| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/Sasl.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/javax/security/sasl/RealmChoiceCallback.html)   [**NEXT CLASS**](http://docs.google.com/javax/security/sasl/SaslClient.html) | [**FRAMES**](http://docs.google.com/index.html?javax/security/sasl/Sasl.html)    [**NO FRAMES**](http://docs.google.com/Sasl.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | CONSTR | [METHOD](#2et92p0) | DETAIL: [FIELD](#3dy6vkm) | CONSTR | [METHOD](#1y810tw) |

## **javax.security.sasl**

Class Sasl

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **javax.security.sasl.Sasl**

public class **Sasl**extends [Object](http://docs.google.com/java/lang/Object.html)

A static class for creating SASL clients and servers.

This class defines the policy of how to locate, load, and instantiate SASL clients and servers.

For example, an application or library gets a SASL client by doing something like:

SaslClient sc = Sasl.createSaslClient(mechanisms,  
 authorizationId, protocol, serverName, props, callbackHandler);

It can then proceed to use the instance to create an authentication connection.

Similarly, a server gets a SASL server by using code that looks as follows:

SaslServer ss = Sasl.createSaslServer(mechanism,  
 protocol, serverName, props, callbackHandler);

**Since:** 1.5

| **Field Summary** | |
| --- | --- |
| static [String](http://docs.google.com/java/lang/String.html) | [**CREDENTIALS**](http://docs.google.com/javax/security/sasl/Sasl.html#CREDENTIALS)            The name of a property that specifies the credentials to use. |
| static [String](http://docs.google.com/java/lang/String.html) | [**MAX\_BUFFER**](http://docs.google.com/javax/security/sasl/Sasl.html#MAX_BUFFER)            The name of a property that specifies the maximum size of the receive buffer in bytes of SaslClient/SaslServer. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_FORWARD\_SECRECY**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_FORWARD_SECRECY)            The name of a property that specifies whether mechanisms that implement forward secrecy between sessions are required. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_NOACTIVE**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_NOACTIVE)            The name of a property that specifies whether mechanisms susceptible to active (non-dictionary) attacks are not permitted. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_NOANONYMOUS**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_NOANONYMOUS)            The name of a property that specifies whether mechanisms that accept anonymous login are not permitted. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_NODICTIONARY**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_NODICTIONARY)            The name of a property that specifies whether mechanisms susceptible to passive dictionary attacks are not permitted. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_NOPLAINTEXT**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_NOPLAINTEXT)            The name of a property that specifies whether mechanisms susceptible to simple plain passive attacks (e.g., "PLAIN") are not permitted. |
| static [String](http://docs.google.com/java/lang/String.html) | [**POLICY\_PASS\_CREDENTIALS**](http://docs.google.com/javax/security/sasl/Sasl.html#POLICY_PASS_CREDENTIALS)            The name of a property that specifies whether mechanisms that pass client credentials are required. |
| static [String](http://docs.google.com/java/lang/String.html) | [**QOP**](http://docs.google.com/javax/security/sasl/Sasl.html#QOP)            The name of a property that specifies the quality-of-protection to use. |
| static [String](http://docs.google.com/java/lang/String.html) | [**RAW\_SEND\_SIZE**](http://docs.google.com/javax/security/sasl/Sasl.html#RAW_SEND_SIZE)            The name of a property that specifies the maximum size of the raw send buffer in bytes of SaslClient/SaslServer. |
| static [String](http://docs.google.com/java/lang/String.html) | [**REUSE**](http://docs.google.com/javax/security/sasl/Sasl.html#REUSE)            The name of a property that specifies whether to reuse previously authenticated session information. |
| static [String](http://docs.google.com/java/lang/String.html) | [**SERVER\_AUTH**](http://docs.google.com/javax/security/sasl/Sasl.html#SERVER_AUTH)            The name of a property that specifies whether the server must authenticate to the client. |
| static [String](http://docs.google.com/java/lang/String.html) | [**STRENGTH**](http://docs.google.com/javax/security/sasl/Sasl.html#STRENGTH)            The name of a property that specifies the cipher strength to use. |

