



Solution domain

Cloud Storage Getting started guide

Date	04/09/2014
Sensitivity	Confidential
Our reference	Click here to enter text.
Contact	Click here to enter text.
E-mail	Click here to enter text.

Table of contents

Table of contents.....	2
Cloud Storage Getting Started Guide	3
1. Ordering:.....	4
1.1 Subscribe to the storage service	4
2. Start using the Cloud Storage Service Portal:	5
3. Exploring the Storage Service console	6
4. Your Tokens and Token Groups view	6
4.1 Understanding tokens and token groups:.....	6
4.2 Storage Service authentication token definitions:.....	7
4.3 Who can create tokens and token groups?	8
4.4 Working with token groups.....	8
4.4.1 Add a token group.....	8
4.4.2 Edit a token group	9
4.4.3 Delete a token group.....	9
4.5 Working with tokens	9
4.5.1 Add a token.....	10
4.5.2 Edit a token.....	10
5. Working with the Activity Dashboard.....	10
5.1 Summary of usage.....	10
5.2 Historical usage	11

Cloud Storage Getting Started Guide

Thank your interest in our **Cloud Storage Service**.

Cloud Storage provides on-demand storage of data objects in a consumption based, pay-per-use billing model. Cloud Storage is a storage solution ideal for custom and packaged applications that need global access to dynamic quantities of unstructured content. The service is accessed using the EMC® Atmos™ application programming interface (API). This API allows you to directly integrate the service with custom applications or off-the-shelf packaged software.

This guide provides some basic information you'll need to start using the service.

Thank you,

The Proximus Cloud Storage Team

1. Ordering:

Once you're returned the completed and signed the order form to your contact person, Proximus will activate the Cloud Storage Service.

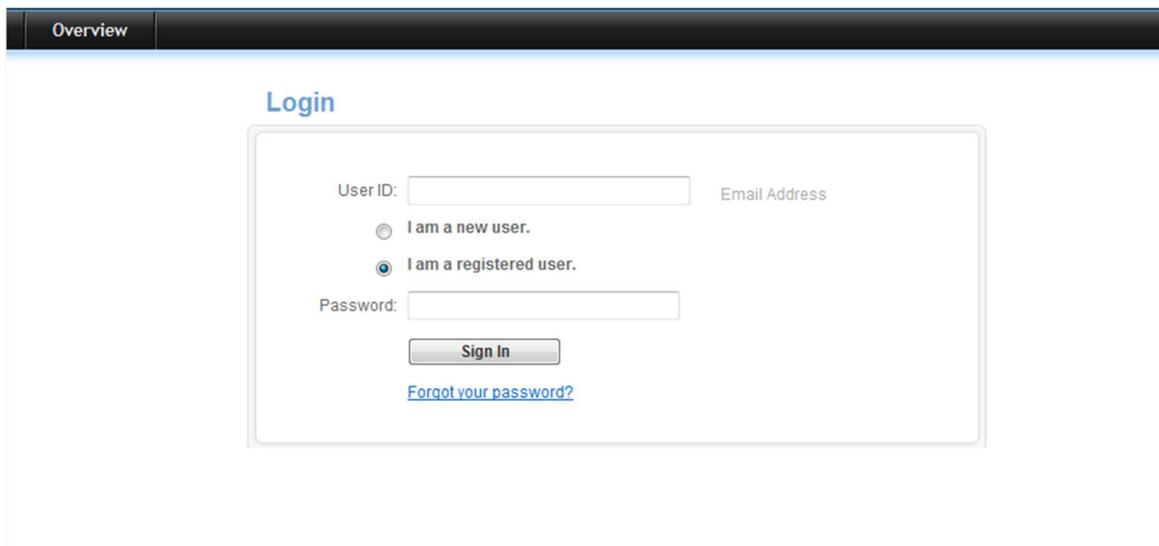
You'll receive an invitation by e-mail to accept the invitation to join the Cloud Service and to complete your registration via the Cloud Storage Portal. The correct address will be included in the welcome mail.

The Cloud Online user portal main web site provides sign up (and sign in) links, contains information that explains the Storage Service, tells you how to get started with cloud computing, provides links to additional resources.

1.1 Subscribe to the storage service

Follow these steps to subscribe to the Cloud Storage Service:

1. Click on the link in the e-mail invitation to accept the invitation.
2. Enter a valid email address, select the 'I am a new user' button, then click Sign Up. The User Registration page displays.



3. Enter the requested information on the User Registration page and click Continue. The User Registration Complete Thank You! page displays. You receive an email confirming successful creation of your account.
4. Click Sign Up for Storage Service.
5. The Sign Up for Storage Service - Terms and Conditions page displays. Review the Service Agreement, check I have read and agree to the Service Agreement, and click Continue.
6. The Login page re-appears and you receive an email approving your request. At this time you can login and begin managing your storage account

2. Start using the Cloud Storage Service Portal:

Once you have an account, you login using the email address and password that you specified during registration.

