virtru

Virtru Control Center
Playbook for Administrators

Table of Contents

Introduction

The Virtru Control Center is your central resource to see what data your organization is protecting, know where it's going, manage who it's shared with, and ensure it stays under your organization's control. This playbook outlines the features, functions, benefits, and actions you can take from the Control Center to meet compliance, preserve privacy, and achieve your data protection goals/needs.

Playbook Terminology

• **Policy:** Dictates who should have access to, and what they can do with, any encrypted email, file, or item that Virtru is protecting. Similarly, the act of "creating a policy" means that someone is encrypting data.

• **End-User:** A person within your organization that has a Virtru license and is using it to encrypt data.

• **Activation:** The process by which an end-user installs Virtru and is able to use the email plugin to start encrypting data.
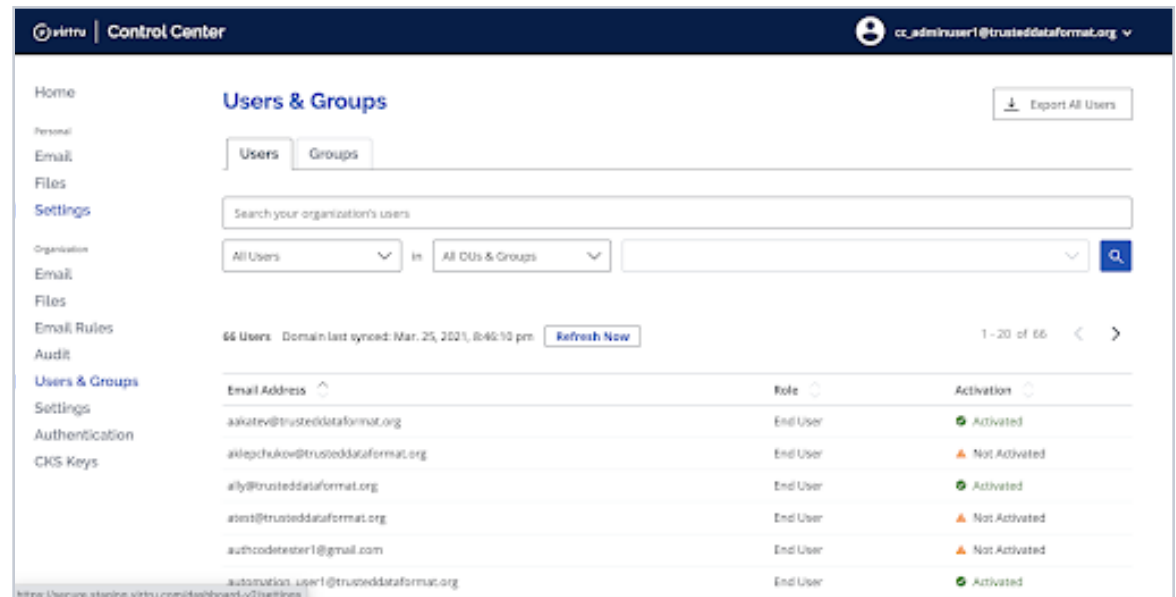
Two Ways to Access the Virtru Control Center

