A Guide for Configuring macOS Catalina Bootstrap Tokens using Jamf Pro

To follow along with this guide you will need the following:

1. Mac computer running macOS Catalina 10.15 or later that's enrolled in Apple Business or School Manager and is assigned to the Jamf Pro server. The Mac Computer MUST be bound to Active Directory with the option to create a mobile account selected.
2. Jamf Pro Sever 10.18 or later (Jamf pro cloud hosted server was used for this guide).
3. Microsoft Windows Active Directory Server 2008-R2 or later.
4. Apple Business or School Manager with Automated Device Enrollment and Volume Purchasing configured on the Jamf Pro Server.

NOTE: macOS Catalina 10.15.4 adds two new features for Bootstrap Tokens:

1. A Standard user created using a PreStage enrollment will now get a Bootstrap token.
2. If a supervised computer does NOT have Bootstrap Token, macOS Catalina 10.15.4 will enable the Bootstrap Token during the first login by a SecureToken-enabled account. If you skipped user account creation during the Setup Assistant, but enabled FileVault or generated a SecureToken for an account by any other means, that account will trigger the generation of the Bootstrap Token during next login.

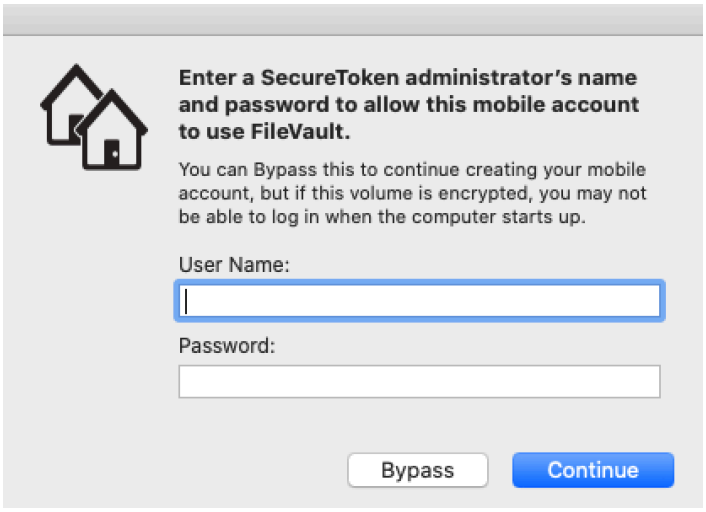
Apple documentation for more information on Bootstrap Tokens:
https://support.apple.com/en-au/guide/deployment-reference-macos/apda5cd41b67/1/web/1
https://support.apple.com/en-au/guide/deployment-reference-macos/apd0815d5748/1/web/1
https://support.apple.com/en-au/guide/deployment-reference-macos/apdef58dd7b5/1/web/1
https://support.apple.com/en-au/guide/deployment-reference-macos/apdf028a757b/1/web/1

Section 1: Bootstrap Tokens and Account Types

What are Bootstrap Tokens?
macOS Catalina 10.15 introduces a new feature called the Bootstrap Token. This feature will help with granting a SecureToken to both mobile accounts and the optional device enrollment-created administrator or Standard user account. When a Bootstrap Token is escrowed on the Jamf Pro Server, macOS Catalina can request and receive it when Mobile accounts sign in and generates a SecureToken for that user account. Jamf Pro 10.18 adds support for escrowing the Bootstrap Token and will deliver it to computers managed by the Jamf Pro Server on request. This process is transparent to the user and does not require any additional configuration on the Jamf Pro Server. A SecureToken is required for any account that needs to unlock a FileVault encrypted volume.

Bootstrap Token Accounts Types
A mobile account is a local cached account created when a user logs into a Mac computer that is bound to a directory server such as Microsoft Active directory. These accounts are not granted a SecureToken when they are created and require administrative credentials to create one. A Managed Administrator or Standard user account is an account created using a PreStage configured on Jamf Pro server.

