# Customer Lockbox in Office 365

This topic covers deployment and configuration guidance for features only currently available in Microsoft 365 E5, Office 365 E5, Information Protection and Compliance and Advanced Compliance SKUs.

Customer Lockbox ensures that no one at Microsoft can access customer content to perform a service operation without the customer’s explicit approval. Customer Lockbox brings the customer into the approval workflow for such access to customer content.

Occasionally, Microsoft engineers are involved during the support process to troubleshoot and help fix customer reported issues. In most cases these are fixed through extensive telemetry and debugging tools we have in place for our services; however, a few of these cases may require Microsoft engineer to access customer content to determine root cause and fix the issue. Customer Lockbox requires the engineer to request access from the customer as a final step in the approval workflow.

Organizations have the option to approve or deny these requests, thereby exercising control over if and when a Microsoft engineer may access their data.

Customer lockbox works with Exchange Online, SharePoint Online, and OneDrive for business. For support for more Office 365 workloads submit your feedback on Office 365 [UserVoice](https://office365.uservoice.com/).

## Customer Lockbox workflow

[Customer Lockbox overview video]

Below is a typical workflow when Customer Lockbox requests are initiated:

1. Someone at an organization has an issue with their Office 365 mailbox.
2. After some troubleshooting, when they can't fix the issue, customers open a support request with Microsoft support.
3. The support engineer reviews the service request and determines that there is a need to access customer’s Exchange Online content to repair the issue.
4. The support engineer logs into Customer Lockbox request tool and makes a data access request by specifying the *tenant name*, *service request number* and *duration* for which access is needed.
5. After Microsoft manager’s approval, the Customer Lockbox system sends the designated approvers an email letting them know there's a pending access request from Microsoft.