| **Method Summary** | |
| --- | --- |
| static [SaslClient](http://docs.google.com/javax/security/sasl/SaslClient.html) | [**createSaslClient**](http://docs.google.com/javax/security/sasl/Sasl.html#createSaslClient(java.lang.String%5B%5D,%20java.lang.String,%20java.lang.String,%20java.lang.String,%20java.util.Map,%20javax.security.auth.callback.CallbackHandler))([String](http://docs.google.com/java/lang/String.html)[] mechanisms, [String](http://docs.google.com/java/lang/String.html) authorizationId, [String](http://docs.google.com/java/lang/String.html) protocol, [String](http://docs.google.com/java/lang/String.html) serverName, [Map](http://docs.google.com/java/util/Map.html)<[String](http://docs.google.com/java/lang/String.html),?> props, [CallbackHandler](http://docs.google.com/javax/security/auth/callback/CallbackHandler.html) cbh)            Creates a SaslClient using the parameters supplied. |
| static [SaslServer](http://docs.google.com/javax/security/sasl/SaslServer.html) | [**createSaslServer**](http://docs.google.com/javax/security/sasl/Sasl.html#createSaslServer(java.lang.String,%20java.lang.String,%20java.lang.String,%20java.util.Map,%20javax.security.auth.callback.CallbackHandler))([String](http://docs.google.com/java/lang/String.html) mechanism, [String](http://docs.google.com/java/lang/String.html) protocol, [String](http://docs.google.com/java/lang/String.html) serverName, [Map](http://docs.google.com/java/util/Map.html)<[String](http://docs.google.com/java/lang/String.html),?> props, [CallbackHandler](http://docs.google.com/javax/security/auth/callback/CallbackHandler.html) cbh)            Creates a SaslServer for the specified mechanism. |
| static [Enumeration](http://docs.google.com/java/util/Enumeration.html)<[SaslClientFactory](http://docs.google.com/javax/security/sasl/SaslClientFactory.html)> | [**getSaslClientFactories**](http://docs.google.com/javax/security/sasl/Sasl.html#getSaslClientFactories())()            Gets an enumeration of known factories for producing SaslClient. |
| static [Enumeration](http://docs.google.com/java/util/Enumeration.html)<[SaslServerFactory](http://docs.google.com/javax/security/sasl/SaslServerFactory.html)> | [**getSaslServerFactories**](http://docs.google.com/javax/security/sasl/Sasl.html#getSaslServerFactories())()            Gets an enumeration of known factories for producing SaslServer. |

| **Methods inherited from class java.lang.**[**Object**](http://docs.google.com/java/lang/Object.html) |
| --- |
| [clone](http://docs.google.com/java/lang/Object.html#clone()), [equals](http://docs.google.com/java/lang/Object.html#equals(java.lang.Object)), [finalize](http://docs.google.com/java/lang/Object.html#finalize()), [getClass](http://docs.google.com/java/lang/Object.html#getClass()), [hashCode](http://docs.google.com/java/lang/Object.html#hashCode()), [notify](http://docs.google.com/java/lang/Object.html#notify()), [notifyAll](http://docs.google.com/java/lang/Object.html#notifyAll()), [toString](http://docs.google.com/java/lang/Object.html#toString()), [wait](http://docs.google.com/java/lang/Object.html#wait()), [wait](http://docs.google.com/java/lang/Object.html#wait(long)), [wait](http://docs.google.com/java/lang/Object.html#wait(long,%20int)) |

| **Field Detail** |
| --- |

### QOP

public static final [String](http://docs.google.com/java/lang/String.html) **QOP**

The name of a property that specifies the quality-of-protection to use. The property contains a comma-separated, ordered list of quality-of-protection values that the client or server is willing to support. A qop value is one of

