Unispeed Bluegate

Appendix 2

The Bluegate Data Retention and Content Intercept system

The Unispeed Blue Shield Gateway System is an Internet Surveillance system designed for small to medium networks where network address translation (NAT) is typically used

The document covers:

- **Basic description of the system**
- **System access (User authorisation)**
- **Continuous data retention IP CDR and protocol extract**
- **Data extract and handover (HI2)**
- **Lawful interception and content intercept (HI3)**
- **HTTP / DNS inspect**

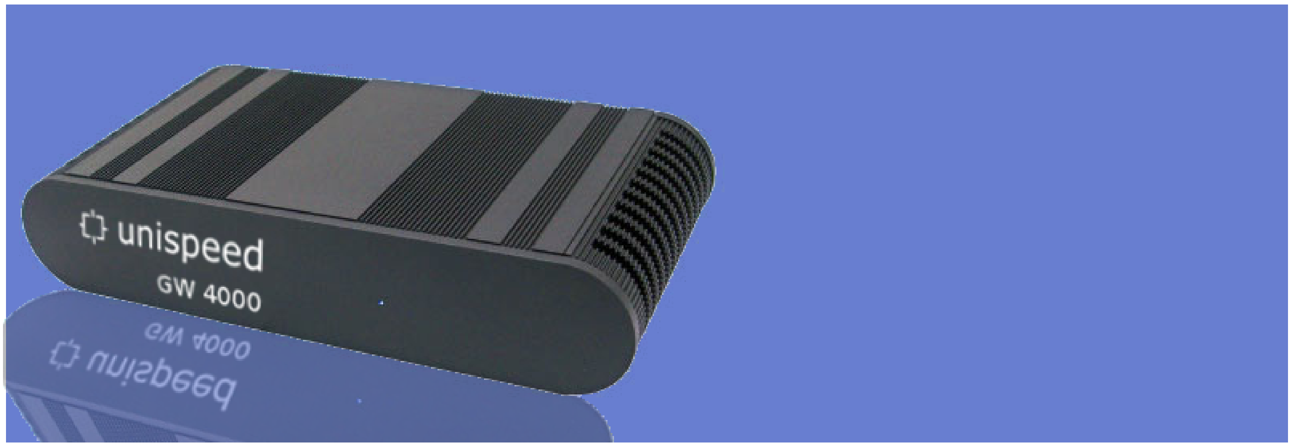


Table of Contents

1 Basic description of the system

The Unispeed Bluegate is designed to facilitate seamless installation and operation of commercial NAT networks. The system is in use at a great number of Hotels, Internet cafés, housing areas and public networks like airbases, schools, public transport and sporting arenas.

If pre installed on the network the Bluegate will function as a standard router gateway offering all required features to operate a small to medium guest network. The network operator will only have access to the components and modules required to configure the network unless authorised to perform data retention and content intercept on behalf of the authorities.

Tactical operation with the gateway in "sniffer" or "bypass" mode is also accommodated for.

2 Authorisation

From the "user admin" tab user authorisation credentials are defined.

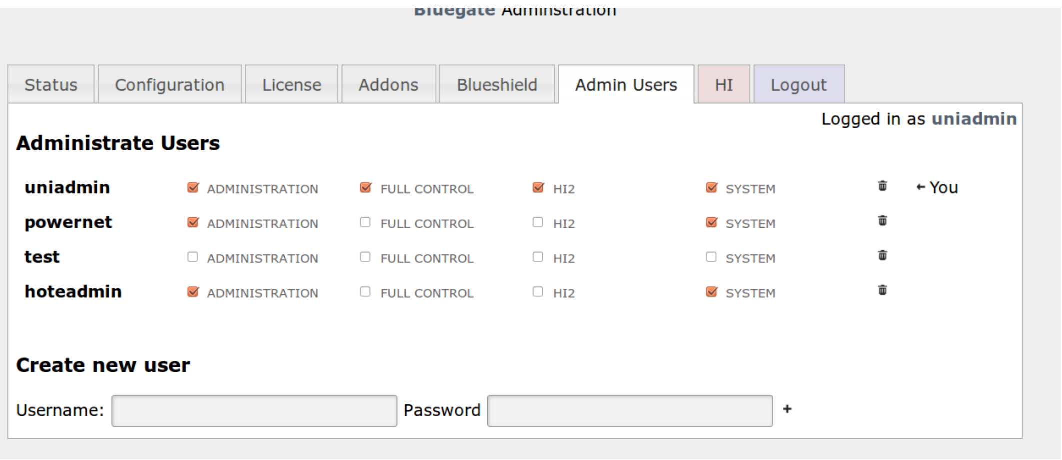
Operators will only have access to the modules that correspond to their authorisation level, and only the relevant modules will be visible in the interface according to the operators responsibility and authorisation level.