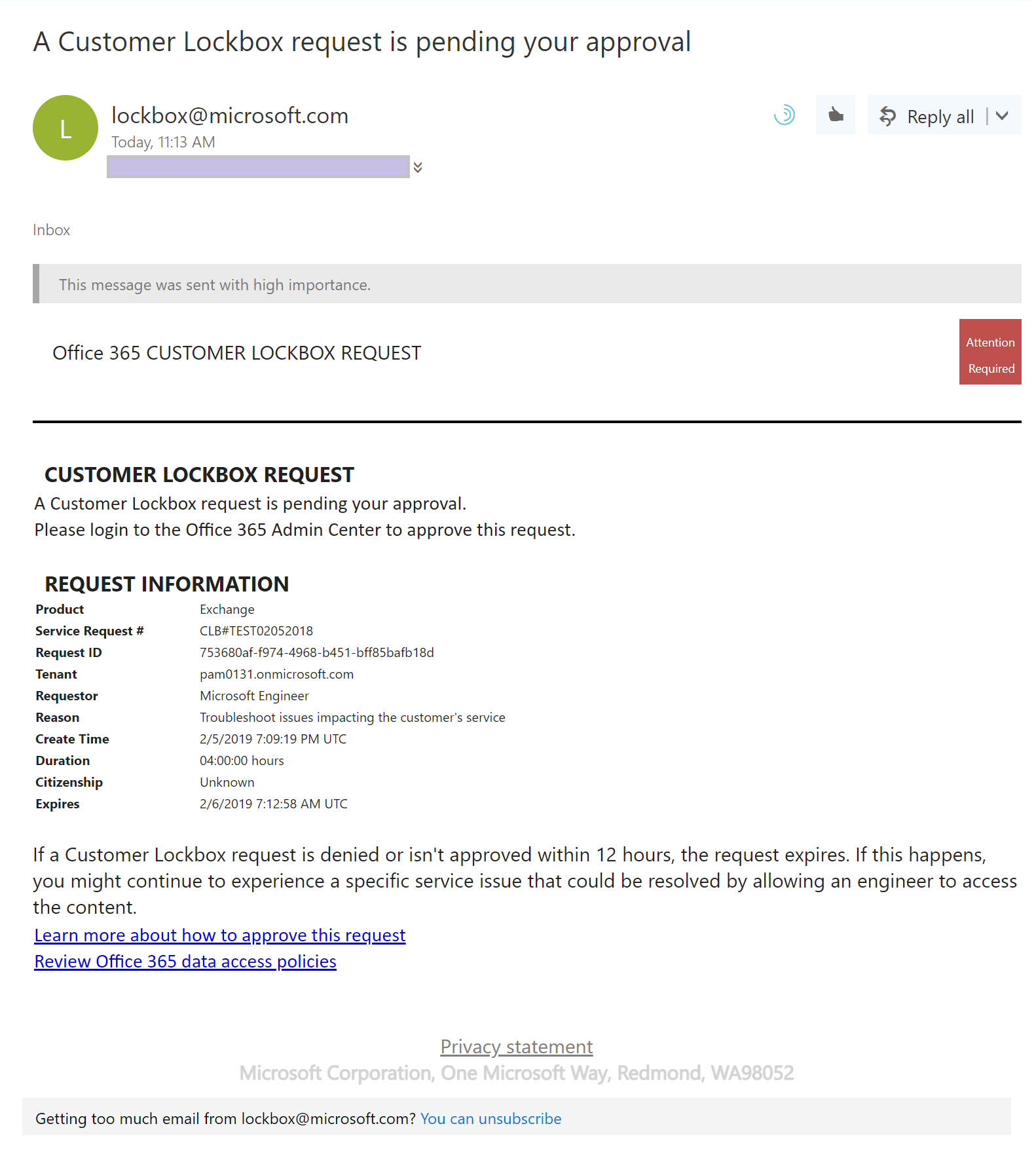


Figure - Customer lockbox request notification email

1. If the request is rejected or isn’t approved in the next 12 hours – when the request expires – no access is granted to Microsoft engineer.
2. Approvers log into the Microsoft 365 admin center and approve the request. This step also creates the Audit log for the Admin Action.

**Note**: We don't include any links in the Customer Lockbox email that requires you to login to Office 365.

1. The engineer receives the approval message, logs into Exchange Online and fixes the issue. Microsoft engineers have the requested duration to fix the issue after which the access is automatically revoked. All actions performed by a engineer are logged and available to review through Audit logs.

## Turn Customer Lockbox request on or off in the Microsoft 365 admin center

An Office 365 administrator can turn on Customer lockbox controls from the Microsoft 365 Admin Center. When this feature is turned on, Microsoft is required to obtain organization’s approval prior to accessing any organization content.

**Note:** To perform the following steps, you must be a Global Administrator, Customer Lockbox Access Approver or get Organization Management Role applied through Office 365 RBAC.

1. Sign in to Office 365 with your work or school account.
2. Go to the Microsoft 365 Admin Center
3. Navigate to **Settings** > **Security & Privacy** and scroll to locate **Customer Lockbox**

