XEP-0377: Spam Reporting

Sam Whited
mailto:sam@samwhited.com
xmpp:sam@samwhited.com
https://blog.samwhited.com/

Guus der Kinderen
mailto:guus.der.kinderen@gmail.com
xmpp:guus.der.kinderen@igniterealtime.org

2025-04-09
Version 0.4.0

Status	Type	Short Name
Experimental	Standards Track	NOT_YET_ASSIGNED

This document specifies a mechanism by which users can report spam and other abuse to a server operator or other spam service.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

Many spam and abuse prevention techniques rely on users being able to report other users who are sending unwanted messages, or specific instances of abuse. Blocking Command (XEP-0191) [1] allows users to block spammers, but does not provide a mechanism for them to report a reason for the block to the server operator. This specification extends the blocking command to optionally provide an abuse report.

2 Background

This document extends the blocking command instead of providing a separate reporting IQ because we hypothesize that this will slightly lower the levels of false reports received by service operators. We have observed a common pattern on the internet where a user becomes mad at or disagrees with another user and begins harassing them by replying to or reporting their every comment even if it is not itself spam or abusive. However, this sort of behavior cannot continue if the harasser can no longer read the messages of the person they are stalking. Giving them a choice between their abusive behavior and being able to read their targets can possibly force them to break the cycle and only create valid reports.

3 Discovering Support

Entities that support Service Discovery (XEP-0030) [2] and abuse reporting using the blocking command as defined in this spec MUST respond to service discovery requests with a feature of 'urn:xmpp:reporting:1'. Support for this namespace also indicates support for the abuse reporting reasons defined in this document. For example, a response from a server that supports reporting and understands the abuse and spam reasons defined later in this specification might look like the following:

Listing 1: Service discovery information response

```
<iq from='example.net'
    id='ku6e51v3'
    to='kingclaudius@example.net/castle'
    type='result'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    <feature var='urn:xmpp:reporting:1'/>…

  </query>
</iq>
```

[1] XEP-0191: Blocking Command <https://xmpp.org/extensions/xep-0191.html>.
[2] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.

4 Payload

The payload for reporting abuse to the server takes the form of a <report/> qualified by the 'urn:xmpp:reporting:1' namespace (see Namespace Versioning regarding the possibility of incrementing the version number).

Listing 2: The most basic report payload

```
<report xmlns="urn:xmpp:reporting:1" reason="urn:xmpp:reporting:spam"/
    >
```

Abuse reports MUST include a reason for the report in the "reason" attribute.
This document defines the following reasons for a report:

urn:xmpp:reporting:spam Used for reporting a JID that is sending unwanted messages.

urn:xmpp:reporting:abuse Used for reporting general abuse.

Reports MAY contain a user provided message explaining or providing context about the reason for the report. See also the Internationalization Considerations section of this document.

Listing 3: Report with optional reason and text

```
<report xmlns="urn:xmpp:reporting:1" reason="urn:xmpp:reporting:spam">
  <text xml:lang="en">
    Never came trouble to my house like this.
  </text>
</report>
```

5 Report Processing Opt-in

Reports MAY contain user provided approval ('opt-in') for processing of the report. This document defines the following processing of a report:

report-origin Forward the report to the domain where the reported message originated.

third-party Forward the report to third-party entities that process reports for purposes including, but not limited to, the collection of statistics, analysis, and block list services.

To express approval of a certain type of processing, a <report-origin> and/or <third-party> element is added to the report.

Listing 4: Report with optional processing opt-in

```
<report xmlns="urn:xmpp:reporting:1" reason="urn:xmpp:reporting:spam">
  <text xml:lang="en">
    Never came trouble to my house like this.
  </text>
  <report-origin/>
  <third-party/>
</report>
```

Servers MAY ignore processing options when their implementation does not support the corresponding functionality. Servers MUST NOT process a report if the report that do not explicitly include the corresponding processing option.
Servers MAY anonymize any submission to third-party services to protect the identity of the reporter. Servers SHOULD NOT protect the identity of the reported entity (the alleged spammer/abuser), as it hurts processing without adding any significant protection: it is likely that the origin server can easily look up the original stanza in their local message archive anyway. Servers can anonymize the report by removing the 'to' attribute of the reported message.