* "auth" - authentication only
* "auth-int" - authentication plus integrity protection
* "auth-conf" - authentication plus integrity and confidentiality protection

The order of the list specifies the preference order of the client or server. If this property is absent, the default qop is "auth". The value of this constant is "javax.security.sasl.qop".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.QOP)

### STRENGTH

public static final [String](http://docs.google.com/java/lang/String.html) **STRENGTH**

The name of a property that specifies the cipher strength to use. The property contains a comma-separated, ordered list of cipher strength values that the client or server is willing to support. A strength value is one of

* "low"
* "medium"
* "high"

The order of the list specifies the preference order of the client or server. An implementation should allow configuration of the meaning of these values. An application may use the Java Cryptography Extension (JCE) with JCE-aware mechanisms to control the selection of cipher suites that match the strength values.

If this property is absent, the default strength is "high,medium,low". The value of this constant is "javax.security.sasl.strength".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.STRENGTH)

### SERVER\_AUTH

public static final [String](http://docs.google.com/java/lang/String.html) **SERVER\_AUTH**

The name of a property that specifies whether the server must authenticate to the client. The property contains "true" if the server must authenticate the to client; "false" otherwise. The default is "false".

The value of this constant is "javax.security.sasl.server.authentication".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.SERVER_AUTH)

### MAX\_BUFFER

public static final [String](http://docs.google.com/java/lang/String.html) **MAX\_BUFFER**

The name of a property that specifies the maximum size of the receive buffer in bytes of SaslClient/SaslServer. The property contains the string representation of an integer.

If this property is absent, the default size is defined by the mechanism.

The value of this constant is "javax.security.sasl.maxbuffer".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.MAX_BUFFER)

### RAW\_SEND\_SIZE

public static final [String](http://docs.google.com/java/lang/String.html) **RAW\_SEND\_SIZE**

The name of a property that specifies the maximum size of the raw send buffer in bytes of SaslClient/SaslServer. The property contains the string representation of an integer. The value of this property is negotiated between the client and server during the authentication exchange.

The value of this constant is "javax.security.sasl.rawsendsize".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.RAW_SEND_SIZE)

### REUSE

public static final [String](http://docs.google.com/java/lang/String.html) **REUSE**

The name of a property that specifies whether to reuse previously authenticated session information. The property contains "true" if the mechanism implementation may attempt to reuse previously authenticated session information; it contains "false" if the implementation must not reuse previously authenticated session information. A setting of "true" serves only as a hint: it does not necessarily entail actual reuse because reuse might not be possible due to a number of reasons, including, but not limited to, lack of mechanism support for reuse, expiration of reusable information, and the peer's refusal to support reuse. The property's default value is "false". The value of this constant is "javax.security.sasl.reuse". Note that all other parameters and properties required to create a SASL client/server instance must be provided regardless of whether this property has been supplied. That is, you cannot supply any less information in anticipation of reuse. Mechanism implementations that support reuse might allow customization of its implementation, for factors such as cache size, timeouts, and criteria for reuseability. Such customizations are implementation-dependent.

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.REUSE)

### POLICY\_NOPLAINTEXT

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_NOPLAINTEXT**

The name of a property that specifies whether mechanisms susceptible to simple plain passive attacks (e.g., "PLAIN") are not permitted. The property contains "true" if such mechanisms are not permitted; "false" if such mechanisms are permitted. The default is "false".

The value of this constant is "javax.security.sasl.policy.noplaintext".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_NOPLAINTEXT)

### POLICY\_NOACTIVE

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_NOACTIVE**

The name of a property that specifies whether mechanisms susceptible to active (non-dictionary) attacks are not permitted. The property contains "true" if mechanisms susceptible to active attacks are not permitted; "false" if such mechanisms are permitted. The default is "false".