1. Visit **https://www.virtru.com/** and in the top right corner, click the "Sign In" option

2. Bookmark this link: **Virtru Control Center**
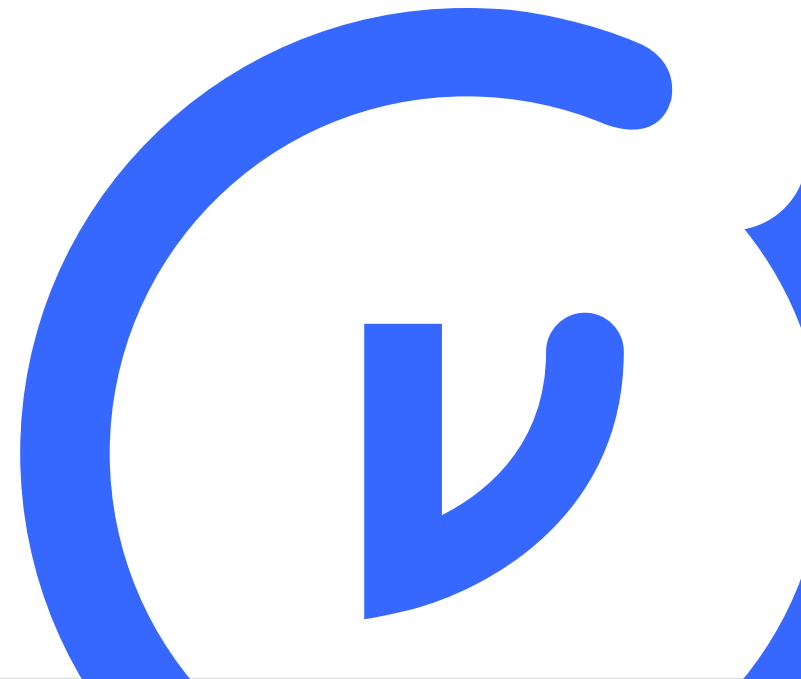
1. Manage Users and Groups

As the administrator of your organization's account, you can use the Virtru Control Center's *Users* page to manage users and licenses for your organization. Additionally, you'll be able to view each user's invitation status, whether or not they have activated the plugin, and what their administrative role is within your team.
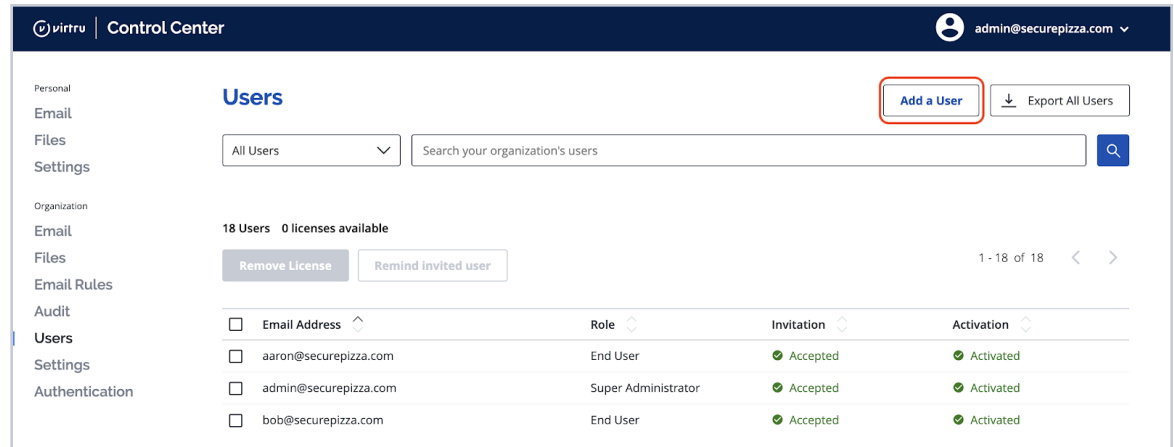

Steps to Add Your End Users in a Synced Domain

1. Your user list is automatically imported to the Virtru Control Center.

2. End users do not need to accept a license; they'll only need to install and activate a Virtru client to appear active in the user list.

3. *Users & Groups* can be used to audit user status and add or remove administrative permissions.

Manage Users and Groups

Steps to Add Your End Users in an Ad Hoc Organization

1. When you are in the Virtru Control Center, click on *Users* within the menu on the left hand side. This will take you to the screen you see below, and you will want to select the *Add a User* button found in the top right corner of the page.

2. When clicking that option, you will be able to enter the email address(es) of user(s) you wish to add.

3. The window will display the number of unused licenses and will update as you add email addresses. Once ready, click *Add* to invite the user to your team.
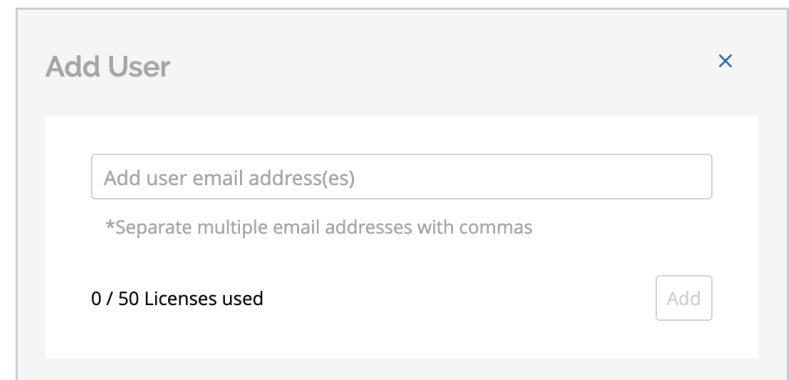
Manage Users and Groups

4. Your users will then receive a team invitation via email from noreply-activation@virtru.com that they must accept if they wish to join your team. Please Note: Once users accept the invitation, they need to then follow the steps to install and activate Virtru.

