Kiteworks

Kiteworks Administrator Guide

August 2025

Version 9.1.0-01

Copyright

Corporate Headquarters

Kiteworks USA, LLC
1510 Fashion Island Blvd., Suite 100
San Mateo, CA 94404, USA

Contact Us

p. 1.650.485.4300 | f. 1.650.485.4308
www.kiteworks.com

Table of Contents

What's new

New features in the Kiteworks Admin Console

Improved storage cleanup ensures continuous system availability when uploading large files

When cleaning up storage, the Nginx cache is also cleared to free up space issues that result when large files uploaded from Repositories Gateway sources consume excessive temporary storage.

See Clean up storage.

SFTP connection improvements

Kiteworks SFTP performance has been significantly improved to enhance the speed and efficiency of SFTP connections. This update replaces Python-based connection scripts with optimized C and Golang implementations, eliminating the overhead of initializing Python interpreters for each connection. The result is up to 60% faster connection times. This improvement is particularly valuable for organizations with high-volume file transfer requirements who need enterprise-grade SFTP performance. Users will experience faster SFTP connection times and more reliable performance under high-load conditions without any workflow changes.

Node Migration Wizard for migrating nodes between on-premises and cloud environments

The Node Migration Wizard (formerly available only for CentOS 7 to Rocky 8 migrations) is now available for general usage, enabling system administrators to migrate nodes between on-premises and cloud environments regardless of operating system upgrade requirements. This provides a guided process for moving server roles between nodes. System administrators can perform node migrations for operational needs such as hardware refreshes, data center relocations, or cloud transitions without waiting for operating system upgrade scenarios.

The wizard supports most server roles, including Anti-virus, Application, File Storage, Search, and Web, making it a versatile tool for infrastructure management. To migrate a node, go to System Setup > Locations. Click the Migration Wizard button and follow the instructions to perform system prechecks, role migration, and post-migration system checks.

See Migrate nodes using the migration wizard.

Review license changes upon license upload

When uploading a new license, administrators must now review and accept the End User License Agreement (EULA) before uploading the license. The upload process provides a clear comparison between the current and new license, highlighting key differences such as feature changes or capacity adjustments. This streamlined process ensures administrators are fully informed about license changes while maintaining proper legal compliance.

See View and upload licenses.

Location mapping enhancements

Location mapping has been enhanced to provide a consistent management approach across all clients. This ensures that user files are always uploaded to the appropriate location based on system priority – the user's preferred upload location (highest priority), the system default location (if no preference is set), or the closest server based on network latency (lowest priority).

- Administrators can set preferred upload locations for non-LDAP and non-SSO users, giving their organization better control over where files are stored to meet compliance requirements or to optimize performance. This provides more predictable file storage behavior and helps ensure data sovereignty requirements are met.
- When configuring location mapping at the system level, administrators can enforce stringent location mapping to route file uploads directly to a specified location instead of routing file uploads through the main host name. Note that the DNS name must be reachable or file uploads will fail.

See Configure location mapping.

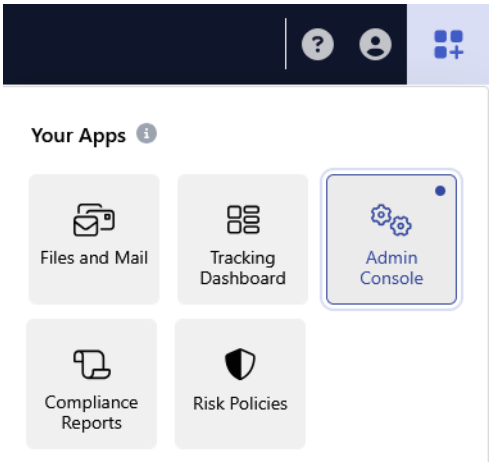
Storage alert enhancements

Administrators assigned the System Admin role can set up more precise notifications for when storage is running low. The feature introduces five distinct storage alert categories (Database Storage, System Storage, Log Storage, File Storage, and Other Storage) with customizable thresholds based on both percentage and absolute gigabyte values. Choose whether to trigger an alert when either condition is met or only when both conditions are met. This granular control helps prevent unexpected system downtime by providing early warnings when storage resources are running low, allowing for proactive management of system resources.

See Configure storage alerts.

New "App Switcher" for navigating between applications

Introducing an App Switcher for quickly navigating between features and applications available to you in the Kiteworks Private Data Network (PDN). In the upper right corner of the admin console, click the App Switcher button.



- Files and Mail - Opens the Kiteworks Web Application for accessing files, folders, and messages.
- Tracking Dashboard - Opens the Tracking Dashboard in the Kiteworks Web Application for tracking messages sent to recipients.
- Admin Console - Opens the Kiteworks Admin Console.

- Compliance Reports - Opens the Compliance Reports app for generating audit log, insider threat, outsider threat, and CMMC 2.0 reports to maintain stringent compliance with industry regulations and internal policies.
- Risk Policies - Opens the Risk Policy Builder app for creating risk policies to protect sensitive content moving through the Kiteworks system.

Note: At this time, the App Switcher is available only in the Kiteworks Admin Console, Kiteworks Web Application, and Kiteworks Compliance Console. Only administrators and users with specific roles can see the App Switcher, and the user's role determines which apps they can access from it.

See Switch between apps.

Automate folder creation for specific Salesforce case types

The Kiteworks for Salesforce Lightning plugin supports using Apex Triggers to automatically create Kiteworks folders based on Case Record Type ID. This enables specifying which Case Record Types should activate the Apex Triggers, rather than having triggers activate for all cases regardless of type. Filtering triggers to run only on relevant case types enables more efficient workflows, reduces unnecessary processing, and implements different automation rules for different types of support cases or business processes within your Salesforce environment. For instructions on how to configure APEX Triggers in Salesforce Lightning, refer to the Kiteworks Administrator Guide.

See the "Apex Trigger on Creation" section in how to configure Kiteworks for Salesforce Lightning.

System stability improvements

Kiteworks now includes advanced resource management capabilities using Linux Control Groups (CGroups) version 2 to protect critical system services during high load. This prevents system hangups by reserving resources for essential services like databases, while setting appropriate limits on non-critical processes. When memory pressure occurs, the new intelligent resource management system automatically identifies and terminates problematic processes, maintaining system stability and preventing extended outages. This significantly reduces the risk of system-wide performance degradation that could previously render Kiteworks as unresponsive for extended periods.

The system automatically organizes Kiteworks processes into resource groups (slices) with appropriate priority levels.

During high memory usage events, the system intelligently terminates non-critical processes to maintain overall system stability.

At this time this feature is available only for single-node deployments without the Kiteworks Email Protection Gateway (EPG) enabled on the node. If it meets your business needs, please contact Kiteworks technical support at https://community.kiteworks.com to have them enable it for you.

New "PubSub-ext" API for subscribing to Kiteworks events

For customers wanting to request a subset of Kiteworks events using an API, the new PubSub-ext API allows for the ability to subscribe and request only desired events from Kiteworks. This eliminates the need for parsing syslog output or output from the various “activities” APIs. Enabling this feature requires assistance from Kiteworks technical support. If it meets your business needs, please contact Kiteworks technical support at https://community.kiteworks.com to have them enable it for you.

Sign in to the Kiteworks Admin Console

Check your email for a welcome email from Kiteworks. This email contains your user name and password.

To sign in:

1. In a web browser, enter the address of your Kiteworks server followed by "/admin".

   Example: https://<kiteworks server host name>/admin
2. Type the user name or email address associated with your account, and then click Next.

   Tip: When LDAP or single sign-on policies are in place for your company, you typically enter a user name instead of an email address. If you don't know your user name, contact your Kiteworks administrator for assistance. You may also see a Contact Us link on the page for contacting your Kiteworks administrator.
3. Type your password, and then click Sign In.

   Alternative: If you forgot your password or need to change it, click the Forgot Password link and then follow the prompts reset your password.

To sign out:

In the upper right corner of the screen, click your user account profile picture, and then click Sign Out.

Designate advisory contacts to receive technical and security notifications

Kiteworks advisory contacts receive email notifications when product updates are released, features change or get deprecated, and when Kiteworks applications reach end of life. They also get notified when security warnings or recommendations are issued, security vulnerabilities are addressed, and security patches and updates are released.

Kiteworks relies on accurate contact information to inform about software updates, feature changes, and security updates necessary for protecting your Kiteworks system. If your company's contact information is not up to date, there may be delays in notifying you if a security event occurs.

Kiteworks recommends you periodically review the list of Kiteworks advisory contacts for your company to ensure that the information is current. At least two advisory contacts must be specified, but you can add additional contacts for receiving technical and security email notifications. To help you remember to periodically review your contact information, you're notified in the following ways:

- 90 days after the contact information was last confirmed, an alert badge is added to the Advisory Contacts button in the navigation pane.
- If more than 180 days have passed since the contact information was confirmed, the advisory contacts page displays each time an administrator signs in to the Kiteworks Admin Console until an administrator confirms the contact information.
- When you update your Kiteworks software license, if more than 180 days have passed since the contact information was confirmed, the advisory contacts page displays when uploading the new license. At this time you must confirm the contact information to update the license.

Add or update Kiteworks advisory contacts

When you add an advisory contact, the system sends that person an email notification requesting their confirmation. The confirmation process differs depending on whether the user has an active user account on the Kiteworks system or they are an external user.

- If the user has an active user account on the Kiteworks system (they have signed into the system at least one time), opening the email notification automatically qualifies as their confirmation. No further action is required from them. If they are a new Kiteworks user and have not yet signed into the system, they will need to click the Confirmation button in their email notification to confirm their status as an advisory contact.
- If the user is an external user (they do not have a user account on the Kiteworks system), they will need to click the Confirmation button in the email notification to confirm their status as an advisory contact.

  An external advisory contact must confirm their status within 10 days of receiving their email notification. If they have not confirmed their status after 5 days, they will receive an email reminder to confirm their status. If they have not confirmed their status after 10 days, they will be removed from the list of advisory contacts and informed of this action. You will also be notified. Throughout this process, you will also receive email notifications keeping you informed of their confirmation status.

Although an advisory contact does not require a user account on the Kiteworks system, if they create a user account, they will consume a new Kiteworks user license.

To add an advisory contact:

1. Access advisory contacts in one of the following ways:
   - In the Kiteworks Admin Console navigation pane, click Advisory Contacts.
   - In the Compliance Console, click Advisory Contacts.
2. On the Company Advisory Contacts page, click Add New Contact.
3. Enter the first and last name of the contact, and their email address for receiving email notifications.
4. To confirm that the information is up to date, click Contacts Are Correct.

   Result: Until a new advisory contact confirms their status, their status on the Company Advisory Contacts page is listed as Pending. Once confirmed, their status changes to Verified.

To edit an advisory contact:

First delete the contact and then add it again as a new contact with the updated information. Then click Contacts Are Correct.

To delete an advisory contact:

In the contact row, click Delete .

Edit your account profile

You can edit your account profile to change your display name (instead of your email address), display the time in your timezone or in GMT, and change your password for accessing the console.

To edit your account profile:

1. In the upper right corner of the screen, click your profile picture, and then click Edit Settings.
2. On the Account Info page, edit your profile settings, and then click Save.

Table 1. Account profile settings

Setting	Description
Display name	Enter a custom name to display in the application. Otherwise, your email address is displayed.
Display date and time	Select whether to display the time using your browser's timezone or in GMT. **Exception:** The audit log always displays GMT time in log reports.
Change password	Enter and confirm your new password.

Change your password

If someone created a password for you, you should change it immediately so that your account is secure.

If you need to change your password, you can reset it in your profile settings.

To change your password:

1. In the upper right corner of the screen, click your profile picture, and then click Edit Settings.
2. On the Account Info page, enter and confirm your new password, and then click Save.
3. To use your new password, sign out and then back in again.

Manage your Kiteworks subscription plan

If you're a Kiteworks Business customer, you can manage your subscription plan though the Kiteworks Admin Console. In the My Account service portal, you can edit your account settings, add user licenses (up to 100), update billing addresses and payment methods, and subscribe to account notifications, including alerts for when credit cards are about to expire.

You can also access the My Account portal from these locations in the Kiteworks Admin Console:

- System Status page. In the "Licenses" section, click the "Add licenses" link.
- User Management tab. In the upper right corner of the page, click the "Add licenses" link.
- Kiteworks License page (Application Setup > Licenses > Kiteworks License). In the "User License" section, click "Add licenses" link.

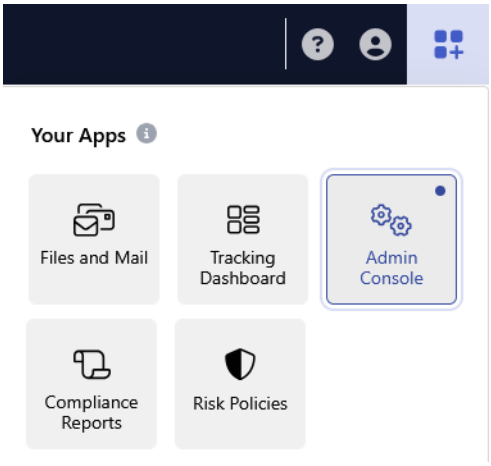
The Manage Subscription Plan menu option is also available to business customers from the Kiteworks Web application user account profile menu. To access the My Account portal, they must also have administrator access to the Kiteworks Admin Console.

View product documentation

From the Help menu you can access administrator guides, view your current Kiteworks software version, get a list of new features in the release, and read the release notes.

Switch between apps

You can easily switch between Kiteworks features and apps that you have access to. In the upper right corner of the admin console, click the App Switcher button.



At this time, the App Switcher is available only in the Kiteworks Admin Console, Kiteworks Web Application, and Kiteworks Compliance Console. Only administrators and other users with specific roles can see the App Switcher, and the user's role determines which apps they can access from it.

- System Admin and Application Admin roles can access all apps from the App Switcher in the Kiteworks Admin Console, Kiteworks Web Application, and the Compliance Console.
- Helpdesk Admin and DLI Admin roles can access only the Admin Console, Files and Mail and Tracking Dashboard apps from the App Switcher only from the Kiteworks Admin Console and the Kiteworks Web Application.
- Compliance role can access only the Files and Mail, Tracking Dashboard, Compliance Reports, and Risk Policies apps from the App Switcher, and only from the Kiteworks Web Application and the Compliance Console.
- Policy Manager role can access only the Files and Mail, Tracking Dashboard, and Risk Policies apps from the App Switcher, and only from the Kiteworks Web Application and the Compliance Console.
- Auditor role can access only the Files and Mail, Tracking Dashboard, and Compliance Reports apps from the App Switcher, and only from the Kiteworks Web Application and the Compliance Console.

Table 2. App Switcher apps

App	Description
Files and Mail	Opens the Kiteworks Web Application for accessing files, folders, and messages.
Tracking Dashboard	Opens the Tracking Dashboard in the Kiteworks Web Application for tracking messages sent to recipients. You can create tracking dashboards to track messages based on subject line keywords, messages that contain file attachments, and messages sent during a specific time period. **Requirement:** To access the Tracking Dashboard from the App Switcher, the feature needs to be enabled in the user's profile. Go to Users > Profiles. In the profile, go to the Send File tab and turn on the Tracking Dashboard switch. See Create and edit user profiles.
Admin Console	Opens the Kiteworks Admin Console.

Table 2. App Switcher apps (continued)

App	Description
Compliance Reports	Opens the Compliance Reports app for generating audit log, insider threat, outsider threat, and CMMC 2.0 reports to maintain stringent compliance with industry regulations and internal policies. The Compliance Reports app is available if the Advanced Governance add-on package was purchased as part of the Kiteworks Enterprise package. For more information, refer to the *Getting Started with the Compliance Console* guide on the Help menu in the Compliance Console.
Risk Policies	Opens the Risk Policy Builder app for creating risk policies to protect sensitive content moving through the Kiteworks system. A limited number of risk policies can be created as part of the Kiteworks Enterprise package. Unlimited risk policies can be created if you purchased the Advanced Governance add-on package. For more information, refer to the *Getting Started with the Compliance Console* guide on the Help menu in the Compliance Console.

Note: In addition to using the App Switcher, you can still switch between the Kiteworks Admin Console and the Kiteworks Web Application from your user profile menu in the upper right corner of the admin console.

- To switch to the Kiteworks Web Application, click your profile picture, and then click Switch to User View.
- To return to the Kiteworks Admin Console, click your profile picture in the Kiteworks Web Application, and then click Switch to Admin Console.

Monitor high-level system activity and health

The System Status page enables you to monitor the overall activity and health of the system.

- Current Activities - Displays the number of used and available licenses, the number of file uploads and downloads during the audit log retention period, and any files that have been quarantined by antivirus, data leak prevention, and advanced threat protection policies.
- Cluster Health - Displays the status, performance, and storage availability of each server in the cluster. Click a server node to expand its dashboard and configuration settings.

See license usage

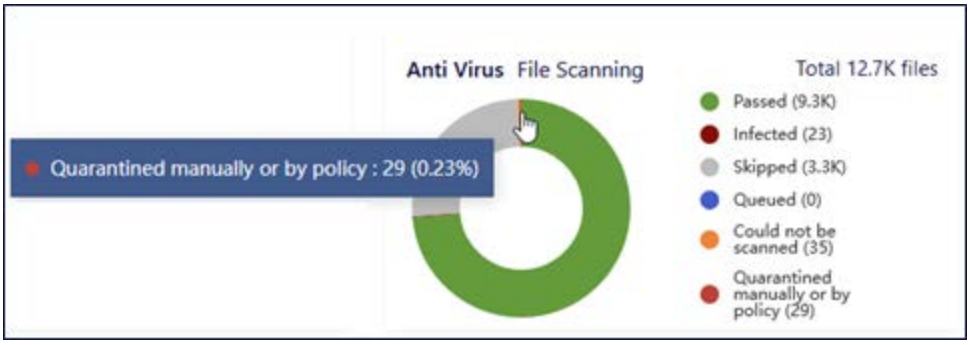
View or hover to display the number of used and available licenses. Click a grey bar in the license section to go to the Users page from which to also view the number of internal and external Salesforce licenses.

Track file activity

See the number of file uploads and downloads that occurred during the configured audit log retention period.

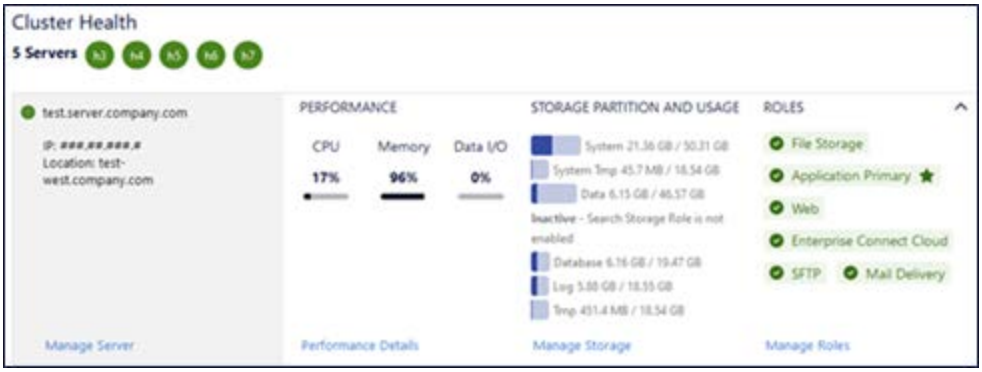
Identify file scan issues

Identify issues, such as files quarantined by antivirus, data leak prevention, and advanced threat protection policies. Click a chart area to drill into the details.



Monitor system health

Monitor the status, performance, and storage availability of each server in the cluster. Click a server node to expand its dashboard and configuration settings



CISO Dashboard

About the CISO Dashboard

The CISO Dashboard is used to monitor all content entering and leaving the Kiteworks enterprise. It provides a global view for drilling down to individual file transfers and generating detailed compliance reports that provide proof of your full visibility and control over the exchange of sensitive enterprise information. Among its capabilities, the CISO Dashboard provides:

- A real-time and historical view of all inbound and outbound file movement.
- All activity of who's sending what to whom, when, and where.
- Ability to group Kiteworks usage by client to easily see how users are accessing or attempting to access Kiteworks. On clicking Uploads, Downloads, Logins, or Invalid Login Attempts, filter by particular client.
- Track mobile usage.
- Export to spreadsheet for further analysis.

Additionally, the CISO Dashboard provides the ability to see files that violate AV, DLP, or ATP service when enabled. Click the pie-chart to view the status per file. The file list shows the file name, who uploaded the file, the Repositories Gateway source (if applicable), and the AV, DLP, or ATP response.

Note: GDPR and HIPAA compliance reports are separately licensed offerings with Kiteworks Advanced Governance, which also include anti-virus, data leak prevention, and advanced threat protection (including CheckPoint) and compliance reporting.

Access the CISO Dashboard

To access the CISO Dashboard and any licensed compliance reports you must be assigned one of the following roles: System Admin, Application Admin, CISO, DLI Admin, or assigned a custom role with access to the dashboard.

Note: Administrators assigned the CISO role can access only the CISO Dashboard, no other pages in the Kitworks Admin Console. Users assigned the DLI Admin role have view-only access to the CISO Dashboard.

You can access the CISO Dashboard in one of the following ways:

- In the navigation pane, click CISO Dashboard.
- Sign in to the CISO Dashboard using the following URL: https://<hostname>/ciso.

Install and configure the CISO Dashboard

To use the Kiteworks CISO Dashboard, download and install the following apps from the Splunkbase marketplace site:

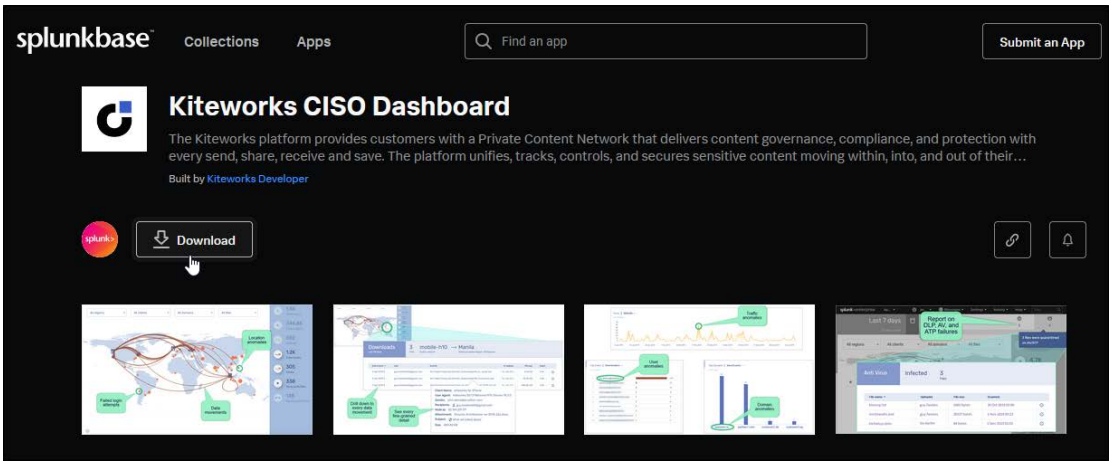
- Kiteworks CISO Dashboard
- Kiteworks CISO Dashboard Add-On

To download and install the Kiteworks CISO Dashboard apps from the Splunkbase marketplace:

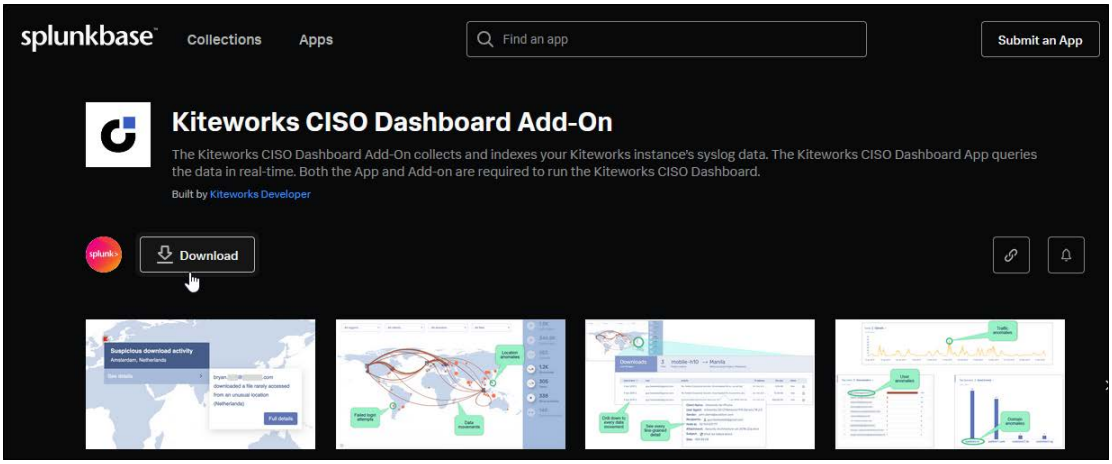
1 On the Kiteworks Admin Console Help menu, click Kiteworks Splunk CISO Dashboard App.

Alternative: Go to the Splunkbase marketplace at https://splunkbase.splunk.com/app/4764.

2 On the Splunk marketplace site, sign in to your Splunk account, and then download the Kiteworks CISO Dashboard app.

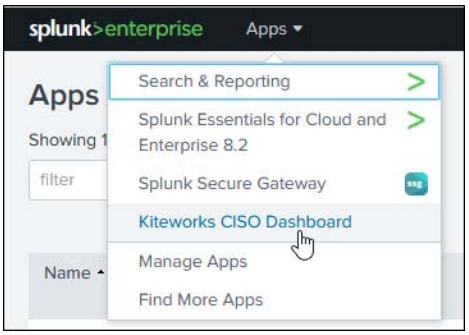


3 In the Splunkbase search box, search for the Kiteworks CISO Dashboard Add-On, and then download the app.

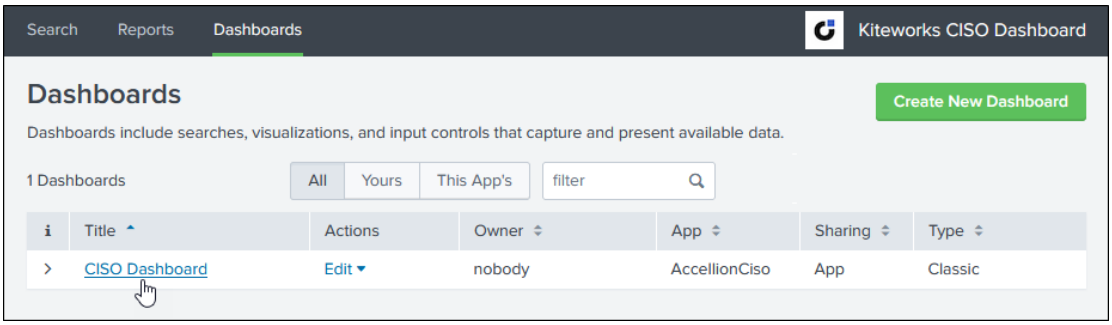


4 From your download folder, install both apps.

5 After installing in both apps, open Splunk Enterprise, and on the menu click Apps > Kiteworks CISO Dashboard.



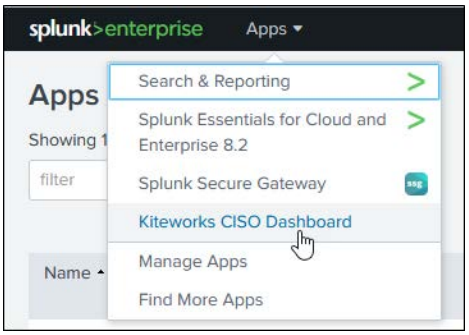
6 On the Kiteworks CISO Dashboard search page, click the Dashboards tab, and then click the CISO Dashboard link.



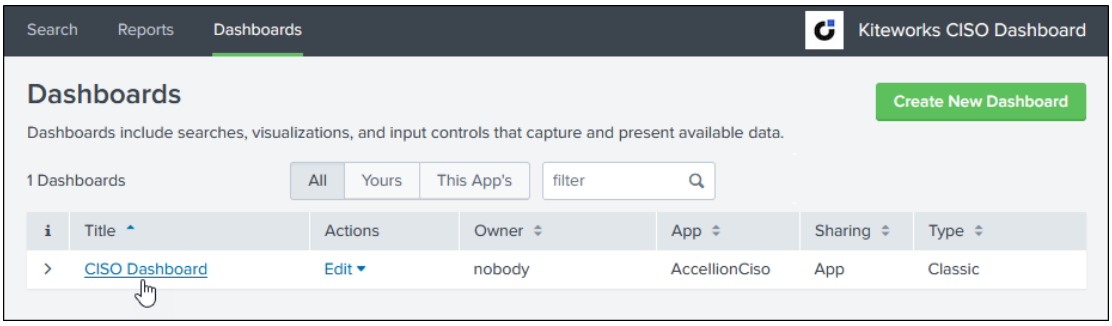
Configure the Kiteworks CISO Dashboard app

To configure the Kiteworks CISO Dashboard app:

1 Open Splunk Enterprise. On the menu click Apps > Kiteworks CISO Dashboard.



2 On the Kiteworks CISO Dashboard search page, click the Dashboards tab, and then click the CISO Dashboard link.



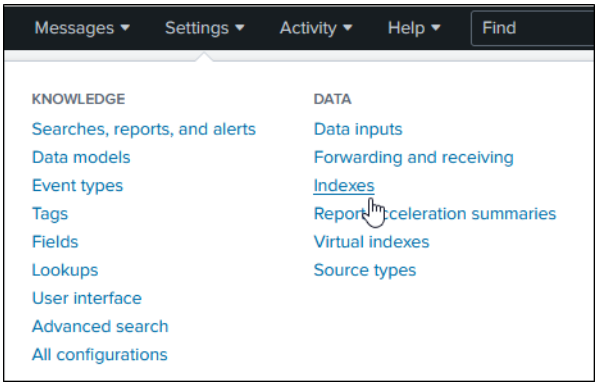
3 Use the instructions in the following sections to configure the app.

Create indexes for storing Kiteworks events and system logs

An index is created on the Splunk indexers for storing Kiteworks logs. If needed, a retention policy, security, and other parameters are configurable. You can create an index or allow the default index to be used.

To create an event index:

1 In Splunk Enterprise, go to Settings > Indexes.



2 On the Indexes page, create the following indexes:

- "accellion_syslog" - for storing Kiteworks events.
- "accellion_system_log" - for storing Kiteworks system logs .

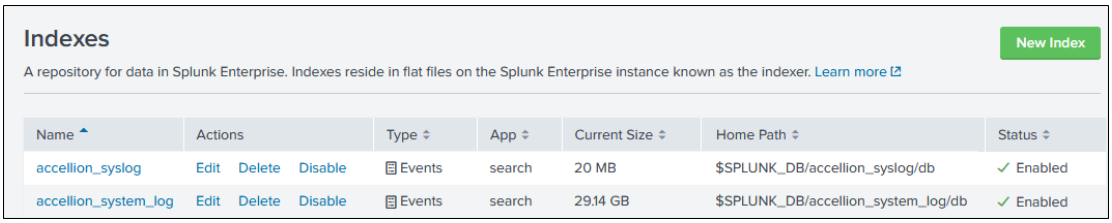
To create the accellion_syslog index:

1 On the Indexes page, click New Index.
2 For the new index name, enter "accellion_syslog".
3 In the App list, select Kiteworks CISO Dashboard.
4 Click Save.

To create the accellion_system_log index:

1 On the Indexes page, click New Index.
2 For the new index name, enter "accellion_system_log".
3 In the App list, select Kiteworks CISO Dashboard.
4 Click Save.

Result: The indexes are added to the Indexes page.



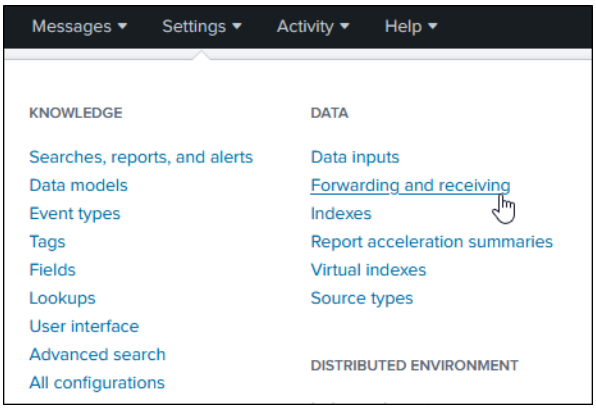
Enable a receiver to receive data from Kiteworks

You can enable a receiver to receive Kiteworks data via Splunk Universal Forwarder or via Kiteworks syslog server.