Operators with "Full control" rights can assign user privileges

Operators with "Administration" rights can exercise gateway configuration duties

Operators with "HI2" rights can access the data retention and lawful intercept interface

Operators with "System" rights can obtain internet through the gateway and view the status page



Logged in as **uniadmin**

Administrate Users

uniadmin	☑ ADMINISTRATION	☑ FULL CONTROL	☑ HI2	☑ SYSTEM	🗑	← You
powernet	☑ ADMINISTRATION	□ FULL CONTROL	□ HI2	☑ SYSTEM	🗑	
test	□ ADMINISTRATION	□ FULL CONTROL	□ HI2	□ SYSTEM	🗑	
hoteadmin	☑ ADMINISTRATION	□ FULL CONTROL	□ HI2	☑ SYSTEM	🗑	

Create new user

Username: □ Password □ +

3 Data retention (IP-CDR)

After installation the Bluegate natively starts recording IP call date, dhcp requests, user logins and activity.

Log files are consistently indexed and compressed to save storage and facilitate swift data extraction.

In Denmark and most other European countries, access to retained data and handover to law enforcement requires special authorisation by the police and a 24/7 contact point is required.

For most network providers a hosted data storage and handover solution with 24/7 contact point is generally favourable.

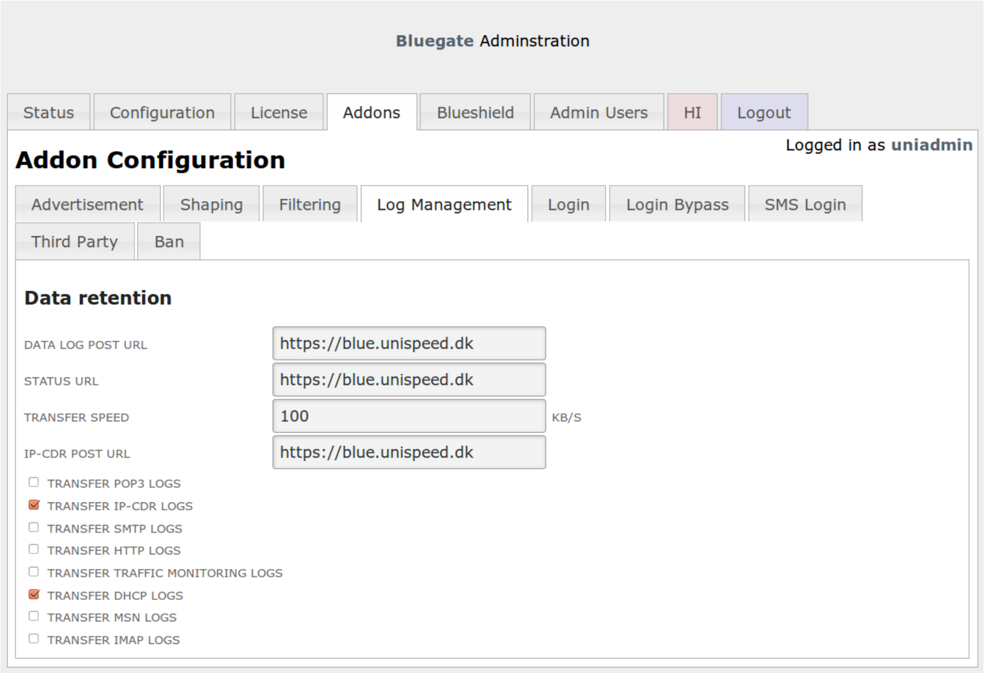
The transfer of data logs to the central Blue Shield component is automated in Bluegate and is configured from the Log management module.

If data transfer is desired simply add the host name of the data hosting server in the applicable fields.

"DATA LOG POST URL" is the host name of the server storing the DHCP and user access log files

"STATUS URL" is the host name of the server hosting the system monitoring and alert functions.

"IP-CDR POST URL" is the host name of the server storing the IP-CDR (session) logs



Addon Configuration

Data retention

DATA LOG POST URL: https://blue.unispeed.dk

STATUS URL: https://blue.unispeed.dk

TRANSFER SPEED: 100 KB/S

IP-CDR POST URL: https://blue.unispeed.dk

- ☐ TRANSFER POP3 LOGS
- ☑ TRANSFER IP-CDR LOGS
- ☐ TRANSFER SMTP LOGS
- ☐ TRANSFER HTTP LOGS
- ☐ TRANSFER TRAFFIC MONITORING LOGS
- ☑ TRANSFER DHCP LOGS
- ☐ TRANSFER MSN LOGS
- ☐ TRANSFER IMAP LOGS

More intrusive data recording is available and easily configured in the Log management module. Such can include continuous recording of WEB traffic, e-mail, IM etc.

If marked Bluegate will transfer such data logs to the "DATA LOG POST URL"

4 Data extracts

Authorised users with access to the Handover Interface (HI) can perform data retrieval from stored log files and provision content intercept directly through the Bluegate interface.

By default the log request system will deliver extracts from the user login data base, the DHCP log files and IP call data log files (sessions)

4.1 DHCP lookup

DHCP lookup accommodates for correlation between a client MAC number and the IP address assigned by the DHCP server. On option 82 enabled networks correlation between IP address, client hardware address, remote ID and circuit ID is available.