Click Manage Service (in the Service Offerings section of the page), and you are directed to the management screen (See screenshot below).

Storage Service

- > **Your Tokens & Groups**
- > Activity Dashboard

Your Token Groups & Tokens

View and manage authentication token groups and tokens

Token Groups

Token Group Name	Description
default	default token group
test	test

[Add Token Group...](#)

[Edit Permission](#)

Authentication tokens for: default

Token ID	Description
A271896937d1ece0e075	[REDACTED]
A271896937c8f2478e3b	[REDACTED]
A2718969371d37ce2efe	[REDACTED]
A271896937212fd4e108	default token

[Add Token...](#)

[Enable Token](#)

[Disable Token](#)

Token Details

Full Token ID:

Shared Secret:

[Reset Token](#)

3. Exploring the Storage Service console

After you sign in, you see a summary of the Storage Service offerings and today's disk usage (if you are currently subscribed).

To access the Storage Service console, click 'Manage Service' in the Storage Services summary area. The Storage Service area of the console includes these views:

- Your Tokens & Token Groups — Use to create, update, and delete token groups, and to create, enable, and disable authorization tokens.
- Activity Dashboard — Use to review resource usage.

To switch to a different page, simply click the link you want.

4. Your Tokens and Token Groups view

This section includes the following topics:

- "Understanding tokens and token groups"
- "Who can create tokens and token groups?"

4.1 Understanding tokens and token groups:

The Storage Service uses the authentication token security model. This means that any application attempting to use the service to access data must provide a valid authentication token/shared secret pair. You use the Tokens and Token Groups view to generate authentication token/shared secret pairs to use with the Storage Service.

Note: The Token Details containing the token ID and shared secret are viewed by selecting the Token ID for the Token Group. The details appear in a separate pane at the bottom of the page as shown in the Screenshot below.

Your Token Groups & Tokens

View and manage authentication token groups and tokens

Token Groups

Token Group Name	Description
default	default token group
test	test

Authentication tokens for: default

Token ID	Description
A271896937d1ece0e075	[REDACTED]
A271896937c8f247863b	[REDACTED]
A2718969371d370e2efe	[REDACTED]
A271896937212fd4e108	default token

Token Details

Full Token ID:

Shared Secret:

4.2 Storage Service authentication token definitions:

- **Subtenant ID** – A 32-character, randomly generated alphanumeric code that is associated with each Site ID. This code uniquely identifies your company to the EMC® Atmos™ platform that underlies Cloud Storage Service. An example Subtenant ID is: 5f8442b515ec402fb4f39ffab8c8179a
- **UID** – A unique identifier that you can assign for separate applications, organizations or individual users. When your account is first created, you will have one UID by default. Through the portal you have the option to create additional UIDs, allowing you to use separate credentials for authentication and access, as well as to itemize usage for internal charge-back purposes. Default UIDs are typically a derivation of your email address, such as: name@domain.be
- **Token ID** – A unique combination of your Subtenant ID and UID that consists of combining the two codes together, separated by a slash (/). Using the example Subtenant ID and UID from above, the Token ID would be: f8442b515ec402fb4f39ffab8c8179a/[name@domain.be](#)
- **Shared Secret** – A random string of 27 characters (base 64) that is uniquely associated with each UID. The shared secret is a 160-bit key that is used to produce a unique, encrypted digital signature for each API request. The signature is a Hash Message Authentication Code (HMAC) that combines various pieces of the message including the Token ID, type of request, date, address and other header information. An example Shared Secret is: MBqhzSzhZJCQHE9U4RBK9ze3K7U=.

4.3 Who can create tokens and token groups?

The Tokens and Token Groups view lets you perform different actions depending on your role, and the token groups you have been granted access to by the Account Manager.

If you are an **Account Manager** you can:

- Create and delete token groups.
- Complete all roles defined for a Token Group Manager.

Note: The Account Manager automatically has Token Group Manager Privileges.

If you are a **Token Group Manager**, you can:

- Edit existing token groups by changing the description, adding account users (as either Token Group Managers or Token Group Users), changing their access role, or removing them from the token group access list.
- For each token group, you can create new token IDs, and enable or disable them.

If you are a **Token Group Reader**, you can:

- View token groups and tokens for the token groups to which you were granted access by the Token Group Manager. When you create a Storage Service account, the system generates a default Token Group (called default) and a single authentication token.