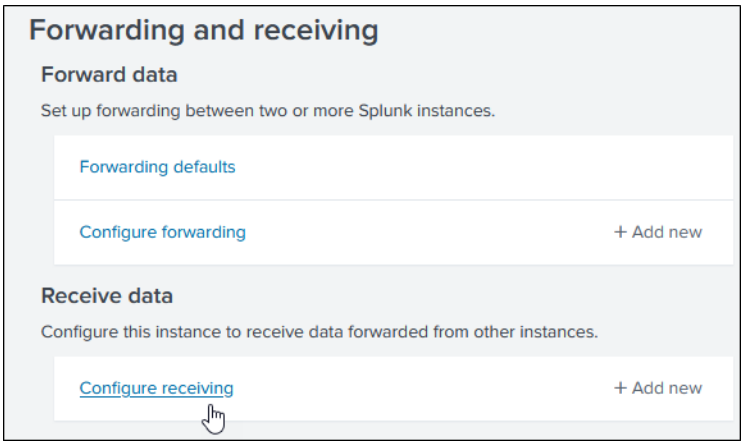
Enable a receiver to receive data from Kiteworks via Splunk Universal Forwarder

To enable a receiver to receive data from Kiteworks via Splunk Universal Forwarder:

1 In Splunk Enterprise, go to Settings > Forwarding and Receiving.



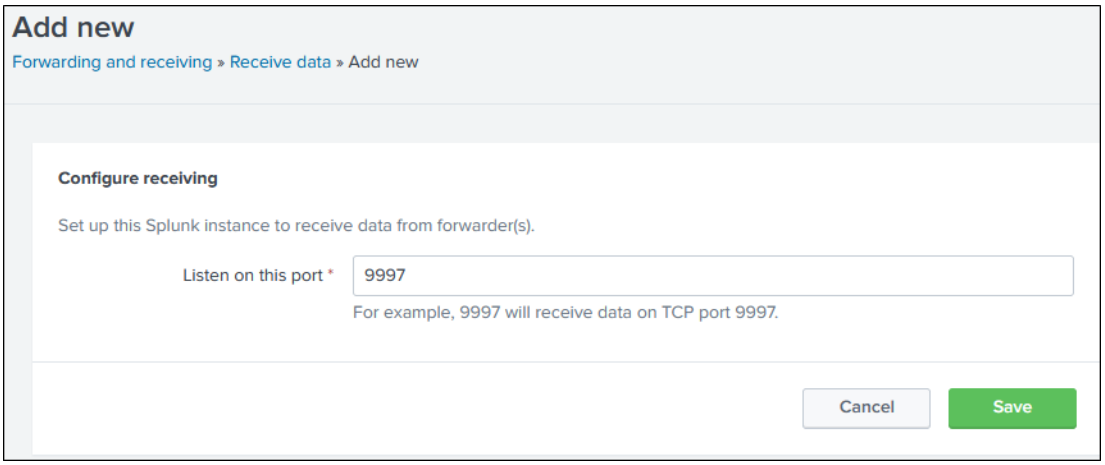
2 On the Forwarding and Receiving page, click Configure Receiving.



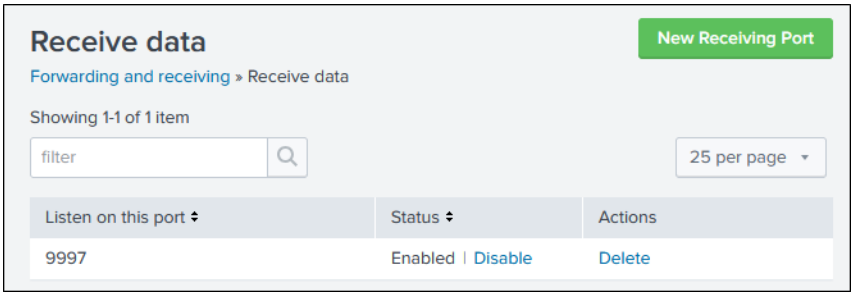
3 On the Receive Data page, click New Receiving Port.

4 On the Add New page, in the "Listen on this port" field, enter 9997.

Result: Receiver on the Splunk environment is enabled (Heavy Forwarder or Indexer) and port number is set (default TCP 9997). Traffic is permitted on a firewall from Kiteworks virtual machine to the Splunk environment (default TCP 9997). The Receiver and Forwarder ports are the same.



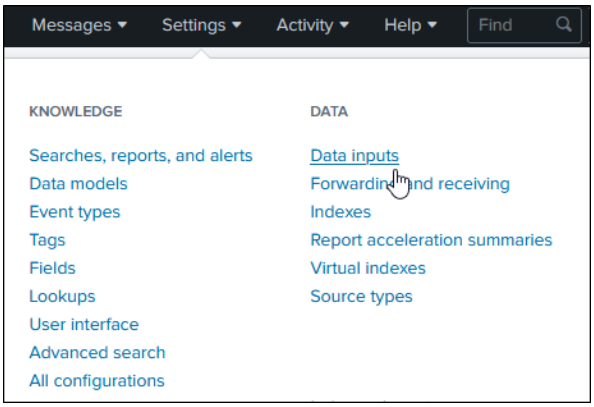
Result: The receiving port is ready to receive data.



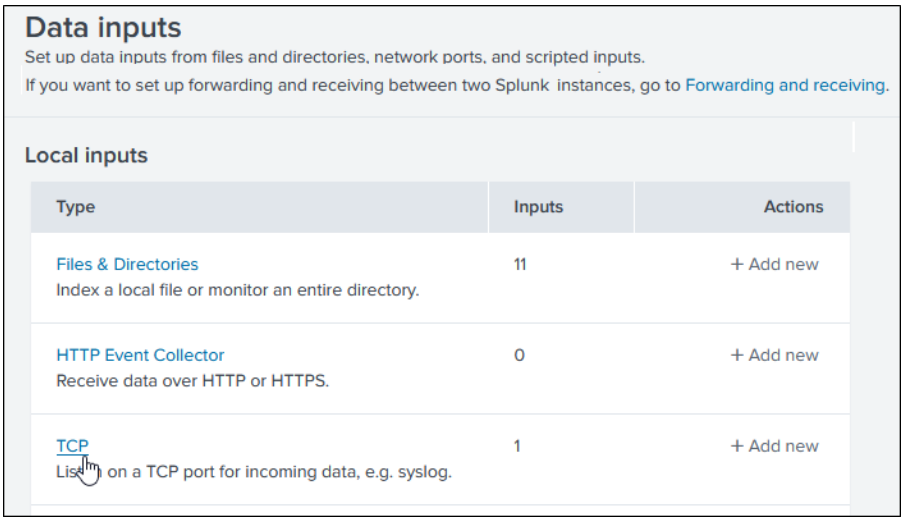
Enable a receiver to receive data from Kiteworks via the Kiteworks syslog server

To enable a receiver to receive data from Kiteworks via the Kiteworks syslog server:

1 In Splunk Enterprise, go to Settings > Data Inputs.

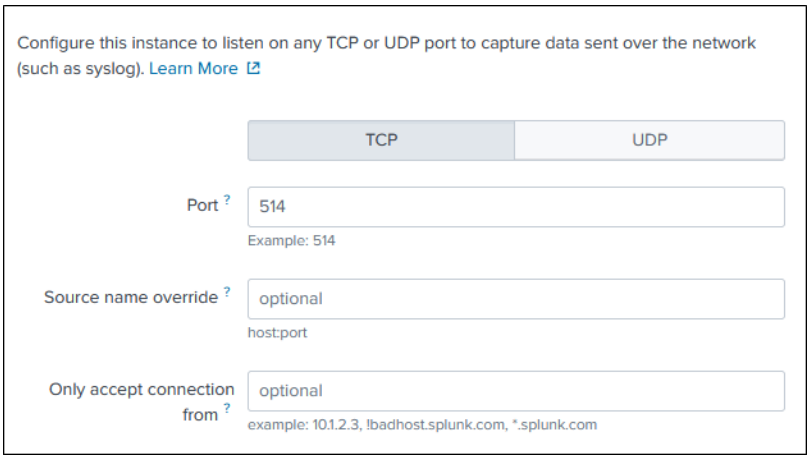


2 On the Data Inputs page, in the Location Inputs section, click TCP.



3 On the TCP page, click New Local TCP.

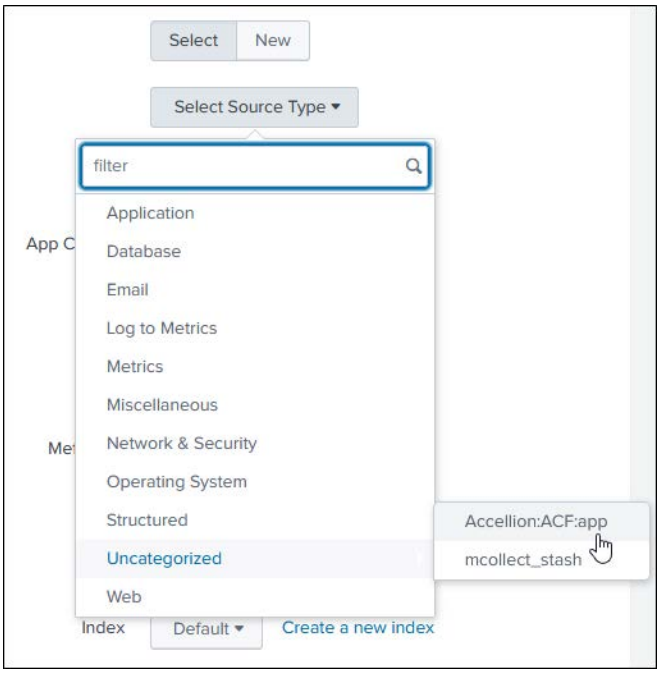
4 On the Add Data - Select Source page, click the TCP button. For the Port number, enter 514.



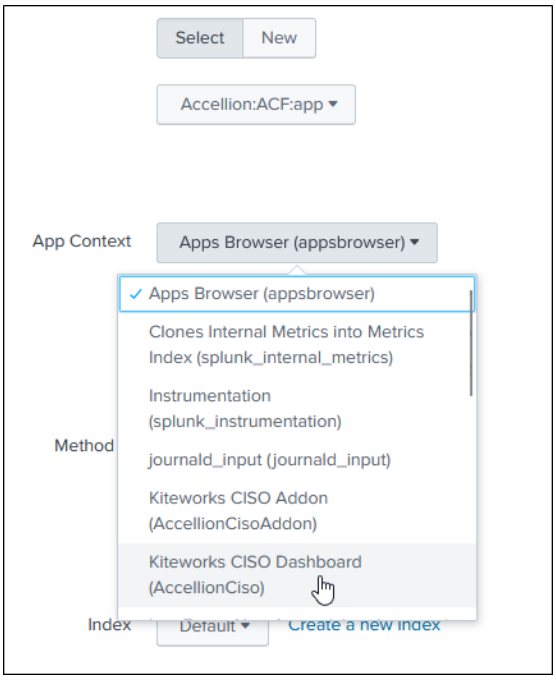
5 At the top of the page, click Next.

6 On the Add Data - Input Settings page, click the Select button and configure the following settings.

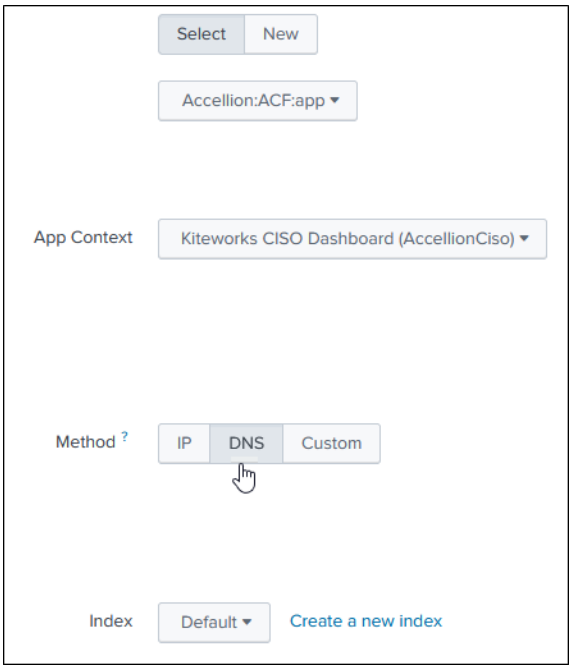
- In the Select Source Type list, in the Uncategorized list, select Accellion:ACF:App.



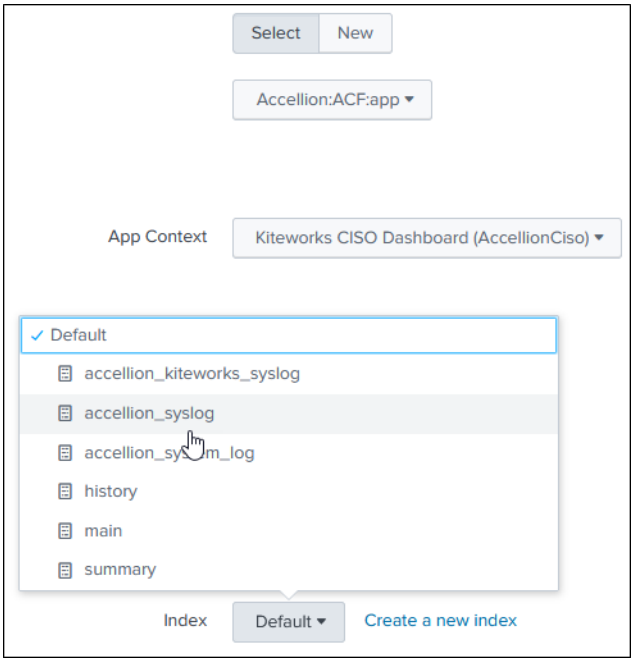
- In the App Context list, select Kiteworks CISO Dashboard (AccellionCiso)



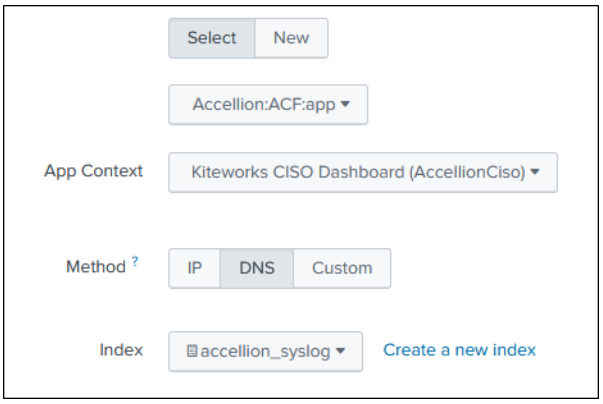
- For the Method, click the DNS button.



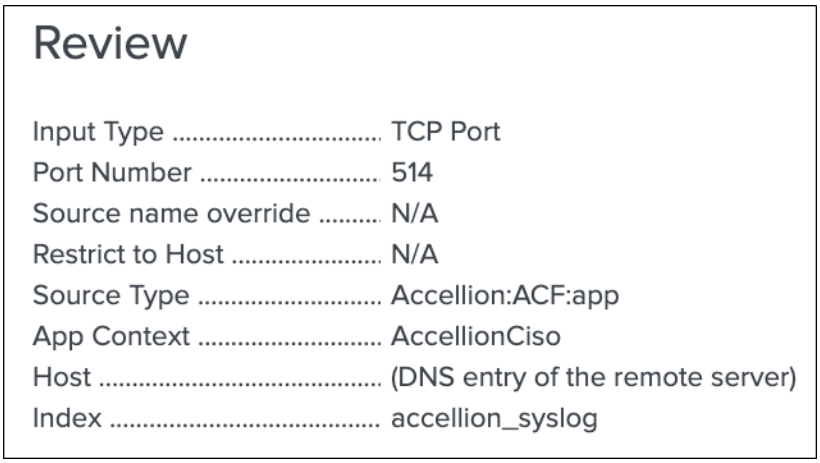
- In the Index list, select "accellion_syslog".



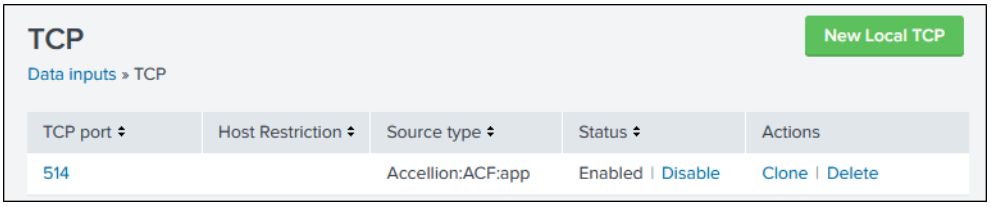
Result: All setting are configured.



7 At the top of the page, click Review and verify that the settings are configured as documented.



8 Click Submit.



Configure the Splunk Universal Forwarder for the Splunk CISO Dashboard

The Splunk Universal Forwarder forwards Kiteworks audit log (syslog) data produced using Splunk elements to the Splunk CISO Dashboard. You can configure multiple hostnames for the indexers (Splunk servers) and enable TLS to ensure secure communication between the Kiteworks server and the Splunk server.

You can configure Splunk Universal Forwarder to forward data using Splunk servers or the Kiteworks syslog server.

Recommendation: Use the Splunk Universal Forwarder on all servers in the cluster to ensure that all audit log and syslog data is forwarded. You can configure the forwarder on one server and then apply the settings to multiple servers.

Configure the Splunk Universal Forwarder to use Splunk servers

To configure the Splunk Universal Forwarder to use Splunk servers:

1. In the Kiteworks Admin Console, go to System Setup > Locations, and then click a server you want to edit.
2. On the External Services tab, click Splunk Universal Forwarder Settings.
3. In the Platform list, select Enterprise or Cloud.

   To configure Splunk to forward data to a Splunk Enterprise instance:

   1. In the Splunk Server field, enter the host names and port numbers of the Splunk servers where you want to forward logs.

      Example when forwarding to multiple Splunk servers: hostname1:port1,hostname2:port2
   2. To secure communication over a secure channel, turn on the Enable TLS switch.

      Result: The Verify Server Certificate switch displays.
   3. To verify the Splunk server certificate, turn on the Verify Server Certificate switch.
   4. Check the common name of the certificate.
   5. Upload the client certificate that will be used to connect to the Splunk servers. This is required for the Splunk server to verify the client.

   To configure Splunk to forward data to a Splunk Cloud instance:

   1. Obtain the Splunk Search Processing Language (SPL) credentials package file (splunkclouduf.spl).
   2. Upload the SPL file.
4. If you want to apply the settings to all servers in the cluster, turn on "Apply the same Splunk Universal Forwarder Settings to all hosts" switch, and then click Save.

   Result: The log forwarding process starts and data starts appearing in the Splunk environment.

Notes:

- Only one Splunk server is configurable, so whenever a new host and port is received from system the previous server will be disabled and new one will be set.
- Universal Forwarder licenses are included with Splunk. You do not need to purchase them separately.

Configure the Splunk Universal Forwarder to use the Kiteworks syslog server

To configure the Splunk Universal Forwarder to use the Kiteworks syslog server:

1. In the Kiteworks Admin Console, go to System Setup > Locations, and then click the server you want to edit.
2. On the External Services tab, click the Syslog Settings.
3. In the Splunk Server field, enter the server IP address.

   Example: <your_localhost_ip_address>
4. For the Protocol, select TCP.
5. For the Port, enter 514.
6. To secure communication over a secure channel, turn on the Use TLS switch.
7. For the Format, select "JSON format".
8. To apply the settings to all servers in the cluster, turn on "Apply the same Splunk Universal Forwarder Settings to all hosts" switch, and then click Save.

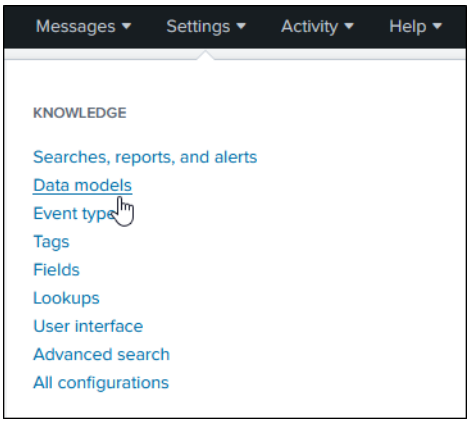
   Result: The log forwarding process starts and data starts appearing in the Splunk environment.

Enable Acceleration (optional)

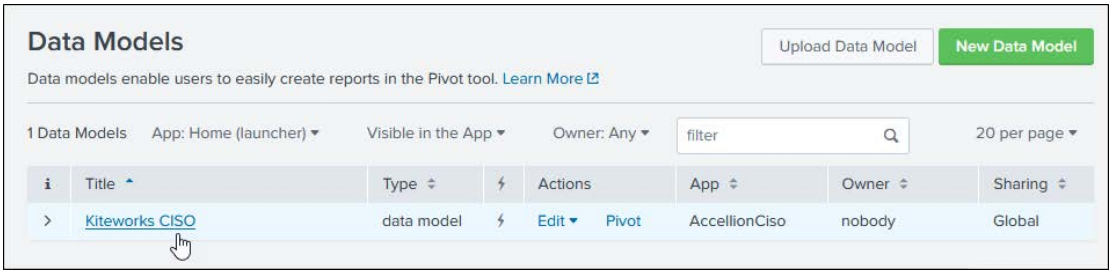
Acceleration is used to improve query performance, but it might cause some app updates to not apply because it still uses the old acceleration summary.

To enable Acceleration:

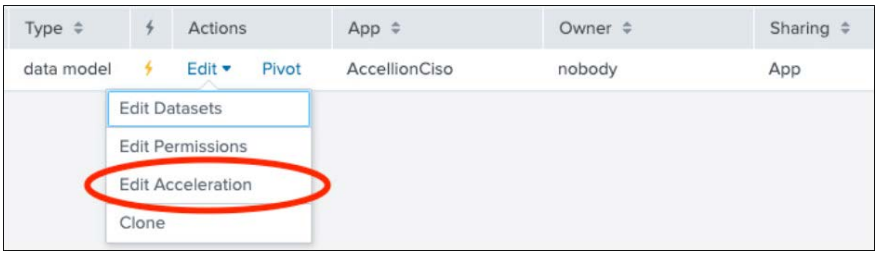
1 In Splunk Enterprise, go to Settings > Data Models.



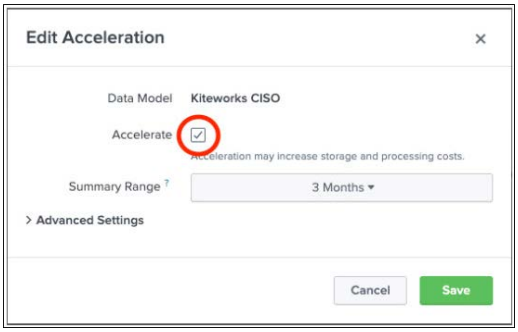
2 On the Data Models page, find and select "Kiteworks CISO".



3 In the Actions column, click Edit > Acceleration.



4 On the Edit Acceleration page, select the Accelerate checkbox, and then click Save.



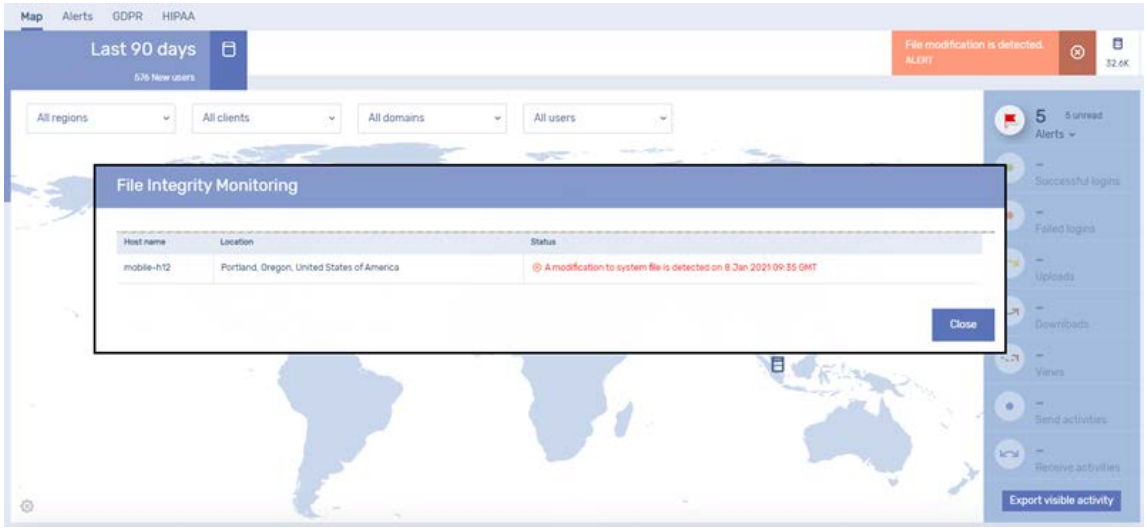
Use the CISO Dashboard

Highlights of the CISO Dashboard

- View a mapped representation of users, files, and files accessed.
  - Display activity such as successful and failed sign in attempts, file uploads and downloads, and files stored by geographical distribution on all clients, enabling retrieving of these events for exception reporting.
  - Display the last 90 days of activity on a system.
  - Specify a date range for file uploads, downloads, new users, and shared domains.
- Zoom out using the middle mouse button to see the entire map. You can also zoom in to view breakdowns into individual groups.
- Resize and re-center the map by clicking the "Re-center the Map"  icon.
- View the IP addresses and locations of servers by clicking the "Map Configurations" (gear) icon to access the map configuration.
- Display files and activity of files on Azure, AWS or other cloud services, such as, Box, Dropbox, and other Repositories Gateway sources.
- Display files that are triggered by DLP, AV, or ATP on the map providing information where sensitive files or viruses are being uploaded from.
- Top user domains for uploads, downloads or sharing email is displayed in an ordered list to help in identifying anomalous activity.
- Filter by client type.
- Display passed, quarantined, and queued statistics.
- Enable actions that can be triggered to warn against risks to augment investigation capabilities, list of rogue IP addresses attempting server access.
- Automated system file integrity monitoring (FIM) is in place to detect any tampering with code or libraries on the system, as well as presence of any malicious files in system areas.
- Generates list of "access denied users".
- Highlight compliance violations.
- All downloads and uploads: Quarantined by AV or Files flagged by DLP/ATP as sensitive will be displayed on the top panel.
- Ability to see emails that were sent through the system.

File integrity monitoring

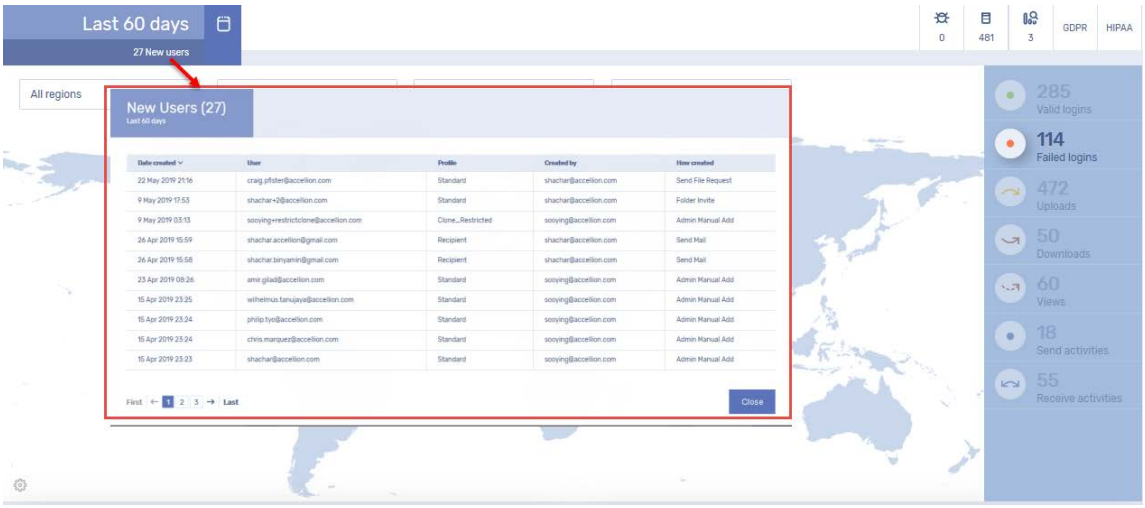
The File Integrity Monitor (FIM) widget monitors the system integrity and displays warnings and alerts and only displays on an alert or warning. The Kiteworks system is scanned and when scanning is complete, real time monitoring alerts and warnings are sent out to the administrator if the scan detects a failure. Email notifications are sent out and these notifications are also logged in the Syslog and Activities.



Note: File integrity monitoring (FIM) alerts and alerts for emails are sent to the administrator if the scan fails during the file integrity monitoring.

New users

The New Users widget provides information on all the new users that were added to the Kiteworks system in the last 7, 14, 30, 60, 90 days or a custom date rage can be set by selecting Custom range. The New Users window displays how and when the users were created.



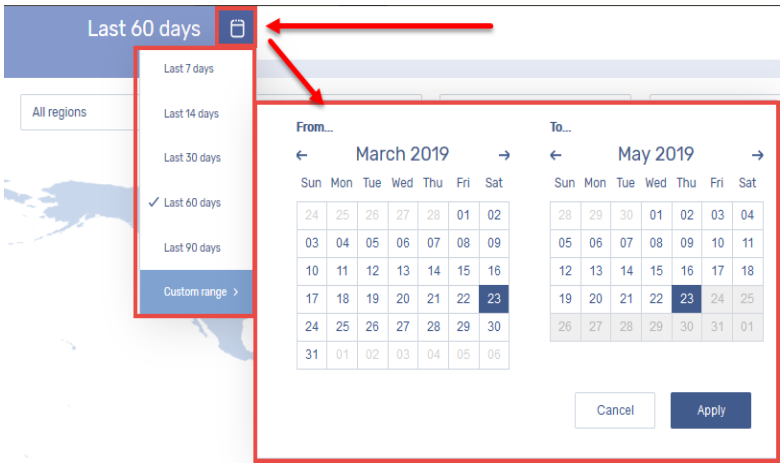
Files count

The total number of files displayed in the header. This total file count excludes replicated files.

Date selection/time filter

The time filter is a dropdown list allowing the first filtering of information displayed on the map.

Data can be viewed for the last 7, 14, 30, 60, 90 days or a custom date rage can be set. This applies to Valid and Failed logins, Uploads and Downloads, Sent Activities, Receive Activities, File Access, User Domain and Top Downloaders.



DLP, AV/ATP and file counts

The DLP, AV and ATP numbers display flagged or quarantined files. You can mouseover the DLP icon that displays the number of files that were DLP-flagged or locked. The AV/ATP displays the number of files that have been quarantined by AV/ATP. You can drill down to get details on the actual files.

Overall Files count gives the total number of files and when you mouse over the exact count is displayed. Click the mouse for details.

Details on the CISO Dashboard

Map displaying geolocation activity information

This widget is a mapping and geolocation activity tracking tool. The following information is displayed on the map:

- Active sessions are represented based on geographic location by user's IP address.
- The widget displays the geolocation activities information for the past 90 days on a Kiteworks system.
- Zooming in and out capability. Zooming in drills down into individual logins.
- All the activity switches toggle and can be turned ON or OFF to display that specific data, giving the user the flexibility to view only the desired activity.
- A green line depicts a File Upload from the User to the File Storage location.
- A Blue line depicts a File Download from the User to the File Storage location.
- The CISO Dashboard is refreshed every 10 minutes. Specific map data can be refreshed immediately by refreshing the page.
- Data can be filtered by all regions, clients and domains.

Information layers

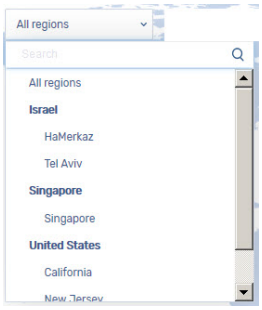
The Information Layers is presented on the right panel of the CISO Dashboard. It includes the total number of alerts, the number of unread alerts, and filters for viewing alert types. Click the drop down list to hide or show alerts, or show only archived alerts.

Once you get the results you want, you can export those results to a CSV file.

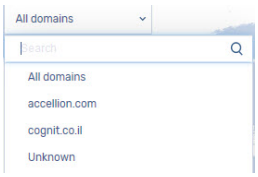
Filters

Data can be filtered by:

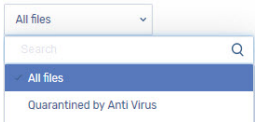
- Data can be filtered by All Regions or Email Domain or specific regions and domains.



- Data can be filtered by All Clients and specific clients. You can also filter on the mobile client such as Android, iPhone, multiple-web client and other clients.
- Data can be filtered by All Domains and specific domains.



- All Files or files quarantined by Anti-Virus or DLP.



The search filters offer the following:

- Multiple search selection on all filters.
- Clicking the mouse on the filter opens the filter which comprises of the following:
  - Filter header displaying the selected items.
  - Search box - allowing dynamic search from the first letter typed.
  - Preview area - displaying all selected items in tags. An item can be removed by clicking the "x".
  - Scrollable list of items – regions and clients filter are multi-level lists and containing main and secondary items.
  - Searching an item is done by scrolling the list or by using the search box.
  - The list is filtered starting from the first letter typed in the search box.
  - The filtered list displays all items containing the search string.
  - If a secondary item corresponds to the searched string, then the parent item of that item appears as well. If the parent item does not contain the searched string than it will be in an inactive state.
- Selecting item from the list is done by mouse click or by pressing Enter on a selected item.
- Each selected item is shown in the preview area and in the filter header.
- After selecting, clicking outside the filter box will close the box and the value/s selected will be shown on the filter. The map, the other filters and the information layers are updated accordingly.
- The selected item/s are shown on the filter when it closed, until it reaches its limit. In addition, a number tag appear at the end of the filter indicating the number of items selected.