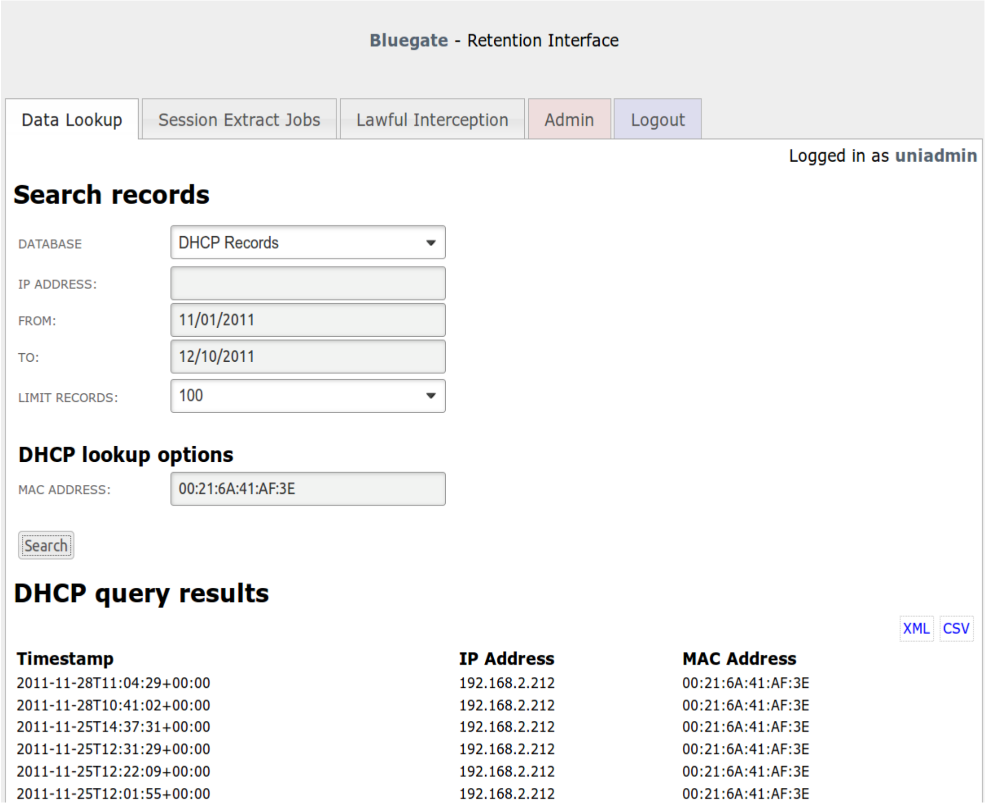
Particular on networks where users are not required to login, correlation between an assigned IP address and the client MAC address is the only means to bind the unique user to the retained call data.

To perform a DHCP lookup select Database > DHCP records

Three options are now available:

1. If entering an IP address Bluegate will retrieve the corresponding MAC addresses in the selected time frame
2. If entering a MAC address Bluegate will retrieve the corresponding IP addresses in the selected time frame
3. If no data is entered in either field Bluegate will extract and display all DHCP assignments in the selected time frame.

The extracted data is displayed on the screen and available for download in CSV and ETSI XML formats by clicking the XML or CSV download links.



Logged in as **uniadmin**

Search records

DATABASE	DHCP Records
IP ADDRESS:	
FROM:	11/01/2011
TO:	12/10/2011
LIMIT RECORDS:	100

DHCP lookup options

MAC ADDRESS:	00:21:6A:41:AF:3E

DHCP query results

Timestamp	IP Address	MAC Address
2011-11-28T11:04:29+00:00	192.168.2.212	00:21:6A:41:AF:3E
2011-11-28T10:41:02+00:00	192.168.2.212	00:21:6A:41:AF:3E
2011-11-25T14:37:31+00:00	192.168.2.212	00:21:6A:41:AF:3E
2011-11-25T12:31:29+00:00	192.168.2.212	00:21:6A:41:AF:3E
2011-11-25T12:22:09+00:00	192.168.2.212	00:21:6A:41:AF:3E
2011-11-25T12:01:55+00:00	192.168.2.212	00:21:6A:41:AF:3E

4.2 Logins extract (users)

On network where user login and authorisation is required Bluegate stores all login data communicated with the access server.

