Enterprise Key Management for Endpoints

**Important** Enterprise Key Management is under controlled availability. To enable this feature for your account, contact Druva Support.

**Overview**

If your organizational policies require you to have full control over the encryption of the data backed up by Druva inSync from the Endpoints, Enterprise Key Management is the option for you. With Enterprise Key Management, you can use keys generated from your own AWS Key Management Service (KMS) account to encrypt and decrypt the data backed up by Druva inSync. This provides an additional layer of encryption over and above Druva’s default data encryption.

Enterprise Key Management is available on request, hence contact Support to acquire this feature for your account.

**Benefits**

Enterprise Key Management offers the following security benefits:

- Use keys from your own KMS account to encrypt and decrypt the data encryption key.
- Generate, revoke, rotate, and destroy the encryption keys as and when required from AWS account.
- Control access to data backed up by Druva inSync.
- Secure data backed up from Endpoints.

**Considerations**

Consider the following points before you enable this feature for your account:

- Once Enterprise Key Management is enabled for your account, you cannot revert to default Cloud Key Management.
- Enterprise Key Management encryption supersedes Cloud Key Management. Hence, Cloud Key Management gets disabled when Enterprise Key Management is enabled for your account.
Prerequisites

Ensure the following before you enable Enterprise Key Management:

- AWS account with Key Management Service (KMS) access, to manage customer master keys
- Support has activated the Enterprise Key Management configuration for your account. Without this activation, the configuration fields do not appear on the inSync Management Console.

Enable Enterprise Key Management

Follow these steps to enable Enterprise Key Management for your organization:

1. Copy the Druva’s AWS account ID from the inSync Management Console:
   1. Login to the inSync Management Console.
   2. Click > inSync Settings and open the Key Management tab.

![Settings](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/Configure_Enterprise_Key_Management_for_Endpoint...)

   ![Settings](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/Configure_Enterprise_Key_Management_for_Endpoint...)

3. Click button to copy the 12-digit numeric value of the Druva’s AWS account ID.

4. Save the numeric value to be used on the AWS Key Management Service (KMS) console.

2. Get the key ARN from your AWS KMS account:
   1. Login to AWS KMS Console.
   2. On the menu, click Services and search for KMS. The Key Management Service (KMS) page opens.
   3. Click Customer managed keys from the left pane. A list of managed keys is displayed.
   4. Click Create key and click Symmetric key on the Key type page.
   5. On the Add labels page, provide the key Alias, used to identify the key and description and click Next.
6. On the Key administrators’ page, select one or more administrators who can control the key. The key administrator selected here can rotate, and revoke the key that you are about to generate.

7. Select **Allow key administrators to delete this key** to enable the delete right for the administrators.

8. On the next page, click **Add another AWS account**. A text box is displayed. This setting defines the account with which the AWS KMS must communicate to authenticate access to the backed up data.

9. On Review and Edit policy screen, allow the following rights on the CMK for Druva inSync

```
{
    "Sid": "Allow use of the key for Druva inSync",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::113356737989:root"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

10. Enter the 12 digits **Druva’s AWS account ID** on the **Key Management** tab of the inSync Management Console.

11. Click **Next** to review the key policy. The page displays the permissions available for the Druva account when it accesses the key during backups and restores.

12. Click **Finish**. The new key is generated and displayed on the AWS KMS console.
13. Click the key Alias on the console to view the key details. The General configuration details are displayed as below:

![General configuration]

14. Copy the value displayed under ARN from the AWS KMS console. This key is required to enable the Enterprise Key Management on the inSync Management Console.

3. Enable Enterprise Key Management from the inSync Management Console:
   i. Click Enable Enterprise Key Management. inSync asks for the KMS key ARN generated from the AWS KMS console.
   ii. Copy the newly created KMS key ARN into the Update KMS key ARN dialog box and click Next. The ARN is validated and upon successful authentication, a confirmation message appears.
   iii. Click Save.
   iv. Click Continue and review the legal terms and conditions of enabling Enterprise Key Management.
   v. Click Yes, I Agree. Enterprise Key Management gets enabled for your account. KMS key ARN is displayed on the Key Management tab, with External Cloud Key Management status as Enabled.

![Update the Enterprise Encryption key]

**Update the Enterprise Encryption key**

You may have to update the Enterprise Encryption key to comply with your organizational security policies. However, it is important to note that you must keep the old and new encryption keys active in your AWS KMS service until you configure the new KMS key ARN on the inSync Management Console. This ensures all the required permissions are transferred from the old key to the new encryption key before the old key is purged by the AWS KMS.
To update the Enterprise Encryption key:

1. Get the new **KMS key ARN** using the steps provided above.
2. On the **Key Management** tab, click **Update KMS Key ARN**.
3. Copy the newly created **KMS key ARN** into the **Update KMS key ARN** dialog box and click **Save**. The **KMS Key ARN** upon successful validation is updated on the inSync Management Console.