Deploy Code42 apps

Overview

This article describes multiple strategies for deploying Code42 apps to user devices. You can integrate your apps with SSO, for example, without user intervention. The article is intended for administrators using device management tools like SCCM for Windows or Jamf Pro for Mac. This article provides:

- Introduction to Code42 app deployment and description of how it works in general.
- Recommendations and links to help you with specific environments and specific deployment strategies.

Considerations

- These instructions apply to the Code42 cloud. If you work in an on-premises Code42 environment, see Manage app installations in your Code42 environment (https://support.code42.com/Administrator/6/Planning_and_installing/Manage_app_installations_in_your_Code42_environment).
- To use these deployment tools, you need to sign in to your Code42 console as a user with the Customer Cloud Admin (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Roles_resources/Roles_reference#Customer_Cloud_Admin) role.
- In the Code42 federal environment, app installations must be deployed with a deployment policy (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference#Deployment_policies) to ensure the use of FIPS encryption in the Code42 app. Users cannot download the installation package from the Code42 console or an email message.
- Creating and using Code42 deployment policies requires familiarity with:
  - The authentication methods (https://support.code42.com/Administrator/Cloud/Configuring/Identity_management#Authentication) that your organizations use to manage users.
  - The process you use to distribute and install applications to user devices (typically a device management tool like SCCM for Windows or Jamf for Mac).

Incydr Professional and Enterprise

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environ...
How deployment works

Before selecting a deployment option, it helps to understand how deployment works from end-to-end:

2. From the policy view in the console, you copy the arguments for a Code42 app installer command.
3. You paste or import those install arguments into your device management software and push them to devices, along with Code42 app executables (https://support.code42.com/Administrator/Cloud/Code42_console_reference/App_Downloads_reference).
4. When install commands run on user devices, Code42 apps retrieve your policy from the Code42 cloud. If the Code42 app fails to connect to the Code42 cloud and find the policy, it will retry every 5 minutes until it succeeds or a user explicitly stops the process.
5. Code42 apps run your policy's detection script (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference) in order to determine usernames, home directories, and optionally, organizations.
6. After a policy automatically registers users, Code42 apps start monitoring data. If automatic registration fails for any reason, the Code42 app retries every hour. It retrieves the policy again and tries to register again until it succeeds.

Select a deployment option

The deployment options available vary with your Code42 environment's configuration:

- Whether you authenticate users with SSO or local authentication.
- Whether and how the deployment's username detection script matches usernames at devices with usernames in your authentication data.

Following are the most common deployment options:

- Registration with SSO
- Registration with local authentication

Registration with SSO

Use this option with SSO authentication set in the organization's Authentication (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#View_organization_details) tab.

- In the deployment policy's user detection script, SSO usernames are email addresses.
  You must customize the installer's detection script to adjust for that.
The Code42 cloud requires a custom script
Because user names in the Code42 cloud must be email addresses, deployments for connection to the Code42 cloud always require a customized user detection script.

• The deployment policy’s user detection script matches usernames at devices with usernames in SSO data. Usernames on endpoint devices must match usernames in SSO data, and usernames for the Code42 cloud must be email addresses. So you will need to modify the default user detection script to provide Code42 apps with usernames that match SSO usernames. See Step 2, below.

Mismatched usernames cause serious errors
If the detection script cannot provide a precise match with SSO data, Code42 creates a user that matches the device username.

Registration with local authentication
Use this option with Local authentication (authentication by the Code42 cloud) set in the organization's Authentication (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#View_organization_details) tab.

• Code42 passwords are hidden. The process described here generates Code42 passwords automatically. Those passwords are not available to users or administrators. To grant a user access to the Code42 console, an administrator needs to sign in to the Code42 console (https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview) and edit the user data (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Users_reference) to set a new password.
• You must customize your deployment policy's detection script to specify the user's email address. Usernames must be email addresses. In your Code42 deployment policy, you must modify the default user detection script. The script needs to take in device usernames and output email addresses. See Step 2, below.

