



Become a Solutions Architect

5 things to do after creating your first AWS account



1. Secure your root account

Enable MFA on the AWS account root user

We recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available. We recommend that you enable multiple MFA devices to your AWS account root user and IAM users in your AWS accounts. This allows you to raise the security bar in your AWS accounts, including your AWS account root user. You can register up to eight MFA devices of any combination of the currently supported MFA types for your AWS account root user and IAM users.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html



2. Create an administrator user

Because you can't restrict what a root user can do, we strongly recommend that you don't use your root user for any tasks that don't explicitly require the root user. Instead, assign administrative access to an administrative user, and sign in as the administrative user to perform your daily administrative tasks.

<https://docs.aws.amazon.com/singlesignon/latest/userguide/getting-started.html>

3. Familiarize yourself with AWS Management console



<https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/working-with-console.html>

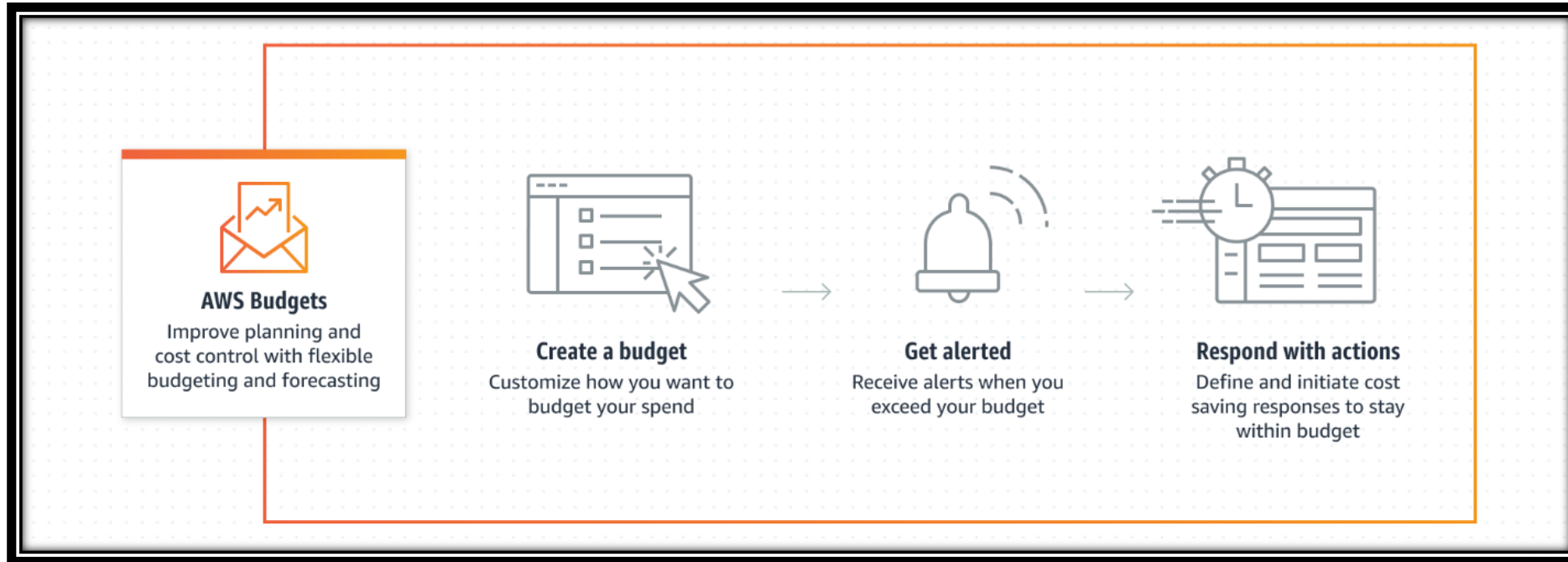
4. Create password policy

The default password policy enforces the following conditions:

- Minimum password length of 8 characters and a maximum length of 128 characters
- Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and non-alphanumeric character (! @ # \$ % ^ & * () _ + - = [] { } | ')
- Not be identical to your AWS account name or email address
- Never expire password