6 Use with the Blocking Command

To send a report, a report payload MAY be inserted into an <item/> node sent as part of a request to block a spammer as defined in Blocking Command (XEP-0191) [3]. For example:

Listing 5: Report sent with blocking command

```
<iq from='juliet@example.com/chamber' type='set' id='block1'>
  <block xmlns='urn:xmpp:blocking'>
    <item jid='romeo@example.net'>
      <report xmlns="urn:xmpp:reporting:1" reason="
          urn:xmpp:reporting:abuse"/>
    </item>
  </block>
</iq>
```

Servers that receive a blocking command with a report MUST block the JID or return an error just as they would if no report were present. Servers then MAY take other actions based on the report, however, such actions are outside the scope of this document.
If the server supports Message Archive Management (XEP-0313) [4] the report MAY also include the stanza-id of specific messages being reported. This is done by including copies of each <stanza-id/> element that the user wishes to report as a child of the <report/> element. The stanza indicated by the provided stanza-id SHOULD be by the same JID being reported and blocked.

[3] XEP-0191: Blocking Command <https://xmpp.org/extensions/xep-0191.html>.
[4] XEP-0313: Message Archive Management <https://xmpp.org/extensions/xep-0313.html>.

Listing 6: Report sent with stanza IDs

```
<iq from='juliet@example.com/chamber' type='set' id='block1'>
  <block xmlns='urn:xmpp:blocking'>
    <item jid='romeo@example.net'>
      <report xmlns="urn:xmpp:reporting:1" reason="
          urn:xmpp:reporting:spam">
        <stanza-id xmlns='urn:xmpp:sid:0' by='romeo@example.net' id='
            28482-98726-73623'/>
        <stanza-id xmlns='urn:xmpp:sid:0' by='romeo@example.net' id='
            38383-38018-18385'/>
        <text xml:lang="en">
          Never came trouble to my house like this.
        </text>
      </report>
    </item>
  </block>
</iq>
```

7 Implementation Notes

Clients that support sending reports as part of the blocking command SHOULD expose interfaces to both block a JID without reporting it as abuse, and to block and report a JID.
The blocking command may be used to block multiple JIDs at the same time. When blocking multiple JIDs any abuse report only applies to a single JID. If the client allows selecting multiple JIDs in an abuse reporting dialog they SHOULD also allow choosing a separate reason, text, and messages for each JID. They MAY choose to only allow reporting a single JID at a time as well when the "block and report" dialog is accessed, and multiple JIDs when the "block" dialog is accessed.
Software clients may offer processing opt-in options to an end-user whenever they are reporting a message, but also could use a (configurable) default that is automatically applied to all reports issued by the client.

8 Internationalization Considerations

If one or more <text/> elements are present they SHOULD include 'xml:lang' attributes specifying the natural language of the XML character data.

9 Security Considerations

This document introduces no additional security considerations above and beyond those defined in the documents on which it depends.

10 IANA Considerations

This document requires no interaction with the Internet Assigned Numbers Authority (IANA) [5].

11 XMPP Registrar Considerations

11.1 Protocol Namespaces

This specification defines the following XML namespace:

- urn:xmpp:reporting:1

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar [6] shall add the foregoing namespace to the registry located at <https://xmpp.org/registrar/disco-features.html>, as described in Section 4 of XMPP Registrar Function (XEP-0053) [7].

11.2 Namespace Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

11.3 Abuse Reporting Registry

The XMPP Registrar shall maintain a registry of abuse report reasons and abuse report processing opt-in options. All abuse report reason and processing opt-in registrations shall be defined in separate specifications (not in this document). Application types defined within the XEP series MUST be registered with the XMPP Registrar, resulting in protocol URNs representing the reason.
In order to submit new values to this registry, the registrant shall define an XML fragment of the following form and either include it in the relevant XMPP Extension Protocol or send it to

[5] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

[6] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

[7] XEP-0053: XMPP Registrar Function <https://xmpp.org/extensions/xep-0053.html>.