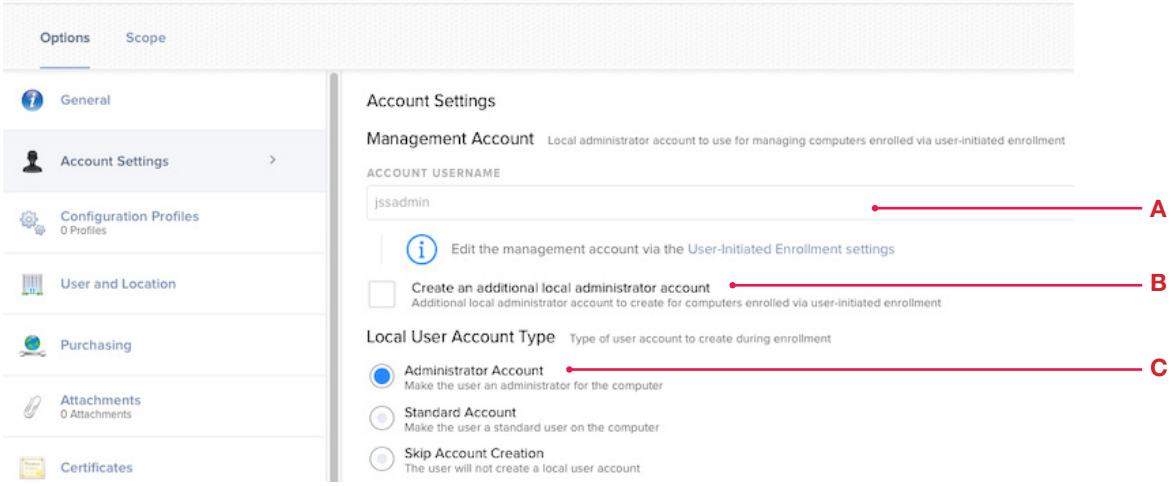
When logging in with a mobile account the user is presented with the message below. The purpose of a Bootstrap Token is to avoid having the user get the message below and will provide a way for the SecureToken to be granted via the Jamf Pro server. This will allow the mobile account user the access needed to unlock a FileVault encrypted volume.



There are three ways to create Managed Administrator accounts using a PreStage in Jamf Pro server.

A. The Management Account is grayed out but will create the first administrative account on a Mac when it enrolls using a PreStage.
B. If you select the Create an additional local administrator account checkbox, you can create an additional admin account.
C. If you select the Administrator Account radio button, the user will create this account via the setup assistant. **This is the only method that will create and escrow a Bootstrap Token at the same time.**

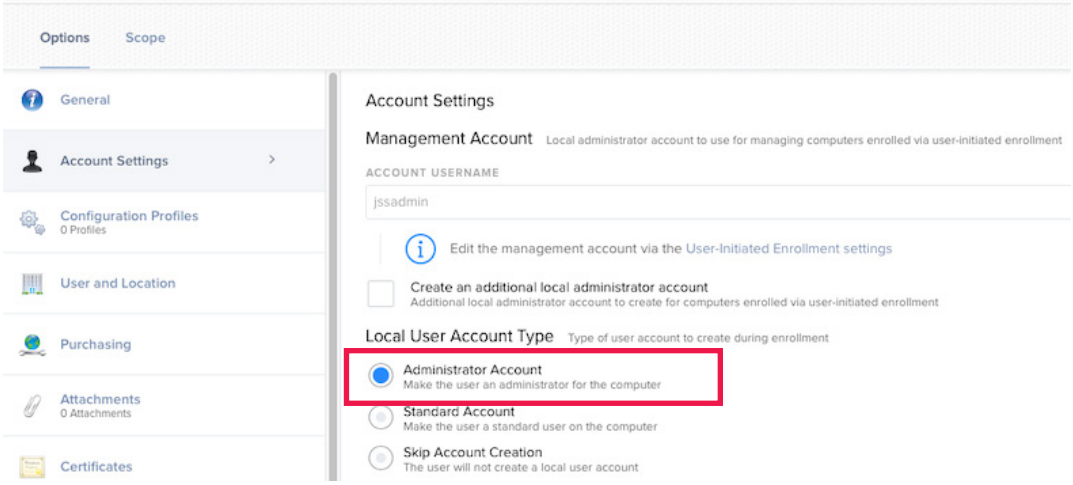
NOTE: Creating an Administrator account via Systems Preferences > Users & Groups or via the command line using sysadminctl will NOT result in the generation of a Bootstrap Token. The Administrator account MUST be created using the three methods listed above to create Bootstrap Tokens.