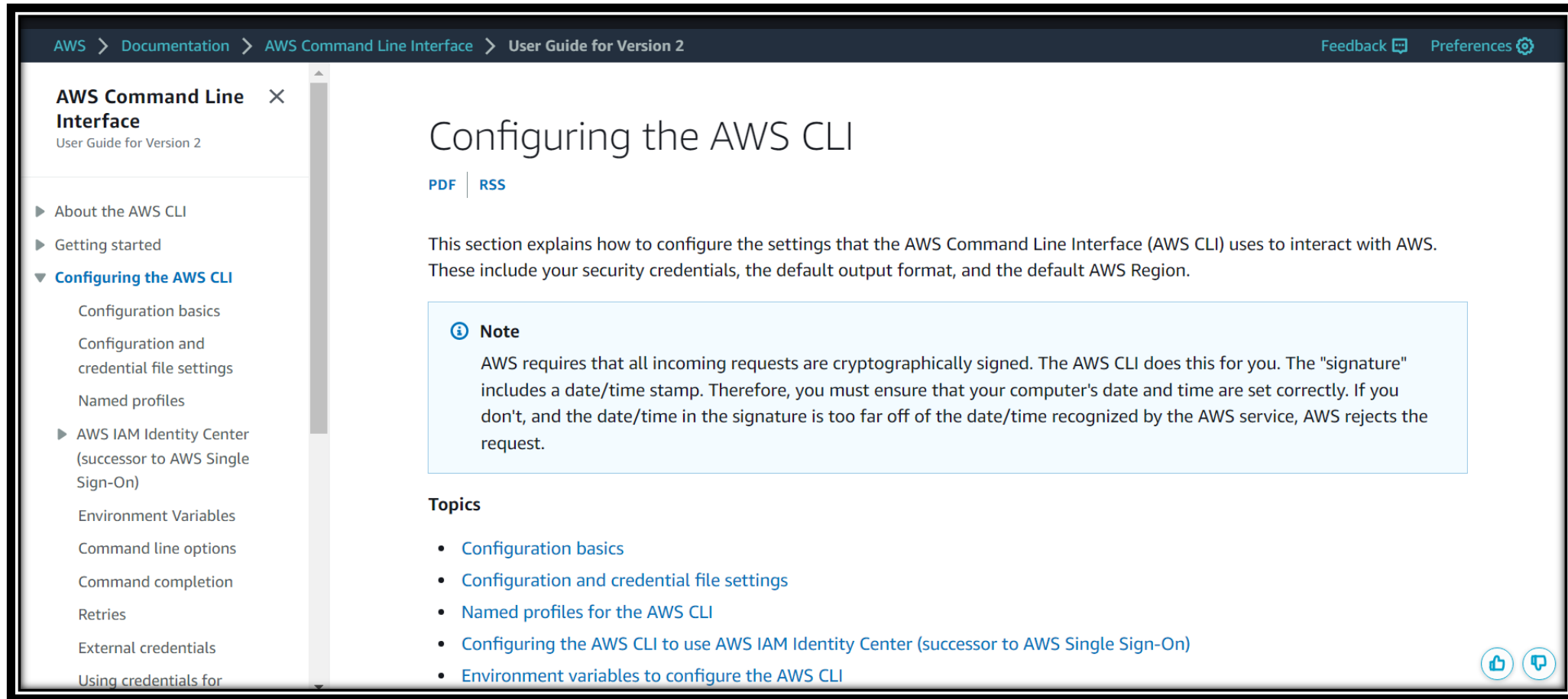
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

5. Configuring AWS Budgets actions



<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>

AWS CLI



AWS > Documentation > AWS Command Line Interface > User Guide for Version 2

Feedback  Preferences 

AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▶ Getting started
- ▼ **Configuring the AWS CLI**
 - Configuration basics
 - Configuration and credential file settings
 - Named profiles
 - ▶ AWS IAM Identity Center (successor to AWS Single Sign-On)
 - Environment Variables
 - Command line options
 - Command completion
 - Retries
 - External credentials
 - Using credentials for

Configuring the AWS CLI

[PDF](#) | [RSS](#)



This section explains how to configure the settings that the AWS Command Line Interface (AWS CLI) uses to interact with AWS. These include your security credentials, the default output format, and the default AWS Region.

