

# CEPHX CONFIG REFERENCE

To identify users and protect against man-in-the-middle attacks, Ceph provides its cephx authentication system to authenticate users and daemons. See [Ceph Authentication & Authorization](#) for an introduction to cephx authentication. See the [Cephx Guide](#) for details on enabling/disabling, creating users and setting user capabilities.

## ENABLE/DISABLE AUTHENTICATION

Depending on the version, Ceph either enables or disables authentication by default. Use the following settings to expressly enable or disable Ceph. See [Ceph Authentication](#) for additional details.

**Authentication Enablement Defaults**

Ceph version 0.54 and earlier versions disable authentication by default. If you want to use Ceph authentication, you must specifically enable it for version 0.54 and earlier versions.

Ceph version 0.55 and later version enable authentication by default. If you do not want to use Ceph authentication, you must specifically disable it for versions 0.55 and later versions.

**Authentication Granularity**

Ceph version 0.50 and earlier versions use `auth_supported` to enable or disable authentication between the [Ceph Client](#) and the [Ceph Storage Cluster](#). Ceph authentication in earlier versions only authenticates users sending message traffic between the client and the cluster, so it does not have fine-grained control.

Ceph version 0.51 and later versions use fine-grained control, which allows you to require authentication of the client by the cluster (`auth_service required`), authentication of the cluster by the client (`auth_client required`), and authentication of a daemon within the cluster by another daemon within the cluster (`auth_cluster required`).

`auth_supported`

*Deprecated since version 0.51.*

**Description:** Indicates whether to use authentication. If not specified, it defaults to none, which means it is disabled.

**Type:** String

**Required:** No

**Default:** none

`auth_cluster required`

*New in version 0.51.*

**Description:** If enabled, the Ceph Storage Cluster daemons (i.e., `ceph-mon`, `ceph-osd`, and `ceph-mds`) must authenticate with each other. Valid settings are `cephx` or `none`.

**Type:** String

**Required:** No

**Default:** Version 0.54 and earlier none. Version 0.55 and later `cephx`.

`auth_service required`

*New in version 0.51.*

**Description:** If enabled, the Ceph Storage Cluster daemons require Ceph Clients to authenticate with the Ceph Storage Cluster in order to access Ceph services. Valid settings are `cephx` or `none`.

**Type:** String

**Required:** No

**Default:** Version 0.54 and earlier none. Version 0.55 and later `cephx`.

`auth_client required`

*New in version 0.51.*

**Description:** If enabled, the Ceph Client requires the Ceph Storage Cluster to authenticate with the Ceph Client. Valid settings are `cephx` or `none`.

**Type:** String

**Required:** No

**Default:** Version 0.54 and earlier none. Version 0.55 and later cephx.

## KEYS

When you run Ceph with authentication enabled, ceph administrative commands and Ceph Clients require authentication keys to access the Ceph Storage Cluster.

The most common way to provide these keys to the ceph administrative commands and clients is to include a Ceph keyring under the `/etc/ceph` directory. For Cuttlefish and later releases using `ceph-deploy`, the filename is usually `ceph.client.admin.keyring` (or `$cluster.client.admin.keyring`). If you include the keyring under the `/etc/ceph` directory, you don't need to specify a keyring entry in your Ceph configuration file.

We recommend copying the Ceph Storage Cluster's keyring file to nodes where you will run administrative commands, because it contains the `client.admin` key.

You may use `ceph-deploy admin` to perform this task. See [Create an Admin Host](#) for details. To perform this step manually, execute the following:

```
sudo scp {user}@{ceph-cluster-host}:/etc/ceph/ceph.client.admin.keyring /etc/ceph/ceph.client.admin
```

**Tip:** Ensure the `ceph.keyring` file has appropriate permissions set (e.g., `chmod 644`) on your client machine.

You may specify the key itself in the Ceph configuration file using the `key` setting (not recommended), or a path to a keyfile using the `keyfile` setting.

### keyring

**Description:** The path to the keyring file.  
**Type:** String  
**Required:** No  
**Default:** `/etc/ceph/$cluster.$name.keyring,/etc/ceph/$cluster.keyring,/etc/ceph/keyring,/etc/ceph/keyring.bin`

### keyfile

**Description:** The path to a key file (i.e., a file containing only the key).  
**Type:** String  
**Required:** No  
**Default:** None

### key

**Description:** The key (i.e., the text string of the key itself). Not recommended.  
**Type:** String  
**Required:** No  
**Default:** None

## SIGNATURES

In Ceph Bobtail and subsequent versions, we prefer that Ceph authenticate all ongoing messages between the entities using the session key set up for that initial authentication. However, Argonaut and earlier Ceph daemons do not know how to perform ongoing message authentication. To maintain backward compatibility (e.g., running both Bobtail and Argonaut daemons in the same cluster), message signing is **off** by default. If you are running Bobtail or later daemons exclusively, configure Ceph to require signatures.

Like other parts of Ceph authentication, Ceph provides fine-grained control so you can enable/disable signatures for service messages between the client and Ceph, and you can enable/disable signatures for messages between Ceph daemons.

### ceph require signatures

**Description:** If set to `true`, Ceph requires signatures on all message traffic between the Ceph Client and the Ceph Storage Cluster, and between daemons comprising the Ceph Storage Cluster.  
**Type:** Boolean  
**Required:** No  
**Default:** `false`

### cephx cluster require signatures

**Description:** If set to true, Ceph requires signatures on all message traffic between Ceph daemons comprising the Ceph Storage Cluster.

**Type:** Boolean

**Required:** No

**Default:** false

cephx service require signatures

**Description:** If set to true, Ceph requires signatures on all message traffic between Ceph Clients and the Ceph Storage Cluster.

**Type:** Boolean

**Required:** No

**Default:** false

cephx sign messages

**Description:** If the Ceph version supports message signing, Ceph will sign all messages so they cannot be spoofed.

**Type:** Boolean

**Default:** true

## TIME TO LIVE

auth service ticket ttl

**Description:** When the Ceph Storage Cluster sends a Ceph Client a ticket for authentication, the Ceph Storage Cluster assigns the ticket a time to live.

**Type:** Double

**Default:** 60\*60