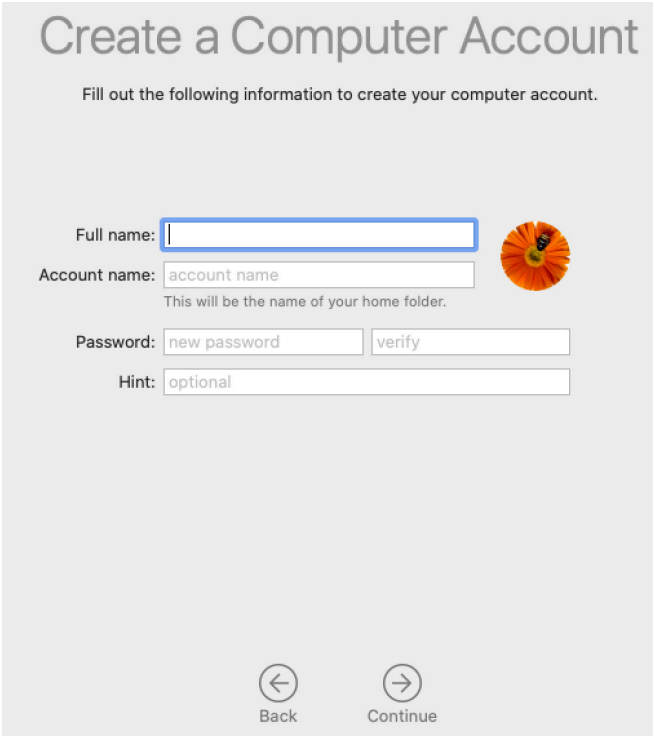
Section 2: Automatic Creation and Escrow of a Bootstrap Token

When configuring the Account Settings section of a PreStage enrollment, make sure to select the Administrator Account radio button. When this option is selected, the user will be required to create an account during the setup assistant. This is the ONLY way to create and escrow the Bootstrap Token at the same time and requires no additional policies or actions on the Mac computer. This method does NOT require LDAP binding to escrow the bootstrap token to the Jamf Pro Server.

NOTE: macOS Catalina 10.15.4 now adds support for the Standard Account to receive a Bootstrap Token when using a PreStage enrollment.



During a PreStage enrollment, Setup Assistant will require you to create an account. This account will be an Administrative account.



After enrolling the Mac computer via the PreStage, Log into the Mac computer as the admin user then open Terminal located in the Applications/Utilities folder. Run the following command:

```
sudo profiles status -type bootstraptoken
```

You will see the following output.

```
profiles: Bootstrap Token supported on server: YES
profiles: Bootstrap Token escrowed to server: YES
```

Check to make sure the user has a bootstraptoken. Run the following command.

```
diskutil apfs listcryptousers /
```

You will see the following output. Notice the MDM Bootstrap Token External Key.

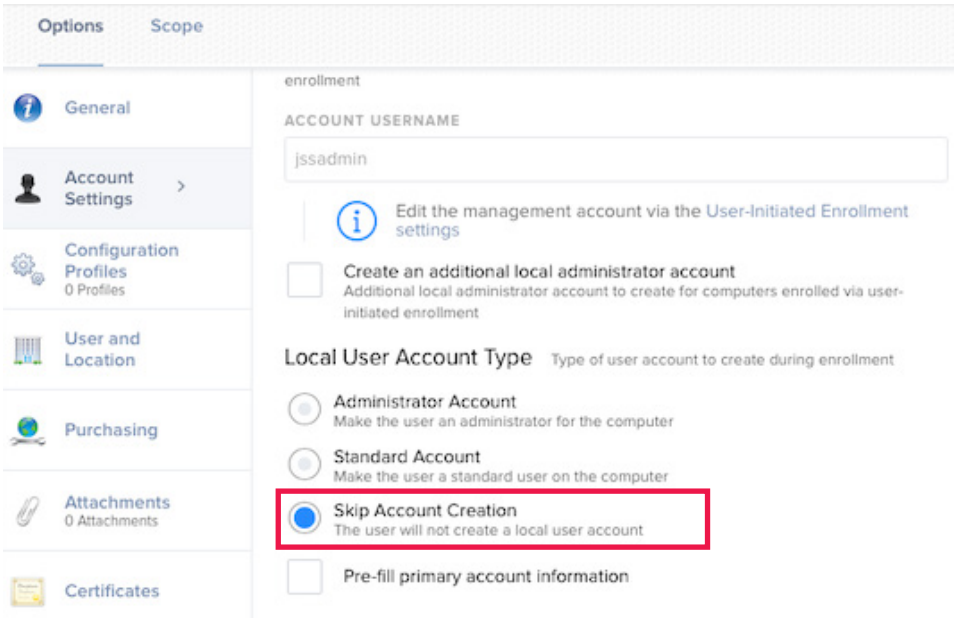
```
Cryptographic users for disk1s5 (2 found)
|
+-- 1C88F8C1-3E10-4018-87B5-354C12D2410F
|   Type: Local Open Directory User
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
    Type: MDM Bootstrap Token External Key
```

This completes the Automatic Creation and Escrow of a Bootstrap Token.