The value of this constant is "javax.security.sasl.policy.noactive".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_NOACTIVE)

### POLICY\_NODICTIONARY

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_NODICTIONARY**

The name of a property that specifies whether mechanisms susceptible to passive dictionary attacks are not permitted. The property contains "true" if mechanisms susceptible to dictionary attacks are not permitted; "false" if such mechanisms are permitted. The default is "false".

The value of this constant is "javax.security.sasl.policy.nodictionary".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_NODICTIONARY)

### POLICY\_NOANONYMOUS

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_NOANONYMOUS**

The name of a property that specifies whether mechanisms that accept anonymous login are not permitted. The property contains "true" if mechanisms that accept anonymous login are not permitted; "false" if such mechanisms are permitted. The default is "false".

The value of this constant is "javax.security.sasl.policy.noanonymous".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_NOANONYMOUS)

### POLICY\_FORWARD\_SECRECY

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_FORWARD\_SECRECY**

The name of a property that specifies whether mechanisms that implement forward secrecy between sessions are required. Forward secrecy means that breaking into one session will not automatically provide information for breaking into future sessions. The property contains "true" if mechanisms that implement forward secrecy between sessions are required; "false" if such mechanisms are not required. The default is "false".

The value of this constant is "javax.security.sasl.policy.forward".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_FORWARD_SECRECY)

### POLICY\_PASS\_CREDENTIALS

public static final [String](http://docs.google.com/java/lang/String.html) **POLICY\_PASS\_CREDENTIALS**

The name of a property that specifies whether mechanisms that pass client credentials are required. The property contains "true" if mechanisms that pass client credentials are required; "false" if such mechanisms are not required. The default is "false".

The value of this constant is "javax.security.sasl.policy.credentials".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.POLICY_PASS_CREDENTIALS)

### CREDENTIALS

public static final [String](http://docs.google.com/java/lang/String.html) **CREDENTIALS**

The name of a property that specifies the credentials to use. The property contains a mechanism-specific Java credential object. Mechanism implementations may examine the value of this property to determine whether it is a class that they support. The property may be used to supply credentials to a mechanism that supports delegated authentication.

The value of this constant is "javax.security.sasl.credentials".

**See Also:**[Constant Field Values](http://docs.google.com/constant-values.html#javax.security.sasl.Sasl.CREDENTIALS)

| **Method Detail** |
| --- |

### createSaslClient

public static [SaslClient](http://docs.google.com/javax/security/sasl/SaslClient.html) **createSaslClient**([String](http://docs.google.com/java/lang/String.html)[] mechanisms,  
 [String](http://docs.google.com/java/lang/String.html) authorizationId,  
 [String](http://docs.google.com/java/lang/String.html) protocol,  
 [String](http://docs.google.com/java/lang/String.html) serverName,  
 [Map](http://docs.google.com/java/util/Map.html)<[String](http://docs.google.com/java/lang/String.html),?> props,  
 [CallbackHandler](http://docs.google.com/javax/security/auth/callback/CallbackHandler.html) cbh)  
 throws [SaslException](http://docs.google.com/javax/security/sasl/SaslException.html)

Creates a SaslClient using the parameters supplied. This method uses the [JCA Security Provider Framework](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#Provider), described in the "Java Cryptography Architecture API Specification & Reference", for locating and selecting a SaslClient implementation. First, it obtains an ordered list of SaslClientFactory instances from the registered security providers for the "SaslClientFactory" service and the specified SASL mechanism(s). It then invokes createSaslClient() on each factory instance on the list until one produces a non-null SaslClient instance. It returns the non-null SaslClient instance, or null if the search fails to produce a non-null SaslClient instance.

A security provider for SaslClientFactory registers with the JCA Security Provider Framework keys of the form

SaslClientFactory.*mechanism\_name*

and values that are class names of implementations of javax.security.sasl.SaslClientFactory. For example, a provider that contains a factory class, com.wiz.sasl.digest.ClientFactory, that supports the "DIGEST-MD5" mechanism would register the following entry with the JCA: SaslClientFactory.DIGEST-MD5 com.wiz.sasl.digest.ClientFactory

See the "Java Cryptography Architecture API Specification & Reference" for information about how to install and configure security service providers.