Virtru Teams Invitation From steven@vtest.com

Inbox ×

noreply-activation@virtru.com
to me

9:52 PM (8 minutes ago)

virtru | simple email privacy

Virtru Teams Invitation

Hi joe@vtest.com,

steven@vtest.com has sent you this email inviting you to a Virtru Teams account.

To accept this invitation: click here
If you do not wish to accept this invitation, you can safely ignore this email.

Thanks!
The Virtru Team

You have received this message as part of Virtru's secure email service. For more information about Virtru, please visit www.virtru.com.

Manage Users and Groups

End-User Authentication

What it Does
Specify how users will authenticate themselves to use Virtru and add any required extra layers of authorization (e.g., through a SAML provider like Okta). Note: Virtru currently supports SAML for authentication & identity purposes only; Virtru licenses cannot be assigned via your SAML / SSO provider.

What it Means for You
Manage Virtru your way to meet your internal policies and security measures, as well as enable the best user experience.

Additional Resources:

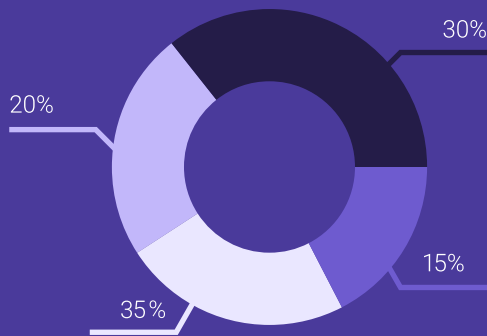**Deep Dive: Managing Users**

Deep Dive: Verification Code Authentication

Deep Dive: Single Sign-on (SSO) Authentication

2. Leverage Actionable Data Sharing Intelligence*

*COMING SOON

30%
20%
15%
35%
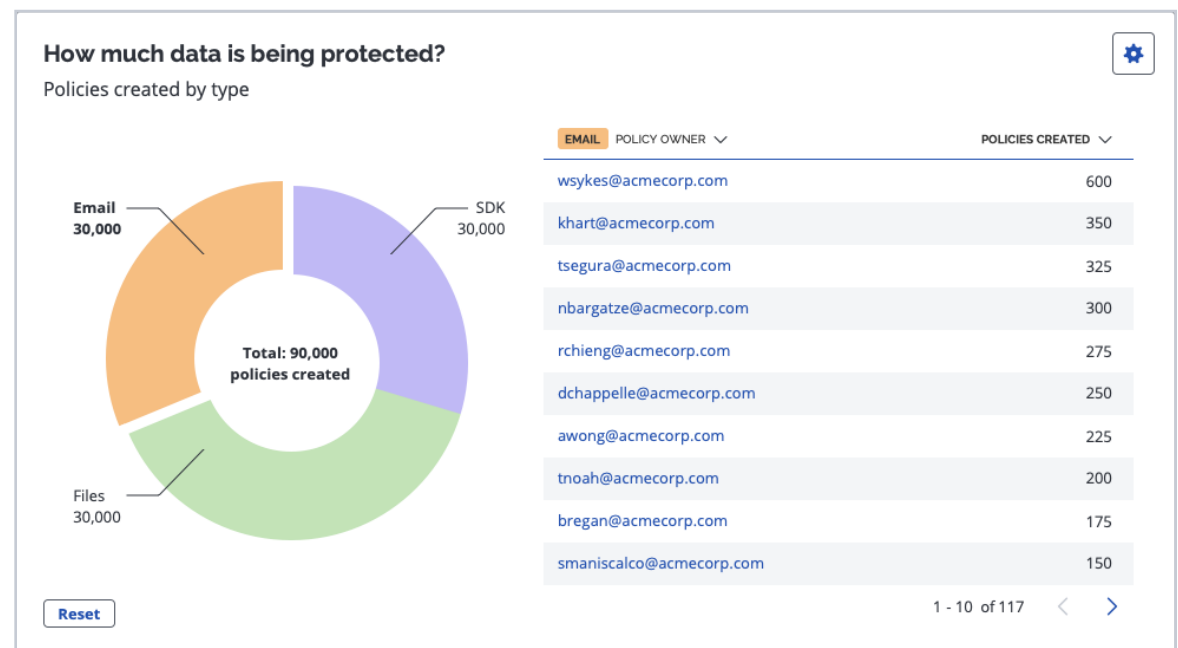
As a Virtru Administrator, the Virtru Control Center is your one-stop shop to see what data your organization is protecting, know where it's going, manage who it's shared with, and maintain control of it at all times. Here's a brief look at the insights you have access to.

