this script
const enable=true

'Please set enable to true to enable AVG Scan - you can download it at
http://www.grisoft.com/us/us_dwnl_free.php

```
const avg=false
'please set path to avgscan.exe
dim avgscan
avgscan="C:\Program Files\Grisoft\AVG6\avgscan.exe"
```

archive=0 'set return value (always Integer)

```
if enable=true then
dim emlpath
dim tempopath
dim foldercreated
dim tempcreated
dim attachments
if emlpath="" then
Dim WshShell
Set WshShell = CreateObject("WScript.Shell")
emlpath = WshShell.regread("HKLM\SOFTWARE\aloaha\path")
tempopath= emlpath
if tempopath<>"" then tempopath=emlpath&"temp"
if emlpath<>"" then emlpath=emlpath&"archive"
Set WshShell = nothing
end if
```

```
if emlpath<>"" then
dim fso, fstream, newfolder, iMsg, iDsrc, IBody
Set fso = CreateObject("Scripting.FileSystemObject")
if foldercreated<>1 then
If Not fso.FolderExists(emlpath) Then
Set newfolder = fso.CreateFolder(emlpath)
foldercreated=1
Set newfolder=nothing
End If
end if
if tempcreated<>1 then
If Not fso.FolderExists(tempopath) Then
```

```
Set newfolder = fso.CreateFolder(tempopath)
tempcreated=1
Set newfolder=nothing
End If
end if
```

```
Set fstream = CreateObject("ADODB.Stream")
fstream.Type = 2
fstream.Charset = "US-ASCII"
fstream.Open
fstream.writetext(input)
Randomize
emlpath = emlpath + "\" + CStr(Int((100000 - 1 + 1) * Rnd + 100000)) + ".eml"
fstream.SaveToFile emlpath, 2
if avg=true then
```

```

Set iMsg = CreateObject("CDO.Message")
Set iDsrc = iMsg.DataSource
iDsrc.OpenObject fstream, "_Stream" 'convert Stream into CDO Object
set IBody=iMsg.Attachments
attachment= IBody.count
if attachment>0 then
hresult=0
for i = 1 to IBody.count
if hresult=0 then
IBody.Item(i).SaveToFile (temppath+"\ "+IBody.Item(i).Filename)
cmdline="/arc /rt /repok /nomem /nohimem /noself /noexport"
hresult=scanfile(avgscan,temppath+"\ "+IBody.Item(i).Filename,cmdline)
else
archive=100
end if
next
end if
set IBody=nothing
Set iDsrc =nothing
Set iMsg = nothing

end if
Set fstream=nothing
if archive<>0 then
Set fso = CreateObject("Scripting.FileSystemObject")
fso.DeleteFile emlpath
Set fso =nothing
end if
end if
end if
End Function

```

```

Function shortpath(longpath)
On Error Resume Next
shortpath=""
Set oFS =CreateObject("Scripting.FileSystemObject")
shortpath= oFS.GetFile(longpath).ShortPath
Set oFS =nothing
End Function

```

```

Function scanfile(scanpath, scanobject, parameters)
On Error Resume Next
Dim WshShell1, oExec1
scanfile=0
Set fso = CreateObject("Scripting.FileSystemObject")
If (fso.FileExists(scanpath)) Then
scanpath=shortpath(scanpath)
kommand=scanpath+" "+scanobject+" " +parameters
Set WshShell1 = CreateObject("WScript.Shell")
Set oExec1 = WshShell1.exec(kommand)
Do While oExec1.Status = 0
WScript1.Sleep 100
Loop
if cint(oExec1.ExitCode)>0 then
scanfile=cint(oExec1.ExitCode)
end if
Set oExec1=nothing

```

```
Set WshShell1=nothing
end if
fso.DeleteFile scanobject
set fso=nothing
End Function
```

5.2. How do I use the Script Engine?

Question:

How do I use the Script Engine?

Answer:

Please refer to [How to use the Script Engine - a LDAP example](#)

6. logfiles

6.1. ProxyService.exe: regi.DeleteValue failed

Question:

What does ProxyService.exe: regi.DeleteValue failed mean?

Answer:

Basically nothing. This function tries to delete an internal connection loss counter. This connection loss could be caused for example by a server restart. If you find them one after each other like:

```
20040728103002 ProxyService.exe: regi.DeleteValue failed
20040728184624 ProxyService.exe: regi.DeleteValue failed
20040728185246 ProxyService.exe: regi.DeleteValue failed
20040728185500 ProxyService.exe: regi.DeleteValue failed
```

it will be even better since that shows that Aloaha is optimal configured.