The Code42 cloud requires a custom script
Because user names in the Code42 cloud must be email addresses, deployments for connection to the Code42 cloud always require a customized user detection script.

Step 1: Identify the deployment organization
A deployment policy (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference) belongs to an organization (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference). When you assign an organization to a deployment policy:

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environ...
• The organization's authentication method ([https://support.code42.com/Administrator/Cloud/Configuring/Configure_an_organization's_authentication_provider_settings](https://support.code42.com/Administrator/Cloud/Configuring/Configure_an_organization's_authentication_provider_settings)) is the policy's authentication method.
• When deployed Code42 apps install, users and devices become members of that organization.
• An organization has one deployment policy only. Child organizations do not inherit their parents' policies.

### Changing the organization can break the policy
Once an organization has a deployment policy, changing the organization's authentication method can easily break the policy. See [Deployment policies reference](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference).

Check configuration of the organization:

1. Sign in to the [Code42 console](https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview).
2. Select **Administration > Environment > Organizations**, and select an organization. **Note the organization name. You will need it later.**
3. Verify settings on the organization's [Authentication](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#View_organization_details) tab:
   1. Verify that the **Authentication method** setting is correct for your selected deployment option:
      - Registration with SSO: **SSO**
      - Registration with local authentication: **Local**
   2. If you need to change the settings, click the **Edit** icon.

### Step 2: Create the deployment policy

Define the deployment policy for the organization you identified in Step 1.

1. In the Code42 console, select **Administration > Agent Management > Deployment**.
2. Click **Create deployment policy**.
3. In **Deployment policy name** enter a name to identify the deployment policy. Since a deployment policy is associated with an organization, we recommend including the organization's name in the policy.
4. Select the **Registration organization** for the policy.
   *If your organization's name does not appear in the list, that organization already has a policy. You can edit or delete that existing policy.*
5. In **User detection scripts** select one or more operating systems that you will deploy Code42 apps to.
6. For each operating system you select, add a custom batch/bash script. Provide a script that identifies the username and home directory that the Code42 app will provide when it registers with your Code42 environment. For example scripts, see [https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment](https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment).
Deployment script and command reference for Incydr Basic and Advanced, CrashPlan Cloud, and other plans
(https://support.code42.com/Administrator/Cloud/Planning_and_installing/
Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference). The script must end by echoing the username and user home directory in accordance with your selected deployment option:

1. Registration with SSO:

   ```
   echo C42_USERNAME=<value>
   echo C42_USER_HOME=<value>
   ```

2. Registration with local authentication:

   ```
   echo C42_USERNAME=<email@address>
   echo C42_USER_HOME=<value>
   ```

7. Click **Create**.

   The policy is created.

8. In the **Details** tab, review the deployment policy and click **Edit** if you need to make changes:

   ◦ **Deployment properties** contain important pieces of information needed for the deployment and are placed in the deployment properties file:

     - **DEPLOYMENT_URL**: The Code42 cloud where the organization’s tenant resides.
     - **DEPLOYMENT_POLICY_TOKEN**: The policy’s authorization token.
     - **DEPLOYMENT_SECRET**: The authorization token for registration. The deployment secret (https://support.code42.com/Administrator/Cloud/Code42_console_reference/
Deployment_policies_reference#Deployment_secrets) authorizes the agent and limits the time in which an agent can register.

   ◦ **Command-line arguments (Windows)** displays the arguments format needed on Windows machines.

9. In the **Scripts** tab, review the user detection script and click **Edit** if you need to make changes. This script associates a username with the device, and can be customized to fit a number of deployment scenarios. For example scripts, see Deployment script and command reference for Incydr Basic and Advanced, CrashPlan Cloud, and other plans (https://support.code42.com/Administrator/Cloud/Planning_and_installing/

---

**Step 3: Deploy Code42 apps to user devices**

**Before you deploy to production**

**Test your deployment plans**

Before deploying Code42 apps to production devices, always test your entire process and all its scripts and files.