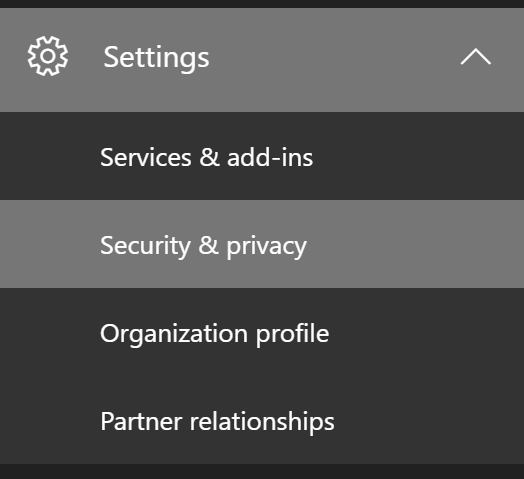


Figure - Navigation to Security and Privacy settings

1. Click **Edit** and move the toggle **On** or **Off** to turn the feature on or off.

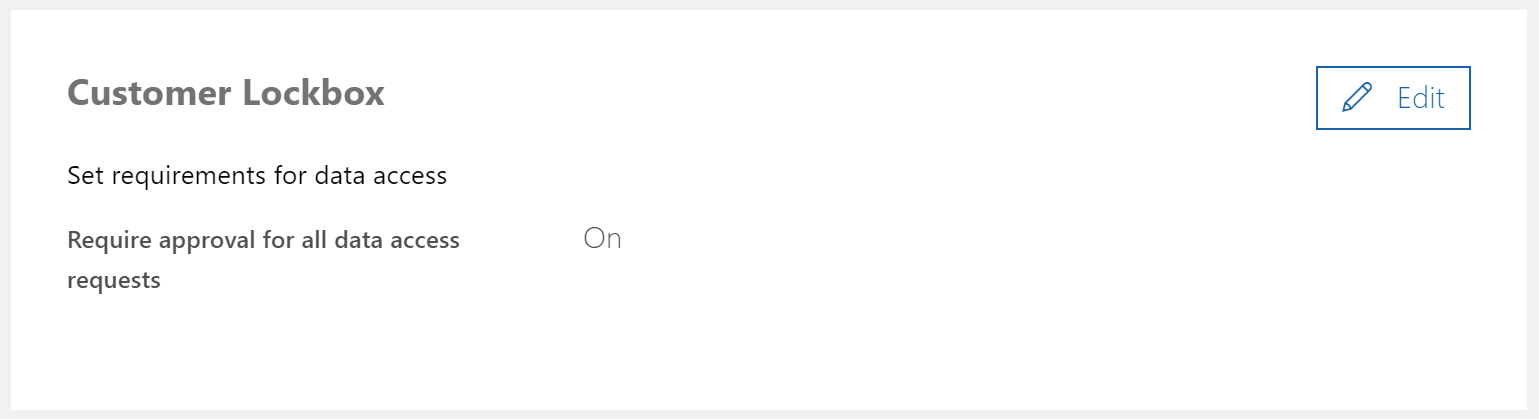


Figure - Customer lockbox settings widget

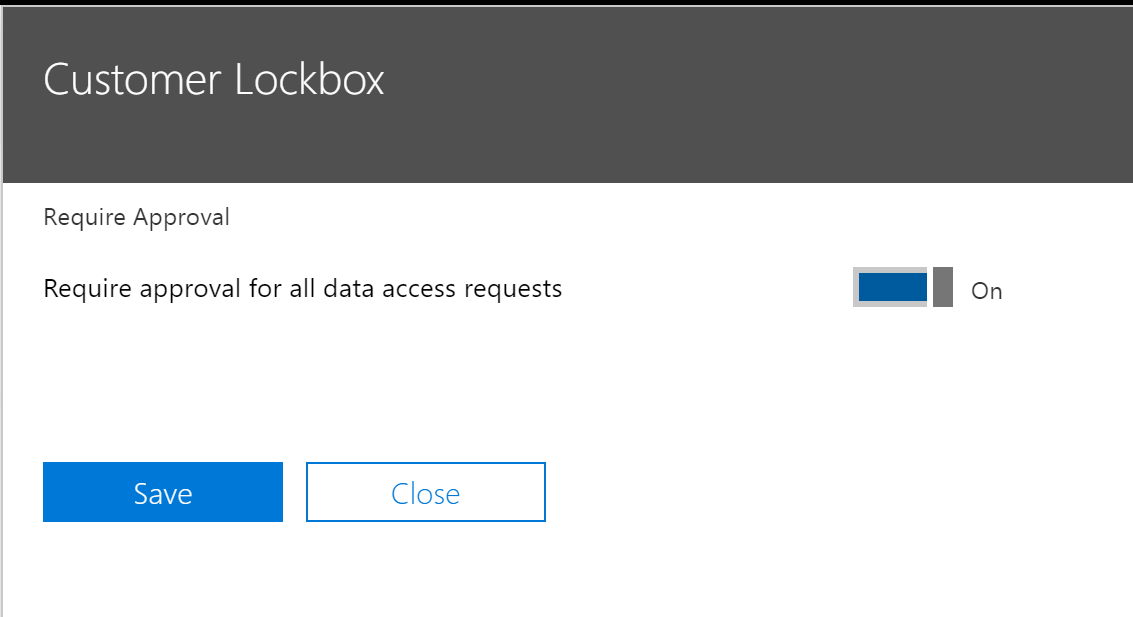


Figure - Customer lockbox settings widget toggle

## Approve or deny a Customer Lockbox request in the Microsoft 365 admin center

**Note:** To perform these steps, you must be a Global Administrator, Customer Lockbox Access Approver or get Organization Management Role applied through Office 365 RBAC.