Understand the Types of Data Your Organization Is Sharing and How Much Is Protected

At Virtru, we have your back. View all of the ways your organization is encrypting data and identify potential gaps or outliers to improve internal operations.

How much data is being protected?
Policies created by type

EMAIL POLICY OWNER ⌄	POLICIES CREATED ⌄
wsykes@acmecorp.com	600
khart@acmecorp.com	350
tsegura@acmecorp.com	325
nbargatze@acmecorp.com	300
rchieng@acmecorp.com	275
dchappelle@acmecorp.com	250
awong@acmecorp.com	225
tnoah@acmecorp.com	200
bregan@acmecorp.com	175
smaniscalco@acmecorp.com	150

Email 30,000
SDK 30,000
Files 30,000
Total: 90,000 policies created

Reset   1 - 10 of 117   ‹ ›

What it Shows
View how much and what type of data is being protected, such as emails, files, and data protected using the **Virtru Software Development Kit (SDK)**.

What it Does
See a comprehensive, outgoing policy-creation view and drill down for further details to see who at your company is sharing encrypted information (i.e., creating a policy) and all of the policies they've created.
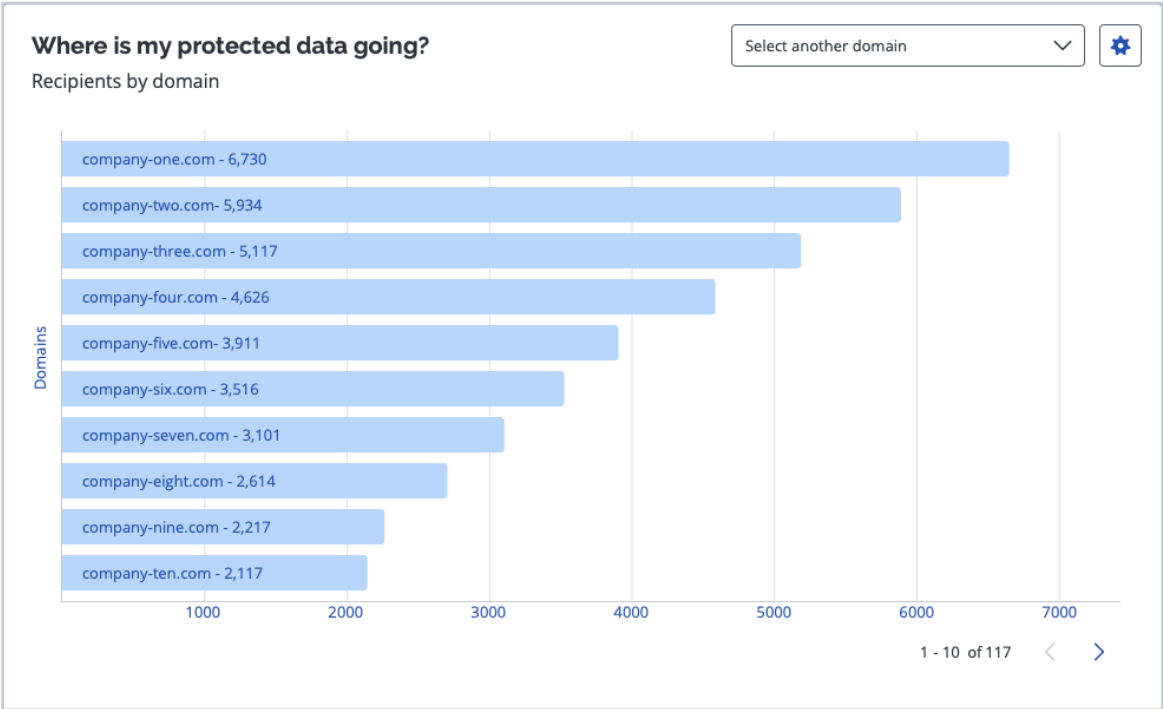
What it Means for You
Know exactly what data is being protected, and better understand your organization's trends and patterns for protecting data. You'll also be able to evaluate if people are encrypting the right types of data, identify opportunities for improvement, and encourage data protection usage across your entire organization.