7. Public API

7.1. without subcategory

7.1.1. How can I download mails from POP3 and scan them?

Question:

How can I download mails from POP3 and scan them?

Answer:

Please check the script on http://www.aloaha.com/download/aloaha_downloader.txt to learn how to download and scan mails with Aloaha. Please note that mails detected as SPAM are marked in the Message Header as SPAM.

Furthermore the minimum requirement for this script is Aloaha 3.0.40.

For further questions and suggestions please contact pop3@aloaha.com

7.2. SPF

7.2.1. Which API do I have to use to retrieve SPF records?

Question:

Which API do I have to use to retrieve SPF records?

Answer:

The SPF and DNS APIs are located in the `spf_dns.DNSClass` COM Object. They are available via script.

Please check the example below:

```
dim spf
Set spf = CreateObject("spf_dns.DNSClass")
MsgBox spf.eval_spf("gmx.ch", "213.165.64.20", "", "", "")
```

```
MsgBox spf.eval_spf("v2.listbox.com", "207.8.214.5", "", "", "")
MsgBox spf.get_spf_records("gmx.ch")
```

7.2.2. Is it possible to use the SPF SDK from VB6?

Question:

Is it possible to use the SPF SDK from VB6?

Answer:

Yes,
sure - all Aloaha SDK's can be used from VB6 since they are all simple COM Objects.
For SPF just have a look at Dave Renos [sample](#)

7.2.3. How can I do a SPF check on my POP Mailbox?

Question:

How can I do a SPF check on my POP Mailbox?

Answer:

Quite easy with the SDK. I will add sample code below. The same code you can download [here](#)

The code scans the remote pop box for SPF and forward clean mails to one account and bad to another account via pop downloader:

```
'Sample Script to demonstrate the use of the pop interface
'needs minimum version 3.0.25 of SDK
```

```
'create objects
Set pop=CreateObject("pop3news.popnews")
Set spf=CreateObject("spf_dns.DNSClass")
```

```
'Set POP3 username, password, server and port
pop.username="pop"
pop.password="pop"
pop.remotehost="192.168.0.111"
pop.remoteport="110"
```

```
'Set forward server properties. if left empty strings it will use pickup
SMTPServer="10.0.0.111"
SMTPPort="25"
```

```
'change mailfrom. if left empty string it will use the original
MailFrom="bla@bla.de"
```

```
'change recipient. If left empty it will use the original one
RCPTto="mymail@mydomain.com"
RCPTtoSPAM="SPAM@mydomain.com"
```

```
'Set buestgues - if empty string it wont be used
buestguess="v=spf1 mx/24 a/24 ptr -all"
```

```
If CInt(pop.getammount)>0 Then
For i=1 to pop.getammount
header=CStr(pop.getheader(CStr(i)))
If spf.eval_header_for_spf(CStr(header),CStr(buestguess),"", "")=true Then
success = pop.send_email(pop.get_cdo(CStr(i)), CStr(SMTPServer), CStr(SMTPPort), CStr(MailFrom), CStr
(RCPTto), "", "")
MsgBox "true"
Else
success = pop.send_email(pop.get_cdo(CStr(i)), CStr(SMTPServer), CStr(SMTPPort), CStr(MailFrom), CStr
```

```
(RCPTtoSPAM), "", "")
MsgBox "false"
End If
If success=true Then
success=pop.deletemail(CStr(i))
End If
Next
End If
```

```
success=pop.close_and_quit
```

```
Set spf=nothing
Set pop=nothing
```

8. Modules

8.1. What are Spam URI Realtime Blocklists?

Question:

What are Spam URI Realtime Blocklists?

Answer:

Please browse to <http://www.surbl.org/> to find a detailed explanation.

9. POP3 Connector

9.1. How does the Connector retrieve envelope information?

Question:

How does the Connector retrieve envelope information? I always thought they are lost if I use a POP3 Connector!

Answer:

The Aloaha POP3 Connector is probably the only one in its category which does not have limitations like some other competing Connectors are suffering from.

The Connector is able to recover the Envelope from the Mime Header Information.

Furthermore the connector does not have the limitation to duplicate emails.

9.2. Can I use Exchange Journaling together with Aloaha?

Question:

Can I use Exchange Journaling together with Aloaha?

Answer:

Can I use Exchange Journaling together with Aloaha?

Yes of course you can use Exchange Journaling together with Aloaha.