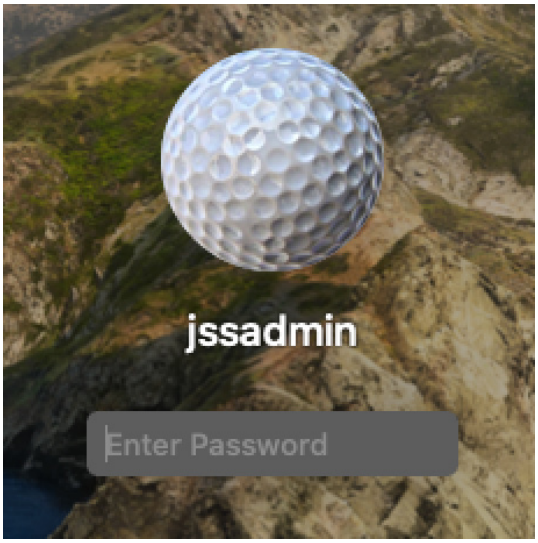
Section 3: Manual Creation and Escrow of a Bootstrap Token

1. When configuring the Account Settings section of a PreStage enrollment, select the Skip Account Creation radio button. When this option is selected, the user will NOT be required to create an account during the setup assistant. The setup assistant will bypass the user account creation screens. The user will log in with their Active Directory account provided the Mac computer is bound to Active Directory so there is no need to create an additional account on the Mac computer.

   NOTE: The Mac Computer MUST be bound to Active Directory with the create mobile account option enabled for this lesson to work correctly.



2. After enrolling the Mac computer via the PreStage, Log into the Mac computer as the admin user that was specified in User Initiated Enrollment on the Jamf Pro server. I.E. they grayed out account in your PreStage enrollment.



3. Open Terminal located in the Applications/Utilities folder. Run the following command.

```
sudo profiles status -type bootstraptoken
```

You will see the following output.

```
profiles: Bootstrap Token supported on server: YES
profiles: Bootstrap Token escrowed to server: NO
```

The Bootstrap Token is NOT escrowed to the server. This is because the administrative account was NOT created via the system assistant.

4. Run the following command to enable the Bootstrap Token:

```
sudo profiles install -type bootstraptoken
```

You will be prompted to enter the admin user name and password.

```
Enter the admin user name:jssadmin
Enter the password for user 'jssadmin':
profiles: Create Bootstrap Token created
profiles: Bootstrap Token created
profiles: Bootstrap Token escrowing to server...
profiles: Bootstrap Token escrowed
```

5. Run the following command to check the Bootstrap Token status:

```
sudo profiles status -type bootstraptoken
```

You will see the following output. Now the token is escrowed on the Jamf Pro Server.

```
profiles: Bootstrap Token supported on server: YES
profiles: Bootstrap Token escrowed to server: YES
```

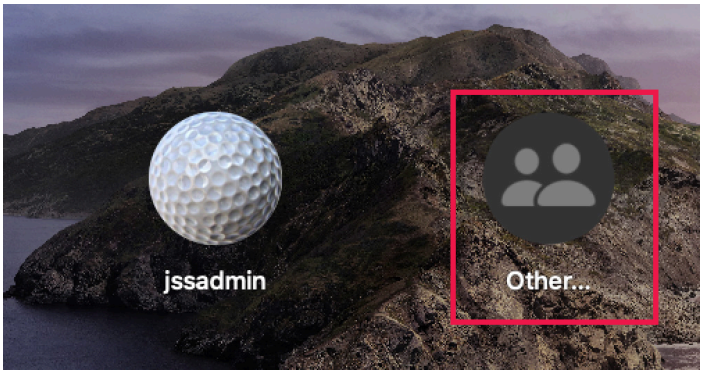
6. Run the following command to check the Bootstrap Token enable users:

```
diskutil apfs listcryptousers /
```

You will see the following output.