See Who Has Access to Your Data

Virtru offers enhanced visibility of your data to ensure it stays under your control, anywhere it travels. You are empowered to review the path data takes and adjust access if needed.

What it Shows
Where your data is going and who it's been shared with—both at the company domain level and individual recipient level.

Where is my protected data going?
Recipients by domain

Select another domain ⌄

Domains

Domain	Value
company-one.com	6,730
company-two.com	5,934
company-three.com	5,117
company-four.com	4,626
company-five.com	3,911
company-six.com	3,516
company-seven.com	3,101
company-eight.com	2,614
company-nine.com	2,217
company-ten.com	2,117

1000   2000   3000   4000   5000   6000   7000

1 - 10 of 117 ‹ ›

Leverage Actionable Data Sharing Intelligence*

What it Does
See who—by company or individual recipient—you've shared protected data with in the last 30 days, review a comprehensive overview of policy creation, and add or adjust access controls.

What it Means for You
Uncover potential data sharing threats, opportunities to share more, better understand your external data sharing patterns, evaluate your business practices for sensitive data sharing, and instantly revoke access within Control Center.

| Where is my protected data going? 30,212 recipients at **company-one.com**		Select another domain ⌄	⚙
hmirren@company-one.com	86	Nov 16, 2020	Nov 16, 2020
djohnson@@company-one.com	85	Nov 16, 2020	Nov 16, 2020
wsmith@@company-one.com	65	Nov 16, 2020	Nov 16, 2020
vkilmer@@company-one.com	54	Nov 16, 2020	Nov 16, 2020
ospencer@@company-one.com	34	Nov 16, 2020	Nov 16, 2020
prudd@@company-one.com	23	Nov 16, 2020	Nov 16, 2020
rgere@@company-one.com	22	Nov 16, 2020	Nov 16, 2020
jchastain@@company-one.com	21	Nov 16, 2020	Nov 16, 2020
dyen@@company-one.com	17	Nov 16, 2020	Nov 16, 2020
iuwais@@company-one.com	11	Nov 16, 2020	Nov 16, 2020

1 - 10 of 117 ‹ ›

3. Granular Audit Capabilities

See where all email and files have been forwarded and shared, throughout the data lifecycle. If needed, adapt controls to selectively revoke access or disable forwarding for all collaborators, or revoke all. Also, access a log for all activity that happens in your Virtru platform.

What it Does
Search for specific types of data, review any action that was taken, and download a CSV file for reporting needs.
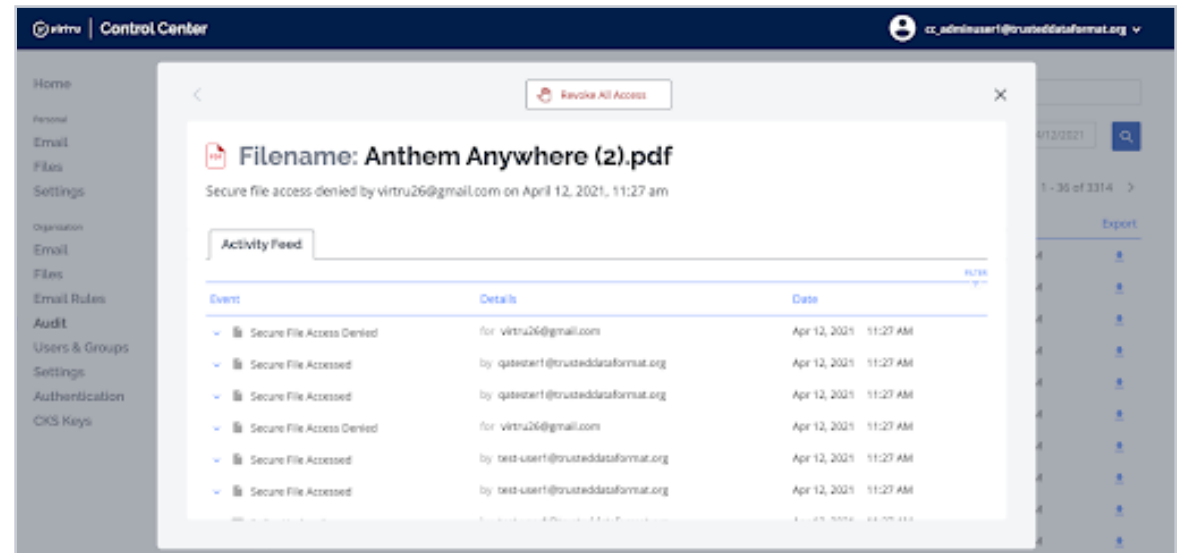
What it Means for You
Get a better view into the lifecycle of data across your organization and easily support any audit requests.