**Parameters:**mechanisms - The non-null list of mechanism names to try. Each is the IANA-registered name of a SASL mechanism. (e.g. "GSSAPI", "CRAM-MD5").authorizationId - The possibly null protocol-dependent identification to be used for authorization. If null or empty, the server derives an authorization ID from the client's authentication credentials. When the SASL authentication completes successfully, the specified entity is granted access.protocol - The non-null string name of the protocol for which the authentication is being performed (e.g., "ldap").serverName - The non-null fully-qualified host name of the server to authenticate to.props - The possibly null set of properties used to select the SASL mechanism and to configure the authentication exchange of the selected mechanism. For example, if props contains the Sasl.POLICY\_NOPLAINTEXT property with the value "true", then the selected SASL mechanism must not be susceptible to simple plain passive attacks. In addition to the standard properties declared in this class, other, possibly mechanism-specific, properties can be included. Properties not relevant to the selected mechanism are ignored, including any map entries with non-String keys.cbh - The possibly null callback handler to used by the SASL mechanisms to get further information from the application/library to complete the authentication. For example, a SASL mechanism might require the authentication ID, password and realm from the caller. The authentication ID is requested by using a NameCallback. The password is requested by using a PasswordCallback. The realm is requested by using a RealmChoiceCallback if there is a list of realms to choose from, and by using a RealmCallback if the realm must be entered. **Returns:**A possibly null SaslClient created using the parameters supplied. If null, cannot find a SaslClientFactory that will produce one. **Throws:** [SaslException](http://docs.google.com/javax/security/sasl/SaslException.html) - If cannot create a SaslClient because of an error.

### createSaslServer

public static [SaslServer](http://docs.google.com/javax/security/sasl/SaslServer.html) **createSaslServer**([String](http://docs.google.com/java/lang/String.html) mechanism,  
 [String](http://docs.google.com/java/lang/String.html) protocol,  
 [String](http://docs.google.com/java/lang/String.html) serverName,  
 [Map](http://docs.google.com/java/util/Map.html)<[String](http://docs.google.com/java/lang/String.html),?> props,  
 [CallbackHandler](http://docs.google.com/javax/security/auth/callback/CallbackHandler.html) cbh)  
 throws [SaslException](http://docs.google.com/javax/security/sasl/SaslException.html)

Creates a SaslServer for the specified mechanism. This method uses the [JCA Security Provider Framework](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#Provider), described in the "Java Cryptography Architecture API Specification & Reference", for locating and selecting a SaslServer implementation. First, it obtains an ordered list of SaslServerFactory instances from the registered security providers for the "SaslServerFactory" service and the specified mechanism. It then invokes createSaslServer() on each factory instance on the list until one produces a non-null SaslServer instance. It returns the non-null SaslServer instance, or null if the search fails to produce a non-null SaslServer instance.

A security provider for SaslServerFactory registers with the JCA Security Provider Framework keys of the form

SaslServerFactory.*mechanism\_name*

and values that are class names of implementations of javax.security.sasl.SaslServerFactory. For example, a provider that contains a factory class, com.wiz.sasl.digest.ServerFactory, that supports the "DIGEST-MD5" mechanism would register the following entry with the JCA: SaslServerFactory.DIGEST-MD5 com.wiz.sasl.digest.ServerFactory

See the "Java Cryptography Architecture API Specification & Reference" for information about how to install and configure security service providers.