Please refer to <http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3Journal/0526b555-4da6-4ab0-93e5-1e6d20962c89.msp>

to learn more about Exchange Journaling.

Exchange Journaling is available in Exchange 2000/2003

Exchange Journaling is a very good way to

- 1) Archive Mails as required by a number of national legislations
- 2) Monitor your complete inbound/outbound/internal mailtraffic

To use Exchange Journaling in Aloaha you need Aloaha 3.0.49 or higher.

Please download Aloaha from <http://www.aloaha.com/download/aloaha.zip>

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>

The configuration of Journaling in Aloaha is quite straight forward. Since the Journaling Mailbox is a simple POP3 enabled Exchange Mailbox Aloaha is using its build in POP3 Connector to retrieve the mails from the Archive Mailbox.

To configure the POP3 Connector you open the Aloaha Configuration, browse to General Options / Service Control / POP3 Downloader

Here you press Create new to create a new entry. Once you have done this you enter the Exchange servername in the Server Field. In Username/Password you fill in the credentials of your archive mailbox.

Next step is to remove the checkboxes at:

- 1) Scan downloaded mails with Aloaha
- 2) Leave mails on Server after download
- 3) TAG emails subject if SPAM
- 4) SAVE SPAM to Badmail

The Textboxes for Badmail and Recipient you can leave empty or default. In Submit Mail to Directory or Server you enter the directory where you want to save your archived/monitored mails to. That could be (in some counties must be) a write only medium such as a CDROM.

If you opt to archive your mails into a remote Server mailbox please enter the remote Server IP/Port here. You need to fill in also the textbox Change Recipient... in this case.

Thats all and your archiving/journaling/monitoring Solution is operating. To see/browse your archived/monitored mails you can use also the inbound Mail Monitor.

If you have further questions please send a mail to journaling@aloaha.com

10. Aloaha SINK Connector

10.1. **Can I bind Aloaha to an event SINK as well?**

Question:

Can I bind Aloaha to an event SINK as well?

Answer:

Even though Aloaha's innovative Proxy has been designed is the most efficient way to stop SPAM, there exist large organisations which are not able to use a rejecting Proxy. These organisations which can not reject mails can now opt to use the SINK. Furthermore the SINK is quite helpful for companies which are using an external backup MX which connects directly via a non standard port to the main MX. These companies are now able to check even mails coming from the backup MX.

10.2. **Do I loose performance if I use the SINK Connector?**

Question:

Do I loose performance if I use the SINK Connector?

Answer:

No, nobody needs to be afraid that emails are being scanned double. Proxy, SINK and POP3 are communicating whith each other to avoid double scanning.

11. Regular Expressions

11.1. **Does Aloaha support Regular Expressions?**

Question:

Does Aloaha support Regular Expressions?

This PDF Document was generated for free by the Aloaha PDF Suite
If you want to learn how to make your own PDF Documents visit:
<http://www.aloaha.com>

Answer:

Yes of course. You can use regular expressions in most of the lists of the configuration.

For example domain black-/whitelist, subject and body checking.

All you need to do is to follow a special syntax. You need to put `regex[]` around your regular expression.

For example `regex[v(i|l)(a|@)g(r|5|)(a|@)]`

12. SPF

12.1. **Can I use SPF if Aloaha is not installed on the perimeter?**

Question:

Can I use SPF if Aloaha is not installed on the perimeter?

Answer:

Yes, Aloaha includes a very intelligent Filter.

If you fill in your LocalIP's properly (or at least the ones Aloaha is retrieving mails from) Aloaha will detect automatically if it is installed on the edge, DMZ or in SINK Mode. In case it gets a connection of a local IP it will postpone some tests until it is able to retrieve and parse the MIME Header for the correct external IP.

12.2. **Can I use SPF if Aloaha is not installed on the perimeter?**

Question:

Can I use SPF if Aloaha is not installed on the perimeter?

Answer:

Yes,

if you fill in your local IP list properly Aloaha will decide fully automatically if it is either to get a direct connection or a relay one. In case of a relay it will postpone the SPF check until the Mime Header arrives.

Then it will parse the Mime header and take the first

IP which is not a Private IP and which is not listed in Local IP's.

This is also valid if you are using the POP3 Connector or SINK input.

Generated: 15.03.2005 02:27
all times are CET (GMT+1)

Content (c) 2004 by Aloaha

Powered by [FAQEngine](#) V4.04 ©2001-2004 Bösch EDV-Consulting

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

<http://www.aloaha.com>