- Clearing all filters inside a filter will bring the filter to the default state: "All".
- Mouse over –a tool tip appears with a caption describing the full string of the filter.

Widgets

The CISO Dashboard displays the following four widgets:

- Map displaying geolocation activity information
- Top Users
- Top Domains
- Trends

Mapping unknown locations

All locations are mapped using IP2Location to map to a city and country.

For IP addresses that do not get mapped to a location, an alert displays in the Unknown location orange box in the center of the map. You can click the Unknown location box, and then click the IP address hyperlink to automatically map it. The Failed Logins window displays when you click Unknown location. Click the IP address which opens the Add IP Address Mapping window enabling you to map the unknown IP addresses. Once all the IP addresses are mapped the Unknown location box disappears and the location is instantly displayed on the CISO dashboard. Even though the unknown locations disappear on mapping them, the historical data is retained.

Map configurations

Several actions can be performed on the Map Configurations page. If location mapping is changed for any existing IP address, the historical data is not altered. In addition, all the changes are logged on the Activities page. On this page you can:

- Import a list of IP addresses from a CSV file.
- Add a new IP address and map to it.
- Edit or bulk edit locations.
- Delete IP address mapping.

All the servers are listed first on the top of the list. If the server IP address is an internal IP address and not recognized a pencil icon will display on the same line allowing you to edit the location and map it correctly.

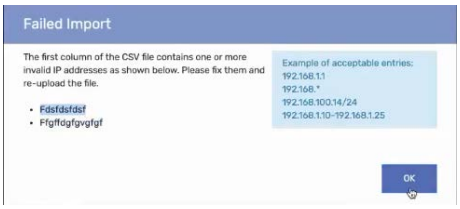
If a server has an external IP address which can be mapped automatically to the Kiteworks geolocation database, it cannot be edited.

Import CSV files

You can import a CSV file with internal IP addresses in the CISO dashboard and map it to locations. The following format should be followed to correctly import internal IP addresses:

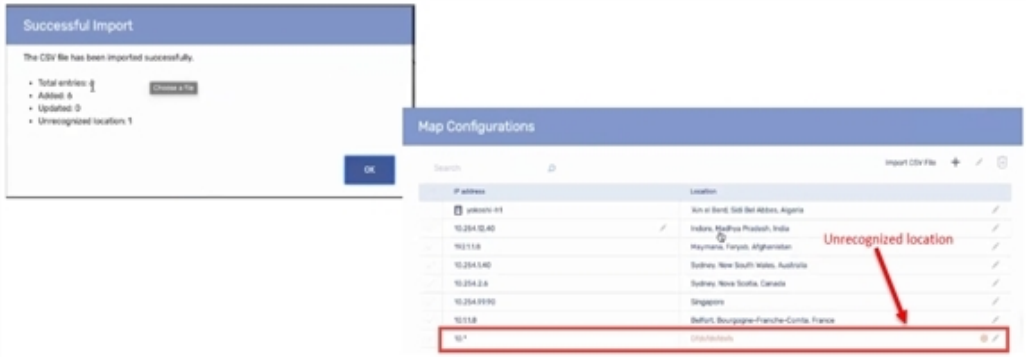
1. First column: IP Addresses or IP Range.
2. Second column: Location consisting of the city, region, country, separated by comma.
3. The first row can contain a header text (optional).

If the format mentioned above is not followed, the import fails and a message displays asking you to fix the format and re-upload the file.



If the CSV file imports successfully, it indicates all the IP addresses have been validated and a Successful Import window displays the data that was imported. Details of the data can be viewed on the Map Configurations window.

All the IP addresses that cannot be validated will display in red. Click the pencil icon to map the invalid entry correctly.



Add IP addresses

You can also add new IP addresses or an IP addresses range from Map Configurations.

Note: You will not be able to edit IP addresses if they were added using the Import CSV feature.

Bulk edit location mappings

You can select several IP addresses and change the location for all the selected addresses using the Bulk Edit Location feature. You can individually edit IP addresses if the "pencil" icon is displayed next to it. If the location cannot be configured because the server has an external IP, no icon is available to edit those IP addresses.

Delete IP address mappings

You can select several IP addresses and click the "delete" icon to delete them. If any of the selected IP addresses are not mapped to any geolocation, they will be removed from the geolocation mapping list.

Valid logins

Valid login attempts are represented based on geographic location by the user's IP address. Mouse over Successful logins to see additional information, and then click any valid login icon to get additional information in a pop up. You can click any of the line items to get more details.

Failed logins

Orange dots on the dashboard display for failed logins.

One of the important statistics displayed are Failed login attempts. They are also represented based on geographic location by the user's IP address. Mouse over Failed logins to see additional information, and then click any valid login icon to get additional information in a pop up.

If a user attempts to access a link they are not authorized to access, the administrator is able to see the failed access attempt and can identify a possible security breach. Data displays on who the original sender was, who the valid recipients are, the subject line of the message, any attached files, and who is the user trying to access the file or files (as well as the date, time, IP, etc.).

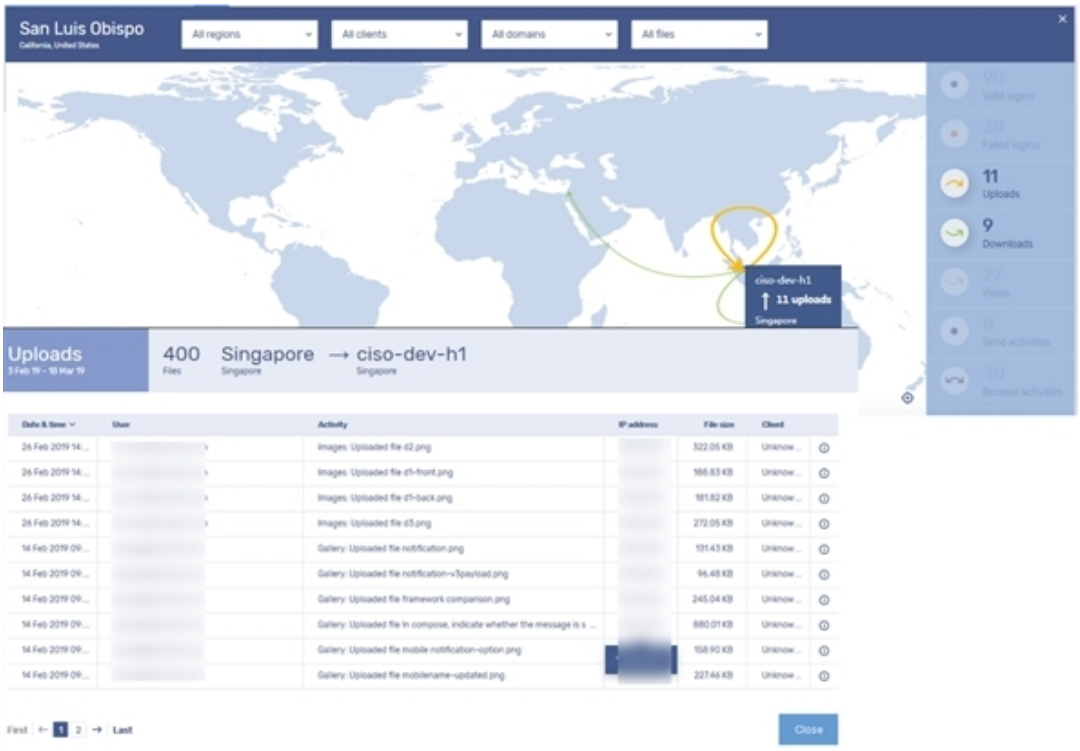
Location-specific data

For locations-specific data all the interactions between a location and the rest of the world are displayed on the CISO Dashboard.

You can also filter data with the interaction between a location and only one other location enabling you to focus in on a certain region and show all the interaction between that region and the rest of the world, or only two locations.

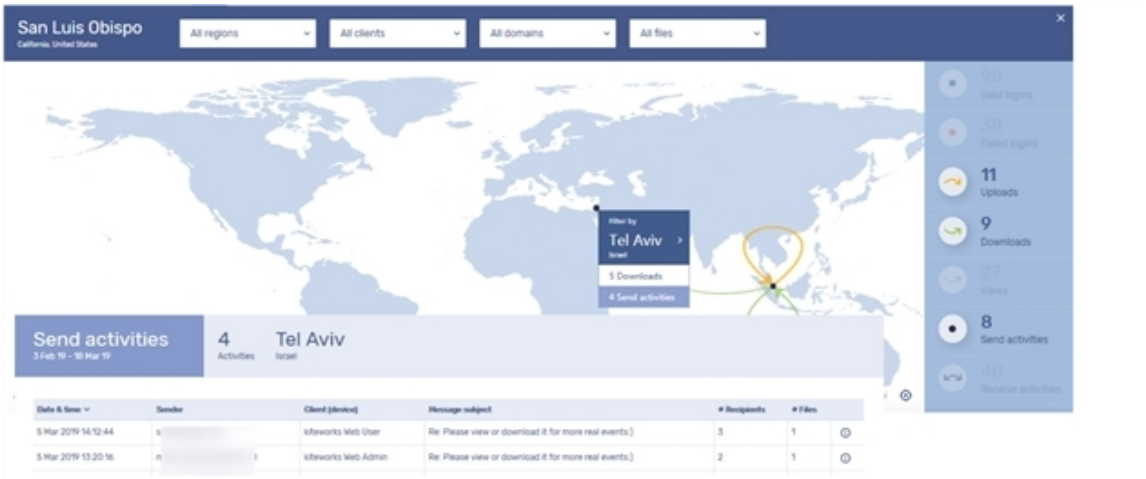
Uploads and downloads

File uploads and downloads are represented by lines from the user to a Storage server or Repositories Gateway source. You can click any of the points to get the actual activity.



Send activities

Send Activities displays where a file was sent. You can click any of the points to get the actual activity and the details of the activity.

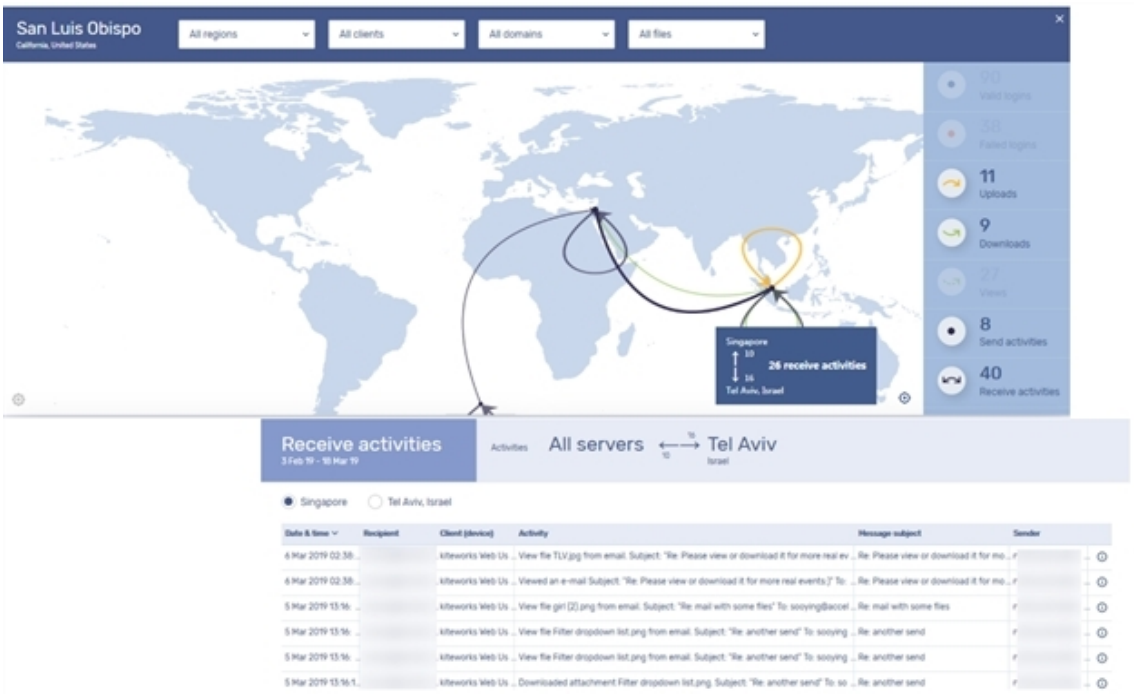


Views

Views displays the viewed activity by users displaying the IP address the files were viewed from and the date and time.

Receive activities

Receive Activities displays where a file was accessed. You can click any of the points to get the actual activity and the details of the activity.



Files

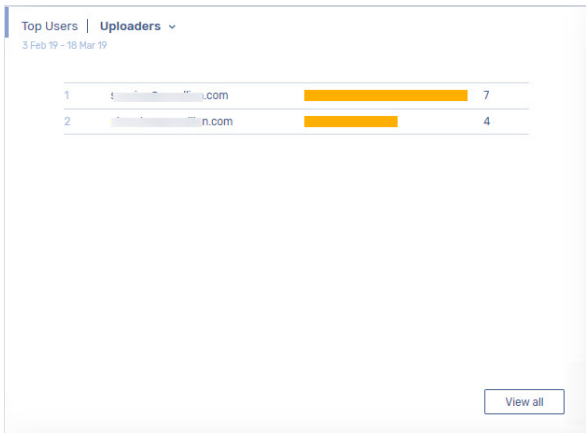
Files Stored are represented by location. You can show or hide files on the map. The count of the number of files listed in the "Map" displaying geo-location, the files listed in the "File Scanning" widget and the total number of files displayed in the "Manage Folders & Files" page in the Kiteworks Admin Console are the same and the count matches.

Retrieve activity reports

All the above activities are recorded and reports on these activities can be viewed and downloaded. A paginated report can be retrieved with the details of the activity.

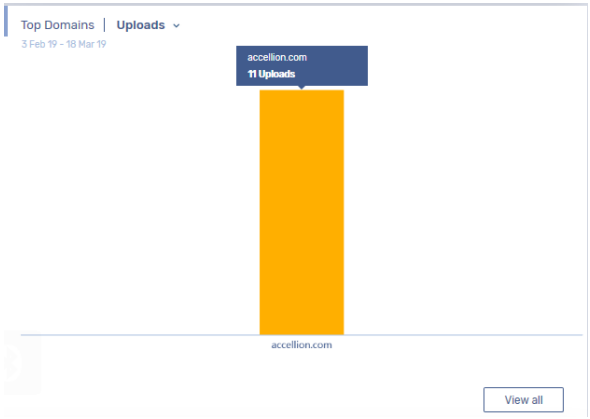
Top Users

You can see a list Top Users: Downloaders, Uploaders, Viewers, Senders and Recipients on the Kiteworks system so that anomalous activity can be identified. A date range can be defined to see Top Users within that date range. Click the name to view the details of the downloads.



Top Domains

You can see a list Top Domains: Uploads, Downloads and Views, Sends, Received on the Kiteworks system so that anomalous activity can be identified. A date range can be defined to see Top Domains within that date range. Click the name to view the details of the downloads.



Trends

You can the trend of all the Uploads and Downloads on the Kiteworks system. Click any location of the Trends panel to get details of the download or upload.

Compliance reports

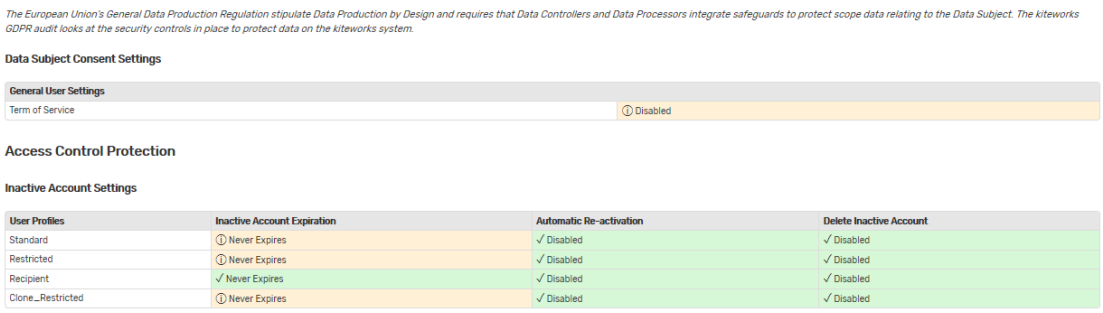
GDPR Report

The GDPR (General Data Protection Regulation) Report aims to create a data protection law framework across the EU and is designed to give citizens control of their personal data, while imposing strict rules on those hosting and processing this data, anywhere in the world. The regulation also introduces rules relating to the free movement of personal data within and outside the EU. This report can be printed or downloaded for audit purposes.

Data subject consent settings

Consent of the data subject fulfills Article 6 of GDPR. Kiteworks Terms of Service feature can be used to require that users accept terms and conditions and explicitly grant consent to data processing before they can upload content to the Kiteworks system.

The Terms of Service, Occurrence and General Terms of Service Content are displayed showing if they are enabled and User Profiles that have enabled it.



The European Union's General Data Production Regulation stipulate Data Production by Design and requires that Data Controllers and Data Processors integrate safeguards to protect scope data relating to the Data Subject. The kiteworks GDPR audit looks at the security controls in place to protect data on the kiteworks system.

Data Subject Consent Settings

General User Settings	
Term of Service	ⓘ Disabled

Access Control Protection

Inactive Account Settings

User Profiles	Inactive Account Expiration	Automatic Re-activation	Delete Inactive Account
Standard	ⓘ Never Expires	✓ Disabled	✓ Disabled
Restricted	ⓘ Never Expires	✓ Disabled	✓ Disabled
Recipient	✓ Never Expires	✓ Disabled	✓ Disabled
Clone_Restricted	ⓘ Never Expires	✓ Disabled	✓ Disabled

The GDPR report displays the following categories:

- Access Control Protection
- Data Security
- System Security

Access Control Protection

Access Control Protection provides the following settings.

Inactive account settings

The following inactive account expiration and settings per user profile are displayed. You can make the adjustments on the User Profiles page.

- Inactive account expiration
- Deleted inactive accounts
- Automatic re-activation of accounts
- Password policy
- Session timeout

LDAP integration

LDAP integration displays the ordered list of LDAP Servers with the following information:

- Server name
- Protocol
- Port
- Status: green if all LDAP servers are configured and available, orange if not configured or if one or more servers have connection issues

SSO integration

SSO integration displays the following:

- SSO Enabled
- SSO Protocol
- SAML idP or Kerberos Keystore

Un-authenticated Access

Un-Authenticated Access displays the list of user profiles that allow unauthenticated downloads or request file links that allow downloading or viewing files. You can make the adjustments on the User Profiles page.

DLP integration

The DLP Integration section displays the audit parameters of DLP/ICAP settings. Green indicates that DLP is configured. Orange indicates that it is not configured.

- DLP IP address
- Protocol (ICAP or ICAPS)
- Port
- Connection status
- Maximum file size
- Policy for existing files
- Policy for files marked as Content Violation
- Policy for files that fail scanning

- Scan Policy for Repositories Gateway files
- Notification Email

Data Security

The following parameters can be configured for Data Security.

Access control

AES 256-bit encryption is used for all user content. All users are assigned a unique identifier and all end user and administrator activities are logged on the Kiteworks system.

Password policy

A salted 256-bit hash of the user password is stored for all users. Kiteworks recommends that user passwords are at least 8 characters long, that account lockout is set to five incorrect attempts or lower, and the lockout period be at least 3 minutes.

Session timeout

The administrator is allowed to set a session timeout for idle sessions. Kiteworks recommends that idle session timeout be 30 minutes or lower. You can make the adjustments in the General User Settings page.

Emergency access procedure

A DLI administrator role is provided with the ability to access end user files. They can export user files via eDiscovery reports or automate the export of user files via eDiscovery APIs.

Audit control

All end user and admin activities are logged on the Kiteworks system. Activity logs can be exported to an external syslog server. You can make the adjustments in the Locations page.

System Security

The following settings can be configured for System Security.

CheckPoint Sandblast integration

The ATP status is displayed. You can make the adjustments in the CheckPoint Settings page. Green indicates that ATP is configured and the row is clear if it is not configured.

The following parameters are displayed:

- ATP IP address or Cloud Service
- Port
- Connection status
- Maximum file size

- Policy for existing files
- Policy for files identified as malware
- Policy for files that fail scanning
- Scan Policy for Repositories Gateway files
- Notification email

Anti-Virus configuration

You can make the adjustments in the Anti-Virus Settings page. Green indicates that AV is enabled and orange indicates that AV is disabled. The following parameters can be configured:

- Enabled or disabled
- Scan before access
- Scan files in Repositories Gateway sources or not
- Update schedule
- Maximum file size
- Policy for files that cannot be scanned
- Last AV update success

Kiteworks integrity check

The server name and the file integrity status is displayed. You can make the adjustments in the Locations page. You can set an email address for anomaly notifications.

Kiteworks deployment

For a Kiteworks deployment the contingency plan, multi-site deployment and file replication can be configured. Kiteworks uses AES 256-bit encryption for all user content, all users are assigned a unique identifier, all end user and administrator activities are logged on the Kiteworks system. You can make the adjustments in the Locations page.

Green indicates that every role is redundant (three servers with the Application role) and replication for every Storage role otherwise the status is orange.

The following parameters are displayed:

- Server name
- Location
- Roles
- Status
- Number of servers
- Number of server with Application role
- Number of locations
- Number of Storage locations (i.e., locations with Storage role)

File replication rules

Details of the file replication rules are displayed. You can make the adjustments in the Location Replication Rules page. The following parameters are displayed:

- Source
- Replication
- Target
- Status
- Number of Storage locations that have replication rules
- Storage locations that do not have replication rules

GDPR Transaction Reports

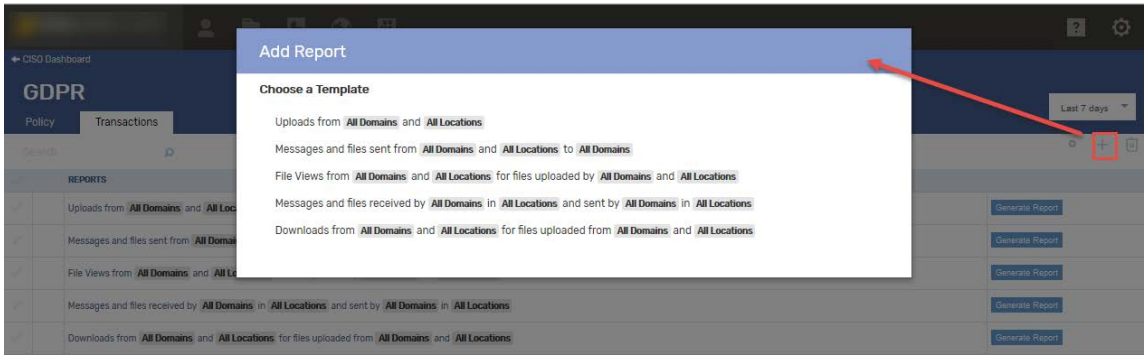
Transaction Reports record uploads, messages and files sent, messages and files received, file views, files uploaded from domains (one, multiple or all) and locations (one, multiple or all).

The report also shows the statistics of DLP scans to support the GDPR compliance of files that were scanned by DLP, flagged, quarantined or released.

A date range is available to select from for each report. A detailed or an aggregate report can be viewed focused on countries (one, multiple or all), email domains, any specific people that shows Uploads, Downloads, View File, and/or Send File. You can run one report at a time and download the file or print it.

Add a report and choose a template

There are 5 report templates to choose from.



Perform the following steps to add a report.

1. Click the + sign to add a report.
2. Click the selected template. The Add Report: Choose a Template window displays.
3. Select any one template from the template list. For this example, Uploads from All Domains and All Locations is selected.
4. Click Uploads from All Domains and All Locations. The Configure Report Filters window displays.
5. Click All Domains and enter the domain names in the Uploader Domain field where you would like files to be uploaded from. Press Enter or click the check mark symbol to add the domain to the report. You can add multiple domains. Click the Trash can icon to delete domains.
6. Similarly, click All Locations to enter the location names in the Uploader Location field where you would like files to be uploaded from. The Uploader Location field autocompletes, displaying a list of locations you can choose from. Press Enter or click the check mark symbol to add the location to the report. You can add multiple locations. Click the Trash can icon to delete or remove locations.
7. Click Add Report. The report will be added to the GDPR Transactions.

Generate a report

1. Click the report you would like to generate.
2. Click the Date Range down-arrow to select a date range. You can select Custom range and select the To and From dates.
3. Click Generate Report. The report generates and displays showing the Date/Time in GMT, Uploader, Location and Activity. You can view the report, download a PDF file or print the report. For printing very large reports you can select a Column View, Merged View or Row View.

HIPAA Compliance Report

The HIPAA Compliance report enforces administrative safeguards. It contains information about the Kiteworks Admin Console settings that are related to HIPAA requirements ensuring that the organization adheres to the HIPAA regulations. It integrates with your security infrastructure and is compliant with on-premise, AWS and Azure systems. This report can be printed or downloaded for audit purposes.

The HIPAA Compliance report displays the following categories:

- Workforce Security - Termination Procedure
- Physical Safeguards
- Technical Safeguards
- Emergency Access Procedure
- Anti-Virus Configuration
- Audit Control

Workforce Security - Termination Procedure

Kiteworks Workforce Security - Termination Procedure addresses terminating access to electronic PHI (Protected Health Information) when employment of a workforce member ends or their role changes.

The following three categories are displayed:

Inactive account settings

This section includes Inactive Account Expiration, Automatic Reactivation and Account Deletion information for all the user profiles.

User Profiles	Inactive Account Expiration	Automatic Re-Activation	Delete Inactive Accounts
Standard	ⓘ 90 days	✓ Disabled	✓ Disabled
Restricted	✓ 30 days	ⓘ Enabled	✓ Enabled
Recipient	✓ Never Expires	✓ Disabled	✓ Disabled
Custom Profile 1	✓ 60 days	✓ Disabled	✓ Disabled
Custom Profile 2	ⓘ Never Expires	✓ Disabled	✓ Disabled

These settings can be found and adjusted through user profiles. Go to Users > Profiles > *expand a profile* > Account > Account Inactivity.

LDAP integration

It is recommended to integrate Kiteworks with LDAP to unify user authentication. The LDAP Integration section includes a List of configured LDAP servers (server, protocol, port), LDAP status for each LDAP server and Authentication via LDAP information.

These settings can be found in the Application Setup > Authentication and SSO > LDAP.

SSO integration

It is recommended to integrate Kiteworks with SSO to unify user authentication. SSO integration includes SSO type, [SAML 2.0 only] Single Sign-On Service URL, [SAML 2.0 only] Sign AuthNRequest, [SAML 2.0 only] RSA Public Key Certificate, [Kerberos only] Authentication Realm and [Kerberos only] Key Distribution Center (KDC).

Using SAML 2.0

SSO Setup	✓ SAML 2.0
Single Sign-On Service URL	✓ https://sso.company.com/
Sign AuthNRequest	✓ Disabled
RSA Public Key Certificate	✓ Provided

Using Kerberos

SSO Setup	✓ Kerberos
Authentication Realm	✓ EXAMPLE.COM
Key Distribution Center (KDC)	✓ kerberos.example.com

Without SSO

SSO Setup	ⓘ None

For SAML 2.0, these settings can be found at Application Setup > Authentication and SSO > SAML 2.0 > Add Idp. For Kerberos, these settings can be found at Application Setup > Authentication and SSO > Kerberos > SSO Auto-Redirect.

Information Access Management

The Information Access Management Administrative Safeguard ensures that a management system in place to authorize access to electronically protected information.

DLP integration

Kiteworks integrates with corporate Data Loss Prevention systems to prevent or report access to sensitive information. It is recommended connecting to a DLP system using ICAP and at least setting

Kiteworks to report on files that are flagged by DLP.

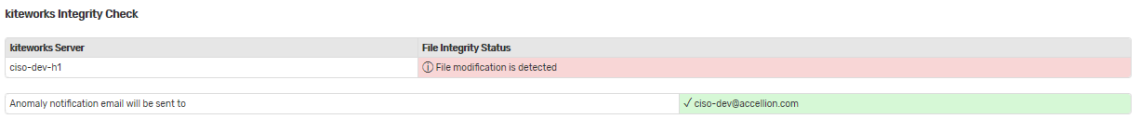
DLP integration includes DLP Server, DLP Status, Policy for Existing Files in Kiteworks, Policy for Files that are Marked Content Violated by DLP, Policy for Files that Could Not be Scanned, Scan files in Repositories Gateway sources and Notify on Violation.

DLP Server	✓ 192.168.16.154:1344 (Protocol: ICAP)
DLP status	ⓘ Down
Policy for existing files	✓ Scan before Access
Policy for files Marked Content Violation	✓ Report Only
Policy for files that fail scanning	✓ Report Only
Scan Policy for Enterprise Connect Files	✓ Scan on uploads and downloads
Notify on Violation	✓ complianceofficer@company.com

Incidence response

The Kiteworks integrity check reports any anomalies found in system or application files.

Kiteworks integrity check



Contingency plan

HIPAA requires that you adopt a contingency plan for disaster recovery.

Kiteworks deployment

kiteworks Server	Location	Roles	Status
hc1.kiteworks.accellion.com	US West	Web, App, Storage	✓ OK
hc2.kiteworks.accellion.com	US West	App	✓ OK
hc3.kiteworks.accellion.com	US West	Web, Search	ⓘ Search role is down
	ⓘ Multiple locations is recommended	ⓘ Additional App roles and Storage roles is recommended	

File Replication Rules

Source	Replication	Target	Status
US West	Unidirectional	US East	✓ OK
US West	Bidirectional	SG	✓ OK

File Replication Rules

HIPAA requires that you adopt a contingency plan for disaster recovery.

Kiteworks deployment

kiteworks Server	Location	Roles	Status
hc1.kiteworks.accellion.com	US West	Web, App, Storage	✓ OK
hc2.kiteworks.accellion.com	US West	App	✓ OK
hc3.kiteworks.accellion.com	US West	Web, Search	ⓘ Search role is down
	ⓘ Multiple locations is recommended	ⓘ Additional App roles and Storage roles is recommended	

Physical Safeguards

Note: Not applicable if the instance is configured on-premise.

- With an AWS installation

  kiteworks.accellion.com is hosted in the Amazon AWS data center. Please contact info@kiteworks.com for SOC2 attestations for AWS.
- With an Azure installation

  kiteworks.accellion.com is hosted in the Microsoft Azure data center. Please contact info@kiteworks.com for SOC2 attestations for Azure.

Technical Safeguards

Access control

Kiteworks uses AES 256-bit encryption for all user content. All users are assigned a unique identifier.

kiteworks Server	Encryption key was last rotated on
[redacted]	✓ 26 Feb 2018 15:45 GMT
[redacted]	✓ 12 Feb 2018 09:32 GMT
[redacted]	✓ 24 Jan 2018 10:46 GMT

Password policy

For users managed by the Kiteworks system, Kiteworks stores a salted 256-bit hash of the user password. Kiteworks recommends that user passwords are at least 8 characters long, that account lockout is set to five incorrect attempts or lower, and the lockout period be at least 3 minutes.

Character length	✓ 8
Number of numeric, uppercase, lowercase, special characters	✓ 1 numeric, 1 uppercase, 1 lowercase, 1 special
Password expiration	✓ 60 days
Password history	✓ No history checking
Max incorrect login attempts	ⓘ 10
Account lockout period	✓ 3 minutes

Session timeout

Kiteworks allows the admin to set a session timeout for idle sessions. Kiteworks recommends that idle session timeout be 30 minutes or lower.

Session timeout	✓ 30 minutes

Emergency Access Procedure

Kiteworks provides a DLI administrator with the ability to access end user files. They can export user files via eDiscovery reports or automated the export of user files via eDiscovery APIs.

DLI Admin	✓ [redacted]@accellion.com

Anti-Virus Configuration

Anti Virus status	✓ OK
Policy for Existing Files in kiteworks	✓ Scan before Access
Scan files in Enterprise Content Sources	✓ Enabled
Daily Update Schedule	✓ 01:30 GMT
Maximum File Size	✓ 100 MB
Policy for files that could not be scanned	✓ Allow download

kiteworks Server with Anti Virus Role	Last successful Anti Virus update
hc1.kiteworks.accellion.com	✓ 24 Feb 2018 15:45 GMT
hc3.kiteworks.accellion.com	✓ 26 Feb 2018 10:46 GMT

Audit Control

All end user and administrator activities are logged on the Kiteworks system. Kiteworks also allows audit logs to be exported to an external syslog server.

kiteworks Server	Primary App Role	Syslog server
[redacted].com	Yes	✓ [redacted]
[redacted].com	No	✓ None
[redacted].com	Yes	ⓘ None

HIPAA Transaction Reports

Transaction Reports record uploads, messages and files sent, messages and files received, file views, and files uploaded from domains (one, multiple, or all) and locations (one, multiple, or all).