4. Manage Encrypted Emails and Files

Managing Encrypted Emails

Under the *Organization > Email* section within the Virtru Control Center, you have the ability to view a record of all the encrypted email policies sent by the members of your team. While this page does not include the actual message content, you can view the associated metadata and manage access permissions simply by clicking on the email you're interested in. To easily locate specific secure emails, we've enabled a search function that will help you narrow down the scope by searching the following criteria: subject line, file name, email address, or date.

What it Means for You

See where all of your organization's secure emails have been forwarded and shared. If needed, adapt controls to selectively revoke access or disable forwarding for specific recipients and collaborators, or revoke all.

Additional Resources:

[Deep Dive on Managing Encrypted Emails](#)

[Advanced Search Syntax for the Virtru Control Center](#)

Manage Manage Encrypted Emails and Files

Managing Encrypted Files

Under the *Organization > Files* section within the Virtru Control Center, you have the ability to view a record of all the secure attachments, Google Drive files, and Virtru SDK outputs shared by the members of your team. While the files themselves are not accessible through the Control Center, you're able to view the associated metadata and manage access permissions simply by clicking on the file you're interested in. To easily locate specific secure files, we've enabled a search function that will help you narrow down the scope by searching the following criteria: subject line, file name, email address, or date.

What it Means for You
See where all of your organization's secure files have been forwarded and shared. If needed, adapt controls to selectively revoke access for some or all recipients and collaborators, or revoke all.
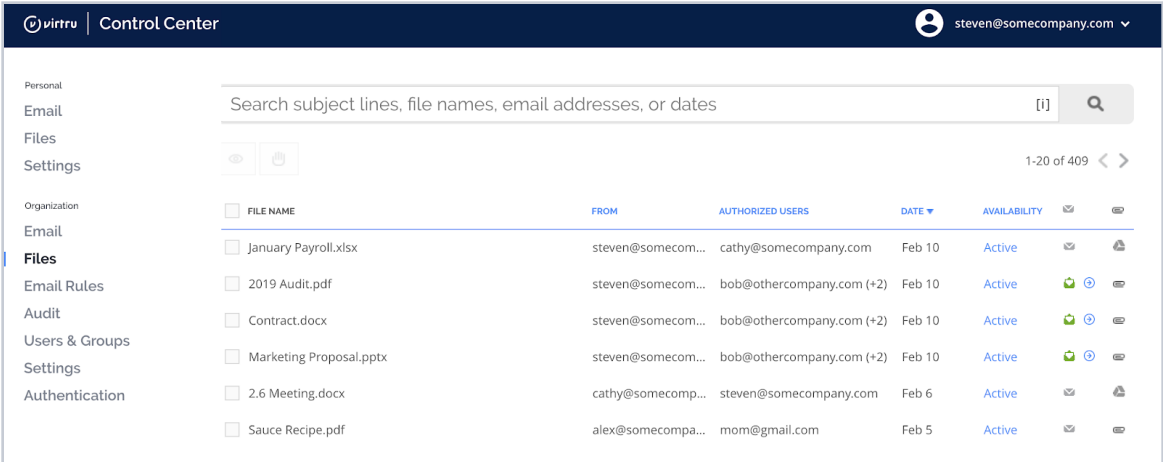
Additional Resource:

Deep Dive on Managing Encrypted Files

5. Email Rules

As an administrator, you can leverage Virtru's Data Loss Prevention (DLP) rules to dictate how Virtru will behave when certain content is found in your users' outgoing emails. You'll configure and manage these rules from the Virtru Control Center's *Email Rules* page. In this next section we'll briefly walk you through the different types of rules and their associated actions.