1. In the Code42 console, create at least one test organization.

2. Add several test users to that organization.

3. Connect test devices for those users to the network that includes your Code42 environment.
4. Deploy Code42 apps to the test devices and make sure they work as intended.

Verify that apps can connect by HTTPS

User devices must be able to reach the Code42 console by the HTTPS protocol. Check your protocol and port configuration:

- The URL must begin with https://
- Your firewalls must allow client requests to reach the Code42 console.

When you add a deployment policy to your Code42 cloud-based deployment, the URL auto-populates with the address. For example:

- United States:
  - US1: https://console.us.code42.com
  - US2: https://console.us2.crashplan.com
  - US3: https://console.gov.code42.com (Code42 federal environment only)
- Ireland:
  - EU1: https://console.ie.code42.com

Deploy to devices

Retrieve installation properties from your deployment policy as follows:

3. In the list of policies, select the policy you want to use.
4. Copy deployment properties, arguments, and scripts from the policy and place them in your device management software so they can be pushed to devices along with Code42 app executables (https://support.code42.com/Administrator/Cloud/Code42_console_reference/App_Downloads_reference).
5. Click Download properties file and place the deployment properties file in the following locations where it will be read on devices:

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environ...
Once the deployment is successful, the Code42 app is registered with Code42, and the Code42 app deletes the deployment properties file.

Step 4: Verify success

Check that deployments succeed by reviewing logs and the number of devices deployed to your organization.

Review logs

Review logs in the following file locations on the endpoints:

- Windows: C:\ProgramData\Code42-AAT\Data\logs\n- Mac: /Library/Application Support/Code42-AAT/Data/logs/
- Linux: /var/opt/code42-aat/data/logs

Check the number of devices deployed

3. Select the organization you deployed to.
4. At the top of the window, click the value under Devices.

   The number of devices listed for your org should match the number of devices you deployed Code42 apps to.

Incydr Basic and Advanced, CrashPlan Cloud, and other plans

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/

Updated: Sat, 25 Sep 2021 00:31:01 GMT

Powered by mindtouch
How deployment works

Before selecting a deployment option, it helps to understand how deployment works from end-to-end:


2. From the policy view in the console, you copy the arguments for a Code42 app installer command.

3. You paste or import those install arguments into your device management software and push them to devices, along with Code42 app executables (https://support.code42.com/Administrator/Cloud/Code42_console_reference/App_Downloads_reference).

4. When install commands run on user devices, Code42 apps retrieve your policy from the Code42 cloud.
   *If the Code42 app fails to connect to the Code42 cloud and find the policy, it will retry every 5 minutes until it succeeds or a user explicitly stops the process.*

5. Code42 apps run your policy's detection script (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference) in order to determine usernames, home directories, and optionally, organizations.

6. When a policy is configured to automatically register users, Code42 apps start security monitoring and backing up data without user intervention. Otherwise, users manually authenticate and register.
   *If automatic registration fails for any reason, the Code42 app retries every hour. It retrieves the policy again and tries to register again, until it succeeds or a user explicitly stops the process.*

Select a deployment option

The deployment options available vary with your Code42 environment's configuration:

- Whether you authenticate users with SSO or local authentication.
- Whether and how the deployment's **username detection script** matches usernames at devices with usernames in your authentication data.

Following are the most common deployment options:

- **Silent registration with SSO**
- **Silent registration with local authentication**
- **Manual registration**

Silent registration with SSO

New Code42 apps register automatically and start security monitoring and backups without user intervention. Use this option with SSO authentication and local directory services set in the organization's **Security** (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Security) tab.

- In the deployment's username detection script, SSO usernames are email addresses.
  You must customize the installer's detection script to adjust for that.
The Code42 cloud requires a custom script
Because user names in the Code42 cloud must be email addresses, deployments for connection to the Code42 cloud always require a customized user detection script.