The report also shows the statistics of DLP scans to support the HIPAA compliance of files that were scanned by DLP, flagged, quarantined or released.

A date range is available to select from for each report. A detailed or an aggregate report can be viewed focused on countries (one, multiple, or all), email domains, any specific people that shows Uploads, Downloads, View File, and/or Send File. You can run one report at a time and download the file or print it.

Add a report and choose a template

There are 6 report templates to choose from. Perform the following steps to add a report.

1. Click the + sign to add a report.
2. Click the selected template. The Add Report: Choose a Template window displays.
3. Select any one template from the template list. For this example, Uploads from All Domains and All Locations is selected.
4. Click Uploads from All Domains and All Locations. The Configure Report Filters window displays.
5. Click All Domains and enter the domain names in the Uploader Domain field where you would like files to be uploaded from. Press Enter or click the check mark symbol to add the domain to the report. You can add multiple domains. Click the Trash can icon to delete domains.
6. Similarly, click All Locations to enter the location names in the Uploader Location field where you would like files to be uploaded from. The Uploader Location field autocompletes, displaying a list of locations you can choose from. Press Enter or click the check mark symbol to add the location to the report. You can add multiple locations. Click the Trash can icon to delete or remove locations.
7. Click Add Report. The report will be added to the HIPAA Transactions.

Generate reports

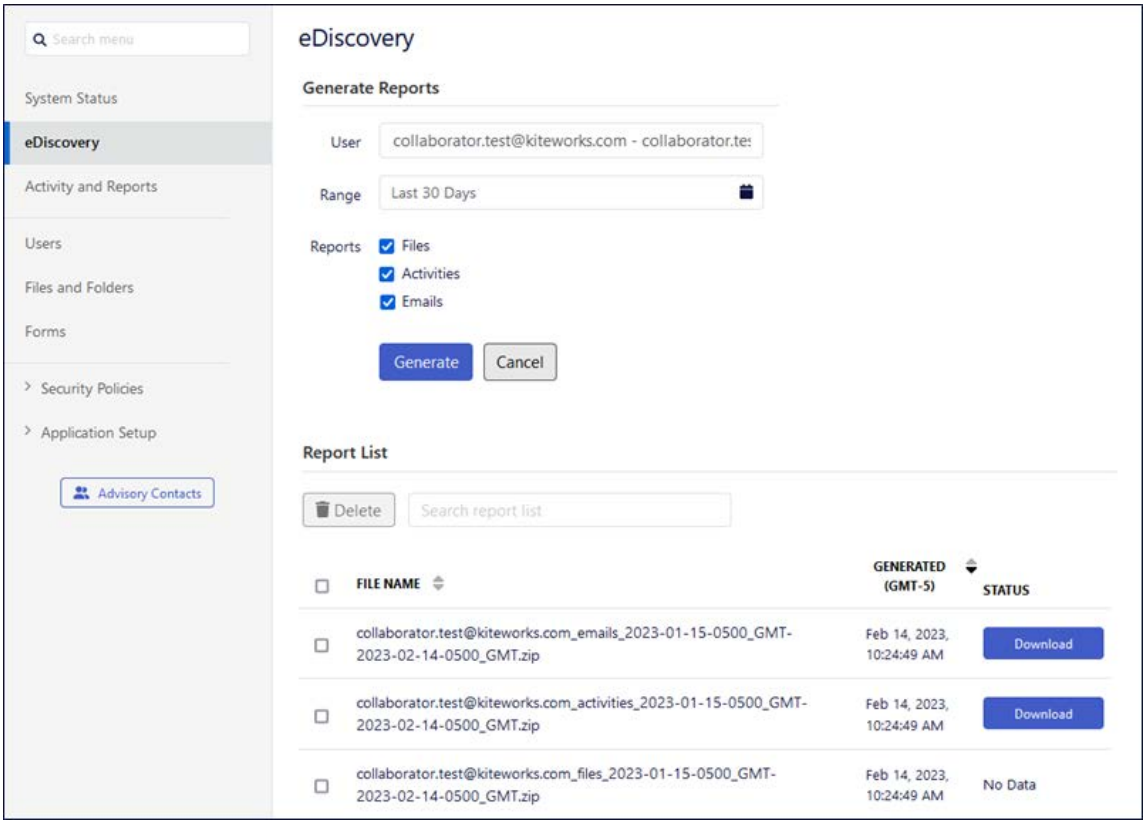
1. Click the report you would like to generate.
2. Click the Date Range down-arrow to select a date range. You can select Custom range and select the To and From dates.
3. Click Generate Report. The report generates and displays showing the Date/Time in GMT, Uploader, Location and Activity. You can view the report, download a PDF file or print the report. For printing very large reports you can select a Column View, Merged View or Row View.

About eDiscovery

Administrators assigned the DLI Admin role have access to the eDiscovery page in the Kiteworks Admin Console and view-only access to the CISO Dashboard. No other pages in the console.

The eDiscovery page enables DLI administrators gain insight into user activity and generate reports if needed for legal proceedings.

- Generate reports for specific users to show activities, emails, and files accessed by them.
- Download reports to CSV files for evaluation in other applications.



Generate user activity reports for eDiscovery

The eDiscovery page is visible only to administrators assigned the DLI Admin role for identifying, collecting, and reporting electronically stored information, including emails, documents, and user activities.

Enable eDiscovery and run eDiscovery report:

1. Upload and enable a DLI license.
2. Create a user with the DLI Admin role. DLI administrators have privileges to run eDiscovery reports. Note: DLI administrator cannot also be a system administrators. DLI privileges can be assigned to more than one user. DLI administrators have the same rights as application administrator as well as the ability to run the DLI reports.
3. In the navigation pane, go to eDiscovery and fill out the requested fields
   - User: Enter the email address of the user on whom you want to run the eDiscovery report
   - Range: Select the start date and end date for the report
   - Reports: Select which reports to run: Files, Activities, and/or Emails

   Caution: The zipped export of eDiscovery files may include files that have been quarantined by the anti-virus software

   Notes:
   - When generating the zip file for an eDiscovery report, the server requires twice as much temporary storage space as the size of the files. Once the zip file is uploaded to ACFS, the temporary storage space is cleaned up.
   - If Advanced Settings is enabled, Kiteworks can access deleted files that haven't been purged from the system.
   - For the audit log, Kiteworks searches logs as far back as specified in the Activity Log Retention parameter. See Set the audit log retention policy.
4. Click Generate.
5. Select the report and click Download.

   Note: On running an eDiscovery report both tasks and comments are listed under a New Value column in the Activity Report when exported to CSV.

Files report

The Files report includes the actual files as well as a spreadsheet with file names and fingerprint.

Email report

The Email report includes the emails sent or received by the user in .eml format.

Activity Log

View system and user activity

The audit log captures granular details about each action taken within the system. For file transfers, this includes information such as the sender, recipient, file name, file size, transfer time, and whether the transfer was successful. User activities are also recorded, such as sign in and sign out times, password changes, and permission modifications. System events such as configuration changes, updates, and restarts are also logged to provide a clear picture of the platform's operational status. In the audit log you can click a row to view the event in greater detail.

You can also refine your view of the log in the following ways:

- Search for event data.
- Use the following built-in filters to narrow the view results by event type:
  - Successful logins
  - Failed logins
  - Successful uploads
  - Failed uploads
  - Successful downloads
  - Failed downloads
  - Views
  - Send activities
  - Receive activities
  - MFT activities
  - MFT client activities
  - EPG activities
  - Admin activities
  - System activities

  Note: Your role determines which filters are available to you.
- Specify a date range to show only events that occurred within a specific time period.

You can also export the data to a comma separated values (.csv) text file for reporting purposes. To export the data, click Export to CSV.

To view system and user activity:

1. Go to Activity and Reports > Activity Log.
2. Search or filter the log to display the information you want.
3. To export the data, click Export to CSV.

Tip: Another way to view a specific user's activity is through the user's account settings. Go to Users > User Management. Click the account you want to access, and then on the User Activity tab you can view, sort, filter and export their activity.

Set the audit log retention policy

The audit log retention policy lets you control how long event data in the audit log will be saved.

By default, event data is saved indefinitely to avoid potential data loss. You can adjust this setting to retain the data for a specific number of days, after which the data will be deleted from the audit log.

Recommendation: If you change the default setting, set a retention period of 365 days or more. A long retention period can give you enough data to find anomalies and avoid potential security incidents.

To configure the audit log retention policy:

1. Go to Application Setup > Logging.
2. On the Activity tab, enter the number of days you want to retain audit log data, and then click Save.

Tip: The number of file uploads and downloads displayed in the Activity Log section of the System Status page is derived according to the audit log retention policy.

Reports

Generate reports

Kiteworks provides user activity and system usage reports that can be run on demand or scheduled to run at specific times.

- Activity Report - Use this built-in report to export all audit log events that occurred within a specified time period.
- Usage Report - Use this built-in report to export system usage metrics from a specified time period.

You can also create custom activity reports to export user activity filtered by domain and location, and within a specified time period. Reports can contain data about file upload and download activity, file views, email messages and file attachments that were sent and received by users, and form-related activities.

Report data is exported to a comma separated values (.csv) text file for download.

Generate reports on demand

To run a report on demand:

1. Go to Activity and Reports > Reports.
2. On the Reports tab, in the report row, click Run It Now.
3. Specify the date range for report data, and then click Run.

   Result: As the report is being generated, the Action column displays "Processing". You can click this button for a status update. Once the report is sent, you can access it from your inbox in the Kiteworks Web application and external email client.

Schedule reports to run at specific times

To schedule a report:

1. Go to Activity and Reports > Reports.
2. On the Reports tab, click the report row.
3. On the Schedules tab, click Add Schedule.
4. Configure the schedule as needed.

- Monthly - Set the frequency to a month to get a monthly report of the previous month's data. For example, run monthly on the 15th day at 2:00 AM GMT time to get the data for the previous month (from the 15th of the last month to the 15th of the current month at 1:59:59 AM).
- Weekly - Set the frequency to weekly for a weekly report which returns the last 7 days report data. For example, run on a weekly basis every Wednesday at 2:00 AM GMT time to get the data report for the last 7 days (from last Wednesday at 2:00 AM to Tuesday at 1:59:59 AM).
- Daily - Set the frequency to daily for a daily report which returns the last 24 hours report data. For example, run daily at 2:00 AM GMT time to get the data report for the last 24 hours from 2:00 AM.

5 Enter the email addresses of the recipients you want to receive the report. If sending the report to yourself, include your email address.

6 Click Save.

7 To add more schedules to the report, for each one click Add Schedule, and then configure the schedule and recipients as needed.

8 Click Save.

To activate or deactivate a report schedule:

In the row corresponding to the schedule, turn the report switch on or off.

To delete a schedule from a report:

In the row corresponding to the schedule, click .

Create custom activity reports

To create a custom activity report:

1 Go to Activity and Reports > Reports.

2 On the Reports tab, click Add Report.

3 Select a template corresponding to the type of report you want to create.

4 On the Configure Report Filters page, click the corresponding filter buttons to configure them as needed.

- When editing All Domain and All Locations filters, you can enter domains and locations manually or click the wrench icon to create custom groups of domains and filters. When configuring future reports you can select these custom groups instead of manually entering domains and locations.
- When editing form filters, you can select the form from which to return data, along with the form fields you want to include in the report.

5 Click Add Report.

6 Enter a name for the report, and then click Add.

Result: The report is added to the list on the Reports tab.

To edit a custom activity report:

1 Go to Activity and Reports > Reports.

2 On the Reports tab, expand the report you want to edit.

3 Click the Report Details tab.

4 Edit the report name and click the corresponding filter buttons to configure them as needed.

- When editing All Domain and All Locations filters, you can enter domains and locations manually or click the wrench icon to create custom groups of domains and filters. When configuring future reports you can select these custom groups instead of manually entering domains and locations.

- When editing form activity filters, you can select the form from which to return data, along with the form fields you want to include in the report.

5 Click Save.

Table 3. Report templates

Template	Description
Uploads from All Domains and All Locations	Provides data such as the date and time a file was uploaded, the email address of the user who uploaded the file, the folder path to the file, and the file name.
Downloads from All Domains and All Locations for files uploaded from All Domains and All Locations	Provides data such as the date and time a file was downloaded, the email address of the user who downloaded the file, the folder path to the file, and the file name. The report also provides the date and time the file was originally uploaded and the email address of the user who uploaded the file.
File Views from All Domains and All Locations for files uploaded by All Domains and All Locations	Provides data such as the date and time a file was viewed, the email address of the user who viewed the file, the folder path to the file, and the file name. The report also provides the date and time the file was originally uploaded and the email address of the user who uploaded the file.
Messages and files sent from All Domains and All Locations to All Domains	Provides data such as the date and time the message was sent, the email address of the message sender, the subject line text, file attachment names, recipient email addresses, and the date and time the message was received by recipients.
Messages and files received by All Domains in All Locations and sent by All Domains in All Locations	Provides data such as the date and time the message was received by recipients, recipient email addresses, the subject line text, and file attachment names. The report also provides the date and time the message was sent and the email address of the message sender.
Form activity from All Form with All Fields	Provides data such as the name of the form, the date and time the form was submitted, the email address of the user who submitted the form, the subject line text, recipient email addresses, and file attachment names.

Delete reports

To delete a report:

1 Go to Activity and Reports > Reports.

2 On the Reports tab, select the checkbox next to the report you want to delete.

3 Click the Delete button.

Storage

View user storage

You can view the amount of storage per user on the system. You can also export the data to a comma separated values (.csv) text file for reporting purposes.

To view user storage:

1. Go to Activity and Reports > Storage.
2. On the Storage tab, filter the user list or sort by the amount of storage used as needed
3. To export the data, click Download as CSV.

Bandwidth

View user bandwidth

You can view the amount of system bandwidth per user on the system and by specified time period. You can also export the data to a comma separated values (.csv) text file for reporting purposes.

To view user bandwidth:

1. Go to Activity and Reports > Bandwidth.
2. On the Bandwidth tab, filter the user list or sort by the amount of uploads and downloads as needed.
3. To limit the information to a specific time period, specify a date range.
4. To export the data, click Download as CSV.

User Management

Create and edit user accounts

You can create a single user account or multiple user accounts at the same time.

If creating multiple user accounts, you can select only one user role and user profile to apply to all of the accounts. After creating the accounts, you can edit individual accounts as needed to assign them different roles and profiles.

Rule: Only administrators assigned the System Admin role can create other system administrator accounts.

To create a user account:

1. Go to Users > User Management.
2. On the User Management tab, click Add Users.
3. On the Add Users page, select the role you want to assign to the account. The list is roles contains a set of built-in roles as well as any custom roles created by administrators.

Table 4. Built-in roles

Role	Description
System Admin	Configure and maintain all aspects of the Kiteworks product, including network configurations and software updates. System administrators are super users with full access to product functionality. **Exception:** Access to the eDiscovery page is available only to administrators assigned the DLI Admin role.
Application Admin	Manage applications in the Kiteworks Admin console. They can also manage all files and folders, licenses, server mappings (locations), Repositories Gateway sources, and end-user accounts.
Helpdesk Admin	Manage end user accounts to perform tasks such as create, unlock, suspend, activate, and delete accounts, reset passwords, revoke active user sessions, remote wipe mobile devices, and enable/disable SFTP keys. Helpdesk Admins can also view some policy and application settings to better understand user capabilities and status, such as profile definitions and storage use. They can also test some configured settings, such as LDAP, two-factor authentication (2FA), and Repositories Gateway source connections to identify potential issues.

Table 4. Built-in roles (continued)

Role	Description
DLI Admin (Data Leak Investigator)	Access to the eDiscovery page to generate reports for all activities, emails, and files accessed by specific users. DLI Admins also have limited access to the Kiteworks Admin console to view and download user activity. They also have view-only access to the CISO Dashboard.
CISO	Access only the CISO Dashboard to monitor all content entering and leaving the enterprise. This global view provides the ability to drill down to individual file transfers and generate detailed compliance reports that provide proof that of full visibility and control over the exchange of sensitive enterprise information. **Note:** GDPR and HIPAA compliance reports are separately licensed offerings with Kiteworks Advanced Governance, which also include anti-virus, data leak prevention, and advanced threat protection (including CheckPoint) and compliance reporting.
Compliance	Access only the Compliance Console to create and apply risk policies for protecting sensitive content as it moves through the system, as well as generate reports for analyzing audit log activity, insider and outsider threat activity, and the CMMC 2.0 compliance of 110 controls across 14 domains.
Policy Manager	Access only the Risk Policy Management page in the Compliance Console to create and apply risk policies for protecting sensitive content as it moves through the system.
Auditor	Access only the Reports Portal page in the Compliance Console to generate reports for analyzing audit log activity, insider and outsider threat activity, and the CMMC 2.0 compliance of 110 controls across 14 domains.
End User	Access the Kiteworks web application and any Kiteworks apps and plugins that have been made available to them.

4. Enter an email address for each user account you want to create. Separate multiple addresses with commas.
5. Select a profile to assign to the account. You can select the built-in Standard profile or Restricted profile, or select a custom profile if available. See Create and edit user profiles.
6. If you want to send the user an email notification inviting them to sign in to the system, select "Send notification email to added users".
7. Click OK.

Edit user accounts

To edit a user account:

On the User Management tab, perform one of the following actions.

- To edit a single account, click the user account.
- To edit multiple accounts, select the checkbox next to each account name, and then use the buttons on the page to perform actions such as change user roles and profiles, reset user account authentication methods, activate and suspend accounts, and delete accounts.

Edit user account email addresses

You can edit the email address that the user will use to sign in to Kiteworks applications.

To edit a user's email address:

1. On the User Management tab, click the account you want to edit.
2. In the information pane, click Edit next to the user's email address.
3. Enter the new email address, and then click Save.

Change or reset user profiles

On the User Management page, if the Profile column indicates "Manually changed" this means that the user's profile was manually configured by an administrator. You can edit user accounts to change assigned user profiles, or you can reset their user profiles to the profile the user was assigned on user creation.

To change or reset a user profile, on the User Management tab, select the account you want to edit.

- To change the user profile, click More, select the new profile, and then click OK.
- To reset a user profile, click More, and then click Reset User Profile.

Add or update user mobile phone numbers

A mobile phone number can be used as an extra step to confirm identity when two-factor authentication is required for signing into the server. It can also be used to text one-time passwords for accessing messages and file attachments without signing in. Once you add a user's mobile number to their account, they can edit their number through the Kiteworks Web Application to be automatically updated in the admin console.

To add or update a user mobile phone number:

1. On the User Management tab, click the account you want to edit.
2. In the information pane, enter the default country code and mobile number for the user, and then click Save.

Migrate email addresses

You can bulk migrate email addresses so that the users can authenticate with new email addresses. Once an email address is successfully migrated, all the data of those users will be associated with the new email addresses. This change of the email addresses is tracked in the system.

To migrate email addresses:

1. Go to Users > User Management.
2. Click the Change Email button. This tool is available for all administrators except those assigned the Helpdesk Admin role.
3. The Migrate Users window displays. You have two options to migrate email addresses:
   - Individual Email
   - Upload CSV

Migrate email addresses using the individual email option

1. Select Individual Email to enter one or several email addresses by clicking Add more.
2. Enter the old email address that needs to be updated in the first autocomplete field and the new email address in the second autocomplete field. If the new email address entered exists, a caution icon and message displays indicating that the email address already exists.

   If you continue the operation, the existing new email account will be deleted but all the top-level folders owned by this account will now be associated with the resulting account.
3. Click Submit or Cancel the action.
4. If a conflict occurs where the target new email address account exists, a warning displays to remind the administrator that the existing new email address will be deleted. Click Submit or Cancel the action. If the email migration to the new address is successful, the end user(s) will be notified by email of the change of address from the old email address to the new email address.

Upload CSV files to migrate email addresses

1. Select Upload CSV to upload a CSV file.

   You will need to upload a CSV file containing email addresses of all the users in 2 columns. List the old email addresses in the first column and the new email addresses in the second column. If there is a formatting error in the CSV file being uploaded, an error message displays. Edit the file and update a CSV file with the corrected format.

   Note: You can download a sample CSV file if needed.
2. If a conflict occurs where the CSV file contains a target new email address that already exists, a warning displays to remind the administrator that the existing new email address will be deleted. Click Submit or Cancel the action.

If the email migration to the new address is successful, the end user(s) will be notified by email of the change of address from the old email address to the new email address.

Track and log email migration

All the details of the migrated email addresses that changed from email A to email B will be tracked and logged on the Activity and Reports page.

Password

After the email has been updated to the new email address, a non-LDAP user will not be able to log in using his new or old user password. The password will need to be set after migration. A Reset password link will be embedded in email notification that will be sent to the user.

An LDAP user will not receive a reset password link via email. The user will be able to login using the new email address with the LDAP credentials.

Any end user account that is affected by email migration will be notified via email informing the recipient that the email address has changed from the old email address to the new email address.

Email content for email migration

Two emails are sent for email migration, one to an existing database user and the other to an LDAP user. These email addresses can be customized on the Application Setup > Configuration > Notification

Templates page using the "Email migration - non LDAP/SSO user" and "Email migration - LDAP/SSO user" notification templates. The LDAP user password descriptor can be customized here. If you do not want to customize the descriptor, you can get it from Application Setup > Kiteworks > General Authentication Settings > Password Descriptor.

Enable or disable SFTP keys

Secure File Transfer Protocol (SFTP) keys provide alternatives to entering passwords. When you enable SFTP, end users see the option in their Kiteworks Web Application preferences. They can generate a list of keys for accessing their account or import their own private keys. SFTP keys are unique to user accounts. To avoid problems with SSH/SFTP logins, end users should not share their keys with other users.

The following public key types are supported for authentication keys:

- RSA - Key size 1024, 2048, 3072, and 16384 bits
- ECDSA - Key size 256, 384, and 521 bits

Enable users to generate and import SFTP keys in the Kiteworks Web Application

Prerequisite: The SFTP role must be enabled on one or more servers.

To enable users to generate and import SFTP keys:

1. Go to Users > Profiles, and then expand the profile assigned to the users.
2. In the Client Access section, turn on the SFTP switch.

For instructions on how end users generate SFTP keys in the Kiteworks Web Application, refer to "Define your Kiteworks preferences" in the *Kiteworks Web User Guide*.

Enable or disable SFTP keys associated with individual user accounts

To enable or disable SFTP keys:

1. Go to Users > User Management.
2. Click the account you want to edit.
3. On the SFTP Keys tab, if the user account has SFTP keys, the number of keys are listed.
4. Click the SFTP key value.
5. Click the keys you want to enable or disable, and then click the Enable or Disable key icon.

Add and generate SFTP keys for user accounts

Role: To add and generate SFTP keys for individual user accounts, you must be assigned a custom role that was based on one of the following built-in roles: System Admin, Application Admin, HelpDesk Admin. Your custom role must also have the "Add/Generate SFTP Key" permission.

To add and generate SFTP keys for individual user accounts:

1. Go to Users > User Management.
2. Click the account you want to edit.

3 On the SFTP Keys tab, perform the following actions:

- To add an SFTP key, click Add SFTP Key. Enter the key name, and then enter or paste the key into the key field. Click Generate.
- To generate an SFTP key, click Generate SFTP Key. In the "Generate public/private key pair for SFTP access" box, enter a key name and pass phrase, and then click Generate.

Increase user account folder quota

After folder quota is calculated, some users may exceed their quota. It is recommended you increase their user profile quota limit to allow them uninterrupted use of the folder. See Create and edit user profiles.

You can also reassign their folder ownership to a user or user profile with a higher quota.

An alert will display in the admin console with the list of the affected users. An email notification will also be sent to the system administrators and application administrators to upgrade the folder quota for the affected users. A weekly notification will be sent to administrators if the user quota has not fixed or updated.

The system will log all activities for the folder storage quota in the Activities Report.

A warning icon appears next to the user's name who had exceeded the folder quota allowance.

In the Status column, you can filter results using the Extra Quota Allowance Only filter to correct the used quota and allowance issues.

Create shared mailboxes

You can create shared mailboxes when multiple people need access to the same mailbox, such as a support email address. Shared mailboxes are not assigned user names and passwords, so users can't sign in to them directly.

Before you create a shared mailbox, here are some things you should know:

- Licenses - No additional license is needed to create a shared mailbox account. However, members you add to shared mailbox accounts must be internal licensed users.
- External users - Only internal users can be given access to shared mailboxes. You can't give people outside your business (such as people with a Gmail account) access to shared mailboxes.
- Mailbox conversion - You can convert existing user accounts to shared mailboxes.

  Note: After you add members to shared mailboxes, those users may need to sign out and back in to the web application again to access their updated settings.
- Administrator roles - Only users assigned the System Admin, Application Admin, and Helpdesk Admin roles can convert internal licensed user accounts and distribution list accounts to shared mailboxes.
- User profiles - You can assign any user profile to the shared mailbox account to enforce the profile policies for mailbox settings, such as file attachment limits, message download rules, link expiration, and so on. Shared mailboxes can also be used to access forms and request files to the shared mailbox inbox.
- You can create as many shared mailboxes as needed, however end users in the Kiteworks Web Application can enable up to 5 shared mailboxes in their user accounts.
- You can use the filter list to quickly discern which accounts are shared mailbox accounts.

Interaction with Outlook

If your users are also using the Kiteworks for Outlook Desktop plugin to send and receive secure mail, they can access up to 5 shared mailboxes directly from their Outlook client. The plugin automatically detects and adds the shared mailboxes that the user has enabled in their account settings in the

Kiteworks Web application. This enables them to select the appropriate "From" address when sending secure mail.

To use a shared mailbox with the Kiteworks for Outlook Desktop plugin:

- You must have preconfigured the shared mailbox in both the Microsoft 365 Admin Center and the Kiteworks Admin Console. For instructions on how to configure shared mailboxes in Outlook, refer to https://docs.microsoft.com/en-us/microsoft-365/admin/email/create-a-shared-mailbox.
- The name of the shared mailboxes in Outlook and Kiteworks must match.
- The user's Outlook account must be a member of the Outlook shared mailbox.
- The user's Kiteworks account must be a member of the Kiteworks shared mailbox.
- The user must have enabled the shared mailbox in the Kiteworks Web application.

Emails sent from shared mailboxes look the same to recipients in Outlook as other messages send from Kiteworks user accounts. If required by the sender, recipients will still need to sign in to the server to access the email, download file attachments, and so on. In Outlook, the only indication that the email was sent from a shared mailbox is that the sender email address will be the address of the shared mailbox, such as "sharedmailbox@company.com".

Create shared mailboxes and add members

Creating a shared mailbox consists of creating a user account, converting it to a shared mailbox account, and then adding members to the account.

To create a shared mailbox user account:

1. Go to Users > User Management.
2. On the User Management tab, click Add Users.
3. In the Add Users dialog box, provide the following information:
   - Role - Ignore this setting. Roles do not apply to shared mailboxes.
   - Email - Enter the email address you want to identify the shared mailbox. To create multiple accounts at the same time, use commas to separate email addresses.
   - Profile - Select the user profile you want to apply.
   - Send notification email to added users - Ignore this setting. It applies only to inboxes for internal user accounts.
4. To create the account, click OK.

To convert the account to a shared mailbox and add members:

1. On the User Management tab, click the user account you just created.

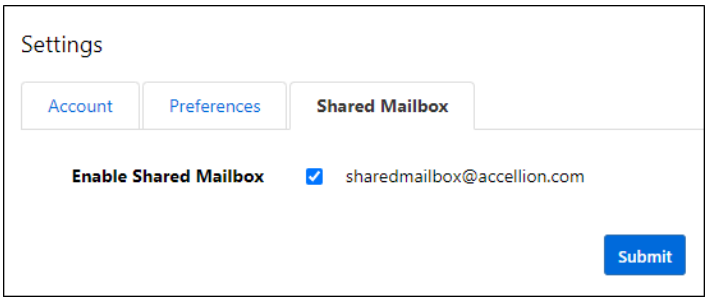
   Tip: To filter the user list by account name, type the name of the account in the search box.
2. In the right pane, go to the Account Type list and select Shared Mailbox.
3. In the search box, enter the email addresses of the members you want to have access to the account.

   Alternative: You can import a list of email addresses from a comma separated values (.csv) text file. See Import member accounts and add them to shared mailboxes.
4. Click Save.
5. In the Retain Data dialog box, select the "Delete all folders owned by the user and all files sent to others" check box.

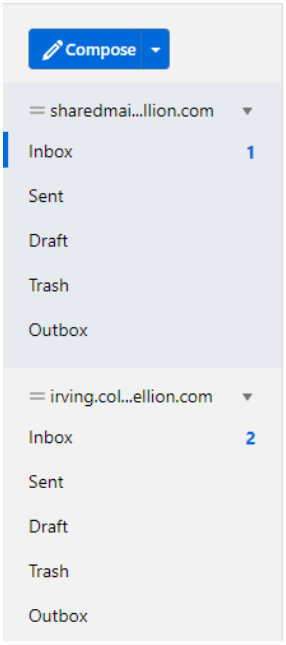
   Rationale: Although there is no data associated with the account, this is required to convert the new user account to a shared mailbox account.

Access shared mailboxes in the Kiteworks Web Application

After you create a shared mailbox and add members to it, those members see the new mailbox in account profile settings in the Kiteworks Web Application. You may want to notify them of this. From the Shared Mailbox tab, they can choose to enable the mailbox to add it to the navigation pane.



When they want to send email from the shared mailbox, they click the mailbox in the navigation pane and then compose their message.



Note: After you add members to shared mailboxes, those users may need to sign out and back in to the web application again to access their updated settings.

Convert existing user accounts to shared mailbox accounts

When converting an existing user account to a shared mailbox, you have the option to also remote wipe their mobile devices and transfer ownership of their Kiteworks folders and files to another user.

To convert an existing user account to a shared mailbox:

1. On the User Management tab, click the user account you want to convert to a shared mailbox.
   Tip: To filter the user list by account name, type the name of the account in the search box.
2. In the right pane, go to the Account Type list and select Shared Mailbox.
3. In the search box, enter the email addresses of the members you want to have access to the account.

Alternative: You can import a list of email addresses from a comma separated values (.csv) text file. See Import member accounts and add them to shared mailboxes.

4 If you want to delete all Kiteworks folders and files from the selected users mobile devices and synced desktops, turn on the "Remote wipe data on desktop and mobile devices" switch.

Folders and files synced using the Kiteworks Desktop Client application will be deleted during the next scheduled sync cycle.

5 Perform one of the following actions:

- To delete all Kiteworks folders and files owned by the selected users, including folders and files that they or other users uploaded to their folders as subfolders, select the "Delete all folders owned by the user and all files sent to others" switch.

  Warning: Deleted folders and files can't be recovered.

- To retain all Kiteworks folders and files owned by the selected users, select the "Retain the data" switch.

  You'll be prompted to transfer ownership to a different user. You can also give the new owner access to folders and files that others shared with the users you are deleting.

6 Click Save.

Import member accounts and add them to shared mailboxes

In addition to searching for each separate email address of the members you wish to add and adding them one at a time, you also have the ability import a CSV file containing the addresses of those same members. This is very helpful in cases where you have many members you want to add to share the mailbox and you need to add them quickly.

When creating the CSV file, here are some things you should know:

- The file must have at least one column containing the valid email addresses of internal users.
- In the case of a multi-column CSV file, all of the values must be comma-separated and the email addresses must be in the first column of the sheet. An example of this might be that you exported a list of users from the Manage Users page, edited that list down to the members who you want to have access to share the mailbox, and have imported the file back into the shared mailbox account. That sheet has multiple columns with additional user information.

To import a CSV file:

1 In the process of adding a new shared mailbox, select "Shared mailbox" from the Account type field drop down list on the user details page. This designates that the user account will now act as a shared mailbox account. Some new fields will now appear below the Account type drop-down list.

2 Below the "This shared mailbox can be accessed by" text, click the Import CSV button to import a CSV file containing the email addresses of the people you want to use the shared mailbox. Use the file browser provided to locate the file you wish to import.

3 When you have located the desired file, click Open to import the CSV file. The selected addresses for the group will appear in a list below the search box if the CSV file is formatted correctly and the addresses are valid internal users. An Import Members status panel will be displayed to inform you of the results of your import operation.

4 When finished, click Save.

Keep in mind the following additional details when using with the Import CSV option:

- The imported CSV file is always considered the most up-to-date user list. The first file import pre-populates the member list with all valid internal addresses and any additional imports in the future will remove the old list and add the new or updated list of member accounts.

- You can click the "X" next to any account address to remove that account from the member list.
- For long member lists that extend off the page User details page due to a large number of members, you can use CTRL-F (Find) to find the address(es) that you wish to locate or remove.