1. Sign in to Office 365 with your work or school account.
2. Go to the Microsoft 365 Admin Center
3. Navigate to Support > Customer Lockbox Requests to view the list of all requests

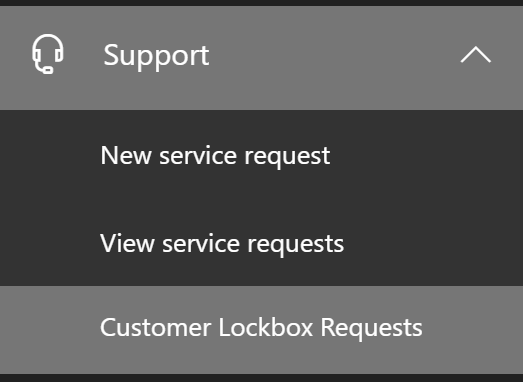


Figure - Navigation to Customer Lockbox requests list

1. Select a Customer Lockbox request and then select **Approve** or **Deny**

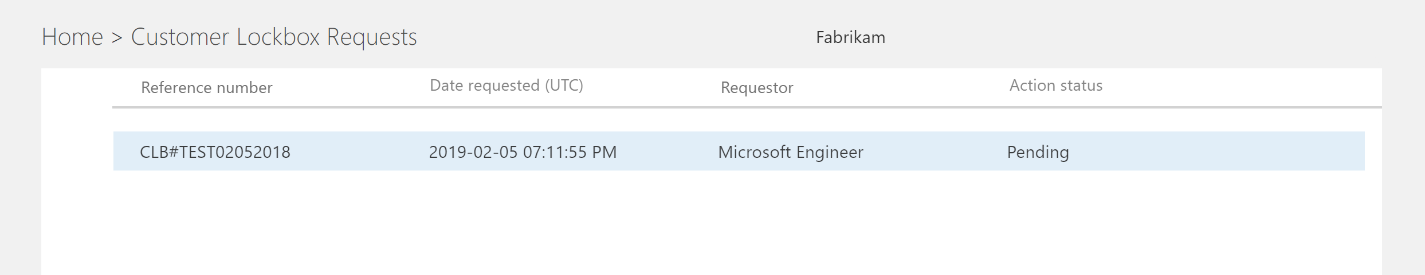


Figure - Customer Lockbox requests list

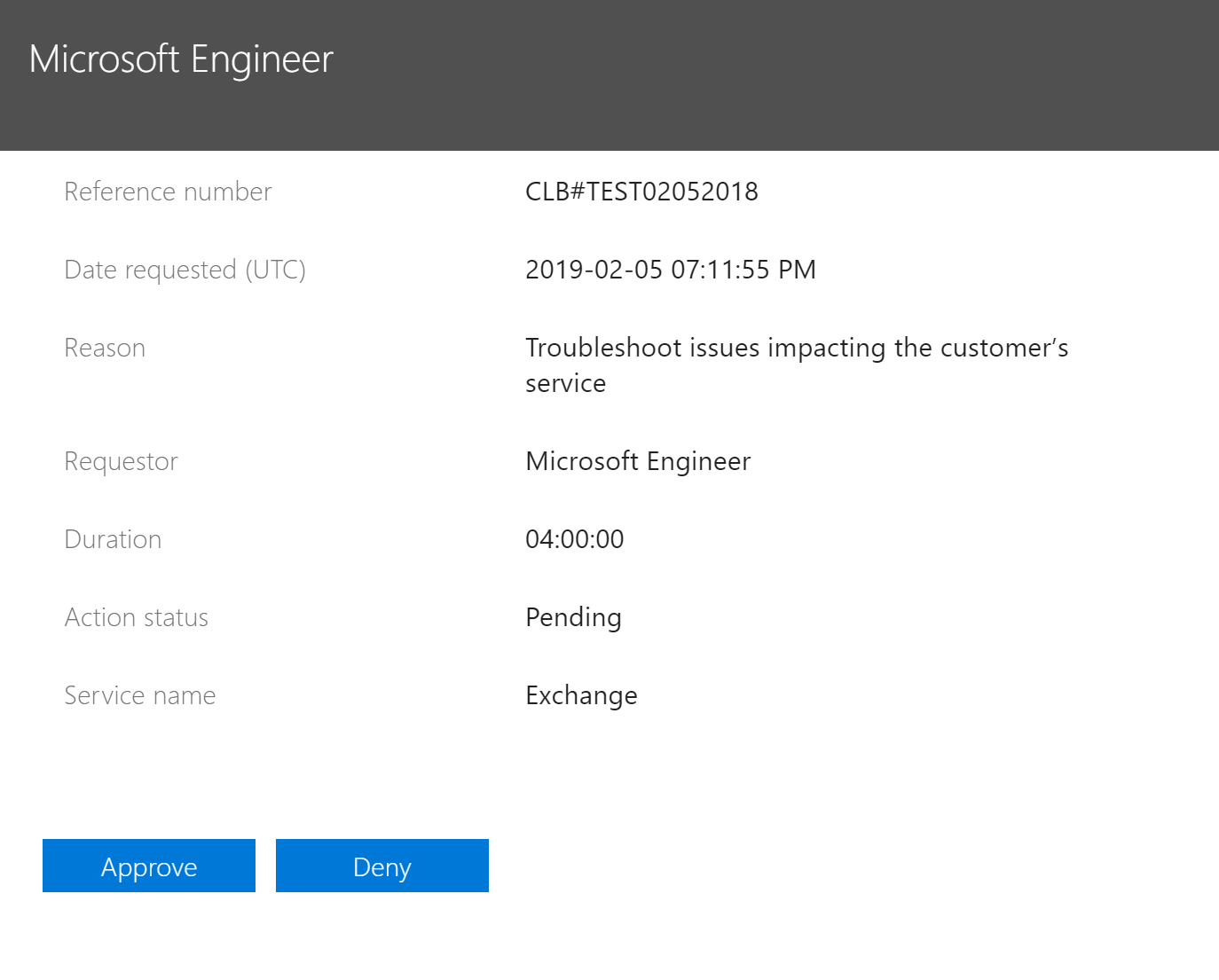


Figure - Customer Lockbox request details