- The deployment's username detection script matches usernames at devices with usernames in SSO data. Usernames on endpoint devices need to match usernames in SSO data, and usernames for the Code42 cloud must be email addresses. So you will need to modify the default user detection script to provide Code42 apps with usernames that match SSO usernames. See Step 2, below.

Mismatched usernames cause serious errors
If the detection script cannot provide a precise match with SSO data, Code42 creates a user that matches the device username. That user has no password, however, and cannot restore backup data or access the Code42 console. If you cannot create a reliable script, do not attempt silent deployment. See Manual registration instead.

Silent registration with local authentication
New Code42 apps register automatically and start backups without user intervention. Use this option with local authentication (authentication by the Code42 cloud) set in the organization's Security tab.

- Code42 passwords are hidden. The process described here generates Code42 passwords automatically. Those passwords are not available to users or administrators. To grant a user access to the Code42 app or the Code42 console, an administrator needs to sign in to the Code42 console and edit the user data to set a new password.

- You must customize your deployment's detection script to specify the user's email address. Usernames must be email addresses. In your Code42 deployment policy, you need to modify the default user detection script. The script needs to take in device usernames and output email addresses. See Step 2, below.

The Code42 cloud requires a custom script
Because user names in the Code42 cloud must be email addresses, deployments for connection to the Code42 cloud always require a customized user detection script.

Manual registration
Require users to manually sign in to the Code42 app. Use this option with:

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment
• Local authentication set in the organization's [Security](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Security) tab, and user-defined names and passwords.

• SSO.

### Step 1: Identify the deployment organization

A deployment policy belongs to an organization. When you [select](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference) or [create](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Add_a_new_organization) that organization:

- The organization's [authentication method](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Security) is the policy's authentication method.
- When deployed Code42 apps install, users and devices become members of that organization.
- An organization has one deployment policy only. Child organizations do not inherit their parents' policies.
- [Custom images and texts](https://support.code42.com/Administrator/Cloud/Configuring/Client_customizations) for Code42 apps also belong to organizations. You can define customizations before or after deployment.

---

**Changing the organization can break the policy**

Once an organization has a deployment policy, changing the organization’s authentication method can easily break the policy. See [Deployment policies reference](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference).

---

**Check configuration of the organization:**

1. Sign in to the [Code42 console](https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview).
2. Select **Administration > Environment > Organizations**, and select an organization. *Note the organization name; you will need it later.*
3. Verify settings on the [Security](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Security) tab:
   1. Click the action menu and select **Edit**.
   2. Select the [Security](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Organizations_reference#Security) tab and verify that the settings are correct for your selected deployment option:
      - Silent registration with SSO:
        - The **Authentication** must be **SSO**.
        - The **Directory service** must be **Local**.
      - Silent registration with local authentication:
        - The **Authentication** must be **Local**.
        - The **Directory service** must be blank.
Step 2: Create the deployment policy

Define the deployment policy for the organization you identified in Step 1.

1. In the Code42 console, select Administration > Client Management > Deployment.
2. Select Create New Deployment Policy or Create deployment policy.
   The prompt differs depending on whether you see the initial welcome screen or your list of existing policies.
3. Enter a Deployment policy name to describe this policy.
4. At Registration organization select the organization you identified at Step 1, above.
   If your organization’s name does not appear in the menu, that organization already has a policy.
   You can edit (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference#Create_or_edit_deployment_policy) or delete (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference#Deployment_policies) that existing policy.
5. At Do you want to automatically register users?, verify that the settings are correct for your selected deployment option:
   1. Silent registration with SSO: Yes
   2. Silent registration with local authentication: Yes
   3. Manual registration: No
6. At Select one or more operating systems, select the systems you will deploy Code42 apps to.
7. For each operating system you select, select Add a custom batch/bash script
   Provide a script that identifies the username and home directory that the Code42 app will provide when it registers with your Code42 environment. For details, see the script reference (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference).
   The script must end by echoing the username and user home directory in accordance with your selected deployment option:
- Silent registration with SSO:

```
echo C42_USERNAME=<value>
echo C42_USER_HOME=<value>
```

- Silent registration with local authentication:

```
echo C42_USERNAME=<email@address.tld>
echo C42_USER_HOME=<value>
```

- Manual registration

```
echo C42_USERNAME=<value>
echo C42_USER_HOME=<value>
```

8. At **Do your clients need a proxy URL to connect to your Code42 authority?**, select **No** or **Yes**, depending on what you determined at Step 1, above.