Shared mailbox events

If you have a syslog server set up as an External Service in the Kiteworks Admin Console, you are able to capture the activity of shared mailboxes via shared mailbox events. The following table provides information on the events that are logged concerning shared mailbox activity.

Table 5. Shared mailbox events

Action taken	Event generated (event name)
Send mail from Shared Mailbox dl1@xyzcompany.com	send_mail (user 1)
Send preview from Shared Mailbox dl1@xyzcompany.com	send_preview (user 1)
Created a draft from Shared Mailbox dl1@xyzcompany.com	created_draft (user 1)
Updated a draft from Shared Mailbox dl1@xyzcompany.com	changed_draft (user 1)
Deleted a draft from Shared Mailbox dl1@xyzcompany.com	delete_draft (user 1)
Send tracking report from Shared Mailbox dl1@xyzcompany.com	send_tracking_report (user 1)
Withdrawn an attachment from Shared Mailbox dl1@xyzcompany.com	file_withdrawn (user 2)
Viewed an attachment from Shared Mailbox dl1@xyzcompany.com (Recipient)	view_mail
Move a mail from Shared Mailbox dl1@xyzcompany.com (Another member)	trash_mail (user 2)
Delete a mail from Shared Mailbox dl1@xyzcompany.com Current User: user2@xyzcompany.com Sender: dl1@xyzcompany.com To: user10@xyzcompany.com Email From: user1@xyzcompany.com (Another member)	delete_mail
Download an attachment from mail sent from Mailbox dl1@xyzcompany.com Current User: user2@xyzcompany.com Sender: dl1@xyzcompany.com To: user10@xyzcompany.com	download_email

Table 5. Shared mailbox events (continued)

Action taken	Event generated (event name)
Download attachments as zip from mail sent from Shared Mailbox dl1@xyzcompany.com Current User: user2@xyzcompany.com Sender: dl1@xyzcompany.com To: user10@xyzcompany.com (Recipient)	download_email_zip
Copy an attachment from Shared Mailbox dl1@xyzcompany.com (Recipient)	copy_file
Update user shared mailbox	user_update_shared_ mailbox
Send tracking report from Shared Mailbox dl1@company.com	send_tracking_report
Add shared mailbox	admin_add_shared_ mailboxa
Update shared mailbox	admin_update_shared_ mailbox
Delete shared mailbox	admin_delete_shared_ mailbox

Reset user account passwords

If a user is unable to change their password through the Kiteworks web application, you can send them a link to reset their password or reset it for them. Resetting a user's password automatically signs them out of any active sessions and requires they sign in again using their new password.

To reset a user account password:

1. Go to Users > User Management.
2. Click the account you want to access.
3. At the top of the page, click Reset Password.
4. On the Reset Password page, if you want to enable the user to change their password, turn on the "Send user password link" switch. An email notification will be sent to the user containing a link for changing their password. You can also create a password for them.

   To create a password for the user:

   1. Turn off the "Send user password link" switch.
   2. Enter and confirm the new password.
   3. If you created a temporary password for the user, turn on the "User must change password at next login" switch. The user will be prompted to change their password when signing in.
5. To finish, click Reset.

Unlock user accounts

If a user account is locked because of too many invalid sign-in attempts, you can unlock their account.

You can unlock a single user account or unlock multiple accounts at the same time.

To unlock a user account:

1. Go to Users > User Management.
2. On the User Management tab, select the accounts you want to unlock, and then click Unlock.

   Tip: You can also filter the user list to display only locked accounts. In the Status column, click the filter icon and select Locked Only. Select the accounts, and then click Unlock.

Reset user account authentication types

For user accounts configured to use authentication such as SSO or certificate-based authentication, you can change those account types back to local accounts so that they can sign in using their user names and passwords.

To reset user authentication types:

1. Go to Users > User Management.
2. On the User Management tab, select the accounts you want to edit.
3. Click More, and then click Reset to Local Authentication.

Suspend and reactivate user accounts

You can suspend end user accounts to immediately prevent those users from signing in until their accounts are reactivated. Suspending a user's account automatically signs them out of any active sessions.

You can suspend a single user account or suspend multiple accounts at the same time.

To suspend a user account:

1. Go to Users > User Management.
2. On the User Management tab, select the accounts you want to suspend, and then click Suspend.

To activate a suspended user account:

1. Go to Users > User Management.
2. Select the accounts you want to activate, and then click Activate.

   Tip: You can also filter the user list to display only suspended accounts. In the Status column, click the filter icon and select Suspended Only. Select the accounts, and then click Activate.

Remote wipe user mobile devices

If a user's mobile device is lost or otherwise compromised, you can use remote wipe to remove all downloaded data contained within the Kiteworks mobile app installed on their device.

To remote wipe a user's mobile devices:

1. Go to Users > User Management.
2. On the User Management tab, click the user's account to edit it.
3. On the Devices tab, select the device to be wiped, and then click Wipe.

Delete user accounts

When deleting user accounts you can transfer their ownership of folders and files to other users. If you want to transfer ownership to the same user, you can select multiple user accounts to delete at one time. If you want to transfer ownership to different users, delete only one user account at a time.

To delete a user account:

1. Go to Users > User Management.
2. On the User Management tab, select the accounts you want to delete, and then click More > Delete Account.
3. If you want to delete all Kiteworks folders and files from the selected users mobile devices and synced desktops, turn on the "Remote wipe data on desktop and mobile devices" switch.

   Folders and files synced using the Kiteworks Desktop Client application will be deleted during the next scheduled sync cycle.
4. Perform one of the following actions:
   - To delete all Kiteworks folders and files owned by the selected users, including folders and files that they or other users uploaded to their folders as subfolders, select the "Delete all folders owned by the user and all files sent to others" switch.

     Warning: Deleted folders and files can't be recovered.
   - To retain all Kiteworks folders and files owned by the selected users, select the "Retain the data" switch.

     You'll be prompted to transfer ownership to a different user. You can also give the new owner access to folders and files that others shared with the users you are deleting.
5. Click OK.
6. If you chose to retain the user's data, enter the email address of the user you want to receive the data.
7. To allow the new owner to retain access to folders and files that were shared with the deleted users, select the "Retain permissions to shared data" switch.
8. Click OK.

Profiles

Create and edit user profiles

Kiteworks provides built-in user profiles for determining which functions assigned users can perform on the application level.

- Standard
- Restricted

You can edit built-in profiles or you can create custom profiles for specific groups of users. For example, if some of your managers need additional storage for big projects, you can create a profile based on the Standard profile, and then configure settings that give them additional storage quota.

To edit a built-in user profile:

1. Go to Users > Profiles.
2. On the Profiles tab, click the profile you want to customize.
3. Use the tabs to configure the profile.

To create a user profile:

1. Go to Users > Profiles.
2. On the Profiles tab, click Add Profile.
3. Enter a name for the profile.

   Rule: You can enter up to 25 characters consisting of letters, numbers, underscore, and hyphens.
4. Select an existing profile to use as the basis for the new profile, and then click OK.

   Result: The new profile is added to the bottom of the profile list.
5. (Optional) Type a description for the profile that may help other administrators understand its use or application. The description will be visible and editable in the profile and also in the Description column on the Profiles tab.
6. To edit the profile, click the profile and then use the tabs to configure the settings as needed.

Built-in profiles

Table 6. Built-in user profiles

Permission control/ability	Standard	Restricted
Maximum storage	2GB	2GB
Link expires	30 days	30 days
Account expires	Never	Never
Personal folder	Yes	—
Edit mobile files	Yes	—
Download mobile files	Yes	—
Share with external users	Yes	—
Send files to external users	Yes	—
Sync	Yes	—
Create top-level folders	Yes	—
Use clients	All	iOS, Android, Windows 8

Profile settings

- Account tab
- File Filtering tab
- Send File tab
- Request File tab
- Clients and Plugins tab
- Collaboration tab
- Collaboration settings for restricted users

Account tab

Table 7. Account tab settings

Setting	Description
Two-factor authentication	Select the two-factor authentication source that will be used for the user profile, such as one-time passcode (OTP) authentication or SMS-based two-factor authentication (2FA).
Inline image display	Specify whether to automatically display inline images in messages sent to users. **Note:** This setting appears only when the Sign In security policy has been configured to allow it to be set at the user profile level. If the setting is not available, it can be configured globally to apply across all profiles. Go to Security Policies > Mail > Send Mail > Mail Options.
Account inactivity	
Automatic account deactivation	Automatically deactivate inactive user accounts after a specific number of days of inactivity.
Deactivate account after # days of inactivity	Specify the number of days after which to automatically deactivate inactive accounts. Deactivated accounts continue to consume licenses, but those users will not be able to sign in again until their accounts are reactivated. System email notifications are sent to users 7 days in advance to inform them that their accounts are set to be deactivated due to inactivity. This gives them the option to reactivate their account by signing in again.
Delete account when deactivated	When accounts are deactivated, automatically delete those accounts and release their licenses. System email notifications are sent to the users 7 days in advance to inform them that their accounts are set to be deleted due to inactivity. This gives them the option to reactivate their account by signing in again. **Note:** Automatically deleting an account automatically deletes all folders and files owned by the user, all files uploaded to the user's folders by other users, and deactivates all links to files that were sent by the user. If you want the option to retain user content and transfer ownership prior to deleting an account, select "No" to prevent automatic deletion.
Geo IP Fencing	Allow or block IP addresses from accessing the system by IP addresses, such as IPs located in high-risk or prohibited regions or countries.

Table 7. Account tab settings (continued)

Setting	Description
Blocked IP addresses	IP addresses you want to block from accessing the server. Enter a single address or a range of addresses separated by commas in the following formats: • Single IP address **Example:** 192.168.1.1 • IP address with wildcard **Example:** 192.168.* • Selection by subnet **Example:** 192.168.100.14/24 • Selection by range **Example:** 192.168.1.10-192.168.1.25/24 • IPv6 format **Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Blocked countries	Countries you want to block from accessing the server. Start typing to see a list of names. **Note:** Kiteworks uses the IP2Location IP Address Geolocation Database to determine the approximate geographic location of an IP address and can't guarantee that the data in this geolocation database is always up-to-date.
Allowed IP addresses	IP addresses you want to have access to the server. The allowed list is dependent on the blocked list. For example, if you block a range of IP addresses using a wildcard (such as 192.168.*), you can specify that specific addresses within that range are allowed access to the server (such as 192.168.1.1 and 192.168.1.2). However, if you don't block any addresses but you enter some allowed IP addresses, all addresses will still be allowed to access the server. Entering addresses in only the allowed list does not block all other addresses from accessing the server.

File Filtering tab

You can allow or block file types that Kiteworks Web Application users can upload to folders.

To allow or block file types from being uploaded to Kiteworks:

1. On the File Filtering tab, specify whether to allow or block new (unlisted) file types by default.
2. In the File Filtering section, expand each category list and select which file types to allow or block.
   - At the top of each category you can choose to block all file types within that category.
   - When you block a file type, associated file types may get automatically blocked as well. For example, if you block Microsoft PowerPoint .ppt files, the .pps file type used for PowerPoint slide shows will also get blocked.
   - In the Custom category, you can add file types not already listed and then allow or block them from being uploaded.
3. Click Save.

Send File tab

The Send File settings apply to users sending messages and files from the Kiteworks web application and the Kiteworks for Outlook Desktop plugin.

Table 8. Send File tab settings

Setting	Description
Allow send mail	Allow users to send messages and files securely through Kiteworks. **Note:** This setting appears only when the Sign In security policy has been configured to allow it to be set at the user profile level. If the setting is not available, it can be configured globally to apply across all profiles. Go to Security Policies > Mail > Send Mail > Send Options.
Default form for the compose page	When composing messages, users see the standard email composer. If you created secure web forms for users to upload sensitive information with messages, select the default form that you want senders to use when composing a message. They will have access to the forms menu and will still be able to select a different form or select the standard email composer to compose the message. To prevent users from bypassing a form to use the standard composer, select the Hide Standard Form checkbox.
Send files to external users	Allow users to send files to recipients outside of your organization.
Mark addresses as external distribution lists	While composing messages, allow users to mark email addresses as external distribution lists. Subsequent messages sent to these email addresses by the user and other users will be sent to the corresponding distribution lists. **Note:** This setting appears only when the Sign In security policy has been configured to allow it to be set at the user profile level. If the setting is not available, it can be configured globally to apply across all profiles. Go to Security Policies > Mail > Send Mail > Send Options.
Maximum attachments limit	The maximum number of file attachments that can be attached to a message, up to 100.

Table 8. Send File tab settings (continued)

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Who can download the file via the secure link</td><td>Recipient settings you want users to be able to see and choose from when sending files to others.
<table>
<tr><td>Recipients only</td><td>Only original recipients can view the message. Anyone who receives a forwarded copy of the message will not be able to access it.</td></tr>
<tr><td>Recipients only and allow SMS one-time passcode to access</td><td>Only original recipients can view the message. Also text one-time passcodes for accessing the message. When sending a message, the sender will be prompted to enter or confirm recipient mobile numbers. Recipients will still have the option to sign in or create an account to access the message.
Note: This setting appears only when SMS-based one-time passcode authentication is configured in the console. See Set up SMS-based two-factor authentication.</td></tr>
<tr><td>Recipients only and allow e mailed one-time passcode to access</td><td>Only original recipients can view the message. Also email one-time passcodes for accessing the message. Recipients will still have the option to sign in or create an account to access the message.
Note: This setting appears only when email-based one-time passcode authentication is configured in the console. See Set up email-based one-time passcode authentication.</td></tr>
<tr><td>Recipients and users in your organization</td><td>Original recipients can view the message, along with anyone in your organization who receives a forwarded copy of the message.</td></tr>
<tr><td>Recipients and anyone with a user account</td><td>Original recipients can view the message, along with anyone with a user account who receives a forwarded copy of the message.</td></tr>
<tr><td>Anyone, no authentication required</td><td>Anyone who receives a copy of the message can view the message and download any file attachments.</td></tr>
</table></td></tr>
<tr><td>Default secure links access control</td><td>Based on your selections for the "Who can download the file via secure link" setting, select the default setting you want selected when users compose their messages.</td></tr>
</table>

Table 8. Send File tab settings (continued)

Setting	Description
Protect message body	Require recipients sign in to view the message and access file attachments. If they don't have an account on the server, they'll be prompted to create one. **Caution:** The subject line text will always be visible to recipients. When the message body is protected, the message body is not sent through the normal email system and requires recipients to connect to the Kiteworks platform utilizing the authentication and security of Kiteworks to access the content through the encrypted connection. This results in the sender, recipients, and DLI administrators being the only users who can access the email body when they have the Advanced Governance package.
Default to enabled	Based on your selection for the "Protect message body" setting, select the default behavior when users compose their messages and they select "User Decides".
Link expiry	The number of days after which file attachments links expire and file attachments get marked for deletion. **Note:** Files are deleted during the server's cleanup event.
Send quota	The maximum amount of send storage space that each sender is entitled to. You can set it to -1 for no limit on send storage. Only sent messages, draft messages, and file request messages are counted in the send quota, not received messages. Quota used is calculated based on the transaction. It does not matter if the file is a new attachment sent from an existing shared folder or forwarded from another message. All sent files are counted. **Note:** This setting appears only when the Sign In security policy has been configured to allow it to be set at the user profile level. If the setting is not available, it can be configured globally to apply across all profiles. Go to Security Policies > Mail > Send Mail > Send Options.
Allow to modify file secure link expiration	Allow message senders to extend the expiration date for file attachment links.
Maximum link expiry	The maximum amount of days by which message senders can extend the file attachment links. **Note:** This setting appears only when the Sign In security policy has been configured to allow it to be set at the user profile level. If the setting is not available, it can be configured globally to apply across all profiles. Go to Security Policies > Mail > Send Mail > Send Options.
Send me a copy	The message sender can choose to email themselves a copy of the message.
Return receipt	The message sender can choose to get notified receipts when recipients open messages.

Table 8. Send File tab settings (continued)

Setting	Description
Tracking report	The message sender can choose to get notified when file attachments expire and also when recipients open, download, and copy attachments to folders. Senders are emailed time-stamped notifications that include file attachment names and the email addresses of users who downloaded the files.
Add digital fingerprint	The message sender can choose to include an SHA3-256 digital fingerprint with each file attachment for recipients to verify the integrity of the file. Recipients can use a third party tool to verify that each file has not been altered.
Draft attachment expiration	The number of days after which file attachments in draft messages expire.
Allow to grant mail tracking to others	The sender can give other users permission to view the tracked activity around their sent messages and attachments.
Tracking dashboard	Give Kiteworks Web Application users the ability to track messages they send to recipients. They can create tracking dashboards to track messages based on subject line keywords, messages that contain file attachments, and messages sent during a specific time period. If you selected the "Tracking report" setting, allows the sender to send the notification to other users as well.

Request File tab

Request to inbox tab

When the requestor sends an email to three different recipients to request a file in the same email, the application generates three different emails in the sent folder. Each recipient receives an email. Each recipient can upload the requested file and reply to the requestor. If the requestor has also checked "Notify Also" for box another person, the reply will also be copied to that inbox.

Table 9. Request to inbox tab settings

Setting	Description
Upload authentication	Who can upload files using the Request File to inbox. • Authenticated user only: Only authenticated users can upload files using the Request File link. • Anyone (no authentication): Anyone can upload files using the Request File link. • User decides: The message sender decides who can upload files using the Request File link. If this option is selected, a default can be set for Default Upload Authentication: No Authentication or Require Authentication.

Table 9. Request to inbox tab settings (continued)

Setting	Description
Link expiration	Specify (in days) the validity of the request. Set to 0 days for no expiration. The number of days can't exceed the User Decides max request expiration. You can set the expiration or select User Decides for the user to decide when the link expires.
Upload limit	Specify the default number of uploads allowed for a request. Set to 0 for unlimited. You can set the limit or select User Decides for the user to decide when the upload limit.

Request to folder tab

Table 10. Request to folder tab settings

Setting	Description
Upload authentication	Who can upload files using the Request File to folder. • Authenticated user only: Only authenticated users can upload files using the Request Folder link. • Anyone (no authentication): Anyone can upload files using the Request Folder link. • User decides: The message sender decides who can upload files using the Request Folder link. If this option is selected, a default can be set for Default Upload Authentication: No Authentication or Require Authentication.
Link expiration	Specifies in days the validity of the request. Set to 0 days for no expiration. The number of days can't exceed the User Decides max request expiration. You can set the expiration or select User Decides for the user to decide when the link expires.
Upload limit	Specify the default number of uploads allowed for a request. Set to 0 for unlimited. You can set the limit or select User Decides for the user to decide when the upload limit.
Allow viewable files	Allow the user to attach files that can be viewed by the recipient of the request.

Clients and Plugins tab

Table 11. Clients and Plugins tab settings

Setting	Description
Client access	

Table 11. Clients and Plugins tab settings (continued)

Setting	Description
SFTP	Allow SFTP access. You must enable Allow SFTP Access for end-users at the User Profile level for the user to use this feature. The primary management for the SFTP keys is handled by the end user. **Note:** The SFTP access can be enabled only after and SFTP role is added on at least one server. • SFTP maximum session - Specify the maximum number of open SFTP sessions allowed for users assigned the profile. When a user tries to sign in using SFTP, the system will check to see if there are sessions available. The default is 10000. Maximum is 50000. You can also limit the number of SFTP sessions for the system globally, along with the session idle timeout and access token expiration time. • SFTP password authentication - Enable users to authenticate using SFTP passwords. Disabling this option limits the authentication method to key-based authentication.
Desktop client	Enable users to access to the Kiteworks Desktop Client application . If you want to force the use of the secure container for syncing, turn on the Secure Container Required switch. **Note:** The Kiteworks Desktop Client does not support synchronization with network drives.
Outlook desktop	Enable users to access to the Kiteworks for Outlook Desktop plugin.
Allow read mode	Enables read mode in the Kiteworks for Outlook plugins. **Warning:** In read mode, the email content may be viewed from other Outlook clients using the same account.
Policy automation for secure email	
Enable policy to enforce Outlook desktop plugin	Enforce a set of policies for all emails being sent using the Kiteworks for Outlook Desktop plugin. Any policy setting combination set by the Kiteworks administrator will be followed and applied automatically to an Outlook email being composed by end users. **Note:** This setting is only visible when the plugin is enabled.
Any of the below conditions are met	These policies will be applied if the administrator selects at least one of the conditions mentioned in this section.

Table 11. Clients and Plugins tab settings (continued)

Setting	Description
All of the below conditions are met	These policies will be applied if the administrator selects all the conditions mentioned in this section.
Recipient domain	
-- No conditions	No conditions are set for the recipient domain.
-- Matches any external domain	Recipients with any email domain will trigger this policy.
-- Matches any specific domain	Recipients with the listed email domains will trigger this policy.
Email attachment	
-- No conditions	No conditions are set for an email attachment.
-- Contains any attachments	When composing an email and adding an attachment, enforce this policy and turn on the Secure Send switch.
-- Contains specific metadata tag	When adding a file attachment to an email containing specific Microsoft metadata tags, enforce this policy and turn on the Secure Send switch. If this option is selected, you can enter one tag per line in the field provided. **Limitation:** Only Microsoft Office files (Office Open XML) with Sensitivity labels are supported.
-- File size threshold	Files that exceed the size will be automatically sent securely using the plugin. For example, if a user attaches a file that exceeds the threshold and then turns off security, the policy will detect this and turn on security again. This policy affects files that users attach using the standard Outlook paperclip or using the attachment options within the plugin pane. When a file attachment meets the policy requirement, the plugin pane automatically opens and the "Secure message attachments" setting turns on indicating that the policy is in effect.

Collaboration tab

Table 12. Collaboration tab settings

Create top-level (root) folders	Users can create folders at the top-level (root) of the All Files page in the web application. By default, this source is named "Kiteworks Files" and is the service name assigned to the server. You can give it a different name. If you don't select this option, users can create folders only in their "My Folder" system folder.
Folders expire	Expire new folders after the number of days specified, following their creation dates. Once folders expire they are deleted from the system. To let folder owners set folder expiration dates, leave the field empty or enter 0. When creating folders in the Kiteworks web application, they can specify expiration dates or set their folders to never expire. Subfolders inherit their folder expiration settings from their top-level folders. Folder expiration email notifications are sent by the system 7 days prior to expiration. **Note:** This setting appears only when the global folder and file policy is configured to allow it to be modified in user profiles. See Set policies for Kiteworks files and folders.
Files expire	Expire new files after the number of days specified, following the dates they were added to folders. Once files expire they are deleted from the system. To let folder owners set file expiration dates, leave the field empty or enter 0. **Note:** This setting appears only when the global folder and file policy is configured to allow it to be modified in user profiles. See Set policies for Kiteworks files and folders.
Apply to existing folders and files	Updating the default "Folder expiration" and "File expiration" settings impacts new folders and files added to the system once the policy change takes effect. If you want to apply these expiration settings to existing folders and files as well, click "Apply to existing folders and files" and specify how you want to apply the change. Once applied, an email notification will be sent to the default system notification email address for administrators informing them of the policy change. If the change can't be applied to specific files, the notification includes the file owner names so that they can manually update the expiration dates for those files. An email notification is also sent to file owners informing them of the policy change. **Note:** This setting appears only when the global folder and file policy is configured to allow it to be modified in user profiles. See Set policies for Kiteworks files and folders.
Total folder quota	The maximum amount of storage space you want to allocate for each user's folders and files. To specify no limit, enter -1.

Table 12. Collaboration tab settings (continued)

Enable folders that use system quota	Enable end users to create system quota folders using system storage quota instead of their personal storage quota. When creating top-level folders in the Kiteworks Web Application, users will have the option to use their personal storage quota or use system storage for the folders. • When configuring storage quota you can specify the maximum number of system folders users can create, the default storage quota that will be selected for them (although they can increase or decrease the amount), and the maximum amount of storage quota they can use for the folder. • When viewing folders on the Files and Folders page, the folder type (User or System) is displayed in the Quota SRC column. • When opening folders from the Files and Folders page, you can edit the default folder quota that will be selected for users. **Note:** This setting appears only if you turned on the "Create top-level (root) folders" setting on the Collaboration tab in the profile. System quota folders can only be top-level folders.
Folder sharing roles that can be assigned to users in this profile	The roles users can assign when sharing folders with others.
Invitee default folder role	When a user in the Kiteworks Web Application shares a folder with others, the Collaborator role is selected by default. You can choose a different role to be the default selected role. When sharing the folder, the user can assign the default role or select a different role from the list of available roles. See also Collaboration tab.
Share folders and files within "My Folder"	Users can share folders under their "My Folder". If you've been allowing users to share folders under My Folder and you choose to remove this permission, all permissions to access the shared folders will be removed and the users will be notified. Those details are listed in the Activities list so that you can track and respond to the event.
Allow users to leave shared folders	Show or hide the "Leave folder" option in the Members page in the web application. By default, when a folder member no longer wants access to a shared folder they can remove themselves as a member of that folder. To access to the folder again, they need to contact the folder owner or a member assigned the Manager role. To prevent users from removing themselves from a shared folder, you can prevent the option from appearing in the web application. **Exception:** Users who were given access to a shared folder as part of their membership in an LDAP group or mailing list never have the option to leave a folder. LDAP users will need to contact a server administrator to be removed as a member of a shared folder.

Table 12. Collaboration tab settings (continued)

Share individual files	Users can share individual files in a folder without giving access to other files in the folder. Once shared, recipients click the "Shared with me" link in the web application navigation pane to see files that were shared with them.
File sharing roles that can be assigned to users in this profile	Roles users can assign when sharing files with other users. See Collaboration tab.

Roles and permissions for working with folders

Table 13. Roles and permissions for working with folders

	Non-restricted folders	Restricted folders
Manager	All permissions to work with the folder and its files.	All permissions to work with the folder and its files.
Collaborator	Folder permissions: Download the folder, subscribe to folder notifications, view folder members and send them messages, create and delete subfolders. File permissions: Open, upload, download, copy, rename, lock, print, annotate, and delete files. Can also send files, request files, create Office files, edit file expiration dates, and assign file tasks.	Folder permissions: Subscribe to folder notifications, view folder members and send them messages, create subfolders. File permissions: Open, upload, rename, lock and annotate files. Can also request files, create Office files, edit file expiration dates, and assign file tasks.
Downloader	Open files in the internal viewer, download and print files, view file comments, view file and folder activity, and subscribe to folder notifications.	Open files in the internal viewer and print files, view file comments, view file and folder activity, and subscribe to folder notifications.
Viewer	Open files in the internal viewer, subscribe to folder notifications.	Open files in the internal viewer, subscribe to folder notifications.
Uploader	Upload, open, download, delete, and rename files they uploaded to the folder. They can't see files uploaded by other folder members and they can't upload multiple versions of the same file.	Upload, open, and rename files they uploaded to the folder. They can't see files uploaded by other folder members and they can't upload multiple versions of the same file.

Roles and permissions for working with files

Table 14. Roles and permissions for working with shared files

Role	Permissions
Collaborator	Open, edit, download, copy, lock, print, and annotate files. Can also send files, create and edit Office files (only to add a new version), work with files offline, and remove their access to the files.
Viewer	Open files in the internal viewer, remove their own access to the files.

Collaboration settings for restricted users

When viewing the Collaboration tab in a Restricted profile, if you turn off the "Collaboration Allowed" switch to prevent users assigned this profile from collaborating, you will see only the following settings and can specify what to do with their existing data.

- Remote wipe data on the desktop and mobile devices - Delete all Kiteworks folders and files from user mobile devices and synced desktops. Folders and files synced using the Kiteworks Desktop Client application will be deleted during the next scheduled sync cycle.
- Delete all Kiteworks folders and files owned by the selected users, including folders and files that they or other users uploaded to their folders as subfolders.

  Warning: Deleted folders and files can't be recovered.
- Retain all data - Retain all Kiteworks folders and files owned by users. You'll be prompted to transfer ownership to a different user. You can also give the new owner access to folders and files that others shared with the users you are deleting.

Profile Mapping

About profile mapping

The User Profile Mapping has the following features:

- User filters can be created for built-in profiles and custom profiles.
- The LDAP user filter uses the LDAP query syntax to guide user profile mapping assignment per LDAP source for LDAP users. For example, you can filter by specific AD/LDAP Groups: (memberOf=CN=YourGroup,OU=Users,DC=YourDomain,DC=com)
- The user profile that a LDAP user matches first in the top down order at login will be the user profile the user is assigned to unless the user is manually mapped to a user profile.
- The Email Domain filter is for non-LDAP users who will be matched against the email domain. Multiple domains can be specified by comma separation or a regex per user profile to create the query to match non-LDAP users.
- User profiles are ordered and the application administrator can reorder them by dragging and dropping.
- A user profile without a filter means no one will automatically be mapped to the profile but You can manually assign a user to that profile.
- Custom profiles are added to the end of the list on creation by default.
- For non-LDAP users the users that match to the internal domain will be mapped to a "Standard"

profile and the users that do not match to the internal domain will be mapped to a "Restricted" profile. These filters can be updated later by the administrator.

The administrator has the ability to perform SSO Profile Mapping which includes the ability to add usertype attributes to the assertion. You can add usertype as an attribute which will allow the administrator to map users logging in via SSO to a profile, for example, a Standard or Restricted profile.

SSO user profile mapping

For LDAP you can assign specific filters for profile mapping from within the Kiteworks Admin Console.

In the User Profile Mapping page, the Priority of the profile, the ID of the profile and the Profiles (name of the profile) are displayed.

If you need to assign a specific user profile to an SSO user, the SSO administrator needs to make certain the attribute "usertype" is returned to Kiteworks within the assertion that is sent back to Kiteworks from the external identity provider (idP) they are using. The value of this attribute must match the ID of the user profile listed on the User Profile Mapping page. For example, to automatically make an SSO user authenticate as a Standard user if we receive the below data within the assertion form the external idP. Take the ID from the User Profile Mapping page and use that as the value in the assertion (ignore the value of the priority).

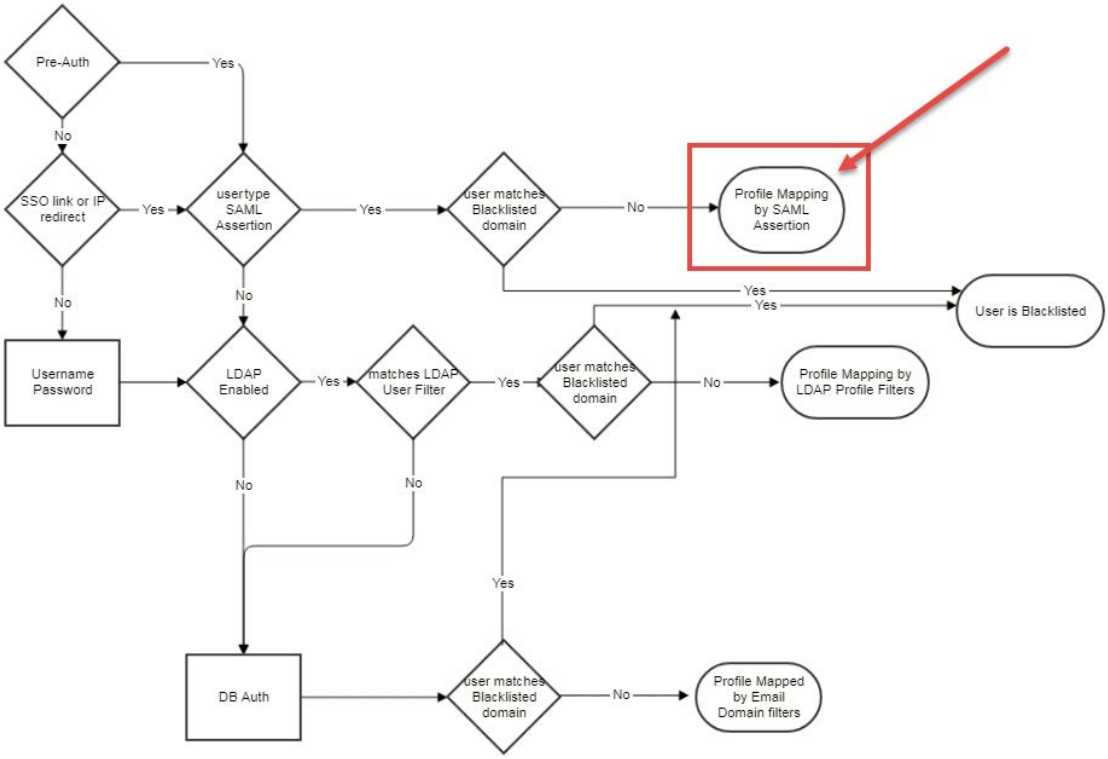
Attribute = usertype

Value = 1

Profile mapping by SAML assertion

If you log in via SSO and if Kiteworks is not connected to the Active Directory, the only way you can do profile mapping is by SAML Assertion, which means when you are using SSO, the SSO server will tell you what profile this user should be mapped to.

Also as an example, if a user logs in via SSO but the usertype is not returned in the SAML assertion. The user is then authenticated via SSO, but user mapping then follows the flow chart to check LDAP then Email Domain mapping.