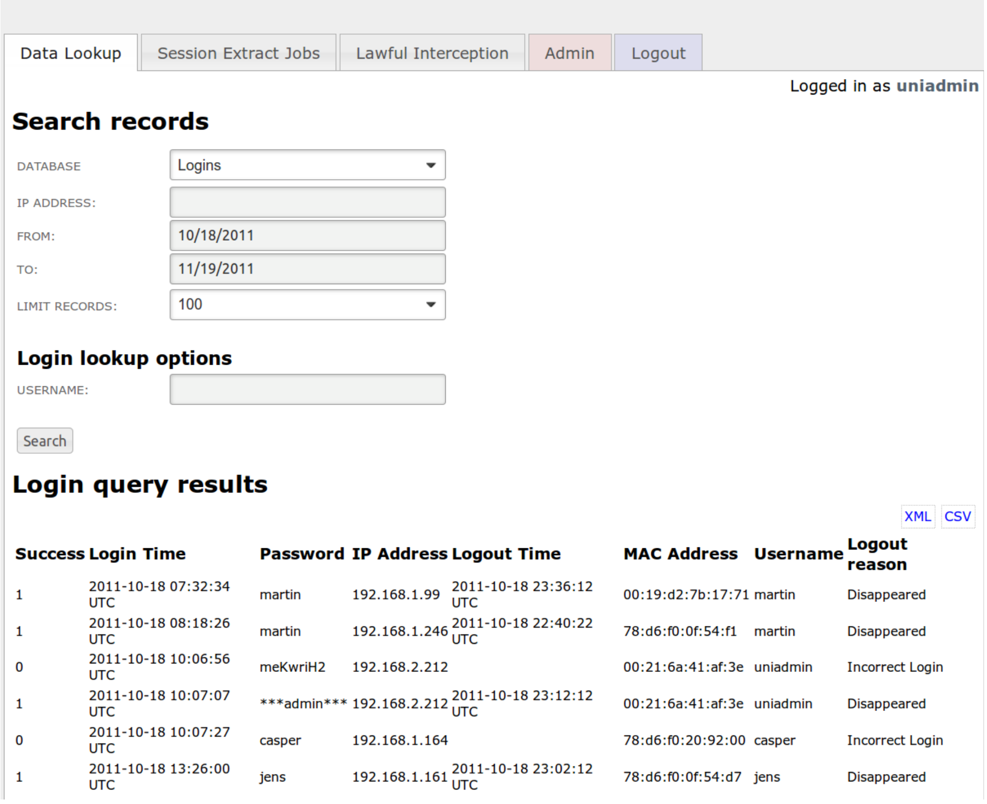
The retained data includes: Login and logout times, user name and password, MAC address and assigned IP address, whether the login was successful and the logout reason.

To perform a user lookup select Database > Logins

Three options are now available:

4. If entering an IP address Bluegate will retrieve the corresponding logins and user ID's and in the selected time frame
5. If entering a User ID Bluegate will retrieve the corresponding IP addresses in the selected time frame
6. If no data is entered in either field Bluegate will extract and display all user login and logout transactions in the selected time frame.

The extracted data is displayed on the screen and available for download in CSV and ETSI XML formats by clicking the XML or CSV download links.



Logged in as **uniadmin**

Search records

DATABASE	Logins
IP ADDRESS:	
FROM:	10/18/2011
TO:	11/19/2011
LIMIT RECORDS:	100

Login lookup options

USERNAME:

Login query results

Success	Login Time	Password	IP Address	Logout Time	MAC Address	Username	Logout reason
1	2011-10-18 07:32:34 UTC	martin	192.168.1.99	2011-10-18 23:36:12 UTC	00:19:d2:7b:17:71	martin	Disappeared
1	2011-10-18 08:18:26 UTC	martin	192.168.1.246	2011-10-18 22:40:22 UTC	78:d6:f0:0f:54:f1	martin	Disappeared
0	2011-10-18 10:06:56 UTC	meKwriH2	192.168.2.212		00:21:6a:41:af:3e	uniadmin	Incorrect Login
1	2011-10-18 10:07:07 UTC	***admin***	192.168.2.212	2011-10-18 23:12:12 UTC	00:21:6a:41:af:3e	uniadmin	Disappeared
0	2011-10-18 10:07:27 UTC	casper	192.168.1.164		78:d6:f0:20:92:00	casper	Incorrect Login
1	2011-10-18 13:26:00 UTC	jens	192.168.1.161	2011-10-18 23:02:12 UTC	78:d6:f0:0f:54:d7	jens	Disappeared

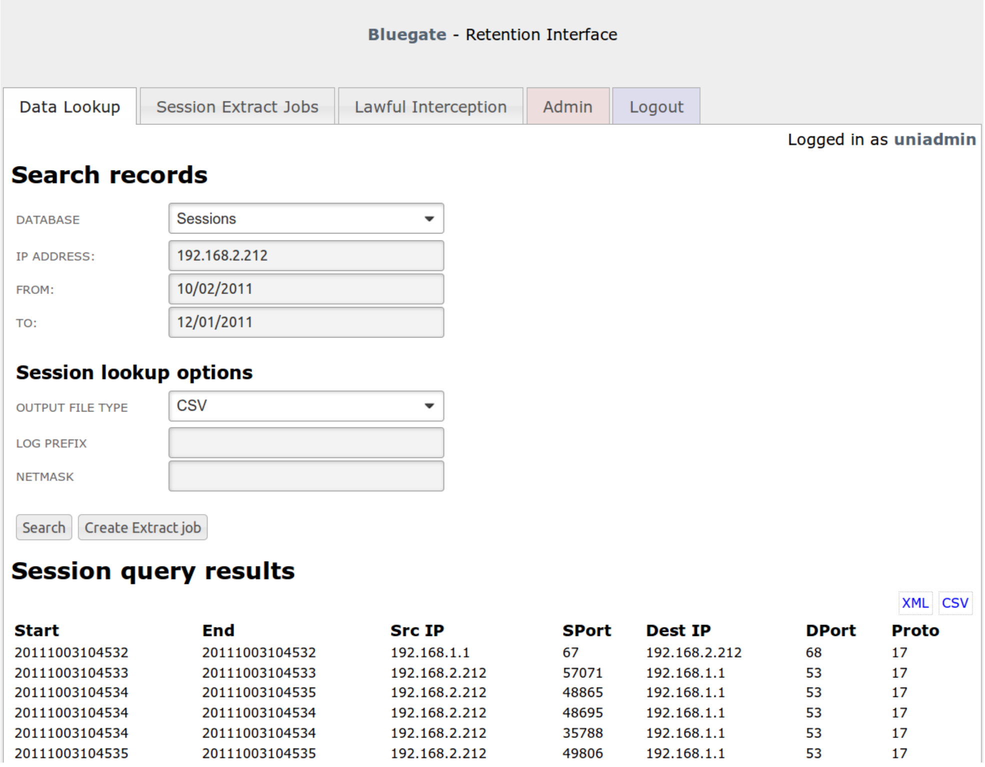
4.3 IP-CDR extract (sessions)