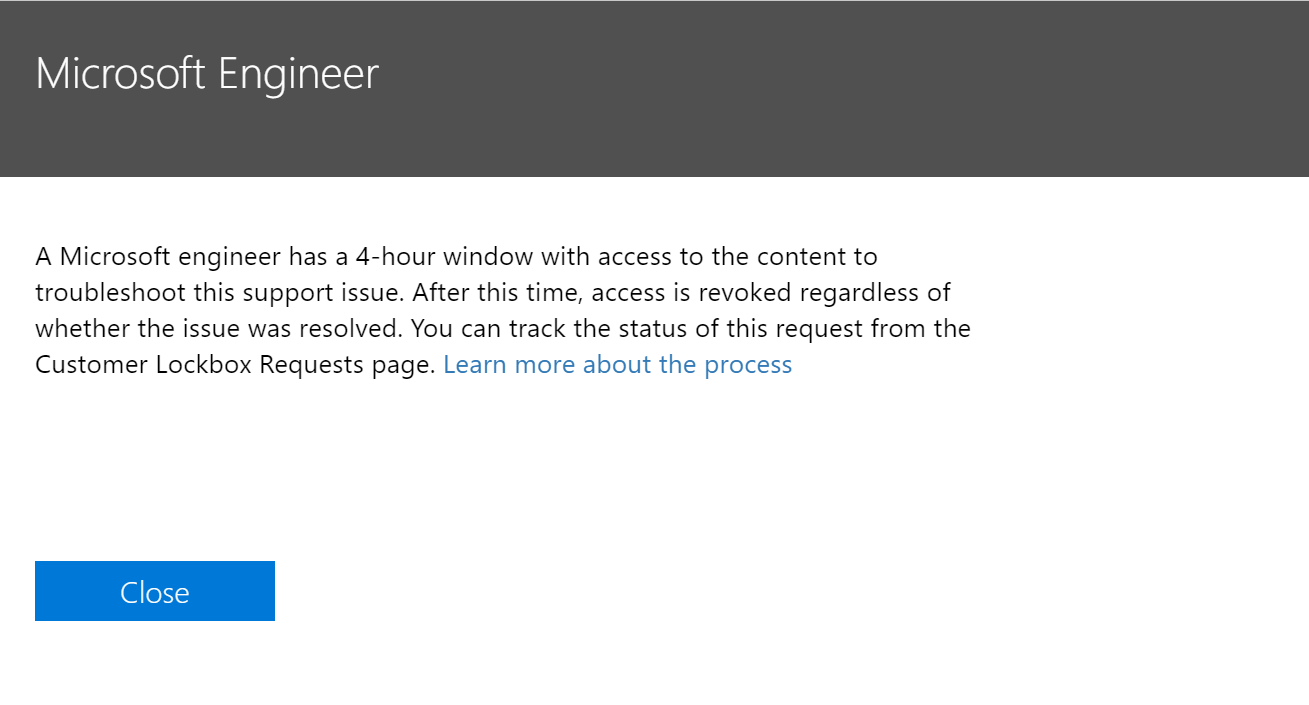


Figure - Customer Lockbox request approval confirmation message

## Auditing Customer Lockbox requests

Audit logs for Customer lockbox are available in the Office 365 [Security & Compliance Center](https://docs.microsoft.com/en-us/office365/securitycompliance/) to view among other Audit logs. Actions taken with respect to individual customer lockbox request decision, and any actions performed by Microsoft engineers when access requests are approved, are logged and available to review.