Notes on profile mapping

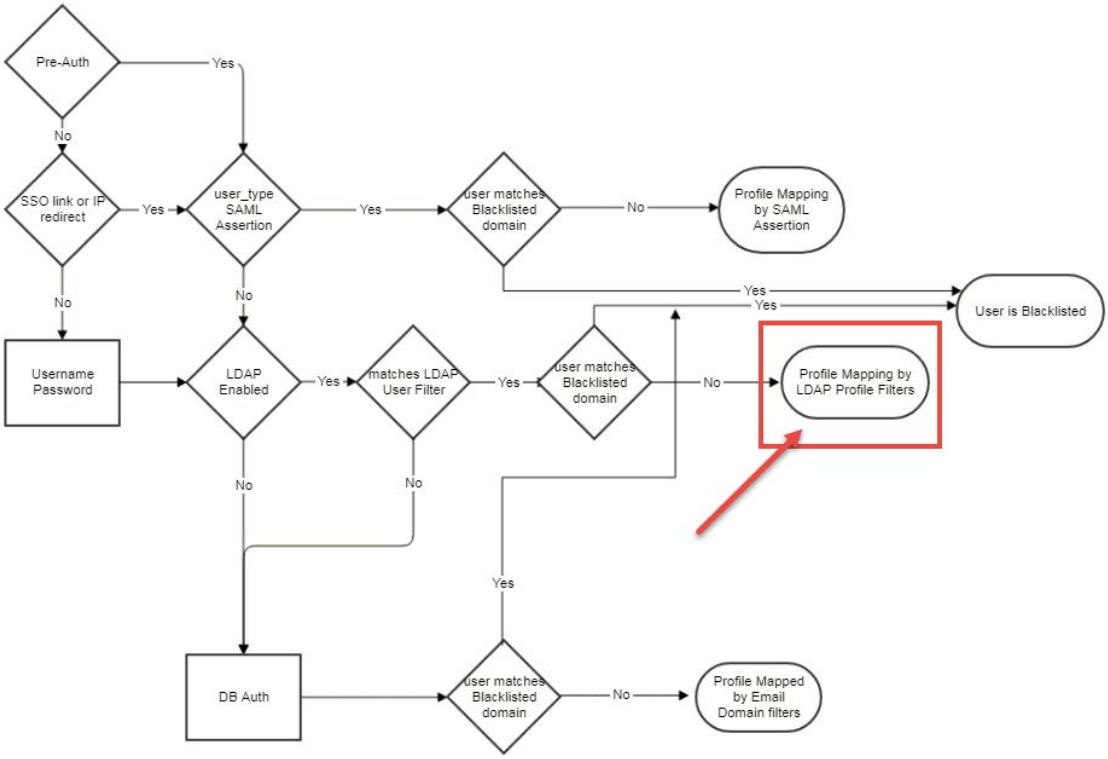
If the SAML assertion contains the "usertype" property then that defines the Profile. This is true for any SAML idP.

If this property is present then it takes precedence over LDAP and LDAP-based profiles are not checked even if they are configured.

If a Kiteworks system is integrated with LDAP, then any user logging in is first checked against the LDAP User filter. If it matches the profile is based on the LDAP profile filter, if not, then the profile is based on Domain-based filters.

If the assertion from SSO defines the profile, then that takes precedence. If not, it falls back to match the LDAP profile and then Domain filters.

If you are integrated with LDAP then you can then you can use this Profile Mapping by LDAP Profile filters.



The basic login works as follows:

- If a user has never logged into Kiteworks and logs in for the first time using SSO, the user should then be registered as an SSO user.
- If the user first logged in as an LDAP user and then connected via SSO they may not be modified.
- If you disable LDAP and then log in with an SSO user that is registered as LDAP this should switch to a SSO user in the admin GUI.

Notes on SSO authentication/authorization and AD/LDAP

The SAML-based SSO supports using any external idP that connects to Kiteworks using a SAML2.0 assertion. Customers may configure the system to use SSO for authentication for all users, or they may allow external users to create a local account on Kiteworks.

User profiles can be mapped via AD filters or via SAML assertion specifying the profile (both are supported for SSO-based login).

Default profiles such as Standard or Restricted are configurable and depend on the settings for these profiles. The settings can be based on AD groups or Domain mapping.

AD groups can be given access to Kiteworks folders. When a user logs in via SSO, AD will be queried for AD group membership and access will be given to folders based on it.

LDAP address book lookups is supported.

Repositories Gateway access via LDAP attribute is supported for homeshares and other Repositories Gateway sources. The user will be prompted to sign into the source.

Self-registration is configurable.

Admin Roles

About administrator roles

Kiteworks supports two types of administrator roles:

- Built-in roles
- Custom roles

Built-in roles are out of box roles that have a fixed set of permissions. These role definitions cannot be modified.

Custom roles can be created based on any of the built-in administrator roles. Granting permissions using custom roles is a two-step process that involves creating a custom role based on an existing role, and then editing its permissions to suit your needs for the role. Once you've created a custom role, you can assign it to a user by editing their user account.

Built-in roles

Built-in role contain a fixed set of permissions.

Table 15. Built-in roles

Role	Description
System Admin	Configure and maintain all aspects of the Kiteworks product, including network configurations and software updates. System administrators are super users with full access to product functionality. **Exception:** Access to the eDiscovery page is available only to administrators assigned the DLI Admin role.
Application Admin	Manage applications in the Kiteworks Admin console. They can also manage all files and folders, licenses, server mappings (locations), Repositories Gateway sources, and end-user accounts.
Helpdesk Admin	Manage end user accounts to perform tasks such as create, unlock, suspend, activate, and delete accounts, reset passwords, revoke active user sessions, remote wipe mobile devices, and enable/disable SFTP keys. Helpdesk Admins can also view some policy and application settings to better understand user capabilities and status, such as profile definitions and storage use. They can also test some configured settings, such as LDAP, two-factor authentication (2FA), and Repositories Gateway source connections to identify potential issues.
DLI Admin (Data Leak Investigator)	Access to the eDiscovery page to generate reports for all activities, emails, and files accessed by specific users. DLI Admins also have limited access to the Kiteworks Admin console to view and download user activity. They also have view-only access to the CISO Dashboard.

Table 15. Built-in roles (continued)

Role	Description
CISO	Access only the CISO Dashboard to monitor all content entering and leaving the enterprise. This global view provides the ability to drill down to individual file transfers and generate detailed compliance reports that provide proof that of full visibility and control over the exchange of sensitive enterprise information. **Note:** GDPR and HIPAA compliance reports are separately licensed offerings with Kiteworks Advanced Governance, which also include anti-virus, data leak prevention, and advanced threat protection (including CheckPoint) and compliance reporting.
Compliance	Access only the Compliance Console to create and apply risk policies for protecting sensitive content as it moves through the system, as well as generate reports for analyzing audit log activity, insider and outsider threat activity, and the CMMC 2.0 compliance of 110 controls across 14 domains.
Policy Manager	Access only the Risk Policy Management page in the Compliance Console to create and apply risk policies for protecting sensitive content as it moves through the system.
Auditor	Access only the Reports Portal page in the Compliance Console to generate reports for analyzing audit log activity, insider and outsider threat activity, and the CMMC 2.0 compliance of 110 controls across 14 domains.
End User	Access the Kiteworks web application and any Kiteworks apps and plugins that have been made available to them.

Create custom roles

You can create custom roles based on the following built-in administrator roles: System Admin, Application Admin, DLI Admin, and Helpdesk Admin. Custom roles based on the CISO role will be supported in a future release.

Before creating custom roles, here are some things to keep in mind:

- Only administrators assigned the built-in System Admin and Application Admin roles can create, edit, and assign custom roles. If you're not assigned one of these roles, the custom roles page will not be accessible.
- You can't base a custom role on a role that is higher than your current level of access. For example, if you're assigned the built-in Application Admin role, you can't create a custom role based on the higher-level System Admin role. You can only create a role based on the Application Admin role or a lower role such as Helpdesk Admin.
- You can assign permissions to a custom role up to your current level of access. For example, if you're assigned the built-in Application Admin role, you can create a custom role based on the Helpdesk Admin role, and then assign that role higher level access up to the application administrator level.

Role: To create and assign custom roles, your role must be the built-in System Admin or Application Admin role.

To create a custom role:

1. Go to Users > Admin Roles.
2. On the Admin Roles tab, click Add Admin Role.

3 On the Add Admin Role page, enter a name for the custom role. You can enter up to 45 characters.
4 Select the role from which to copy permissions, and then click Save.

To edit a custom role:

1 On the Admin Roles tab, click the gear icon below the custom role and then click Edit.
2 On the custom role page, perform any of the following actions:
   - To edit the role name, click the edit icon next to the role name.
   - To edit permissions for the role, expand the options in the left pane to see the pages available to the role, and then select the permissions you want for those pages. Changing access to a parent-level page applies that permission to any child-level pages as well.
3 Click Save.

Assign custom roles to users

To assign a custom role:

1 Go to Users > User Management.
2 On the User Management tab, select the users who you want to assign the role.
3 Click More > Change User Role.
4 Select the new role you want to assign, and then click OK.

   Result: An email notification is sent to the selected users to inform them that their roles were changed to the custom role.

Delete custom roles

Prior to deleting a role, assigned users must be reassigned to different roles. See Assign custom roles to users.

Role: To delete custom roles, your role must be the built-in System Admin role or Application Admin role.

To delete a custom role:

1 Go to Users > Admin Roles.
2 On the Admin Roles tab, click the gear icon below the custom role and then click Delete.

Files and Folders

About file encryption

In Kiteworks version 7.4.1 and later, the following types of user-generated files are encrypted when uploaded to the system:

- Files uploaded to folders
- Files attached to email
- Files replicated across server locations

Other user uploaded files, such as custom user documentation and installers, are excluded from the encryption process.

File encryption when upgrading Kiteworks

If you upgraded from a version prior to Kiteworks version 7.4.1, an encryption migration script runs in background to encrypt existing user-generated files on Storage nodes. For the script to run on a node, the following requirements must be met:

- No active storage migration is in progress.
- There's enough space to encrypt the files.

  As each cycle begins, a check is performed to ensure there's enough space to encrypt the files. If there is less than 100 MB of available disk space, the process stops and an email notification is sent to the server administrator indicating the minimum amount of space required for encrypting the files. Once storage has been added, the encryption process automatically resumes.

If the requirements are met, the script encrypts files in batches of 500 files, and continues to run in the background for each batch until the process completes.

File encryption dashboard alerts

An alert on the dashboard shows the status of the encryption process. It disappears once the process completes.

If there is a problem encrypting one or more files, the files are queued to be retried. If the files can't be encrypted after 50 retries, an alert is displayed on the dashboard indicating the number of files that were not encrypted.

File encryption error handling

Here are some reasons why a file will fail to be encrypted:

- The file is locked - For example, a user is downloading the file at the same time the script is trying to encrypt it. Initially the file is placed in a retry queue, but if retrying does not resolve the issue the encryption of that file will ultimately fail.
- Insufficient disk space - The file is larger than the available amount of disk space. In this instance, the file is placed in a retry queue and a notification is sent to the server administrator to increase the storage space. The script will attempt to encrypt the file in subsequent cycles.

If a file fails to be encrypted, you have the option to retry encrypting the file or deleting the file. Otherwise it remains unencrypted on the system. The alert remains on the dashboard so that you can click it to view the details of the failure.

File encryption event logging

When uploading files to the system, file encryption is automatic and no events are logged in the Activities list. When encrypting files as part of an upgrade or migration, the content migration script runs to encrypt migrated files. Each node checks its own volumes and reports start and end progress to the Activities list. The following events are logged:

- "Background content encryption started on <server_name>"
- "Background content encryption completed on <server_name>. Files Processed/Total: #/#"
- After the files are encrypted, if additional files are migrated to the system, the encryption script restarts and encrypts the newly migrated files. A new "reset" event is logged, along with new start and stop events. The following set of events are logged in the Activities list:
- "Background content encryption reset on <server_name>"
- "Background content encryption started on <server_name>"
- "Background content encryption completed on <server_name>. Files Processed/Total: #/#"

Search for files and folders

You can search for information such as folder and file names, user names, and files and folders that were deleted, quarantined, or locked.

You can filter your search results to view a subset of results. For example, when searching for a user name, your search includes metadata so that all instances of the user name are found, including the list of shared folders accessible by the user.

To search for files and folders:

1. Go to Files and Folders.
2. On the Files and Folders page, type part or all of the folder or file name in the search box. Along with your search term, use the filter options to display a subset of items based on your filter criteria.

   Note: If you apply the Folders filter prior to clicking the Advanced Filter button, the advanced filter options will be limited to options used only for finding folders.

Table 16. Advanced filter options

Category	Description
Folders	Folders created or uploaded by users
Files	Files uploaded by users.
Sent files	Files sent through Kiteworks and stored on the server.
Files in draft	Files attached to draft messages in user inboxes.
Salesforce	Files and folders attached to Salesforce objects, such as Salesforce cases.
Not deleted	Files still in the system

Table 16. Advanced filter options (continued)

Category	Description
Deleted	Files that were deleted from the system, but are recoverable.
Temp files not deleted only	Temporary files that have not been deleted yet, but are unwanted ghost files in the system. For example, if a user composes an email and then attaches a file and deletes it, the file that was attached and deleted is a temporary file and is not deleted until the cleanup occurs on the following day.
Quarantined	Files that are quarantined by the anti-virus policy as possibly being infected or containing malicious information.
DLP locked	Files that are locked by the data leak prevention (DLP) policy as potentially containing sensitive information.
File/folder name	Search by file or folder name.
Members	Find a user according to their access to shared files and folders, their folder ownership, or files they uploaded to the server.

Change file and folder expiration dates

You can change the expiration date of files and folders, or you can set them to never expire. The following rules apply when selecting files and folders:

- At the root level, you can select a single top-level folder to change, or you can select one or more files to change.
- Within a folder, you can select one or more subfolders to change, or you can select one or more files to change.

When you select a folder, you can choose whether to change only its subfolders, only its files, or change of its subfolders and files.

To change file and folder expiration dates:

1. Go to Files and Folders.
2. On the Files and Folders page, select the items you want to change.
   - If you're at the root level, select a top-level folder or select one or more files in the same folder.
   - If you're within a folder, select one or more subfolders, or select one or more files.
3. Click the Update Expiry button.
4. On the Change Expiration Date page, specify the new expiration date you want to apply. If you don't want the items to expire, turn on the Never Expire switch.
5. If you selected a folder, select how you want the changes to apply to its subfolders and files.
   - Folders only - Apply the new date to the folder and its subfolders. Does not change the dates of the files in the folder.
     Exception: File expiration dates can't exceed the expiration dates of the folders in which they are stored. If you shorten the expiration date of a folder and it contains files with later expiration dates, the expiration dates of those files will also be shortened to match the new folder expiration date.

- Files only - Apply the new date to only the files in the folder and it's subfolders. Does not change the date of the folder and subfolder expiration dates.
- Folders and files - Apply the new date to the folder, its subfolders, and all of the files in the folder and subfolders.

Release files from quarantine

If a file is found to be contaminated after an Anti-Virus scan, it is displayed with a red virus icon. If you hover the cursor over the red virus icon Quarantined displays informing you that the file is quarantined.

You can select the quarantined file, and then click the Release from Quarantine icon to release the file.

Check file scan results

Files are scanned when uploaded or downloaded from connected content management systems.

The following three content security integrations are offered:

- DLP
- AV
- Check Point Sandblast ATP (license required)

You can click a file to get more information about its scanning results, such as whether the file was identified as infected, malicious or containing sensitive information (DLP-prohibited), or if it was identified as not-infected, benign, or DLP-passed. Also, whether scanning failed or if the scan was skipped. Scanning results are shown per scanning service.

Release locked DLP files

After DLP scanning any DLP violated file displays with a red lock icon. If you hover the cursor over the red lock icon DLP Locked displays informing you that the file is locked.

You can select the DLP locked file, and then click the Unlock DLP icon to unlock the file.

Recover deleted files and folders

Deleted files are recoverable up to the time specified in the file settings recovery period (the default is 14 days). Deleted files still count in the owner's quota until you permanently deleted them or they are deleted by the system.

Each file is individually encrypted with a unique encryption key. For security purposes, Kiteworks deletes the key and the file from the file system using the standard file deletion protocol.

To recover files and folders:

1. Go to Files and Folders.
2. At the top of the Files and Folders page, click the Advanced Filter button.
3. Configure the filter to narrow the list to the items you want to find, and then click Apply Filter.
4. In the filter results, select the items you want to recover, and then click More > Recover.

   Result: The selected folders and files are recovered and the event is recorded in the audit log.

Clean up storage

To reclaim storage space, each day the system runs a cleanup_expiry script on each server node to remove expired content and stray files. This includes quarantined files older than 90 days. The cleanup process runs at 3:00 AM GMT time. You can schedule a different time for the process to run. You can

also manually start the cleanup process as needed. The process can run while the system is in maintenance mode, unless the system is undergoing a software update. When manually cleaning up storage, the Nginx cache is also cleared to free up space issues that result when large files uploaded from Repositories Gateway sources consume excessive temporary storage.

When you clean up storage, a cleanup script runs a collection of cleanup functions on each node. On the application server, it deletes expired folders and files, and permanently deleted files. If you've enabled secure delete (Security Policies > Files and Folders > Retention tab > Advanced Settings), purged files are deleted securely by overwriting the file encryption keys with random bits. On server nodes, the cleanup script clears the local cache and deletes temporary files.

Before the cleanup script runs, the following prechecks are run on each node. If a precheck fails, the process is not started.

- Cleanup is not already in progress.
- The database is accessible.
- No software updates are in progress.
- The cleanup schedule time is consistent between the database and the local cron file. If different, the value in the local cron file is updated to match the value in the database.

To clean up storage:

You can reschedule the automated cleanup or manually start the process.

- To reschedule cleanup, go to System Setup > Cluster Configuration > System Configuration. In the Storage Cleanup section, enter a new GMT time for the cron job to begin.
  - For hours, enter a value from 0-23.
  - For minutes, enter a value from 0-59.

  When you change the time, a "system_setting_changed" event is tracked in the audit log.
- To clean up storage immediately, click Run Cleanup Now.

  Alternative: You can also manually clean up storage from the Files and Folders page. At the bottom of the page, click Clean Up Storage.

As the cleanup process runs, the overall percent complete for all nodes is shown. To view the percent complete for each node, click Show Progress Log.

When you view the progress log, it shows the details of the cleanup. For example:

- For each cleanup function:
  - How long it took to perform the cleanup.
  - The details of any errors that may have occurred.
- The total time it took to perform cleanup.

Other details are listed for each server node. For example:

- "completed_tasks": 1,
- "total_tasks": 3,
- "completed_percent": 33,
- "failures": 0

Log data is retained for 30 days.

Transfer folder ownership

If you transfer folder ownership to a user who already has a folder with the same name, an index number is appended to the name of the transferred folder. To transfer folder ownership, open the folder, and then in the details pane, click Edit next to the owner name.

You can change the owner of a folder if the folder is not marked as deleted. Click the current owner and type in the name of the new owner. When you change the owner of a folder, the name of the folder changes.

About the LostAndFound folder

Every 7 days a data inconsistency check is performed on the source and destination server nodes to check for inconsistencies between the database records and the disks -- for example, metadata for a user file exists in Kiteworks but the physical file no longer exists in storage. When inconsistencies are found, the data is moved to the LostAndFound folder. Items remain in the folder for 180 days and then are automatically deleted from the system. In addition to running weekly, a data inconsistency check is run whenever you move storage between servers. These are the types of inconsistencies that can be identified and the actions you can take on them.

Table 17. File types in the LostAndFound folder

Type	Description	Possible Causes	Actions You Can Take
Broken link	When a broken link occurs, a 0 byte file is created to fix the link inconsistency. Files that result in broken links are given the "00LOST_" prefix to indicate that they are lost files. Example: "00LOST_<filename>".	A file that was created or uploaded by a user is no longer on the disk, but a link to it remains in the database. A system-generated file is no longer on the disk, but a record of it remains in the database.	View the file metadata. Delete the file. Note that the file is 0 bytes it does not take up space. It will get automatically deleted after 180 days.
Orphan file	Orphaned files are given the "00FOUND_" prefix to indicate that they are found files. Example: "00FOUND_9827_ FwDxe2VRkNN68JXpFnF05i6AAdB1pAW4".	The file is on the disk, but its reference is missing from the database.	Delete the file. It will also get automatically deleted after 180 days.

To access the LostAndFound folder:

1. Go to Files and Folders.
2. On the Files and Folders page, type "lost" in the search box.

   Result: The LostAndFound folder is listed, along with files with the "00LOST_" and "00FOUND_" prefixes. To view all of the lost and found files, click the LostAndFound folder.
3. Here are some things you can do:
   - View the date the file is scheduled to be deleted. The date is listed in the Expiration (GMT) column. To view the number of days remaining, point your mouse to the date to view the tooltip. You can also click the date to set the file to never expires.

- Click the file to view its details. In the file details you can also scan the file.
- Delete the file. Although the file gets automatically deleted after 180 days, you can choose to manually delete the file. Select the file, and then click Delete.

Create and edit forms

Secure Forms in Kiteworks are administrator-driven to create a template which is consumed by the end user mainly to ingest data in a specific format. Once a form is composed, it enables end users to enter data to get sent in a certain format that is useful for processing, archiving, or any other purpose.

In the navigation pane, click Forms. If there are existing forms, a list of existing forms displays on this page with the default view listing the forms sorted by when they were last modified.

Create a form

To create a new form, go to the navigation pane and click Forms. On the Forms page, click the Add Form button. A new form layout displays with standard compose page template fields such as To, cc, bcc, Subject and Message. The layout looks very similar to an email template.

To start building a form, click the "Untitled Form" field and enter a form name. Next, click the New Field button at the bottom of the page to add a new field. Fields such as Text, Radio, Checkbox, Dropdown list, and more are available to add to the form. Fields can be required or read-only.

Forms are WYSIWIG and You can see the preview of the form as it is being built.

You can build the form in stages over a period of time, save the form and make it available later.

Configure form settings

Once the form is built, you can configure it. Forms can be made available in two formats:

- Embedded - An embedded form is available only to Kiteworks users. They display in the Fill Out Form dropdown menu on the Compose page for selection by end-users. This is the default setting. Embedded Forms require authentication by default.
- Standalone - A Standalone form is a link to the form. It can directly be accessed using the form URL. The administrator needs to specify a URL where the end user can directly access the form using the specified URL. Standalone forms have the option to require or not require authentication.

On the form listing page, You can provide the option to copy an existing form to create a new form irrespective of Standalone or Embedded.

If no authentication is set for the form, another form account owner is required. All the files uploaded using the no authenticated form will be under this form owner account quota.

If the form is set as Embedded or Standalone, the end user will see whichever form is set in the form dropdown menu in the web application.

You can choose to assign the form available to only certain user profiles and turn the form on or off for the form status.

Files and Folders

Retention

Set policies for Kiteworks files and folders

To policies for Kiteworks files and folders:

1. Go to Security Policies > Files and Folders > Retention.
2. On the Folder/File Settings tab, edit the settings, and then click Save.

Table 18. Folder/File Settings tab settings

Setting	Description
Allow collaborators to move files	By default, only folder owners and members assigned the Manager role can move files between folders. This setting extends that capability to members assigned the Collaborator role. This setting applies to non-restricted folders only. Users assigned the Collaborator role can never move files from restricted folders.
Allow configure settings per user profile	Select whether to apply the "Folder expiration" and "File expiration" settings globally across all user profiles or through individual user profiles. • To set the folder and file expiration policy at the global level, select "Enable for all user profiles", and then configure the "Folder expiration" and "File expiration" settings on this page. • To set folder and file expiration settings at the profile level, select "Enable per user profile". This removes the "Folder expiration" and "File expiration" settings from this page. To configure these settings, go to Users > Profiles, click the profile you want to edit, and then configure the expiration settings on the Collaboration tab.
Folder expiration	Expire new folders after the number of days specified, following their creation dates. Once folders expire they are deleted from the system. To let folder owners set folder expiration dates, leave the field empty or enter 0. When creating folders in the Kiteworks web application, they can specify expiration dates or set their folders to never expire. Subfolders inherit their folder expiration settings from their top-level folders. Folder expiration email notifications are sent by the system 7 days prior to expiration.
File expiration	Expire new files after the number of days specified, following the dates they were added to folders. Once files expire they are deleted from the system. To let folder owners set file expiration dates, leave the field empty or enter 0.

Table 18. Folder/File Settings tab settings (continued)

Setting	Description
Apply to existing folders and files	Updating the default "Folder expiration" and "File expiration" settings impacts new folders and files added to the system once the policy change takes effect. If you want to apply these expiration settings to existing folders and files as well, click "Apply to existing folders and files" and specify how you want to apply the change. Once applied, an email notification will be sent to the default system notification email address for administrators informing them of the policy change. If the change can't be applied to specific files, the notification includes the file owner names so that they can manually update the expiration dates for those files. An email notification is also sent to file owners informing them of the policy change.
Expiration reminder	Send folder expiration reminders to folder owners and members assigned the Manager role. The default is 7 days. An email notification will be sent after the number of days specified and also one day before the folder expires.
Allow users to extend file expiration	Enable folder owners and folder members assigned the Manager role or Collaborator role to extend expiration dates of files in folders. Once a file has a been assigned an expiration date, it no longer follows the folder's expiration setting. Updating the folder expiration will not have any impact on the files in the folder.
File versioning	The number of file versions that can be stored in folders. The default is 10 versions.
File recovery	The time period in which deleted files are recoverable. The default is 14 days. Recoverable files still count as part of a folder owner's file quota.
Default file added notifications subscription	When a folder owner or members assigned the Manager role shares a folder, automatically subscribe new folder members to receive email notifications when files are uploaded to the folder. Owners and Managers will still be able to turn off this setting when sharing a folder.
Zip folder size limit	The maximum size allowed for users to upload zipped folders. You can specify up to 1.3 GB (due to browser limitations).
Retain folder history after moving	When a user moves a folder, also move the folder's activity history with the folder. Folder activity is viewable by folder owners and members assigned the Manager role or Collaborator role.

Table 18. Folder/File Settings tab settings (continued)

Setting	Description
External scanned folder	The UUID for folders in which files will be locked for processing by external scanners. You can find the folder UUID in two places. • In the URL of the folder. **Example:** https://<server>/#/folder/<UUID> • In the folder link visible in the Kiteworks Web application. The UUID follows "w/f-" in the folder link. **Example:** https://<server_name>/w/f-<UUID> When using a Kiteworks Secure MFT Server to implement an external file-scanning workflow, you must configure one or more folders to be used for initial uploads. When marked as an external scanned folder, files uploaded to this folder will be locked until processed by an external scanner. See Configure external scanning services.
Disable purging of files	Prevent expired and permanently deleted folders and files (including file versions) from being automatically removed from storage disks. The retained folders and files continue to behave as set by expiration dates. For example, folders and files that expire are no longer visible to users. However, they can be retrieved by a user who is assigned the DLI Admin role. **Caution:** Retaining expired and deleted files takes up disk space, even when files are marked as permanently deleted.
Secure delete	When purging deleted files from the system, delete them securely by overwriting the file encryption keys with random bits. Secure delete complies with the NIST SP 800-88 standard for ensuring that purged files are irretrievable. **Exception:** Temporary files held in storage for scanning and generating file previews are not encrypted and won't be securely deleted. However, these files are stored on an encrypted partition.

Set policies for Kiteworks files and folders stored in Salesforce

You can set the retention policy for Kiteworks files and folders stored in Salesforce to specify file and folder expiration dates and whether end users can extend file expiration dates from within Salesforce. The retention policy applies only to new files and folders added in Salesforce.

Access to these settings requires that a Salesforce license (for using the Kiteworks for Salesforce Lightning plugin) be installed on the Kiteworks system.

To set policies for Kiteworks files and folders stored in Salesforce:

1. Go to Security Polices > Files and Folders > Retention > Salesforce Folder/File Settings.
2. Edit the settings, and then click Save.

Table 19. Salesforce Folder/File Settings tab settings

Setting	Description
Folder expiration	Expire new folders after the number of days specified, following their creation dates. Once folders expire they are deleted from the system. To let folder owners set folder expiration dates, leave the field empty or enter 0. When creating folders in the Kiteworks web application, they can specify expiration dates or set their folders to never expire. Subfolders inherit their folder expiration settings from their top-level folders. Folder expiration email notifications are sent by the system 7 days prior to expiration.
File expiration	Expire new files after the number of days specified, following the dates they were added to folders. Once files expire they are deleted from the system. To let folder owners set file expiration dates, leave the field empty or enter 0.
Allow users to extend file expiration	Enable folder owners and folder members assigned the Manager role or Collaborator role to extend expiration dates of files in folders. Once a file has a been assigned an expiration date, it no longer follows the folder's expiration setting. Updating the folder expiration will not have any impact on the files in the folder.

Security Scanning

About security scanning policies

You can configure the system to communicate with multiple ICAP servers so that content is scanned against multiple systems. You also have the option to add additional security scan systems. Three types of scanning services are supported:

- Anti-Virus (AV)
- Data Leak Prevention (DLP)
- Advanced Threat Protection (ATP) - Both CheckPoint and FireEye

AV, CheckPoint, and FireEye perform malware scanning. DLP scans files for content that violates your organization's DLP policies.

Features of multi-CSI

Some of the important features of multi-CSI are:

- The Anti-Virus service is available only if the license is enabled.
- If the Anti-Virus service is disabled, a warning displays only after the last Anti-Virus role is turned off.
- The administrator is not allowed to disable the AV/DLP/ATP role if one of these services is enabled.
- The admin must enable the AV/DLP/ATP role in order to enable the scanning service.
- You cannot delete the Anti-Virus (F-Secure Atlant) protocol, it can only be disabled.
- Only one F-Secure Atlant service can be configured. Read the information below to learn how to configure Kiteworks to AV-scan files in all locations.
- The options displayed in the dropdown menu for Scanning Type are based on the license. Currently only Anti-Virus, Data Loss Prevention and Advanced Threat Protection are available.
- Once a scanning setting is configured, the scanning type and protocol cannot be edited. To change either of these options you would need to delete the scan setting and create a new scan setting.

- Anti-Virus has two protocols: F-Secure Atlant and ICAP.
- DLP has only one protocol: ICAP.
- ATP has two protocols: Check Point Sandblast and ICAP.
- Multi-CSI Location Specific Scanning - You can configure Kiteworks to communicate with multiple ICAP servers so that content is scanned against the closest DLP, AV or ATP server. Based on the location a Kiteworks file is uploaded to, different AV/ATP/DLP scanning rules will apply to the file. For Repositories Gateway files, rules for uploaded files are based on the location of the web node. For downloaded Repositories Gateway files, the rules are based on the location of the Repositories Gateway node which accessed the file.

Multiple scanning services can be configured and turned on. As new files are uploaded to Kiteworks, they are scanned by each scanning service as applicable and the details of the scan results will display on the Manage Folders/Files page. If a file is flagged by one or more security scans, the admin Activity Report indicates which scan flagged the file. If file is flagged as both quarantined and locked, the admin will need to perform both actions, unquarantine and unlock the file.

Configure anti-virus scanning

Add a scanning service

A new security scan can be added for which a name for the connection and the connection to flag as AV or ATP quarantined or flag as DLP locked can be set.

Anti-virus

Kiteworks server uses F-Secure Atlant anti-virus to check incoming and outgoing files. Anti-virus is disabled by default. If you purchased the Anti-virus/DLP license, configure the anti-virus settings in the following ways:

- Enable anti-virus on the servers you want to scan. Go to System Setup > Locations, and then click to expand the server you want to configure. In the roles section, turn on the Anti-virus/DLP role.
- Configure the anti-virus proxy. On the anti-virus server, go to System Setup > Locations, and then click to expand the server you want to configure. On the Proxy Settings tab, configure the anti-virus proxy to specifies a web proxy to be used for anti-virus.

You are notified if the AV license is purchased but AV is not configured on any of the servers. You will be directed to the Locations page to configure the AV role. If AV is configured and not enabled, you will be directed to the page for enabling it.

F-Secure Atlant scanning

Kiteworks supports and follows all the best practices and limitations documented by F-Secure Atlant. For details, refer to the F-Secure Atlant documentation. Some F-Secure Atlant settings can be configured in the Kiteworks Admin Console. Unexposed configurations, such as, archive (.tar, .gz or .zip) scanning, symbolic link is enabled and scanning timeout is 2 minutes. The default is 5 levels deep nested archives (files can be zipped 5 times). All other F-Secure Atlant options are set at the default value.

Set policies to quarantine files

There are 3 policies users can configure to quarantine files:

- Policy for files that are larger than max size - Files will be quarantined if they are too large to be scanned or if they are encrypted.
- Policy for files that could not be scanned - A file can be quarantined if configured, for example, if scanning fails because the scanning service is not reachable.
- For encrypted files, the setting will be applied in the Skip password protected files scanning field. If this option is unchecked, then encrypted files will be quarantined.

Configure anti-virus settings

This section explains the parameters that need to be set for anti-virus.