9. At **Launch desktop app after initial install?**, select the correct value for your selected deployment option:
   - Silent registration with SSO: **No**
   - Silent registration with local authentication: **No**
   - Manual registration: **Yes**

10. Click **Create**.
    
    You can view the policy and copy the installation properties at any time.

---

**To disable a deployment policy, generate a new deployment token**

As a security measure, you can disable a deployment policy at any time by **generating a new deployment token** ([https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference#Policy_details](https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference#Policy_details)). The policy definition remains intact, but Code42 apps actively making requests for this policy can no longer use the policy. You must uninstall and reinstall the Code42 app with the new deployment token to enable devices to register with this policy.

---

**Example username detection scripts for the Code42 cloud**

For example username detection scripts, see the [Deployment script and command reference for Incydr Basic and Advanced, CrashPlan Cloud, and other plans](https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference).

**Step 3: Deploy Code42 apps to user devices**

**Before you deploy to production**

---

[https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference](https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference)
Test your deployment plans

Before deploying Code42 apps to production devices, always test your entire process and all its scripts and files.

1. At your Code42 console, create at least one test organization.
2. Add several test users to that organization.
3. Connect test devices for those users to the network that includes your Code42 environment.
4. Deploy Code42 apps to the test devices and make sure they work as intended.

Verify that apps can connect by HTTPS

User devices must be able to reach your Code42 console by the HTTPS protocol. Check your protocol and port configuration:

- The URL must begin with https://
- Your firewalls must allow client requests to reach the Code42 console.

When you add a deployment policy to your Code42 cloud-based deployment, the URL auto-populates with the address. For example:

- United States:
  - US1: https://console.us.code42.com
  - US2: https://console.us2.crashplan.com
- Ireland:
  - EU1: https://console.ie.code42.com

Code42 console URL for US2

Code42 console URL console.us2.crashplan.com was formerly www.crashplan.com/console. For more information, see Changes to server URLs (https://support.code42.com/Terms_and_conditions/Product_lifecycle_policy/Changes_to_server_URLs).

Deploy to devices

Retrieve installation properties from your deployment policy as follows:

2. Select Administration > Client Management > Deployment.
3. In the list of policies, click on the name of the policy you want to use.

4. Copy deployment properties from the policy:
   - Windows or Linux: Copy the properties and paste them into your deployment software.
   - Mac: Download the deploy.properties file and provide it to your deployment process.

Distribute installation properties and Code42 app installers to your target devices. Then run the installers. Details for those two tasks depend on your device management tool and endpoint operating systems:

- Consult the vendor's documentation for your device management tool.
- For deployment to Mac devices, see details about placing the deploy.properties (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference) file.
- For details about Code42 app install commands, see the Deployment script and command reference for Incydr Basic and Advanced, CrashPlan Cloud, and other plans (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference).

**Step 4: Users sign in to the Code42 app**

With the "silent registration" deployment options, users are automatically signed in to the Code42 app.

With the "manual registration" deployment option, users manually sign in to the Code42 app:

- On Windows and Mac devices, the Code42 app opens on the desktop automatically.
- On Linux, users should run this command: /usr/local/crashplan/bin/CrashPlanDesktop

Instruct users to provide names and passwords as prompted by the Code42 app. For details, direct users to Sign up with newly deployed Code42 app (https://support.code42.com/CrashPlan/6/Get_started/Sign_up_with_newly_deployed_Code42_app).