IP-CDR (session data) is extracted by a highly optimised data query system, capable of carving through millions of records in a few seconds.

Extracts are available for both source IP's and destination IP's over any given time frame, and ranges of IP addresses by setting the netmarsk.

A data search functionality is provided to verify if any data is present for the targeted IP address. The search functionality will extract and display the first 100 records in the data set.

To acquire all data from a targeted IP address the "Create Extract job" should be used.



Logged in as **uniadmin**

Search records

DATABASE: Sessions

IP ADDRESS: 192.168.2.212

FROM: 10/02/2011

TO: 12/01/2011

Session lookup options

OUTPUT FILE TYPE: CSV

LOG PREFIX:

NETMASK:

Session query results

Start	End	Src IP	SPort	Dest IP	DPort	Proto
20111003104532	20111003104532	192.168.1.1	67	192.168.2.212	68	17
20111003104533	20111003104533	192.168.2.212	57071	192.168.1.1	53	17
20111003104534	20111003104535	192.168.2.212	48865	192.168.1.1	53	17
20111003104534	20111003104534	192.168.2.212	48695	192.168.1.1	53	17
20111003104534	20111003104534	192.168.2.212	35788	192.168.1.1	53	17
20111003104535	20111003104535	192.168.2.212	49806	192.168.1.1	53	17

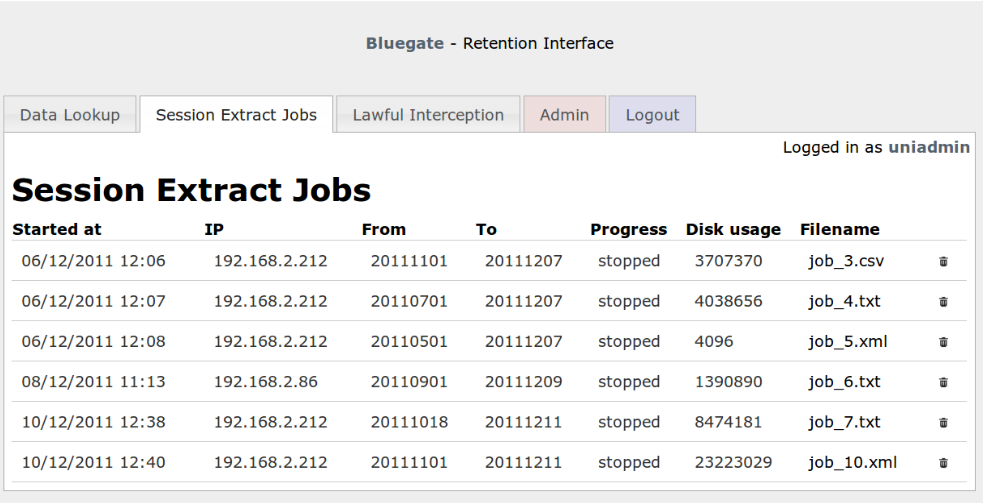
Session lookup options include:

1. The "output file type", CSV, ETSI XML or Plain text
2. The "Log prefix" is used if Bluegate is retaining data from multiple networks and the retention system is set to assign different prefix to the log files retained from each network. If the field is left blank Bluegate will extract data from all log files regardless of the file prefix.
3. "Netmask" is set to retrieve data from a range of IP's or an entire subnet.

When the "Create Extract job" button is clicked the extract job is initiated and the operator is referred to the Session Extract job status page.

The status page list details about the running and completed jobs, the size and their status.

From The status page data completed extract jobs can be downloaded and deleted.