### Decisions on Customer Lockbox access requests

Approver actions on Customer Lockbox are logged to the Audit logs with this information:

|  |  |
| --- | --- |
| Date | Date time when the request was approved |
| IP address | The IP Address of the machine approver used to approve a request |
| User | BOXServiceAccount@[customerforest].prod.outlook.com |
| Activity | Set-AccessToCustomerDataRequest |
| Item | Guid of the customer lockbox request |

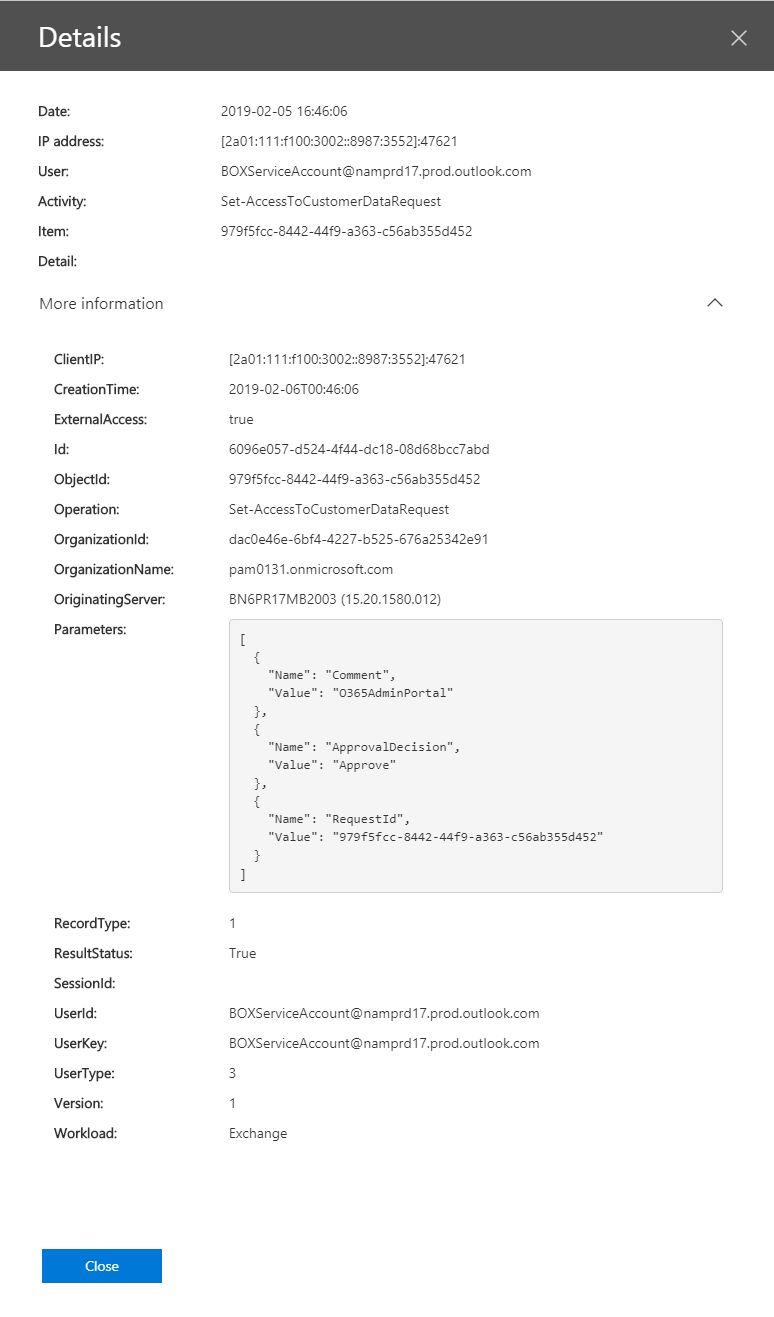


Figure - Audit log detail for approver action

### Microsoft engineer sample actions

Microsoft engineer actions that access customer content – performed when a Customer Lockbox request has been approved – are also logged to the Audit Logs with this information:

|  |  |
| --- | --- |
| Date | Date time when the action was performed |
| IP address | The IP Address of the machine Microsoft engineer used |
| User | Microsoft Operator |
| Activity | Name of the activity performed |
| Item | <empty> |