the email address <registrar@xmpp.org>:

```
<reason>
  <name>The human-readable name of the abuse report reason.</name>
  <feature>URN representing the reason.</feature>
  <desc>A natural-language summary of the reason.</desc>
  <doc>
    The document in which the report reason is specified.
  </doc>
</reason>

<processing>
  <name>Element name representing the processing opt-in.</name>
  <namespace>A unique qualifier of the element name</namespace>
  <desc>A natural-language summary of the processing functionality.</
     desc>
  <doc>
    The document in which the report processing functionality is
       specified.
  </doc>
</processing>
```

11.4 Abuse Reporting Reasons

This specification defines the following abuse reporting reasons:

- urn:xmpp:reporting:spam
- urn:xmpp:reporting:abuse

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar [8] shall add the following definition to the abuse reporting reasons registry, as described in this document:

```
<reason>
  <name>spam</name>
  <feature>urn:xmpp:reporting:spam</feature>
  <desc>Used to report a JID that was sending spam messages.</desc>
  <doc>XEP-0377</doc>
</reason>
```

[8] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

```
<reason>
  <name>abuse</name>
  <feature>urn:xmpp:reporting:abuse</feature>
  <desc>Used to report general abuse that is not covered by a more
     specific reason.</desc>
  <doc>XEP-0377</doc>
</reason>
```

11.5 Abuse Reporting Processing

This specification defines the following processing opt-in identifiers:

- report-origin
- third-party

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar [9] shall add the following definition to the abuse report processing opt-in options registry, as described in this document:

```
<processing>
  <name>report-origin</name>
  <namespace>urn:xmpp:reporting:spam</namespace>
  <desc>Forward the report to the domain where the reported message
     originated.</desc>
  <doc>XEP-0377</doc>
</reason>
```

```
<reason>
  <name>third-party</name>
  <namespace>urn:xmpp:reporting:spam</namespace>
  <desc>
    Forward the report to third-party entities that process reports
       for purposes
    including, but not limited to, the collection of statistics,
       analysis, and
    block list services.
  </desc>
  <doc>XEP-0377</doc>
</reason>
```

[9] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

12 XML Schema

```
<?xml version='1.0' encoding='UTF-8'?>

<xs:schema
    xmlns:xs='http://www.w3.org/2001/XMLSchema'
    xmlns:sid='urn:xmpp:sid:0'
    xmlns='urn:xmpp:reporting:1'
    targetNamespace='urn:xmpp:reporting:1'
    elementFormDefault='qualified'>

  <xs:annotation>
    <xs:documentation>
      The protocol documented by this schema is defined in
      XEP-0377: https://xmpp.org/extensions/xep-0377.html
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace='http://www.w3.org/XML/1998/namespace'
      schemaLocation='https://www.w3.org/2009/01/xml.xsd'/>
  <xs:import namespace='urn:xmpp:sid:0'
      schemaLocation='xep-0359.xsd'/>

  <xs:element name='container'>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref='report' minOccurs='0' maxOccurs='unbounded'/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name='report'>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref='sid:stanza-id' minOccurs='0' maxOccurs='
            unbounded'/>
        <xs:element ref='text' minOccurs='0' maxOccurs='unbounded'/>
        <xs:element ref='report-origin' minOccurs='0' maxOccurs='1'/>
        <xs:element ref='third-party' minOccurs='0' maxOccurs='1'/>
      </xs:sequence>
      <xs:attribute name='reason' type='xs:string' use='required'/>
    </xs:complexType>
  </xs:element>

  <xs:element name='spam' type='empty'/>

  <xs:element name='abuse' type='empty'/>

  <xs:element name='text'>
```

```
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base='xs:string'>
          <xs:attribute ref="xml:lang" use="optional"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>

  <xs:element name='report-origin' type='empty'/>

  <xs:element name='third-party' type='empty'/>

  <xs:simpleType name='empty'>
    <xs:restriction base='xs:string'>
      <xs:enumeration value=''/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

13 Acknowledgements

Thanks to the participants of the XMPP Summit 20 in Austin, TX who discussed this XEP: specifically to Waqas Hussain, Kevin Smith, Lance Stout, and Matthew Wild. A special thanks to Daniel Wisnewski for giving the presentation that kicked off the anti-abuse work.
Thanks also (in no particular order) to Jonas Wielicki, Georg Lukas, Daniel Gultsch, and Matthew Wild for their feedback.