Logged in as **uniadmin**

Session Extract Jobs

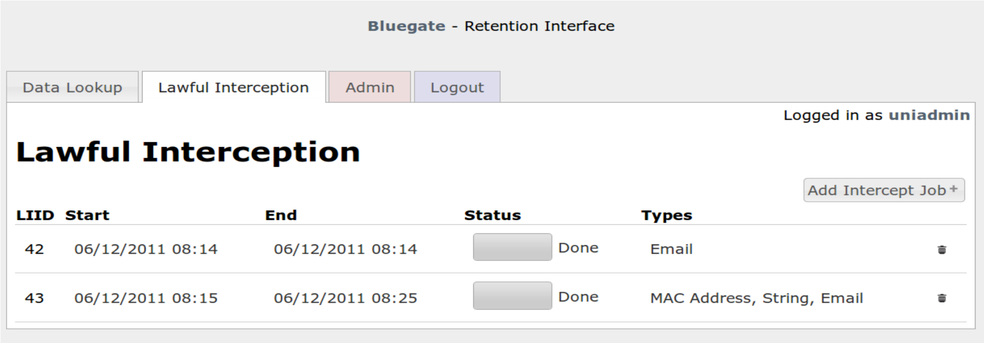
Started at	IP	From	To	Progress	Disk usage	Filename	
06/12/2011 12:06	192.168.2.212	20111101	20111207	stopped	3707370	job_3.csv	🗑
06/12/2011 12:07	192.168.2.212	20110701	20111207	stopped	4038656	job_4.txt	🗑
06/12/2011 12:08	192.168.2.212	20110501	20111207	stopped	4096	job_5.xml	🗑
08/12/2011 11:13	192.168.2.86	20110901	20111209	stopped	1390890	job_6.txt	🗑
10/12/2011 12:38	192.168.2.212	20111018	20111211	stopped	8474181	job_7.txt	🗑
10/12/2011 12:40	192.168.2.212	20111101	20111211	stopped	23223029	job_10.xml	🗑

5 Content interception (LI)

The content intercept module enables the operator to provision intercepts targeting any user on the network.

When accessing the module a summery of current intercept jobs is shown.

The operator can add new intercept job to the command cue via the "Add Intercept Job" button.



Logged in as **uniadmin**

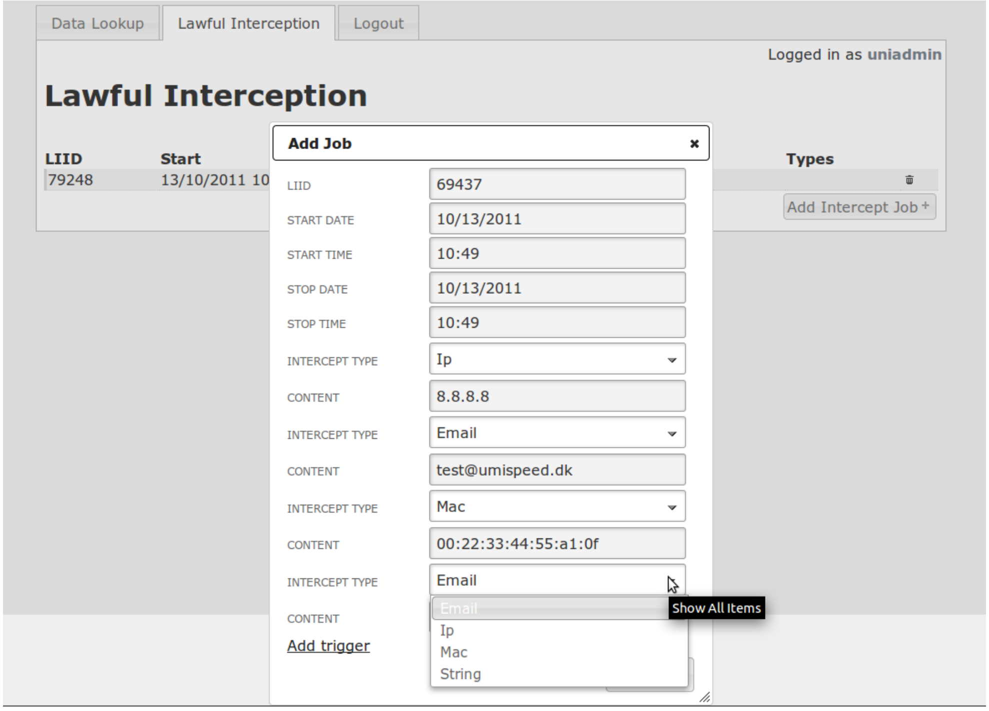
Lawful Interception

LIID	Start	End	Status	Types
42	06/12/2011 08:14	06/12/2011 08:14	Done	Email
43	06/12/2011 08:15	06/12/2011 08:25	Done	MAC Address, String, Email

The Content intercept functionality enables the operator to target users using different "triggers"

The "triggers" include IP address (IPv4 and IPv6), Mac address, E-mail addresses and "content strings"

Several triggers can be active for the same intercept job defined by the assigned LI number