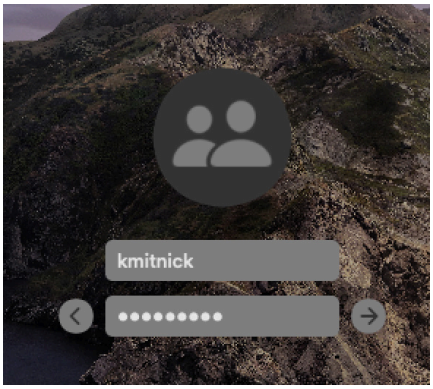
```
Cryptographic users for disk1s5 (2 found)
|
+-- 1C88F8C1-3E10-4018-87B5-354C12D2410F
|   Type: Local Open Directory User
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
    Type: MDM Bootstrap Token External Key
```

Logout of the Mac computer. Select Other.

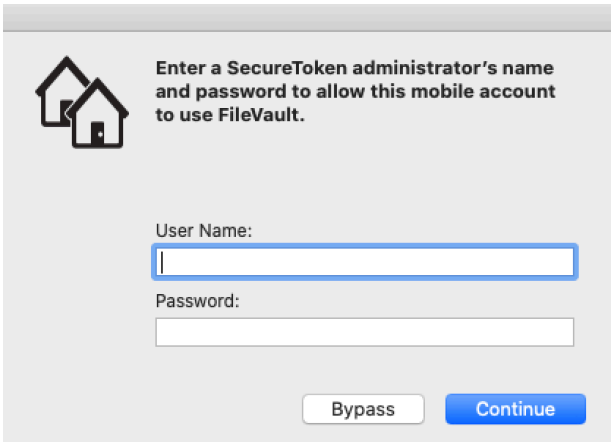


7. Log in as an Active Directory user.

NOTE: Your Mac computer must be bound to Active Directory to login as an Active Directory user. The create mobile account option MUST be enabled as well.



8. If everything went well, you will NOT see the screen below upon login. This is because the Bootstrap Token was able to provide the SecureToken to the Active Directory user via the escrowed Jamf Pro Server Bootstrap Token.



9. Open Terminal located in the Applications/Utilities folder. Run the following command to check the SecureToken enable users:

```
diskutil apfs listcryptousers /
```

You will see the following output. Notice we now have three users in the list. The Active Directory user is now part of this list.

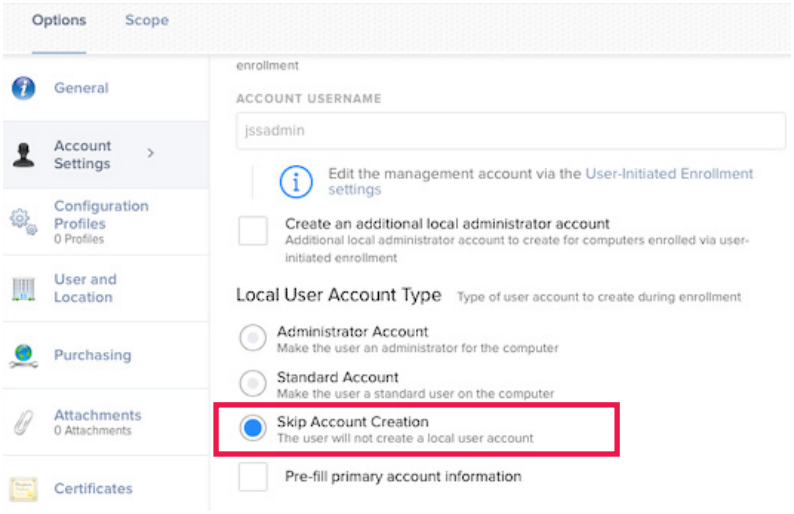
```
Cryptographic users for disk1s5 (3 found)
|
+-- 1C88F8C1-3E10-4018-87B5-354C12D2410F
|   Type: Local Open Directory User
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
  Type: MDM Bootstrap Token External Key
|
+-- 4C88F8C1-8E10-6542-90B5-354C12E76F09
|   Type: Local Open Directory User
```

This completes the Manual Creation and Escrow of a Bootstrap Token.

Section 4: Scripted Creation and Escrow of a Bootstrap Token

The steps in the previous section outlined how to manually create and escrow the Bootstrap Token. This section will show you how to script the process for an automated workflow.

1. When configuring the Account Settings section of a PreStage enrollment, select the Skip Account Creation radio button. When this option is selected, the user will NOT be required to create an account during the setup assistant. The setup assistant will bypass the user account creation screens.



2. Create a script on the Jamf Pro Server with the following info:
   A. Script Name: Enable Bootstrap Token
   B. Use the sample script below. This is an expect script that will automatically answer the interactive questions when running the profiles command.
   C. Save the script when done.