Text Pattern Rules

The rules listed under "*When I type these text patterns...*" use Regular Expressions (RegEx) to match consistently formatted number and text patterns. The default patterns included with Virtru are Social Security Number, Credit Card Number, IP Address, Federal Employee Identification Number (EIN), and Possibly Sensitive.

When I type these text patterns... [i]	Encrypt	Warn	Log Only	Enabled
Social Security Number	●	○	○	ON
Federal EIN	○	●	○	ON
IP Address	○	●	○	ON
Possibly Sensitive	○	○	●	ON
Credit Card Number	●	○	○	ON

Email Rules

Keyword Rules

Rules under the "*When I type these keywords...*" section are triggered by a precise match with a listed keyword. You can add your own keywords to this list by clicking the + icon in the bottom row. A list of keywords can be added at one time by including a comma after each entry.

Recipient Rules

The "*When I send to...*" section allows you to specify an action based on the recipient of the email. This can be configured either by exact email address or by domain name. Email addresses and domains cannot be added in bulk; entering a list will result in only the first item being added to your rules.

When I type these keywords... [i]	Encrypt	Warn	Log Only	Enabled
proprietary	○	○	◉	ON
account number	○	○	◉	ON
confidential	○	◉	○	ON
PII	○	○	◉	ON
password	○	◉	○	ON
Non Disclosure Agreement	◉	○	○	ON
subpoena	○	○	◉	ON
HIPAA	○	○	◉	ON
FINRA	○	◉	○	ON
off the record	○	○	◉	ON
+	●	●	●	ON

When I send to... [i]	Encrypt	Warn	Log Only	Enabled	
virtru.com	○	◉	○	ON	🗑
+	●	●	●	ON	

Email Rules

Rule Actions

Rules in the *Text Patterns*, *Keywords*, and *Recipients* sections can be assigned to take one of three possible actions when the rule is triggered:

1. **Encrypt Email:** This will automatically encrypt the email as soon as the user hits *Send*. They'll see the Virtru encryption animation without any option to have the email go out unencrypted.

2. **Warn Me:** This will trigger an alert to the end user when they hit *Send*. The warning dialog will show exactly what the offending text is, and give the end user the option to either send the message encrypted, or disregard the warning and send unencrypted.