All actions performed by a Microsoft engineer can be filtered by using “Microsoft Operator” for User field:

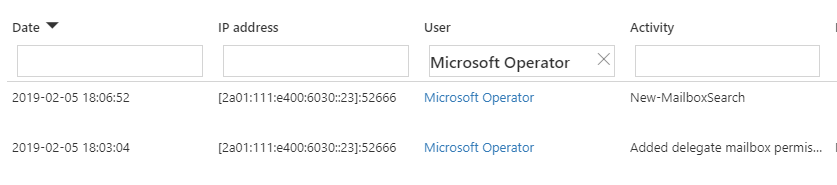


Figure - Audit log search for actions performed by Microsoft engineer

## Frequently asked questions

#### Which Office 365 services does Customer Lockbox apply to?

Customer lockbox is currently supported in Exchange Online, SharePoint online and OneDrive for business.

#### Is Customer Lockbox available to all Office 365 customers?

Customer Lockbox is included with the Microsoft 365 or Office 365 E5 plan and can be added to other plans through Information Protection and Compliance or the Advanced Compliance SKU. Check out [Plans and pricing](https://products.office.com/en-us/business/office-365-enterprise-e5-business-software) for more info.

#### What is customer content?

Customer content is the data created by users of Office 365 Services. Examples of customer content include:

* E-mail body or e-mail attachments
* SharePoint site contents
* Information in the body of a SharePoint file
* Skype for Business Presentation File body
* IM or Voice Conversations
* Customer generated blob or structured storage data (e.g., SQL Containers)
* Customer-owned security information (e.g., certificates, encryption keys, passwords)
* Inferences, and all subsequent inferences, if customer content remains

For additional details on customer content within Office 365, see the [Office 365 Trust Center](http://trust.office365.com/).

#### Who is notified when there is a request to access my content?

The Global Administrators and the Customer Lockbox Approver Roles are notified. They are also the approvers for Customer Lockbox requests.

#### Who can approve or reject these requests in my organization?

Users who are assigned Global Admin or Customer Lockbox Approver roles are eligible to approve Customer Lockbox requests. Customers control these role assignments within their organizations.

#### How do I opt-in to Customer Lockbox?

The tenant administrator can enable and configure Customer Lockbox from the Microsoft 365 Admin Center.

#### If I grant access, what can the engineer do and how can I see what the engineer did?

Once the customer grants access through Customer Lockbox, the engineer has privileges to access customer content using pre-approved cmdlets. Actions taken by Microsoft engineers in response to Customer Lockbox requests are logged and accessible via the audit logs in the Office 365 [Security and Compliance center](https://docs.microsoft.com/en-us/office365/securitycompliance/).

#### How do I know that you follow this process?

Customers can cross-reference the email approval notifications received by Tenant Admins and the Customer Lockbox request history in the Microsoft 365 Admin Center.

Additionally, Customer Lockbox was included in the latest [SOC 1 SSAE 16 audit report](https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=91592749-e86a-43ac-801e-121382614681&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_SOC%20%2F%20SSAE%2016%20Reports). For more details you can find the latest reports in [Service Trust Portal](https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=91592749-e86a-43ac-801e-121382614681&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_SOC%20%2F%20SSAE%2016%20Reports).

#### Can Microsoft modify the list of approvers for my tenant? If not, how is it prevented from happening?

The Tenant Admin group is an identity within Azure Active Directory that is solely managed by the customer.

#### What if I need more information on the content access requests to approve it?

Each Customer Lockbox request will contain an Office 365 service request number that you can reference when you contact Microsoft Support Services for additional details.

#### What happens if I don’t respond to a Customer Lockbox request in a timely manner?

Customer Lockbox requests have a default lifetime of 12 hours, after which they expire and cannot be acted upon.

#### When a Customer Lockbox request is approved, how long are the permissions valid?

The maximum period for permissions granted following a Customer Lockbox approval is currently 4 hours. The Microsoft engineer may request a shorter period as well.