**Step 5: Verify success**

**For silent registration deployment options**

Perform the following verification steps if you use the following silent deployment options:

- Silent registration with SSO
- Silent registration with local authentication

**Review device data in Code42 console**

Check that deployments succeed by reviewing the number of devices signed in to your organization and backing up data.

https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/

2. Select Administration > Environment > Organizations.

3. Select the organization you deployed to.

4. At the top of the window, click the value under Devices. The number of devices listed for your org should match the number of devices you deployed Code42 apps to. The quantity of data stored for each device should be greater than zero.

Review client logs

At your test devices, or a selection of your production devices, check the Code42 app service.log.0

1. Find service.log.0 in one of these locations:
   - **Windows**: C:\ProgramData\CrashPlan\log
     To view this hidden folder, open a file browser and paste the path in the address bar. If you installed per user, see the file and folder hierarchy (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/File_and_folder_hierarchy#Installed_per_user).
   - **Mac**: /Library/Logs/CrashPlan
     If you installed per user, see the file and folder hierarchy (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/File_and_folder_hierarchy#Installed_per_user_2).
   - **Linux**: /usr/local/crashplan/log

2. Open service.log.0 with a text editor.

3. Search for **CP_ARGS=DEPLOYMENT**
   Find a line like the following and verify that the installer arguments are correct.

   CP_ARGS=DEPLOYMENT_URL=https://authority.example.com:4285&DEPLOYMENT_POLICY_TOKEN=e675f3e1-ebb3-496e-9cef-c669db6ffac6&SSL_WHITELIST=7746278a857f64717094c44eeb2bbc32357ece44

4. Search for **Results of running user script**.
   Find lines like the following that verify the Code42 app retrieved the deployment policy and ran the detection script without error.

   Deploy:: Successfully retrieved deployment package
   Results of running user script: UserScriptExecutionResults [username=exampleUser, userHomeDirectory=/home/exampleUser]

5. Search for **LoginRequest**
   Find lines like the following that verify that the Code42 app logged in and is authorized to backup data.

   UserActionRequest: LoginRequestMessage[809641607873065038] LOGIN: username=exampleUser, password=****, serverAddress=authority.example.com:4287
   AUTH:: CPC session is LOGGED_IN
Troubleshooting

If a user opens the desktop UI for a newly deployed Code42 app, but the UI never progresses beyond the message Connecting..., then the deployment has probably failed.

Confirm the error as follows:

1. Find service.log.0 in one of these locations:
   - **Windows**: C:\ProgramData\CrashPlan\log
     To view this hidden folder, open a file browser and paste the path in the address bar. If you installed per user, see the file and folder hierarchy [here](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/File_and_folder_hierarchy).
   - **Mac**: /Library/Logs/CrashPlan
     If you installed per user, see the file and folder hierarchy [here](https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/File_and_folder_hierarchy).
   - **Linux**: /usr/local/crashplan/log
2. Open service.log.0 with a text editor.
3. Find deployment errors by searching for Deploy::, for example:

   ```text
   deploy:: Unable to make request
   Deploy:: Unable to process deployment package, USERNAME_NOT_IN_OUTPUT
   ```

For the manual registration deployment option

If you use the manual registration deployment option, after users sign in, check that deployments succeed by reviewing the number of devices signed in to your organization and backing up data.

1. Sign in to the Code42 console [here](https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview#Access_the_Code42_console).
2. Select Administration > Environment > Organizations.
3. Select the organization you deployed to.
4. At the top of the window, click the value under Devices.
   The number of devices listed for your org should match the number of devices you deployed Code42 apps to.
The quantity of data stored for each device should be greater than zero.

Related topics

- Deployment policies reference (https://support.code42.com/Administrator/Cloud/Code42_console_reference/Deployment_policies_reference)
- Deployment script and command reference for Incydr Basic and Advanced, CrashPlan Cloud, and other plans (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deployment_script_and_command_reference)