Logged in as **uniadmin**

Lawful Interception

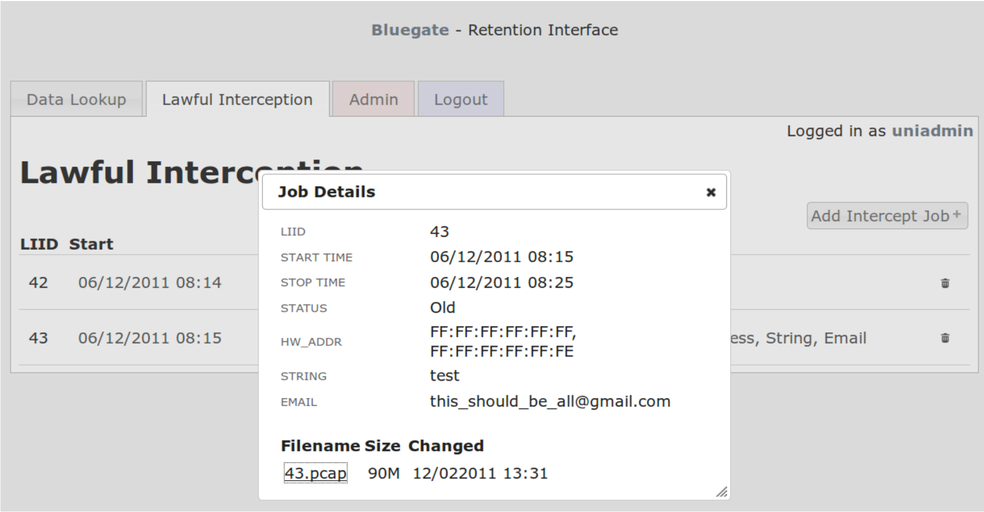
LIID	Start	Types
79248	13/10/2011 10	

Add Job

LIID	69437
START DATE	10/13/2011
START TIME	10:49
STOP DATE	10/13/2011
STOP TIME	10:49
INTERCEPT TYPE	Ip
CONTENT	8.8.8.8
INTERCEPT TYPE	Email
CONTENT	test@umispeed.dk
INTERCEPT TYPE	Mac
CONTENT	00:22:33:44:55:a1:0f
INTERCEPT TYPE	Email
CONTENT	

To create a content intercept job click the "Add Intercept job" button and set the time frame and applicable triggers. Each intercept is automatically assigned a LI nr. (Lawful intercept number) if not set by the operator.

The content files are available for download in Pcap format. The content files are named by the respective LI number and retrieved by clicking the file name



Lawful Interc

LIID	Start	
42	06/12/2011 08:14	
43	06/12/2011 08:15	ess, String, Email

Job Details

LIID	43
START TIME	06/12/2011 08:15
STOP TIME	06/12/2011 08:25
STATUS	Old
HW_ADDR	FF:FF:FF:FF:FF:FF, FF:FF:FF:FF:FF:FE
STRING	test
EMAIL	this_should_be_all@gmail.com

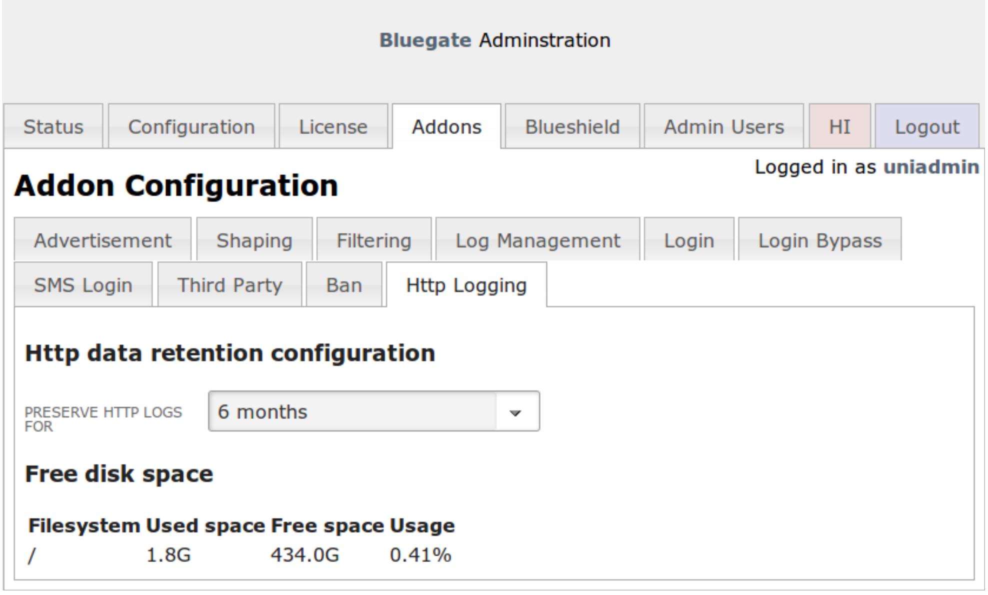
Filename	Size	Changed
43.pcap	90M	12/022011 13:31

6 Web visit & DNS tracking (Http inspect)

The Web and DNS tracking module is provided for operator who wish to track visits to web sides including deep links. The module blends data from the HTTP and DNS extractors with the unique user ID, if available and inserts the records into the data base.

From the Addons > Http Logging menu the time to preserve records can be selected.

A disk space counter is provided showing the currently **Used** and **Free** disk space on the unit.