3. **Log Only:** This trigger will take no noticeable action on an outgoing email. If the email is being sent unencrypted, the rule will have no effect at all. If the email is sent encrypted, however, any Log Only rules triggered by that email will be logged in that email's *Validation Report* in the Virtru Control Center.
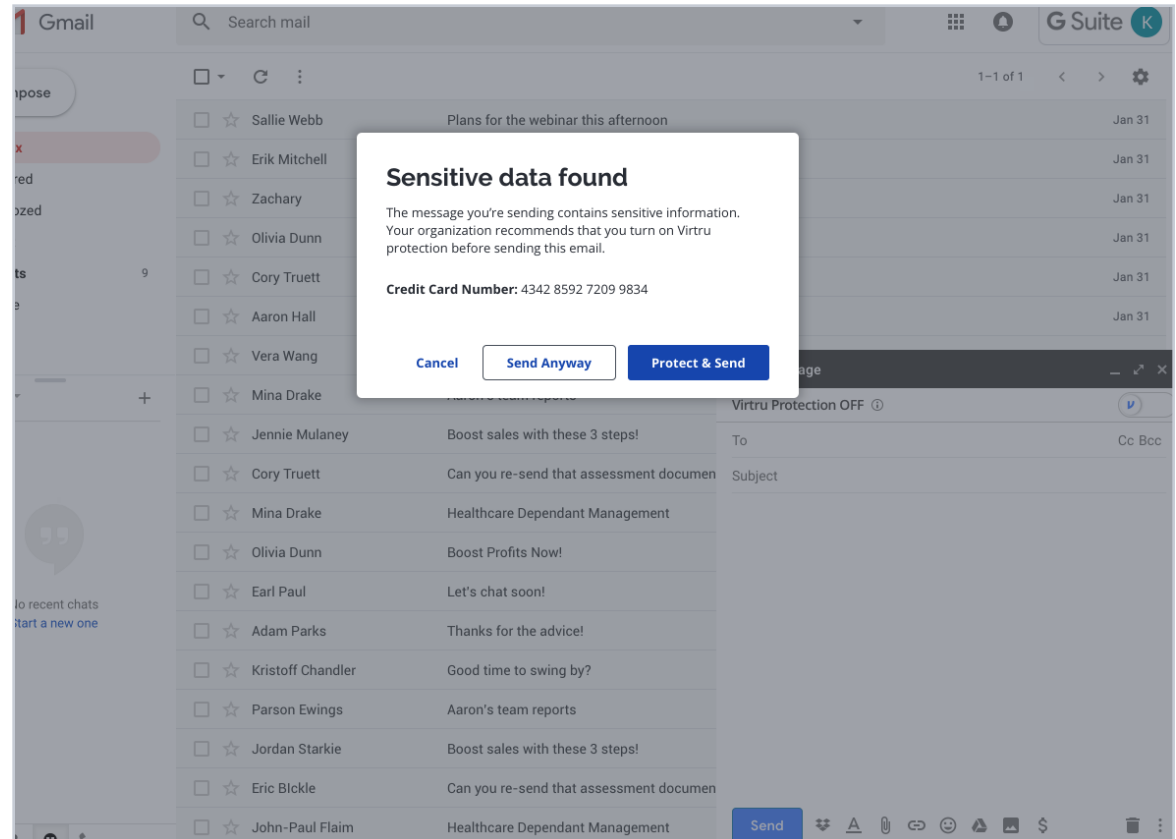
Email Rules

Custom Rules

To perform more complex DLP operations—including multiple scan parameters, multiple actions, and additional action types—you'll want to use a Custom Rule. More information on how to create a custom rule can be found in the deep dive below.

Additional Resources:

[Deep Dive on Managing DLP Rules](#)

[Deep Dive on Creating Custom DLP Rules](#)

6. Additional Features and Products

1. **Customer Key Server (CKS)**

Virtru **Customer Key Server (CKS)** adds a layer of protection that lets you directly host encryption keys in your own cloud environment, or on-premise, and integrate with hardware security modules (HSMs) for the highest levels of confidentiality and control. This helps you fulfill data residency and data sovereignty requirements and strengthens your position on compliance including CJIS, ITAR, and EAR. Keys can be rotated in the Virtru Control Center.

Additional Resource:

Deep Dive: Virtru Customer Key Server (CKS)

Additional Features and Products

2. **Data Protection Gateway**

The Virtru Data Protection Gateway automatically protects email and attachments shared by unprotected endpoints and applications (custom internal applications, or enterprise SaaS applications for CRM, IT helpdesk, human resources, etc.). These emails and attachments then all become actionable from the Virtru Control Center. Flexible, hosted deployments align with your current applications and workflows so you can realize the full potential of your existing tools.

Additional Resource:

[Virtru Data Protection Gateway Data Sheet](#)

3. **Software Development Kit (SDK)**

With access to the Virtru Platform, developers are empowered to proactively protect the data utilized by their applications without slowing down the development process. The SDK allows you to innovate at scale and eliminate the burden of creating data protection infrastructure across the entire data lifecycle so you can focus on delivering the next great application. Manage access and track the encrypted data in Virtru's Control Center.

Additional Resources:

[Virtru Trusted Data Platform Overview](#)

[Virtru Software Development Kit (SDK)](#)

[Virtru Software Development Kit (SDK) Use Cases](#)

Summary

We hope this playbook provided you with the resources you need to unlock the benefits of the **Virtru Control Center**. As a reminder, our Support Team is always happy to answer your questions and provide additional help. Head over to our **Support Center** to browse how-to articles, submit a ticket, and more. Also, visit our **Customer Resource Library** to view on-demand webinars, detailed customer resources, and subscribe to our monthly newsletter.

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.