Table 20. Anti-virus settings

Scanning type	Specifies that this is Anti-Virus security scanning.
Protocol	Specify the protocol used for scanning.
Service name	Set a service name for each type of security scan.
Scan files in Repositories Gateway sources	Select from the following options in the dropdown menu: • Off - Files in Repositories Gateway sources will not be AV scanned. However, files in Kiteworks will still be scanned. • Recommended - All files downloaded from Repositories Gateway sources in the cloud and all files uploaded to Repositories Gateway sources on-premise will be scanned. • Uploads only - Files uploaded to all Repositories Gateway sources (cloud and on-premise) will be scanned. • Downloads only - Files downloaded from all Repositories Gateway sources will be scanned. • Both - Files uploaded to and downloaded from all Repositories Gateway sources will be scanned. **Notes:** • When scanning is enabled there might be delay in downloading/uploading Repositories Gateway files. • Apply Scanning to Repositories Gateway files can be enabled only after adding a Repositories Gateway role on at least one server. • This setting is disabled by default. If you had anti-virus scanning enabled for files stored on Kiteworks it will not automatically scan Repositories Gateway files. You will still need to enable Apply Scanning to Repositories Gateway Files to make sure file uploads to your Repositories Gateway sources are scanned for viruses.

Table 20. Anti-virus settings (continued)

Scan email body	By default, emails containing embedded images are scanned for viruses. If threats are detected, the messages are quarantined. Although scanning the email message body can lead to longer processing times, it's recommended you not change this default setting. If you're concerned about time delays in sending emails, at a minimum choose to scan only if the message contains embedded images.
Maximum file size	The maximum size of files that can be scanned.
Policy for files that are larger than max size	If the file is larger than the maximum file size, it can either be quarantined or allowed to be accessed. • Allow download • Quarantine file
Policy for existing files in Kiteworks	• Allow access - Option to allow users to download, preview and send existing files before they have been AV-scanned. • Scan before access - Prevent downloading of existing files by locking the system until the system confirms the scans are virus free.
Policy for files that could not be scanned	If the system is unable to scan a file, it can either be quarantined or allowed for access. Files larger than the Maximum File Size setting are not affected by this policy. **Note:** To avoid issues connecting to the F-Secure Atlant update server, ensure that ports 80 and 1443 are open (Kiteworks version 7.9 or lower) or port 443 is open (Kiteworks version 7.9.1 or higher). These ports are used to get anti-virus definition updates from the F-Secure update server. The system regularly checks fsupdate.kiteworks.co for anti-virus updates and applies them as soon as they are available. Check your firewall settings to ensure that there are no outbound restrictions for accessing fsupdate.kiteworks.co. You can also allow access through a proxy server.
Scan timeout	The time frame from when the scan request is generated to when the scan result is returned by the scanning service. If scanning large files or sets of files, increase the default value to allow enough time to complete the scan. Insufficient scan time will result in failure. You can monitor scan activity on the Activities page.
Skip password protected file scanning	Skips password protected files so they are not quarantined when they fail the AV scan. If selected, the Status column on the Files and Folders page will display the AV scan result as "non-infected".

Table 20. Anti-virus settings (continued)

Scan depth for archives	When scanning a compressed archive file (such as ZIP or RAR) containing nested archives (embedded folders), specify how many layers of nested folders to open and examine within the archive to check for potential threats. • To scan only the top level of files within the archive, set the scan depth to "1". • To scan files the top level of files and then delve into subfolders within the archive, set the scan depth to "2" or more. **Caution:** If viruses exist on levels exceeding the specified scan depth, those infected files will not be quarantined.
Enable F-Secure debug mode	Enable debug mode so that the Kiteworks technical support can trigger debug mode to assist with troubleshooting.
Notify by email	There are three options to choose from: Off, Send notification to all administrators and Send notification to the specified email address. If this option is selected, specify the email address. If not set to Off, a notification email will be sent to all administrators of the Kiteworks appliance or to a specified email address in the following scenarios: • If a file is found to be malicious or is marked as content-violated by the scanning service. • If a file could not be scanned.
Locations	By default, the scanning service is used for files uploaded to any Kiteworks location. You can choose to instead map this service for some locations and exclude other locations from scanning. This is useful when a scanning service is distant from a given location or if different scanning policies should apply to different locations. **Note:** Location Mapping is only available for ICAP integrations and Check Point Sandblast On-Prem systems. Built-in AV and Check Point sandblast Cloud are mapped to all locations.
IP whitelist uploader	Files uploaded from an IP address range (set of individual IP addresses or set of ranges) in the Whitelist Uploader box will bypass the scan. Leaving this box blank indicates all files will be scanned. You can use a comma as a delimiter for multiple entries.
File type whitelist	This option allows the administrator to specify which types of files should not be scanned. Specify the MIME types that will bypass a scan. For example, to whitelist a gif file, you will need to enter the MIME type: image/gif, image/x-xbitmap, application/pdf, image/jpeg. The MIME type for log files is text/x-log. Leave the field blank to indicate that no filter is used. Use a comma as a delimiter for multiple entries. **Note:** If both IP Whitelist Uploader and File Type Whitelist fields are populated with IP addresses, the IP Whitelist Uploader will take priority and only this scan will be skipped not the File Type. Click Save to save the changes.

Update the anti-virus software

Update anti-virus software to get latest definitions

If AV updates fail for any reason an AV update failure error message displays on the Kiteworks dashboard. You can run an AV update by clicking the Update Anti-Virus Now button to manually trigger AV updates to get the latest definitions.

Once updated a message displays confirming a successful update.

Upgrade anti-virus software

Upgrade the F-Secure anti-virus software to F-Secure Atlant

F-Secure is the anti-virus software used for scanning incoming and outgoing files.

Kiteworks version 7.4 and higher support F-Secure Atlant, a newer version of F-Secure that allows for unlimited file size scanning. When you upgrade to Kiteworks version 7.4 or higher, the F-Secure anti-virus software is automatically upgraded to F-Secure Atlant on all servers with the anti-virus role enabled. To confirm that the update occurred on an anti-virus server, go to System Setup > Locations, and then click to expand the server. In the roles section, open the anti-virus role to verify that F-Secure Atlant is installed.

If there was a problem upgrading the software, you're notified in the following ways:

- An email notification informing you that a new version of the anti-virus software is available to install on the server.
- An alert on the Kiteworks Admin Console dashboard.

From the email notification or the alert you can open the anti-virus role on the corresponding server to upgrade the software yourself.

To upgrade the anti-virus software on the server, ensure that Ports 80 and 1443 are open. These ports are used to get anti-virus definition updates from the F-Secure update server. The system regularly checks fsupdate.kiteworks.co for anti-virus updates and applies them as soon as they are available. Check your firewall settings to ensure that there are no outbound restrictions for accessing fsupdate.kiteworks.co.

To upgrade the F-Secure anti-virus software:

1. Go to System Setup > Locations, and then click to expand the server you want to update.
2. Next to the Anti-virus role, click the arrow, and then click Configure.
3. Click the Upgrade to F-Secure Atlant button.

Upgrade the F-Secure Atlant anti-virus software to use HTTPS

Prior to Kiteworks version 7.9, anti-virus definition updates were retrieved from the F-Secure update server using HTTP. Kiteworks version 7.9.1 and higher support HTTPS for getting anti-virus definition updates securely from the F-Secure update server.

After updating to Kiteworks version 7.9.1, the system automatically upgrades the F-Secure Atlant anti-virus software to use HTTPS. To confirm that the upgrade occurred on an anti-virus server, go to System Setup > Locations, and then click to expand the server. In the roles section, open the anti-virus role to verify that F-Secure Atlant update protocol is using HTTPS.

If there was a problem upgrading the software, you're notified in the following ways:

- An alert on the Kiteworks Admin Console dashboard informing you that the anti-virus software on one or more servers should be upgraded to use HTTPS. From the alert you can open the anti-virus role on the corresponding server to upgrade the software yourself.
- When viewing the anti-virus role status on a server that is still using HTTP, an "Upgrade to HTTPS" button is displayed for you to update the software.
- An alert in the audit log indicating that the upgrade to HTTPS failed.

To upgrade the anti-virus software on the server, ensure that Ports 80, 443, and 1443 are open. Ports 80 and 1443 are used to get anti-virus definition updates from the F-Secure update server. Port 443 is then used to activate F-Secure Atlant using HTTPS. Once activated, ports 80 and 1443 are no longer used.

Exception: If you installed Kiteworks starting with Kiteworks version 7.9.1, only port 443 needs to be open. Kiteworks version 7.9.1 and higher require only port 443 to activate and update the F-Secure Atlant anti-virus software.

Recommendation: The system regularly checks fsupdate.kiteworks.co for anti-virus updates and applies them as soon as they are available. Check your firewall settings to ensure that there are no outbound restrictions for accessing updates from fsupdate.kiteworks.co. You can also allow access through a proxy server.

To upgrade the F-Secure anti-virus software to use HTTPS:

1. Perform one of the following steps:
   - In the admin console, click the alert informing you that the anti-virus software on a server needs to be upgraded to use HTTPS.
   - Go to System Setup > Locations, and then click to expand the server you want to update. Next to the Anti-virus role, click the arrow, and then click Configure.
2. Click the "Upgrade to HTTPS" button.
3. On each server running the anti-virus role, repeat the steps above to upgrade the anti-virus software.

Configure advanced threat protection scanning

CheckPoint Integration - Advanced Threat Protection (License-Enabled)

You can now configure Kiteworks to connect to a CheckPoint SandBlast server to scan files for threats using the local or cloud SandBlast service. Kiteworks can be configured to scan for threats, quarantine failing files and notify the appropriate personnel.

Some CheckPoint features are:

- For files that can't be scanned, quarantine the files or only report them as unable to be scanned.
- The ability to notify the sender and all administrators with specific email address.
- Cloud and local scanning can be done in parallel.
- File size limit is 100MB.
- Only one cloud connection can be configured which is named CheckPoint SandBlast Cloud and if the connection in on-prem, it will be named Sandblast "hostname".

Configure advanced threat protection scanning

To add the advanced threat protection service:

1. Go to Security Policies > Files and Folders > Security Scanning.
2. On the Security Scanning page, click Add to add a new scan service.

3 In the Scanning Type list, select Advanced Threat Protection.

4 Once completed, click Add.

Table 21. ATP settings

Scanning type	Specifies that this is Advanced Threat Protection security scanning.
Protocol	Specify the protocol used for scanning, such as Check Point Sandblast.
Service name	Set a service name for each type of security scan.
Scan files in Repositories Gateway sources	Select from the following options in the dropdown menu: • Off - Files in Repositories Gateway sources will not be AV scanned. However, files in Kiteworks will still be scanned. • Recommended - All files downloaded from Repositories Gateway sources in the cloud and all files uploaded to Repositories Gateway sources on-premise will be scanned. • Uploads only - Files uploaded to all Repositories Gateway sources (cloud and on-premise) will be scanned. • Downloads only - Files downloaded from all Repositories Gateway sources will be scanned. • Both - Files uploaded to and downloaded from all Repositories Gateway sources will be scanned. **Notes:** • When scanning is enabled there might be delay in downloading/uploading Repositories Gateway files. • Apply Scanning to Repositories Gateway files can be enabled only after adding a Repositories Gateway role on at least one server. • This setting is disabled by default. If you had anti-virus scanning enabled for files stored on Kiteworks it will not automatically scan Repositories Gateway files. You will still need to enable Apply Scanning to Repositories Gateway Files to make sure file uploads to your Repositories Gateway sources are scanned for viruses.
Maximum file size	The maximum size of files that can be scanned.
Policy for files that are larger than max size	Specify whether files above the 2 GB scan limit be quarantined or available only for download.
Policy for existing files in Kiteworks	• Allow access - Option to allow users to download, preview and send existing files before they have been AV-scanned. • Scan before access - Prevent downloading of existing files by locking the system until the system confirms the scans are virus free.

Table 21. ATP settings (continued)

Policy for files that could not be scanned	You can specify to either Report only or Lock file for files that could not be scanned by DLP. Files larger than the Maximum File Size setting are not affected by this policy. • Server: CheckPoint Sandblast Local • Server host: Specify the host name for the ATP server. • Server port. Specify the host name for the ATP server. • API version: Specify the API version. The current supported API version is 1.0. • CheckPoint Sandblast Cloud • API key: Specify an API Key.
Notify by email	There are three options to choose from: Off, Send notification to all administrators and Send notification to the specified email address. If this option is selected, specify the email address. If not set to Off, a notification email will be sent to all administrators of the Kiteworks appliance or to a specified email address in the following scenarios: • If a file is found to be malicious or is marked as content-violated by the scanning service. • If a file could not be scanned.
Locations	By default, the scanning service is used for files uploaded to any Kiteworks location. You can choose to instead map this service for some locations and exclude other locations from scanning. This is useful when a scanning service is distant from a given location or if different scanning policies should apply to different locations. **Note:** Location Mapping is only available for ICAP integrations and Check Point Sandblast On-Prem systems. Built-in AV and Check Point sandblast Cloud are mapped to all locations.
IP whitelist uploader	Files uploaded from an IP address range (set of individual IP addresses or set of ranges) in the Whitelist Uploader box will bypass the scan. Leaving this box blank indicates all files will be scanned. You can use a comma as a delimiter for multiple entries.
IP whitelist downloader	Files downloaded from an IP address range (set of individual IP addresses or set of ranges) in the Whitelist Downloader box will bypass the scan. Leaving this box blank indicates all files will be scanned. You can use a comma as a delimiter for multiple entries.
File type whitelist	This option allows the administrator to specify which types of files should not be scanned. For example, if your DLP service is unable to scan image files or PDFs for sensitive information, this section could list those file formats separated by a comma: .pdf, .jpeg The DLP service will skip these files from being scanned. **Note:** If both IP Whitelist Uploader and File Type Whitelist fields are populated with IP addresses, the IP Whitelist Uploader will take priority and only this scan will be skipped not the File Type. Click Save to save the changes. On the Files and Folders page, you can click a file and go to the Content Scanning tab to get more information about its scanning results.

FireEye AX Integration

FireEye is a remote appliance that scans for malware, zero-day, advanced threat protection attacks on files, email attachments, links, and web pages for Kiteworks. This SIEM integration adds another layer of security scanning with features such as:

- Security scanning enabling Kiteworks to submit files to a remote FireEye appliance for detailed analysis.
- Scanning performed on all operating systems
- No file size limit.
- On demand from Kiteworks, the FireEye appliance returns the analysis results which are saved in Kiteworks.

When this feature is enabled, files to be scanned are submitted using REST API to FireEye, where analysis is executed in two modes on virtual machines for various operating systems: Sandboxed Mode for first level of malware detection or Live Mode for deep level scanning including code and links in the file.

FireEye will indicate whether the file is malicious or benign for any operating system. You have the option to specify which operating system to use for analysis.

Note: This feature is available with the purchase of the enterprise package with the Advanced Governance option.

Configure FireEye AX

To add the FireEye AX service:

1. Go to Security Policies > Files and Folders > Security Scanning.
2. On the Security Scanning page, click Add to add a new scan service.
3. In the Scanning Type list, select Advanced Threat Protection.
4. In the Protocol list, select FireEye AX, and then configure the protocol settings.
5. Once completed, click Add.

Table 22. FireEye AX Settings

Setting	Description
Scanning type	The type of security scan you want to perform.
Protocol	The protocol that you want to use for scanning.
Service name	The service name for the type of security scan.
Scan files in Repositories Gateway sources	Select "Off". Files in Repositories Gateway sources are not scanned by FireEye.

Table 22. FireEye AX Settings (continued)

Setting	Description
Scan email message body	By default, emails containing embedded images are scanned for viruses. If threats are detected, the messages are quarantined. Although scanning the email message body can lead to longer processing times, it's recommended you not change this default setting. If you're concerned about time delays in sending emails, at a minimum choose to scan only if the message contains embedded images.
Maximum file size	Specify the maximum size of files that can be scanned.
Policy for files that are larger than max size	Specify whether files above the scan limit should be quarantined or available only for download.
Policy for existing files in Kiteworks	• Allow access - Allow the download, preview, and sending of existing files before they have been scanned by FireEye AX. • Scan before access - Prevent the download of existing files by locking the system until the system confirms that scans are virus free.
Policy for files that could not be scanned	Specify whether to report or quarantine files that can't be scanned by the system. **Exception:** Files exceeding the maximum file size setting are not affected.
Server host	The host name for the FireEye server.
Server port	The port number of the FireEye server.
API username	The user name for API calls to the FireEye server.
API password	The password for API calls to the FireEye server.
Analysis image profile	The guest image profile used for the malware analysis. This image must be installed on the FireEye server. You can enter single entry, or a range of entries separated by commas. Examples: winxp- sp3m, win7-s p1m, win7x64-s p1m, win10x64m, osx-1 0.8. 2, osx-1 0.1 1.3.
Analysis type	• Live: Analyze suspected files live within the AX Series Multi-Vector Virtual Execution (MVX) analysis engine. This process takes more time than the default Sandbox analysis type. • Sandbox: Analyze suspected files in a closed, protected environment.
Notify by email	Specify how to notify administrators of the system when the scan blocks files that are found to be malicious, marked as content violated, or files that could not be scanned.

Table 22. FireEye AX Settings (continued)

Setting	Description
Email address	For the "Notify by email" setting, if you choose to notify a specific administrator when the scan blocks files, enter the email address of the administrator.
Locations	By default, the scanning service is used for files uploaded to any Kiteworks location. You can choose to map this service for some locations and exclude other locations from scanning. This is useful when a scanning service is distant from a given location or if you want different scanning policies to apply to different locations. You can select All Locations or clear the checkbox to select specific locations. If you select Unlisted Locations, this covers all unmapped Kiteworks storage servers (servers not attached to a location), as well as any new locations added after the service has been configured.
IP whitelist uploader	You can specify IP addresses you want to be exempt from file scanning. You can enter a single address, or a range of addresses separated by commas, in the following formats: • Single IP address Example: 192.168.1.1 • IP address with wildcard Example: 192.168.* • Selection by subnet Example: 192.168.100.14/24 • Selection by range Example: 192.168.1.10-192.168.1.25, 192.168.1.10-192.168.1.25/24
File type whitelist	You can specify file types you want to be exempt from file scanning. You can enter a single address, or a range of addresses separated by commas. Examples: .pdf, .jpeg.

Configure FireEye Detection On Demand

To add the FireEye Detection on Demand service:

1. Go to Security Policies > Files and Folders > Security Scanning.
2. On the Security Scanning page, click Add to add a new scan service.
3. In the Scanning Type list, select Advanced Threat Protection.
4. In the Protocol list, select FireEye Detection on Demand, and then configure the protocol settings.
5. Once completed, click Add.

Table 23. FireEye Detection on Demand settings

Setting	Description
Scanning type	The type of security scan you want to perform.
Protocol	The protocol that you want to use for scanning.
Service name	The service name for the type of security scan.
Scan files in Repositories Gateway sources	Select "Off". Files in Repositories Gateway sources are not scanned by FireEye.
Scan email message body	By default, emails containing embedded images are scanned for viruses. If threats are detected, the messages are quarantined. Although scanning the email message body can lead to longer processing times, it's recommended you not change this default setting. If you're concerned about time delays in sending emails, at a minimum choose to scan only if the message contains embedded images.
Maximum file size	Specify the maximum size of files that can be scanned.
Policy for files that are larger than max size	Specify whether files above the scan limit should be quarantined or available only for download.
Policy for existing files in Kiteworks	• Allow access - Allow the download, preview, and sending of existing files before they have been scanned by FireEye Detection on Demand. • Scan before access - Prevent the download of existing files by locking the system until the system confirms that scans are virus free.
Policy for files that could not be scanned	Specify whether to report or quarantine files that can't be scanned by the system. **Exception:** Files exceeding the maximum file size setting are not affected.
API key	Specify the API key for the FireEye server.
Enable FireEye debug mode	Enables debug mode so that Kiteworks technical support can trigger the debug mode when needed.
Notify by email	Specify how to notify administrators of the system when the scan blocks files that are found to be malicious, marked as content violated, or files that could not be scanned.
Email address	For the "Notify by email" setting, if you choose to notify a specific administrator when the scan blocks files, enter the email address of the administrator.
Locations	By default, the scanning service is used for files uploaded to any Kiteworks location.

Table 23. FireEye Detection on Demand settings (continued)

Setting	Description
IP whitelist uploader	You can specify IP addresses you want to be exempt from file scanning. You can enter a single address, or a range of addresses separated by commas, in the following formats: • Single IP address Example: 192.168.1.1 • IP address with wildcard Example: 192.168.* • Selection by subnet Example: 192.168.100.14/24 • Selection by range Example: 192.168.1.10-192.168.1.25, 192.168.1.10-192.168.1.25/24
File type whitelist	You can specify file types you want to be exempt from file scanning. You can enter a single address, or a range of addresses separated by commas. Examples: .pdf, .jpeg.

Configure a proxy for FireEye Detection on Demand

Prerequisite: Configure FireEye Detection on Demand.

To configure a proxy for FireEye Detection on Demand:

1. Go to System Setup > Locations, and then click to expand the server on which to configure the proxy.
2. On the Proxy Settings tab, expand the FireEye on Demand Proxy section.
3. Configure the proxy settings, and then click Save.

Table 24. FireEye Detection on Demand Proxy settings

Setting	Description
Same as Software Update Proxy	Use the same settings as configured for the Software Update Proxy server.
Scanning via proxy server	The server URL or IP address of the FireEye Detection on Demand proxy server that will be used to scan files. If the server requires authentication, enter the user name and password for the server.

Configure data loss prevention scanning

Add a scanning service

A new security scan can be added for which a name for the connection and the connection to flag as AV or ATP quarantined or flag as DLP locked can be set.

DLP Settings (License-Enabled)

When DLP is enabled, Kiteworks can integrate with commercially available DLP content filters that use the industry standard ICAP protocol. Files that are uploaded to a Kiteworks server will be sent in their entirety to an ICAP server for evaluation when a content filter has been configured and enabled. Files will be flagged as allowed or denied by this content filter based on the ICAP server's DLP policy. Users will be allowed or denied the ability to download files from the Kiteworks server/location based on the content filter's DLP policy.

Kiteworks integrates with DLP products from Symantec (Vontu), RSA, Fidelis, Palisades, Websense, and Code Green networks.

When DLP is enabled, it shares a server with the Anti-Virus role.

Enable DLP scanning

To enable DLP scanning:

1. Go to Security Policies > Files and Folders > Security Scanning.
2. On the Security Scanning page, click Add to add a new scan service.
3. In the Scanning Type list, select Data Loss Prevention.
4. Once completed, click Add.

Table 25. DLP settings

Scanning type	Specifies that this is Data Loss Protection security scanning.
Protocol	Specify the protocol used for scanning.
Service name	Set a service name for each type of security scan.

Table 25. DLP settings (continued)

Scan files in Repositories Gateway sources	Select from the following options in the dropdown menu: • Off - Files in Repositories Gateway sources will not be AV scanned. However, files in Kiteworks will still be scanned. • Recommended - All files downloaded from Repositories Gateway sources in the cloud and all files uploaded to Repositories Gateway sources on-premise will be scanned. • Uploads only - Files uploaded to all Repositories Gateway sources (cloud and on-premise) will be scanned. • Downloads only - Files downloaded from all Repositories Gateway sources will be scanned. • Both - Files uploaded to and downloaded from all Repositories Gateway sources will be scanned. **Notes:** • When scanning is enabled there might be delay in downloading/uploading Repositories Gateway files. • Apply Scanning to Repositories Gateway files can be enabled only after adding a Repositories Gateway role on at least one server. • This setting is disabled by default. If you had anti-virus scanning enabled for files stored on Kiteworks it will not automatically scan Repositories Gateway files. You will still need to enable Apply Scanning to Repositories Gateway Files to make sure file uploads to your Repositories Gateway sources are scanned for viruses.
Scan email body	By default, emails containing embedded images are scanned for viruses. If threats are detected, the messages are quarantined. Although scanning the email message body can lead to longer processing times, it's recommended you not change this default setting. If you're concerned about time delays in sending emails, at a minimum choose to scan only if the message contains embedded images.
Maximum file size	The maximum size of files that can be scanned. Policy for files that are larger than max size Specify whether files above the 2 GB scan limit be quarantined or available only for download.
Policy for files that are larger than max size	If the file is larger than the maximum file size, it can either be quarantined or allowed to be accessed. • Allow download • Quarantine file

Table 25. DLP settings (continued)

Policy for files that are marked content violated by DLP	Policy for files that are marked content violated by DLP.
Policy for existing files in Kiteworks	• Allow access - Option to allow users to download, preview and send existing files before they have been AV-scanned. • Scan before access - Prevent downloading of existing files by locking the system until the system confirms the scans are virus free.
Policy for files that could not be scanned	You can specify to either Report only or Lock file for files that could not be scanned by DLP. Files larger than the Maximum File Size setting are not affected by this policy.
Scan timeout	The time frame from when the scan request is generated to when the scan result is returned by the scanning service. If scanning large files or sets of files, increase the default value to allow enough time to complete the scan. Insufficient scan time will result in failure. You can monitor scan activity on the Activities page.
ICAP server host	Enter the ICAP server host.
ICAP server port	Enter the ICAP server port.
ICAP server URI	Obtain ICAP URI from ICAP server.
ICAP method	GET or POST method for content filtering. • GET - The server uses the Response Modification (respmod) mode of the ICAP protocol to communicate with the DLP server. The server sends the file to the DLP server for scanning as part of the HTTP response. • POST - The server uses the Request Modification (reqmod) mode of the ICAP protocol to communicate with the DLP server. The server sends the file to the DLP server for scanning as part of an HTTP request.
Enable ICAP transfer encoding chunked	Click the Enable Transfer Encoding Chunked checkbox to enable it.
ICAP KeyWords	Specify comma-separated list of key words that the Kiteworks server will search for in the ICAP response to indicate that the content violates the DLP policy (for example: violate, fail, disallow, etc.).

Table 25. DLP settings (continued)

ICAP X-Authenticated-User	The X-Authenticated-User is the user who uploaded the file that violated the DLP policy. Format of the authenticated user name sent to the ICAP server. Policy for Files that are Marked Content Violated by DLP and Policy for Files that Could Not be Scanned by ICAP.
Enable ICAP SSL mode	Click this checkbox to enable ICAP SSL Mode.
Enable ICAP debug mode	Click this checkbox to enable ICAP Debug Mode so that Kiteworks technical support can trigger the debug mode easily.
DLP scan for email	Enforce the scanning of file attachments before they get sent to recipients. File attachments are scanned immediately after the user clicks Send. If a scan fails, the file is marked as failed in the user's outbox and the failure is logged in the Activities list. You can also choose to send notify all administrators or specific users after a failure occurs.
Notify by email	There are three options to choose from: Off, Send notification to all administrators and Send notification to the specified email address. If this option is selected, specify the email address. If not set to Off, a notification email will be sent to all administrators of the Kiteworks appliance or to a specified email address in the following scenarios: • If a file is found to be malicious or is marked as content-violated by the scanning service. • If a file could not be scanned.
Locations	By default, the scanning service is used for files uploaded to any Kiteworks location. You can choose to instead map this service for some locations and exclude other locations from scanning. This is useful when a scanning service is distant from a given location or if different scanning policies should apply to different locations. **Note:** Location Mapping is only available for ICAP integrations and Check Point Sandblast On-Prem systems. Built-in AV and Check Point sandblast Cloud are mapped to all locations.
IP whitelist uploader	Files uploaded from an IP address range (set of individual IP addresses or set of ranges) in the Whitelist Uploader box will bypass the scan. Leaving this box blank indicates all files will be scanned. You can use a comma as a delimiter for multiple entries.
IP whitelist downloader	Files downloaded from an IP address range (set of individual IP addresses or set of ranges) in the Whitelist Downloader box will bypass the scan. Leaving this box blank indicates all files will be scanned. You can use a comma as a delimiter for multiple entries.

Table 25. DLP settings (continued)

File type whitelist	This option allows the administrator to specify which types of files should not be scanned. For example, if your DLP service is unable to scan image files or PDFs for sensitive information, this section could list those file formats separated by a comma: .pdf, .jpeg The DLP service will skip these files from being scanned. **Note:** If both IP Whitelist Uploader and File Type Whitelist fields are populated with IP addresses, the IP Whitelist Uploader will take priority and only this scan will be skipped not the File Type.

Kiteworks DLP configuration with the Code Green DLP server

The following configure a Code Green Server:

DLP Server Host: [[DLP server host name or IP]]

DLP Server Port: [[DLP port (typically it is 1344)]]

DLP Server URI: ICAP://[[DLP server host name or IP]]/request

DLP Method: POST

Enable Transfer Encoding Chunked: Yes

DLP KeyWords: Blocked

Kiteworks DLP configuration with the Fidelis DLP server

The following configure a Fidelis Server:

DLP Server Host: [[DLP server host name or IP]]

DLP Server Port: [[DLP port (typically it is 1344)]]

DLP Server URI: ICAP://[[DLP server host name or IP]]/fss-resp

DLP Method: GET

Enable Transfer Encoding Chunked: No

DLP KeyWords: [[Hello,Fail]]

Kiteworks DLP default configuration with the Vontu DLP server

In the default configuration for Vontu, it generates 204 ICAP response code for no violation and 200 for violation. In order for the library to detect a violation, specify 200 as the keyword.

DLP KeyWords: [[200]]

Kiteworks DLP configuration with the Websense Triton DLP server

Websense DLP configuration:

DLP Server Host: [[IP/Hostname of the Data Protector]] (Not the Triton Management Server)

DLP Server Port: [[DLP port (typically it is 1344)]]

DLP Server URI: icap://x.x.x.x/reqmod/http (case sensitive) icap://***IP of Data Protector***/reqmod/http

DLP Method: POST

DLP KeyWords: Leave Blank

X-Authenticated-User: WinNT://<location hostname>/<user name>

Policy for Files that are marked content violated by DLP: Lock File

Policy for Files that could Not be scanned by DLP: Report Only

The policy required to block this data would need to either be a quick "Web DLP Policy" or a custom DLP policy with "Web" as the destination, and Triton would need to be configured to block Web, not just report it. Forcepoint support should have more info if the customer is not aware of how to make certain they have a proper Web policy to "block".

Notes:

- The server URI is case sensitive.
- The DLP Method is POST, not GET.
- Ensure you have a Web DLP Policy properly configured to "block" to work.
- Kiteworks appliance needs to point to the IP address of the Data Protector and not the Triton Management server.

Contact Forcepoint Support if the server is not triggering properly on the Websense/Forcepoint side.

Configure external scanning services

Kiteworks and Kiteworks Secure MFT Server can be combined to create workflows that leverage external scanning services, such as CDR (Content Disarm and Reconstruction) or DLP, to ensure uploaded and downloaded files are processed in a secure fashion according to their status.

For example, a file-upload workflow could be constructed as follows:

- Files are uploaded to a Kiteworks server located in an external segment of your network. When uploaded, files are placed in an External Scanned Folder and immediately locked pending scan results.
- A Secure MFT Server registers the upload and initiates the external scanning workflow. The external scanning workflow can combine multiple scanning services, such as anti-virus and CDR.
  This is in parallel with any scanning done by the Kiteworks server.
- Once scanning is complete, the files can be processed based on their scan results.
  - Clean files can be moved to a location on an internal segment of the network, either a different Kiteworks server or a configured upload server.
  - Quarantined files remain locked, only accessible to a Kiteworks administrator.

A file-download process is much the same, but in reverse and potentially using a DLP scanning service.

- Files are uploaded to a Kiteworks server located in an internal segment of your network. When uploaded, files are placed in an External Scanned Folder and immediately locked pending scan results.
- A Secure MFT Server registers the upload and initiates the external scanning workflow. The external scanning workflow can combine multiple scanning services, such as anti-virus and DLP (Data Leak Prevention) to ensure files are safe and do not contain sensitive data.
- Once scanning is complete, the files can be processed based on their scan results.
  - Clean files can be moved to a location on an external segment of the network, either a different Kiteworks server or a configured server and made available for external download.
  - Quarantined files remain locked, only accessible to a Kiteworks administrator.

The external scanning workflows require the use of specific Secure MFT Server operators as well as the configuration of external scanned folders in Kiteworks.

To create an external scanned folder:

1. Go to Security Policies > Files and Folders > Retention.
2. On the Retention tab, go to Folder/File Settings.

3. In the External Scanned Folder field, enter the UUID for the desired folder. The UUID of a folder can be found in two places:
   - In the URL of the folder - https://<server>/#/folder/<UUID>
   - In the folder link visible in the Kiteworks Web application. The UUID follows "w/f-" in the folder link. - https://<server_name>/w/f-<UUID>
4. To add more than one server, click Add another External Scanned Folder.
5. Click Save when finished adding folders.

Location Replication Rules

Set location replication rules

You can create new rules, update rules, or delete rules.

Location Mapping and Replication rules use pre-defined Server Locations. Server Locations are defined by system administrators. For questions about Server Locations, contact your system administrator.