4.4 Working with token groups

This section describes how a user with the appropriate permissions performs the following token group management tasks:

- “Add a token group”
- “Edit a token group”
- “Delete a token group”
- “Working with tokens”

4.4.1 Add a token group

Only an Account Manager can add a token group. Add a token group as follows:

1. Navigate to the Storage Service > Your Token & Groups view.
2. Click Add Token Group.
3. Fill in the fields as follows:

Field	Description
Token Group Name	Provide a meaningful name.
Description	Provide a meaningful description.

4. Click Edit Permission and in the User Permissions panel select the users in the Account Users role who you want to access this token group, then click Add. Change the users' role by selecting either Token Group Manager or Token Group User from the drop down list. The Token Group Access List identifies the users with permission to view or modify the Token Group and the tokens in that group.
5. Click the X to close the dialog when you complete adding/editing users.

4.4.2 Edit a token group

1. The description of a token group, access to a token group, and access roles can be modified by a Token Group Manager.
2. Navigate to the Storage Service > Your Tokens & Groups page and select the description of the Token Group to edit it.
3. Click Edit Permission and in the User Permissions panel select the users in the Account Users role who you want to access this token group, then click Add. Change the users' role by electing either Token Group Manager or Token Group User from the drop down list.
4. The Token Group Access List identifies the users with permission to view or modify the Token Group and the tokens in that group.
5. Remove a user from the access list by selecting the User ID and clicking Remove.
6. Click the X to close the dialog when you complete adding/editing users.

4.4.3 Delete a token group

Only an Account Manager can delete a Token Group. Delete the Token Group as follows:

1. Navigate to the Storage Service > Your Tokens & Groups page.
2. Select the Token Group you want to delete, then click Delete Token Group.
Note: The Delete Token Group button is only enabled if the token group has no tokens, and you are in the Account Manager role.
A warning dialog displays and asks you to verify whether to continue.
3. To confirm the deletion of the token group, click Yes. To cancel the deletion, click No.

4.5 Working with tokens

This section provides procedures for adding, editing, and disabling a token.

4.5.1 Add a token

Only a user with Token Group Manager privileges can add a token. Add a token as follows:

1. Navigate to the Storage Service > Your Token & Groups page.
2. Select the token group where you want to create the new token.
3. In the Authentication token for: panel, click Add Token. You are prompted for the description of the token.
4. Enter a description and click OK. The token is created and enabled. You can learn more about the token by double-clicking the Token ID and looking at the Token Details which appear at the bottom of the page. This will tell you the Full Token ID and the Shared Secret.
5. If you click Reset Token, the system generates a new shared secret for this token.

4.5.2 Edit a token

Only a user with Token Group Manager privileges can edit a token. Edit the description of a token or enable/disable the token as follows:

1. Navigate to the Storage Service > Your Token & Groups page.
2. Select the token group containing the token you wish to edit and select the token in the Authentication tokens for: pane. You can complete the enable/disable token and reset shared secrets as follows:
 - Click in the description field of the token to edit the description.
 - Enable the token by clicking Enable Token.
 - Disable the token by clicking Disable Token.
 - Click Reset Token to generate a new shared secret.

5. Working with the Activity Dashboard

The Activity Dashboard lets you view disk usage and bandwidth in a variety of ways. This section shows different views of disk usage shown in the Activity Dashboard.

- “Summary of usage”
- “Historical usage”

5.1 Summary of usage

Selecting the Summary tab from within the Activity Dashboard allows you to view a summary of usage aggregated for a selected time period (up to 90 days) using hourly weighted averages.

You can display data aggregated for all token groups, for a single token group, or for individual tokens. In addition, you can display disk usage metrics broken down by storage policy type.

These examples show usage for all token groups and storage policies. You can display the data in the following ways:

- “Disk usage by token group”
- “Bandwidth usage by token group”
- “Data grid by token group”

- “Disk usage by policy”
- “Bandwidth usage by access method”
- “Data grid by policy and access method”

Usage Guidelines

This section provides additional information about how the Activity Dashboard aggregates and displays data:

- Disk usage in the activity dashboard indicates average disk usage (based on an hourly weighted average) and includes user metadata (disk usage = disk (object data) usage + user metadata disk usage) unless otherwise stated.
- Disk usage does not include the amount of space taken up by mirrored copies, etc.
- The Activity Dashboard allows you to query the last 90 days of summary usage data and 31 days of historic usage data.
- For ease of use, pie charts with more than 10 elements do not display labels. Hover over the slice to view the label.

5.2 Historical usage

The Historical tab in the Activity Dashboard displays daily disk usage based on policy and bandwidth usage based on access method for your token groups for a period of up to 31 days. Set your start and end times and select an entry from the Groups field under the Options panel to filter the results displayed in the graphs.