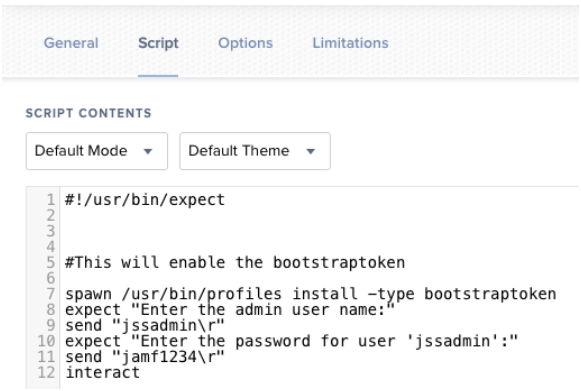
   NOTE: This script is using jssadmin as the administrative user. Change it to whatever admin account you are using.

```
#!/usr/bin/expect

#This will create and escrow the bootstraptoken on the Jamf Pro Server

spawn /usr/bin/profiles install -type bootstraptoken
expect "Enter the admin user name:"
send "jssadmin\r"
expect "Enter the password for user 'jssadmin':"
send “jamf1234\r”
interact
```

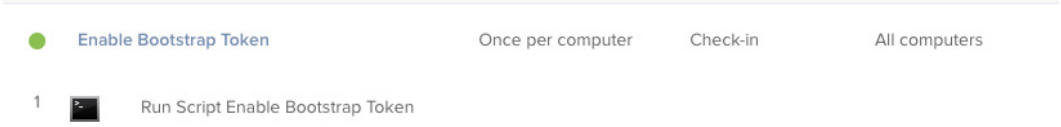
Enable Bootstrap Token



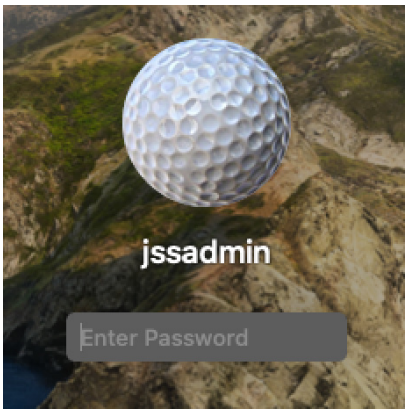
3. Create a policy on the Jamf Pro Server with the following settings:
    A. Name the policy - Enable Bootstrap Token
    B. Set a Category - select a category of your choosing
    C. Set the trigger to Check In (see note below)
    D. Set the frequency to Once per Computer
    E. Select the Scripts payload.
    F. Select the configure button
    G. Select the Enable Bootstrap Token script
    H. Select Scope and scope it to your needs.
    I. Select Save, then done.

    The end result will look like the policy shown below.

    NOTE: I originally was running the policy at enrollment complete but had mixed results. Running it at check in works with no issues.



4. After enrolling the Mac computer via the PreStage, Log into the Mac computer as the admin user.



5. Open Terminal located in the Applications/Utilities folder. Run the following command to check the Bootstrap Token status:

```
sudo profiles status -type bootstraptoken
```

    NOTE: If you don't see the above output, you may need to force a Jamf Pro check-in by running the sudo jamf policy command.

    You will see the following output. Now the token is escrowed on the Jamf Pro Server without any user interaction.

```
profiles: Bootstrap Token supported on server: YES
profiles: Bootstrap Token escrowed to server: YES
```

This completes the Scripted Creation and Escrow of a Bootstrap Token.

Section 5: Commands to manage the Bootstrap token

```
sudo profiles install -type bootstraptoken
```

This command generates a new Bootstrap Token and attempts to escrow it to the MDM solution. This command requires existing SecureToken administrator information to initially generate the Bootstrap Token, the MDM solution must support the feature, and the Mac must be enrolled in MDM and Apple School Manager or Apple Business Manager.

```
sudo profiles remove -type bootstraptoken
```

Removes the existing Bootstrap Token on the Mac and the MDM solution.

```
sudo profiles status -type bootstraptoken
```

Reports back whether the MDM solution supports the Bootstrap Token feature, and what the current state of the Bootstrap Token is on the Mac.

```
sudo profiles validate -type bootstraptoken
```

Verifies that the Bootstrap Token escrowed in the MDM solution is valid on the Mac.

Other useful commands:

```
diskutil apfs listcryptousers /
```

Shows a list of all crypto users on the Mac computer.

```
sysadminctl -secureTokenStatus usernamegoeshere
```

Shows the SecureToken status for a user

```
profiles renew -type enrollment
```

This will prompt a user to be added to Automated Device Enrollment.