**Parameters:**mechanism - The non-null mechanism name. It must be an IANA-registered name of a SASL mechanism. (e.g. "GSSAPI", "CRAM-MD5").protocol - The non-null string name of the protocol for which the authentication is being performed (e.g., "ldap").serverName - The non-null fully qualified host name of the server.props - The possibly null set of properties used to select the SASL mechanism and to configure the authentication exchange of the selected mechanism. For example, if props contains the Sasl.POLICY\_NOPLAINTEXT property with the value "true", then the selected SASL mechanism must not be susceptible to simple plain passive attacks. In addition to the standard properties declared in this class, other, possibly mechanism-specific, properties can be included. Properties not relevant to the selected mechanism are ignored, including any map entries with non-String keys.cbh - The possibly null callback handler to used by the SASL mechanisms to get further information from the application/library to complete the authentication. For example, a SASL mechanism might require the authentication ID, password and realm from the caller. The authentication ID is requested by using a NameCallback. The password is requested by using a PasswordCallback. The realm is requested by using a RealmChoiceCallback if there is a list of realms to choose from, and by using a RealmCallback if the realm must be entered. **Returns:**A possibly null SaslServer created using the parameters supplied. If null, cannot find a SaslServerFactory that will produce one. **Throws:** [SaslException](http://docs.google.com/javax/security/sasl/SaslException.html) - If cannot create a SaslServer because of an error.

### getSaslClientFactories

public static [Enumeration](http://docs.google.com/java/util/Enumeration.html)<[SaslClientFactory](http://docs.google.com/javax/security/sasl/SaslClientFactory.html)> **getSaslClientFactories**()

Gets an enumeration of known factories for producing SaslClient. This method uses the same algorithm for locating factories as createSaslClient().

**Returns:**A non-null enumeration of known factories for producing SaslClient.**See Also:**[createSaslClient(java.lang.String[], java.lang.String, java.lang.String, java.lang.String, java.util.Map, javax.security.auth.callback.CallbackHandler)](http://docs.google.com/javax/security/sasl/Sasl.html#createSaslClient(java.lang.String%5B%5D,%20java.lang.String,%20java.lang.String,%20java.lang.String,%20java.util.Map,%20javax.security.auth.callback.CallbackHandler))

### getSaslServerFactories

public static [Enumeration](http://docs.google.com/java/util/Enumeration.html)<[SaslServerFactory](http://docs.google.com/javax/security/sasl/SaslServerFactory.html)> **getSaslServerFactories**()

Gets an enumeration of known factories for producing SaslServer. This method uses the same algorithm for locating factories as createSaslServer().

**Returns:**A non-null enumeration of known factories for producing SaslServer.**See Also:**[createSaslServer(java.lang.String, java.lang.String, java.lang.String, java.util.Map, javax.security.auth.callback.CallbackHandler)](http://docs.google.com/javax/security/sasl/Sasl.html#createSaslServer(java.lang.String,%20java.lang.String,%20java.lang.String,%20java.util.Map,%20javax.security.auth.callback.CallbackHandler))

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/Sasl.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/javax/security/sasl/RealmChoiceCallback.html)   [**NEXT CLASS**](http://docs.google.com/javax/security/sasl/SaslClient.html) | [**FRAMES**](http://docs.google.com/index.html?javax/security/sasl/Sasl.html)    [**NO FRAMES**](http://docs.google.com/Sasl.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | CONSTR | [METHOD](#2et92p0) | DETAIL: [FIELD](#3dy6vkm) | CONSTR | [METHOD](#1y810tw) |

[Submit a bug or feature](http://bugs.sun.com/services/bugreport/index.jsp)

For further API reference and developer documentation, see [Java SE Developer Documentation](http://docs.google.com/webnotes/devdocs-vs-specs.html). That documentation contains more detailed, developer-targeted descriptions, with conceptual overviews, definitions of terms, workarounds, and working code examples.

Copyright 2006 Sun Microsystems, Inc. All rights reserved. Use is subject to [license terms](http://docs.google.com/legal/license.html). Also see the [documentation redistribution policy](http://java.sun.com/docs/redist.html).