Addon Configuration

Http data retention configuration

PRESERVE HTTP LOGS FOR: 6 months

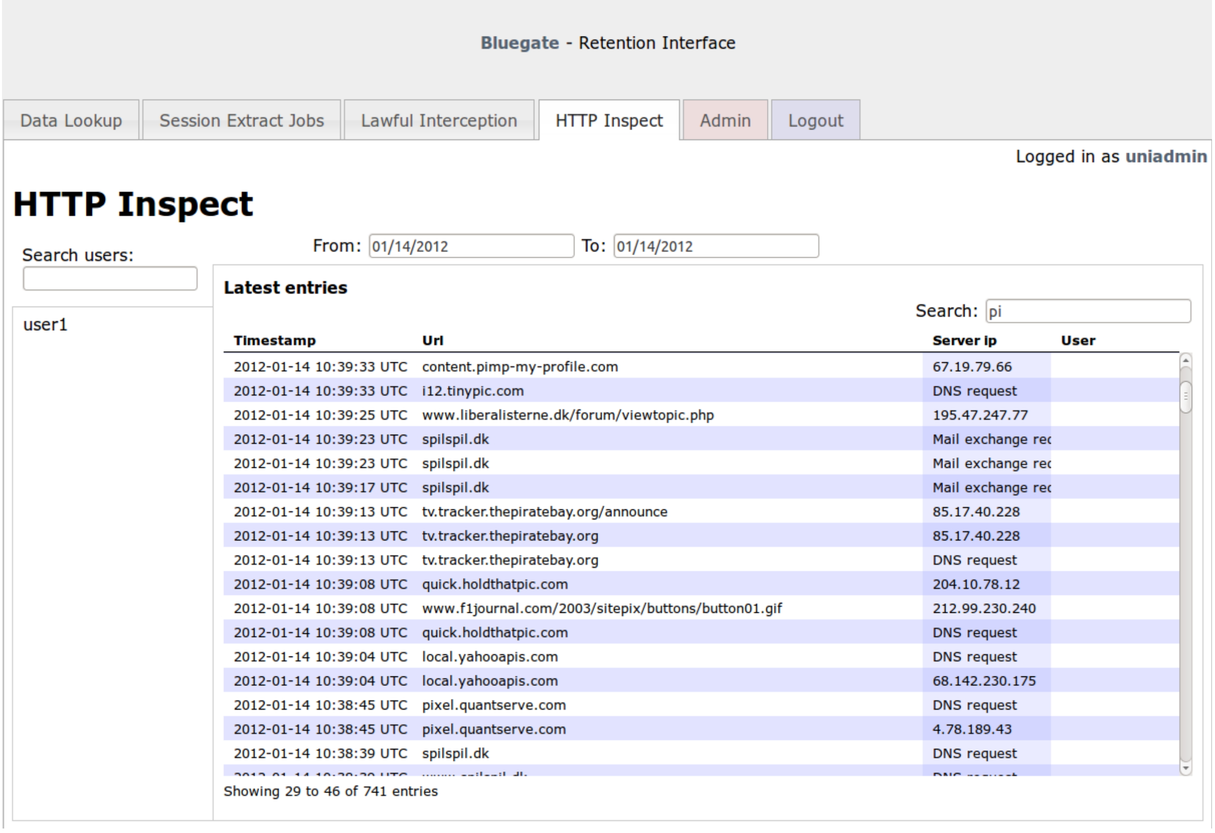
Free disk space

Filesystem	Used space	Free space	Usage
/	1.8G	434.0G	0.41%

The HTTP inspect module allow the operator to swiftly view web visits and DNS queries for all users of the network or limited by a single user.

Search functions are provided to search users by User name and the shown records can be limited by user and date interval.

A URL record "free text search" filters records seeming-less as the operator enters search strings.



Logged in as **uniadmin**

HTTP Inspect

Search users:

user1

From: 01/14/2012 To: 01/14/2012

Latest entries

Search: pi

Timestamp	Url	Server ip	User
2012-01-14 10:39:33 UTC	content.pimp-my-profile.com	67.19.79.66	
2012-01-14 10:39:33 UTC	i12.tinypic.com	DNS request	
2012-01-14 10:39:25 UTC	www.liberalisterne.dk/forum/viewtopic.php	195.47.247.77	
2012-01-14 10:39:23 UTC	spilspil.dk	Mail exchange rec	
2012-01-14 10:39:23 UTC	spilspil.dk	Mail exchange rec	
2012-01-14 10:39:17 UTC	spilspil.dk	Mail exchange rec	
2012-01-14 10:39:13 UTC	tv.tracker.thepiratebay.org/announce	85.17.40.228	
2012-01-14 10:39:13 UTC	tv.tracker.thepiratebay.org	85.17.40.228	
2012-01-14 10:39:13 UTC	tv.tracker.thepiratebay.org	DNS request	
2012-01-14 10:39:08 UTC	quick.holdthatpic.com	204.10.78.12	
2012-01-14 10:39:08 UTC	www.f1journal.com/2003/sitepix/buttons/button01.gif	212.99.230.240	
2012-01-14 10:39:08 UTC	quick.holdthatpic.com	DNS request	
2012-01-14 10:39:04 UTC	local.yahooapis.com	DNS request	
2012-01-14 10:39:04 UTC	local.yahooapis.com	68.142.230.175	
2012-01-14 10:38:45 UTC	pixel.quantserve.com	DNS request	
2012-01-14 10:38:45 UTC	pixel.quantserve.com	4.78.189.43	
2012-01-14 10:38:39 UTC	spilspil.dk	DNS request	
2012-01-14 10:38:39 UTC	www.spilspil.dk	DNS request	

Showing 29 to 46 of 741 entries