Lawful Interception

- Configuring Interception Settings
- Report Message Formats

The CommuniGate Pro Server implements Lawful Interception - the functionality that plays a crucial role in helping law enforcement agencies to combat criminal activity.

The Server Administrator can specify the names of CommuniGate Pro Accounts that should be monitored. All login operations with those Accounts, as well as all message manipulation activity in those Accounts is reported via E-mail messages sent to the specified addresses.

The reports can be sent to external programs via the PIPE module. Those programs can convert the reports generated with the CommuniGate Pro Server into the format required by the local law enforcement agencies.

Configuring Interception Settings

To configure the Interception settings, open the Intercept page in the Master realm of the WebAdmin Interface:

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Send Reports to</th>
<th>Login Signals</th>
<th>New Mail</th>
<th>Sent Mail</th>
<th>Mailbox Access</th>
<th>Partial Deleted</th>
<th>Mailbox Access</th>
<th>Partial Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:john.dripper@domain1.com">john.dripper@domain1.com</a></td>
<td>Sgt. Smith <a href="mailto:joe.smith@fbi.gov">joe.smith@fbi.gov</a></td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
</tr>
<tr>
<td><a href="mailto:jim.dripper@domain2.com">jim.dripper@domain2.com</a></td>
<td>&quot;law-report-n-type1&quot;@pipe</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
<td>✔️ ✔️</td>
</tr>
</tbody>
</table>

To add an element to list, fill the Account Name field in the last empty row and specify the E-mail address to send the reports to, select the checkboxes for the reports your want to generate, and click the Update button.

To remove an element, enter an empty line into the Account Name field and click the Update button.

In a Dynamic Cluster environment, the links for Server-wide and Cluster-wide pages appear. Enter the account names on the Cluster-wide page if accounts belong to Shared Domains served by the entire Cluster.

Note: If an element with an Account name has been added, removed, or modified, and the specified Account is currently in use, the changes will take effect on that Account within 1 minute.

If the Account name specified in an element is renamed, the element is automatically updated with the new Account name. If the Account name specified in an element is removed, the element is automatically removed.

Report Message Formats

The report messages are composed using the following formats.

Login Report
The Login report is sent when a monitored user logs into the System. The report message has the text/plain format and contains the information about:
- The Account (User) name.
The network (IP) address and the port the user logged in from
The Protocol used (POP, IMAP, WebUser, XMSS, SIP, XMPP, etc.)

Signal Report
The Signal report is sent when a monitored user sends or receives a Signal request or response. The report message has the text/plain format and contains the information about:
- The Account (User) name.
- The object type (Request or Response).
- The network (IP) address the object is received from.
- The Request or Response data.

New Message Report
The New message report is sent when a message is added to any Mailbox in the monitored Account.
The report message format is multipart/mixed. The first part has the text/plain format and contains the information about:
- The Account (User) name.
- The Action name (attached message stored)
- The Protocol, network (IP) address, and the port the user logged in from
- The Mailbox name
- The UID assigned to this message
- The time stamp
- The source of the message (incoming mail, copied from other Mailbox, appended, etc.)

The second part is a message/rfc822 part and it contains a copy of the message added to the Mailbox.

Mailbox Report
The Mailbox report is sent when a monitored user creates, renames, or removes a Mailbox. The report message has the text/plain format and contains the information about:
- The Account (User) name
- The Action (Mailbox created, Mailbox renamed, Mailbox removed)
- The Protocol, network (IP) address, and the port the user logged in from
- The Mailbox name and, for the rename operation, the new Mailbox name

Access Report, Partial Access
The Access report is sent when a monitored user reads or removes a message from one of the Account Mailboxes. The Partial Access report is sent when a monitored user reads a portion of a message (the message header, a message subpart, etc.) The report message has the text/plain format and contains the information about:
- The Account (User) name
- The Action (message read, messages deleted)
- The Protocol, network (IP) address, and the port the user logged in from
- The Mailbox name
- The UID(s) of the message(s) read or deleted. For partial access reports, the message portion specification is included, too

Sent Message Report
The Sent Message report is sent when a monitored user submits a new message. The report message format is multipart/mixed. The first part has the text/plain format and contains the information about:
- The Account (User) name
- The Action (message sent)
- The Protocol, network (IP) address, and the port the user logged in from
- The name of an authenticated user (if any); (self) means the monitored user name

The second part is an application/x-envelope part and contains a copy of the message envelope data.

The third part is a message/rfc822 part and contains a copy of the submitted message.

Deleted Message Report
The Deleted Message report is sent when a monitored user removes a message from some Mailbox. The report message format is `multipart/mixed`. The first part has the `text/plain` format and contains the information about:

- The Account (User) name
- The Action (attached message deleted)
- The Protocol, network (IP) address, and the port the user logged in from
- The Mailbox name
- The UID of the deleted message.
- The time stamp of the deleted message.

The second part is an `application/x-envelope` part and contains a copy of the message envelope data.

The third part is a `message/rfc822` part and contains a copy of the submitted message.