Note

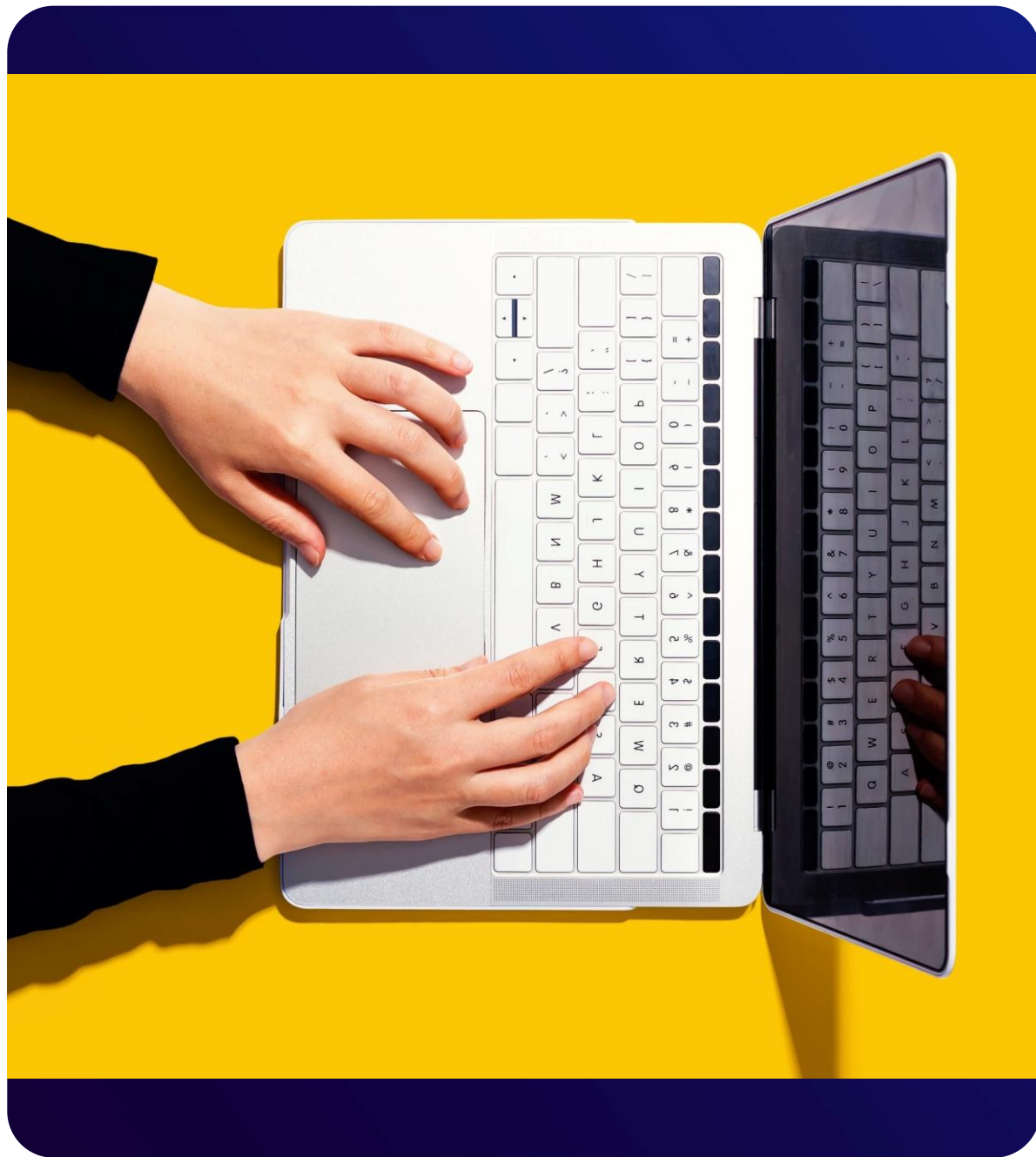
AWS requires that all incoming requests are cryptographically signed. The AWS CLI does this for you. The "signature" includes a date/time stamp. Therefore, you must ensure that your computer's date and time are set correctly. If you don't, and the date/time in the signature is too far off of the date/time recognized by the AWS service, AWS rejects the request.

Topics

- [Configuration basics](#)
- [Configuration and credential file settings](#)
- [Named profiles for the AWS CLI](#)
- [Configuring the AWS CLI to use AWS IAM Identity Center \(successor to AWS Single Sign-On\)](#)
- [Environment variables to configure the AWS CLI](#)

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>



Thank you!

See you next week!