#### How can I get a history of all Customer Lockbox requests?

All Customer Lockbox requests can be viewed directly from the Microsoft 365 Admin Center.

#### How do I correlate the content access requests with the access logs that I have?\

The Compliance Center Activity Feed will contain log activities of Customer Lockbox. Customers can cross-reference the Customer Lockbox log activities from the activity feed against the email request they receive.

#### What happens to requests where a customer does not respond to Customer Lockbox request?

Customer lockbox requests have a validity of twelve (12) hours. Requests that are not acted on within 12 hours expire and cannot be approved.

#### What does Microsoft do in case the customer rejects a Customer Lockbox request?

If a customer rejects a Customer Lockbox request no access to customer content will occur. If a tenant user was experiencing a service issue that required Microsoft to access customer content in order to resolve the issue (though such circumstances are rare) then the service issue might persist, and Microsoft would inform the customer of this outcome.

#### Does Customer Lockbox protect against data requests from law enforcement or other third party?

No. Microsoft takes third-party requests for customer data very seriously. As a cloud service provider, we always advocate for the privacy of customer data. In the event we get a subpoena, we always attempt to redirect the third party to the customer to obtain the information. (Please read Brad Smith's blog: [Protecting customer data from government snooping](https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/)). We periodically publish detailed information of the request we receive [here](https://www.microsoft.com/en-us/trustcenter/Privacy/govt-requests-for-data).

See the [Microsoft Trust Center](https://www.microsoft.com/en-us/trustcenter/default.aspx) regarding third-party data requests and "Disclosure of Customer Data" in the [Online Services Terms (OST)](https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx) for more information.

#### How does Microsoft ensure that a member of its staff does not have standing access to customer content in Office 365 applications?

Microsoft implements extensive preventive measures through access control systems, and detective measures to identify and address attempts to circumvent the access control systems. Office 365 operates with the principles of least privilege and just-in-time access. Therefore, no Microsoft personnel have permission to access customer content on an ongoing basis. If permission is granted, it is for a limited duration. [Please refer to the Online Services Terms (OST) for more detail on our general security practices](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fen-us%2FLicensing%2Fproduct-licensing%2Fproducts.aspx&data=04%7C01%7Cabhiku%40microsoft.com%7Cf859cbccf4884b56828908d68bb90f75%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636850025352464694%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C-1&sdata=jvhIyLPthEDUXirWt3xeEy6SeP8LlIq6d2vPcO5eBrM%3D&reserved=0).

Office 365 uses an access control system called Lockbox to process requests for permissions that grant the ability to perform operational and administrative functions within the service. An operator must request access to customer content using Lockbox, which then requires a second person to take action on the request (e.g., approve it) before access is granted. That second person cannot be the requestor and must be designated to approve access to customer content. Only if the request is approved does the operator acquire temporary access to customer content. Once the elevation period expires the access is revoked by Lockbox.

[Please refer to the Online Services Terms (OST) for more detail on our general security practices as it pertains to access restrictions.](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.microsoft.com%2Fen-us%2FLicensing%2Fproduct-licensing%2Fproducts.aspx&data=04%7C01%7Cabhiku%40microsoft.com%7Cf859cbccf4884b56828908d68bb90f75%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636850025352474690%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C-1&sdata=I29KTn3vsv6b7uRW%2BoWgGFj1gRfCU9fLOBqbwInNWw0%3D&reserved=0)

#### Under what circumstances do Microsoft engineers need access to my content?

The most common scenario where Microsoft engineers may need to access customer content is when the customer makes a support request that requires access to troubleshooting. A foundational principle of Office 365 is that we should be able to operate our service without Microsoft personnel having access to customer content, and nearly all service operations performed by Microsoft are fully automated and the human involvement is highly controlled and abstracted away from customer content. What we aspire to achieve for Office 365 is that we never have access to customer content to support the service until the customer approves a specific request that allows Microsoft personnel such access. The ability to offer Customer Lockbox reflects our engineering progress.

#### I already thought my data was secure with the Microsoft cloud, so why do I need Customer Lockbox?

Customer Lockbox provides an additional layer of control by offering customers the ability to give explicit access authorization for service operations. By demonstrating that procedures are in place for explicit data access authorization, Customer Lockbox may also help customers meet certain compliance obligations such as HIPAA and FEDRAMP.