Note: Location rules are not retroactive. Once you create a rule it will be applied only to those files that are uploaded after the rule was created. The rule will not apply to files that existed before.

Replication states

There are three location replication states:

1. Busy: When the replication starts the status is set to Busy. The system in this state is verifying whether or not it is possible to replicate the files according to the given rule.
2. OK: When the replication rule is verified and the rule is valid.
3. Error: When the replication rule is not valid and thus is not working. This state typically occurs due to connectivity. If the error status displays for a period of time, check connectivity between the locations in your cluster. All nodes need to be able to reach each other over port 443. If connectivity is good, but the error status is still displaying, it is recommended to turn replication off and back on to attempt to resolve the problem.

Add replication rules

Location Replication Rules define which source servers are replicated to target servers.

To set location replication rules:

1. Go to Security Policies > Files and Folders > Location Replication Rules.
2. On the Location Replication Rules tab, click Add.
3. Enter a unique replication name.
4. Select the location source. This is the server that will be replicated to the target location.
5. Select the location target. This server will hold the replicated content.
6. Bidirectional:
   - If checked, files are replicated on both the source and target servers, creating mirror images of each other.
   - If unchecked, replication is unidirectional; the source and target servers may not be mirrored images. The target may have files that are not replicated to the source.

7 Test rule: Checks connectivity between the two locations and checks storage available for executing the rule. The return will tell you if the target has enough space to accommodate the source files.
8 Click OK to save the new rule.

Location Mapping

Configure location mapping

Location mapping ensures that user files are always uploaded to the appropriate location based on system priority – the user's preferred upload location (highest priority), the system default location (if no preference is set), or the closest server based on network latency (lowest priority).

You can set preferred upload locations for non-LDAP and non-SSO users, providing better control over where files are stored to meet compliance requirements or to optimize performance. This provides more predictable file storage behavior and helps ensure data sovereignty requirements are met.

When configuring location mapping at the system level, you can enforce stringent location mapping to route file uploads directly to a specified location instead of routing file uploads through the main host name. Ensure the DNS name is reachable or file uploads will fail.

Notes:

- If location mapping is not being used and is turned on at a later date, location mapping will not apply to existing files.
- At this time, location mapping is implemented for the following Kiteworks applications and plugins:
  - Kiteworks Web Application
  - Kiteworks for One Outlook plugin
  - Kiteworks for Outlook Desktop plugin
  - Kiteworks for Salesforce Lightning plugin
  - Kiteworks mobile apps

To set a user's preferred upload location:

1 Go to Users > User Management.
2 Select the user account, and then click More > Change Location Mapping.
3 Select the preferred location.

To set the system default upload location:

1 Go to Security Policies > Files and Folders > Location Mapping.
2 On the Location Mapping tab, click Add.
3 On the Add Location Mapping page, provide the following information:
  - Match type
  - Location pattern
  - Mapped location - Select the default location for files that will be uploaded, based on LDAP or SSO user profile parameters.
    Note: If an internal user is governed by location mapping rules and a folder is created and shared by an external party, for example, by a Collaborator, the internal user location mapping rules govern if the "request file" feature is used. If the user is added as a Collaborator, location mapping rules will be based on the mapping rules of the Collaborator.
  - Location pattern
  - (Optional) Turn on "Enable stringent location mapping"
4 Click OK.

Mail

Send Mail

Activate or deactivate send mail

The mail options in this section apply to all mail sent via Kiteworks.

To activate or deactivate send mail:

1. Go to Security Policies > Mail.
2. On the Send Mail tab, configure the settings, and then click Save.

Send Mail tab

Table 26. Send Mail tab settings

Mail Options	
Mail delivery	The Mail Delivery field specifies where the mail gets delivered. There are 2 options for mail delivery: • SMTP and Service Inbox • Service Inbox Only If the SMTP and Service Inbox option is selected, the email is sent to SMTP and the Kiteworks inbox. You can retrieve your email from the Kiteworks inbox. If the Service Inbox Only option is selected, the user will not receive the email on the mail client.

Table 26. Send Mail tab settings (continued)

Allow send mail	By default, users can send email and files securely through Kiteworks. You can disable this feature globally or through user profiles. Disabling send mail prevents the Compose button, along with the Inbox, Sent, Draft, Trash, and Outbox folders from appearing to users impacted by the restriction. It also removes menu options for using web client forms, sending files, and requesting files to inboxes. It also removes the ability to search for email-related records. **Exception:** Disabling send mail does not affect users assigned the Recipient user profile. If you want to disable send mail for users with existing mailboxes, keep the following information in mind: • Users with existing mailboxes will see their mail-related features disappear the next time they sign in to the Web client. You can reassure them that their existing mail remains on the server and will be restored if you re-enable the feature again. File attachments expiration rules will continue to take effect. • If you previously allowed users to request files to their inbox, this setting will be automatically disabled in their user profiles as well. When you view their user profile settings, you'll see that the "Request to inbox" section was removed from the Request File tab. • If other users send email to those users whose send mail access was removed, the senders will receive a message stating that the user mailboxes are no longer available.
Include notification/alert emails in inbox	Send system notifications and alerts to user inboxes in the Kiteworks Web Application. System notifications are stored indefinitely and can take up disk space in the database. To manage this space, you can also implement a policy that periodically deletes system notification emails from user inboxes. To set this policy, also enable the Lifetime of Notification/Alert Emails check box.
Apply link expiration to message	When email links expire, delete the email messages and attachments from user inboxes and Sent folders. If the Data Leak Investigator (DLI) role is enabled on the server, expired emails are permanently deleted, but not purged from the database. If DLI is not enabled on the server, expired emails are deleted permanently and purged from the database. When you select the "Apply Link Expiration to Message", you can also have the system send email notifications to users when messages expire.

Table 26. Send Mail tab settings (continued)

Lifetime of the notification/alerts emails	The number of days after which system notification emails get automatically deleted from user inboxes in the Kiteworks Web Application. If the Data Leak Investigator (DLI) role is enabled on the server, system notification emails are permanently deleted, but not purged from the database. If DLI is not enabled on the server, emails are deleted permanently and purged from the database.
Inline image display	Specify whether to automatically display inline images in messages sent to users. You can set this behavior at the global level to apply to all users, or set it up in individual user profiles. In a user profile, you set this behavior on the Account tab.
Mail connector	The Mail Connector setting is available when: • A Secure MFT Server is registered as a remote satellite on the Kiteworks server. • The Kiteworks Mailbox Connector license is activated on the server. To view installed licenses, see View and upload licenses. The Kiteworks Mailbox Connector license is listed in the Features section. The mail connector enables an MFT satellite server to use "Kiteworks Archived Mail" SMTP operators to download emails and attachments from the Kiteworks server, and then pass them to other operators such as generic scanner, file upload, or mail archival services. • Disabled - The default setting. • Enabled for all users - Allow the MFT server to access all user emails on the Kiteworks server. If you selected "Enabled for all users", in the Accounts with Access box, enter the email addresses of the recipients you want to give access to the archived emails. Separate multiple addresses with commas or new lines. **Requirements:** Recipients must have accounts on the Kiteworks server, and be assigned one of the following roles: System Admin, Application Admin, or DLI Admin. • Configurable per user profile - Allow the server to access user emails only in specified user profiles. User profile settings take precedence over global settings. If you select this option, you also need to enable it in the user profile. For each profile you want to access, go to Users > Profiles > *select the profile* > Send File > select the "Mail Connector" check box. **Exception:** Not applicable to Recipient profiles.

Table 26. Send Mail tab settings (continued)

Send preview option	When users file previews, specify how the files get sent. View-only and DRM protected files can be viewed only in the secure Kiteworks viewer. **Requirement:** The file preview feature must be enabled on the server. See Enable users to preview files using the Kiteworks Web Application. • View-only link - Send only a link to the file. The file is not sent as a file attachment and it can't be downloaded. View-only files can be viewed by authorized and unauthorized users. This is the default setting. • DRM protected file - Send a DRM protected file as a file attachment in the email message. DRM controls ensure that only authorized recipients can view the files, while preventing them from copying, printing, or modifying the files in any way. They can open the files directly from their email messages and also download links to the files for use later on. To view the files, they must sign in to the server.
External Distribution Lists	
Mark addresses as external distribution lists	While composing messages, allow senders to mark email addresses as external distribution lists. Users who send messages to these email addresses will send them to the associated distribution lists. • Disabled - The default setting. • Enabled for all users - Allow this option to all users globally across servers. • Configurable per user profile - User profile settings take precedence over global settings. If you allow this option, you also need to enable it in the user profile. Go to Users > Profiles > *select the profile* > Send Files > "Mark Addresses as External Distribution Lists".
Exclude domains	Email domains you want to block from being used as external distribution lists. Separate multiple domains with commas or new lines. Regular expressions are supported. If you add a domain that is already associated with an external distribution list, those lists will no longer be marked as distribution lists. In the future, if you want these addresses to be distribution lists again, you'll need to unblock the domains and have someone mark the addresses as distribution lists again. **Note:** You can also mark an email address as an external distribution list by editing the user's account. Go to Users > User Management > *click a user account* > "External Distribution List".
Send Options	
Draft attachment expiration	When "Enabled per user profile", the admin can configure the "Draft Attachment Expiration" for all user profiles between 0 (never expires) and 999 days.
Send quota	This option enables managing storage for better usage. Check the checkbox for no limit on send storage.

Request file tab

In the Storage location of uploaded files list, specify whether files requested to user inboxes or folders get uploaded to the storage location associated with the requestor's user account or the uploader's user account. Users specify their default storage location in their account settings in the Kiteworks Web Application.

When files are uploaded by an unauthenticated user, the system will try to get the location from the uploader's browser. If it can't detect the location, the location of the requestor will be used.

Request File

Set the storage location files uploaded on request

To set the storage location for files uploaded on request:

1. Go to Security Policies Mail.
2. In the "Storage location of uploaded files" list, specify whether files requested to user inboxes or folders get uploaded to the storage location associated with the requestor's user account or the uploader's user account. Users specify their default storage location in their account settings in the Kiteworks Web Application. When files are uploaded by an unauthenticated user, the system will try to get the location from the uploader's browser. If it can't detect the location, the location of the requestor will be used.

Sign In

User Security

Set user authentication policies

The User Policies page allows you to set security and password policies. Set the parameters for your users that fit with your company's security protocols. You can also configure the general profile setting from this screen.

To set the user authentication policy:

1. Go to Security Policies > Sign In > User Security.
2. On the User Security tab, configure the settings, and then click Save.

Table 27. User Security tab settings

Internal user domain filter	Filter to specify internal user domains (for example, YourCompany.com and YourClientsCompany.com). You can enter more than one domain separated by a comma. To map users to a specific user profile either use the LDAP Mapping Filter or Email Domain Filter under the appropriate user profile in the User Profile Mapping page.

Table 27. User Security tab settings (continued)

Blacklist domain filter	You can blacklist or whitelist sharing with any email domain. For domains that allow sharing, external users can be automatically provisioned to a specific user profile, rather than the default "Restricted" profile. Once a blacklist domain filter is set it works globally and only applies to new users. These users can no longer be invited to use the system by other end users. Any attempt to send a file or share a folder with a Blacklisted Domain email ID will be rejected. However, any existing user accounts that match the blacklisted domain will continue to work unless searched for and deleted manually from Kiteworks. Additionally, the administrator is still allowed to add a new user that matches the blacklisted domain. If you need to manually add a user from a blacklisted domain, an error message displays if automatic profile mapping is done. Manually match the user to the appropriate profile to add the user. There are 2 aspects of the blacklisting function: • You can blacklist domains by specifying email addresses that will be blacklisted in the Blacklisted Domain Filter field in the General User Settings page in the General Profile Settings tab. • The Domain Filter in the Email Domain field under User Profile Mapping may also be used to map users to different profiles based on the domain. Users for the internal domain will be mapped to a Standard user profile and external users would be set to map to a Restricted user profile. This allows the administrator to adjust the filters to map domains to specific user profiles. Like LDAP mapping, users map to the first profile in the ordered list. If a user maps to no profile, they fall out and are not assigned a profile and cannot sign in. **Note:** For most users, the Restricted user profile is a catch-all that users map to, but if the administrator makes this more restrictive, there is a possibility that a new user will not map to any domain. In such a situation, Kiteworks does not create an account for that user. Regular expressions can be used in the Domain Filter in the Email Domain field under User Profile Mapping to assign a specific profile to a user. Regular expression or regex is a special text string for describing a search pattern. Multiple blacklisted domains can be separated by commas or regular expressions. **Notes:** • If the LDAP protocol is integrated in the system, it will take precedence over Email Domain Mapping. LDAP users will map against the LDAP filter not the Email Domain Mapping filter. • In addition, if an account already exists or was created by the administrator, the user will be able to sign into Kiteworks (or reset password, etc.), even though the user has a blacklisted email domain.

Table 27. User Security tab settings (continued)

Require activation code for external accounts	• A second form of authentication is required when new external users are being invited to the platform. The default status is off. • This activation code has the following features: • The default length of the activation code is 8 alphanumeric, all uppercase characters. It expires 120 hours after creation. • External users cannot invite new users. • The sender and the recipient must connect via other forms to pass to receive an activation code, for example, a phone call. • A sender can continue to send emails and invite users to a folder. • When a new external user is activating an account, a unique activation code is sent to the sender via email. This will be unique for each sender. • During account creation/activation, the new user will need to enter the activation code before completing the process. • Access is not permitted without the activation code. You will have request for the activation code before entering the password.
Self-registration	When set to Enable, a URL is displayed on the portal to allow a new user to self-register. Set to Disable to disallow self-registration. Check this option to disable self-registration.
Restrict only to emails matching domain filter	When set to Enable, self-registration is limited to emails matching the Domain Filter in the Email Domain section under User Profile Mapping.
Session timeout	Specify the time (in hours) when a user's web session will time out due to inactivity.
Max. login attempts	Set the maximum number of unsuccessful login attempts before the account will be locked.
Account locked period	Specify how long the account will be locked after the maximum number of unsuccessful login attempts has been reached. Minimum is one minute.
Verification link expiration	Specify the expiration date for the verification link. The Verification Link is sent to verify the email address of new users (non-LDAP).

Table 27. User Security tab settings (continued)

Enable CAPTCHA	A users will see a CAPTCHA when they • Change their account password. • Sign in after a second failed sign-in attempt. • Self-register to create a new user account. An LDAP user will receive an email to sign in using their LDAP password. • Sign in for the first time to access a Kiteworks folder that was shared with them through email or a folder link. As part of the account creation process, prior to creating a password they will need to complete the CAPTCHA to register their new account.
Enable checking for consistent IP address	When checked, this option enables the checking for IP address matching. A user's IP address will be checked and verified to match the current session. It is recommended to disable it if you are experiencing any issues when Location Proximity is enabled and a user's IP address gets recognized differently by different Kiteworks servers or in cases where the client IP address changes within a session.
Enable Checking for Consistent IP Address	Allows users to sign in to the Kiteworks Web application across multiple browsers using the same credentials. If you want to prevent concurrent sign-ins, turn off this setting. Users with concurrent sessions will see their older sessions end, retaining only their most recent session. If they try to create a concurrent session again, the sign-in page will display a message informing them that they already have another session in progress. They can choose to end the older session and proceed, or cancel their attempt to create another session.
Geo IP fencing	For increased security, you can allow or block IP addresses from accessing the system by IP addresses, such as IPs located in high-risk or prohibited regions or countries. You can block IPs at the user account level, through user profiles, and global to apply to all users who try to access the system.

Geo Fencing

Allow or block domains

To allow or block domains:

1. Go to Security Policies > Sign In > User Security.
2. On the User Security tab, allow or block domains as needed, and then click Save.

Table 28. Geo IP fencing settings

Setting	Description
Internal user domain filter	Filter to specify internal user domains (for example, YourCompany.com and YourClientsCompany.com). You can enter more than one domain separated by a comma. To map users to a specific user profile either use the LDAP Mapping Filter or Email Domain Filter under the appropriate user profile in the User Profile Mapping page.
Blacklist domain filter	You can blacklist or whitelist sharing with any email domain. For domains that allow sharing, external users can be automatically provisioned to a specific user profile, rather than the default "Restricted" profile. Once a blacklist domain filter is set it works globally and only applies to new users. These users can no longer be invited to use the system by other end users. Any attempt to send a file or share a folder with a Blacklisted Domain email ID will be rejected. However, any existing user accounts that match the blacklisted domain will continue to work unless searched for and deleted manually from Kiteworks. Additionally, the administrator is still allowed to add a new user that matches the blacklisted domain. If you need to manually add a user from a blacklisted domain, an error message displays if automatic profile mapping is done. Manually match the user to the appropriate profile to add the user. There are 2 aspects of the blacklisting function: • You can blacklist domains by specifying email addresses that will be blacklisted. • The Domain Filter in the Email Domain field under User Profile Mapping may also be used to map users to different profiles based on the domain. Users for the internal domain will be mapped to a Standard user profile and external users would be set to map to a Restricted user profile. This allows the administrator to adjust the filters to map domains to specific user profiles. Like LDAP mapping, users map to the first profile in the ordered list. If a user maps to no profile, they fall out and are not assigned a profile and cannot sign in. **Note:** For most users, the Restricted user profile is a catch-all that users map to, but if the administrator makes this more restrictive, there is a possibility that a new user will not map to any domain. In such a situation, Kiteworks does not create an account for that user. Regular expressions can be used in the Domain Filter in the Email Domain field under User Profile Mapping to assign a specific profile to a user. Regular expression or regex is a special text string for describing a search pattern. Multiple blacklisted domains can be separated by commas or regular expressions. **Notes:** • If the LDAP protocol is integrated in the system, it will take precedence over Email Domain Mapping. LDAP users will map against the LDAP filter not the Email Domain Mapping filter. • In addition, if an account already exists or was created by the administrator, the user will be able to sign into Kiteworks (or reset password, etc.), even though the user has a blacklisted email domain.

Allow or block IP addresses

For increased security, you can allow or block IP addresses from accessing the system by IP addresses, such as IPs located in high-risk or prohibited regions or countries. You can block IPs at the user account

level, through user profiles, and global to apply to all users who try to access the system.

You can block a specific IP address, a range of IP addresses, or entire countries from accessing the server. Anytime someone tries to connect to the server using a blocked IP address, those details are listed in the Activities list so that you can track and respond to the event.

Geofencing rules applied through user accounts or user profiles take precedence over global policies. For example, if you allow a set of user accounts to access the system using a specific IP address, but you block that IP address as a global policy, those users will still be allowed to sign in from the IP address. All other users will be blocked.

Each time an authenticated user tries to sign in to the system, the system checks to allow or block their IP address in the following sequence. If the first check passes, it proceeds to the next check in the sequence and continues until their IP is blocked or allowed to pass all checkpoints.

- Check #1 - The user account's allowed IP address list.
- Check #2 - The user account's blocked IP address and blocked countries list.
- Check #3 - The user account's user profile allowed IP address list.
- Check #4 - The user account's user profile blocked IP address and blocked countries list.
- Check #5 - The global user policy allowed IP address list.
- Check #6 - The global user policy blocked IP address and blocked countries list.

When unauthenticated users try to access the system, here's how their IP addresses are checked:

- When an unauthenticated user tries to create a user account, the user profile that you automatically assign to new accounts is used to determine whether the user's IP address is allowed or blocked.
- When an unauthenticated user tries to upload files requested by another user or download files sent by a user, the unauthenticated user's IP address is checked against only the global allow and block lists.

Role: To allow or block IP addresses, your role must be System Admin, Application Admin, or DLI Admin.

To allow or block IP addresses:

1. Access how you want to allow or block IP addresses.
   - To allow or block IPs at the global level, click Security Policies > Sign in > Geo Fencing.
   - To allow or block IPs at the user profile level, click Users > Profiles, and then click the profile you want to edit.
   - To allow or block IPs for an individual user account, go to Users > User Management and then click the user account you want to edit. On the Security Policy tab, allow or block IPs as needed.
2. Configure Geo IP Fencing settings according to your security policy.

Table 29. Geo IP fencing settings

Setting	Description
Blocked IP addresses	IP addresses you want to block from accessing the server. Enter a single address or a range of addresses separated by commas in the following formats: • Single IP address **Example:** 192.168.1.1 • IP address with wildcard **Example:** 192.168.* • Selection by subnet **Example:** 192.168.100.14/24 • Selection by range **Example:** 192.168.1.10-192.168.1.25/24 • IPv6 format **Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Blocked countries	Countries you want to block from accessing the server. Start typing to see a list of names. **Note:** Kiteworks uses the IP2Location IP Address Geolocation Database to determine the approximate geographic location of an IP address and can't guarantee that the data in this geolocation database is always up-to-date.
Error message for blocked access (global setting only)	A custom message you want users to see when their IP address is blocked. The default message is "Your access is denied." **Note:** The custom message can be set only at the global level.
Allowed IP addresses	IP addresses you want to have access to the server. The allowed list is dependent on the blocked list. For example, if you block a range of IP addresses using a wildcard (such as 192.168.*), you can specify that specific addresses within that range are allowed access to the server (such as 192.168.1.1 and 192.168.1.2). However, if you don't block any addresses but you enter some allowed IP addresses, all addresses will still be allowed to access the server. Entering addresses in only the allowed list does not block all other addresses from accessing the server.

Search user accounts for allowed or blocked IP addresses

You can quickly find an IP addresses that has been allowed or blocked in a specific user account. In the Manager Users list, enter the IP address in the search box. To search for multiple addresses, use quotations. For example: "192.168.1.1", "192.168.1.2".

Password Policy

Set the password policy

You can enforce the use of strong passwords through an appropriate password policy.

To set the password policy:

1. Go to Security Policies > Sign In.
2. On the Password Policy tab, set the password complexity, expiration, history, and autofill rules, and then click Save.

Table 30. Password policy settings

Setting	Description
Minimum	Set the password complexity requirements. • Characters - Set the least number of characters that can make up a password for a user account. You can set a minimum value of 2 characters. • Numeric characters - Set the number of numeric characters that must be in the password. Specify a value from 0 through 9. • Uppercase alphabet characters - Set the number of uppercase letters (A through Z) that must be in the password. • Special characters - Set the number of non-alphanumeric characters (special characters) that must be in the password. • Lowercase alphabet letters - Set the number of lowercase letters (a through z) that must be in the password.
Password expiration	Set the period of time (in days) that a password can be used before the system requires the user to change it. To specify that passwords never expire, set the number of days to 0.
Password history	Set the number of unique new passwords that must be associated with a user account before an old password can be reused. Specify a value from 1 through 25. **Best practice:** Set the password history to 25. This will help mitigate vulnerabilities that are caused by password reuse. Specifying a low number allows users to continually use the same small number of passwords repeatedly.
Auto fill user name	Set whether browsers are allowed to fill in user names automatically based on previously entered user names. **Best practice:** To minimize security risk, auto fill should not be allowed.
Auto fill password	Set whether browsers are allowed to fill in passwords automatically based on previously entered passwords. **Best practice:** To minimize security risk, auto fill should not be allowed.

Terms of Service

Enforce terms of service

The Terms of Service feature enables you to present information that end users must review and accept prior to accessing content in the system. You can enforce terms of service globally across all user profiles or through individual user profiles. Once you enable the terms of service, you can specify how often end users must review and accept the terms. The terms can be displayed the first time users sign in, each time they sign in, or at intervals according to a specific number of days.

The terms of service page displays after end users authenticate and must be accepted in order to access the system. It does not display to administrators when signing in to the admin console.

Recommendation: If you want to provide custom terms of service through individual user profiles, first configure the messaging at the global level. When configuring a profile, you can then choose to use the default terms of service or customize it specifically for that profile.

To configure terms of service globally across all user profiles:

1. Go to Security Policies > Sign in > Terms of Service.
2. Configure the settings, and then click Save.

To configure terms of service through individual user profiles:

1. Go to Users > Profiles, and then click the profile you want to edit.
2. On the Account tab, in the Enable Terms of Service list, select one of the following options:
   - Use settings from general profile section - Applies the settings you configured at the global level.
   - Use the following settings - Enables you to customize the settings for the profile as needed.
3. Click Save.

Table 31. Terms of service settings

Setting	Description
Terms of service	Select one of the following options: • To enforce the settings across all user profiles, select "Enabled for all users". • To enforce the settings through individual user profiles, select "Enabled per user profile".
Occurrence	How often you want users to review and accept the terms of service. To specify a specific number of days, select Custom.
General terms of service	Select one of the following options: • Use text below - Provide custom terms of service text to display to users. You can enter up to 10,000 characters and use these HTML tags to format the text: <b>, <i>, <u>, <a>, , <sup>, <sub>, . • Use URL - Enter a URL to a terms of service page located on your organization's website. The URL will display on the sign in page so that users can click on it to open and review the terms. Then they can return to the sign in page to accept the terms.
Acceptance text	Additional text you want to displayed at the bottom of the terms of service, such as "I have read and accept the terms of service". A checkbox is inserted before the text for users to select in order to accept the terms.

Risky Settings

Monitor and resolve risky settings

Each time the Kiteworks server is updated, the system checks to see if settings in the Kiteworks and Email Protection Gateway (EPG) consoles are configured in a way that may be risky. If risky settings are detected, you are alerted in multiple ways so that you can confirm the settings or update them to strengthen the security of the system.

- After a software update, a page displays to alert you that risky settings have been detected. From this page, you can go to the security settings to confirm or update them. If you close this page without confirming or updating settings, a "Security settings need attention" alert displays at the top of the console for accessing the risky settings page again. The alert continues to display every time you sign in to the console until you or another administrator confirms or updates the settings.
- An alert symbol displays next to the Security Policies menu. Expand this menu and click Risky Settings to view an aggregate of risky settings on the system to confirm or update them. Settings that have not yet been verified are indicated by an alert symbol. Settings that were previously reviewed and verified are also listed so that you can updated them needed. To go to a setting, click the setting row. The Risky Settings menu is always available for accessing settings that you may want to review periodically to ensure the security of the system.

At any time you can also review the states of all potentially risky settings in the console and update them if needed. Changes or confirmations of security settings are tracked in the Kiteworks and EPG audit logs. On the navigation menu, go to Activity and Reports > Activity Log.

Role: To access the Risky Settings menu, your role must be the built-in System Admin or Application Admin role.

To review potentially risky settings:

1. Go to Security Policies > Risky Settings.
2. To change a setting, click on the setting, make and then confirm your changes.

Configuration

Kiteworks

Customize Kiteworks settings

The Kiteworks page enables you to configure general settings for your Kiteworks deployment.

Kiteworks settings

Table 32. Kiteworks settings

Application URL	Enter the URL that will be used by end-users or administrators to access Kiteworks. An alert is displayed if the Application URL does not match the SSL certificate. This enforces SSL certificate checks for calls within the Kiteworks cluster. This security measure is switched on only if the system has a wild card SSL certificate. **Note:** The DNS must be in place for the server with a Web role, and a valid SSL certificate must be uploaded for the chosen hostname.
Service name	Specify the Kiteworks service name that is displayed on the browser title bar and in the notification emails sent by Kiteworks.
Landing page	Set the Kiteworks Landing Page for first time users. You can select from the following 3 options: • All Files/Kiteworks Files **Note:** If this setting is selected, Kiteworks files will be loaded as 'All files' on mobile applications • Secure Mail (Inbox) • Secure Mail (Compose)
Home logo URL	Specify a custom URL for the logo displayed on the Kiteworks Web Application home page. For example, you can set the URL to your company website for end users. If you don't specify a custom URL, the Application URL you specified on this page is the default URL.
Default country code	The Default Country Code setting for SMS.
Support email	The email address you want to display on the Help screen for end-users to request administrator support.

Table 32. Kiteworks settings (continued)

Notification email	Email credentials for sending system alerts and notifications to administrators, such as the availability of software updates, storage usage alerts, system communication issues, virus detection and quarantined files, and so on. • For the display name, the name or email address from whom the email notification to administrators will be sent. • The email address you want to send email notifications to administrators.
From address for notification email	Email credentials for sending system-generated emails to administrators and users, for example registration and password reset emails. • For the display name, the name or email address from whom the email notification will be sent. • The email address which all system-generated emails to administrators and users will be sent, for example registration and password reset emails.
Use from address on behalf of	This should be enabled, if the mail relay is setup to forward emails only from a specific email ID. You can select from the following 3 options: • None • All end users • External users If you enable using the notification email ID as the sender ID only for external senders, it avoids email spoofing warning for external users whose domains cannot be whitelisted on the email relay used by the Kiteworks system.
CORS hostnames	CORS (Cross-Origin Resource Sharing) allows specified domains to access Kiteworks resources from within the context of a web page outside the Kiteworks-configured domain. The administrator must specify the domains allowed that can request Kiteworks resources. The users' browser must also support CORS for allowed sites to request resources via the users' browser. Without the specified domain, the browsers same-origin security policy would prevent access to the Kiteworks resources.

General authentication settings

Table 33. General authentication settings

Username descriptor	Specifies a descriptor that will be displayed above the username field on the login page. If left blank, the default is "Username or email".
Password descriptor	You can customize the description for the Password field on the Sign In page, for example, "Use your SSO Password." Default is "Password."
Change password URL	Enter the URL that LDAP users must use to change their passwords. This URL will be sent by email when a user clicks the Forgot Password link.

Administration UI IP restriction settings

Table 34. Administration UI IP restriction settings

Include IP	Specify IP address(es) or IP address ranges from which You can sign in as administrator. Leave this blank for no restrictions. Separate IP addresses with commas.

Alerts and notifications settings

Specify when system-level alerts and notifications are sent to administrators assigned the System Admin role for when the number of licenses are running low and the number of days at which to email license expiration notifications.

Table 35. Alert and notifications settings

Low license alert	Send an alert when the number of user licenses falls below the percentage of available user licenses. The default and recommended setting is 10%. Maximum is 100%.
License expiry alert	Send an alert when the Kiteworks license expiration threshold is within the set number of days. The default is 5 days. The recommended number is either 60 or 90 days to provide sufficient notice of pending expiration. The maximum is unlimited.

Branding

About server branding

Branding is a standard feature that is part of every license. It enables you to customize the branding in the Kiteworks web application, email templates, and mobile apps. You can configure custom colors and images (mostly logos) on your instance.

Branding allows you to create different brands for different organizations across your Kiteworks deployment. Each organization can have a unique brand for its end users. When a customer or prospective client receives a secure link or invitation, the link takes them to the specified host name with the logo of the entity they are dealing with, not the larger corporation's branding. Each branded site is still on the Kiteworks server, and end users have access to all of their files, regardless of which branded site they are on.

For example, a large consumer products or advertising company with multiple brandings can have a Kiteworks server called "kiteworks.company.com" with their corporate branding. Each business unit or division within the organization can also have their own branding at each of their host names, such as brandA.company.com, brandB.company.com, and brandC.company.com.

Enable and set up multi-branding

To enable and set up multi-branding:

1. Obtain a license from Kiteworks to enable multi-branding, and then upload the license to your Kiteworks server.
2. Determine the host names to use for the multi-branded sites and add them to your DNS.
3. Point the DNS entries for all multi-site host names to the Kiteworks server's primary IP address to allow users to access the multi-branded sites.
4. Obtain and upload a wildcard or SAN SSL certification.

   Recommendation: Using wildcard SSL certificates over SAN certificates. If a SAN certificate is used, any new multi-branded sites will require a new SAN certificate be generated. Wildcard certificates will work for any multi-branded host name added without having to be re-generated.

Create and edit branding templates

To create a branding template:

1. Go to Application Setup > Configuration > Branding.
2. On the Branding tab, click Add Branding Template.
3. Specify a name for the template, and then select the Kiteworks default template or an existing custom template on which to base the new template.

   Result: The new template is added to the templates list.

Edit branding templates

To edit a branding template:

1. To edit a branding template, click the template you want to edit, and then in the upper right corner of the page, click Edit.
2. Scroll through each tab and customize the settings to suit your needs. Click a yellow number to edit the item.
   - Web Sign-In - The page for signing into the Kiteworks web application. You can customize the background color of the page, replace or remove the logo at the top of the page, change the color of the "Next" button, and add a disclaimer to appear at the bottom of the page.

     Recommendation: For the page background color, use a transparent color or one that matches your logo.
   - Mobile Sign-In - Not editable. Branding will be inherited from the design you apply to the Web Sign-In page.
   - Web Page - The landing page of the Kiteworks web application. You can replace the logo that appears at the top of the navigation pane, along with its background color and position. After customizing the color behind the logo, you can reset the color to its default transparent state if needed
   - Email - The template used for email notifications sent to users. You can replace the logo at the top of the page and add a disclaimer to appear at the bottom of the page.
3. When finished editing the template, click Save.

Enable the branding template for users

To enable the branding template, on the Branding Templates page, click the ON button.

Notification Templates

Customize email notification templates

You can customize the content of email notifications that get sent to end users.

At the global level you can truncate the body of every email notification sent through Kiteworks to display no more than 140 characters.

To customize an email notification template:

1. Go to Application Setup > Configuration > Notification Templates.
2. Expand the template you want to customize.
3. As you make changes, your changes are displayed in the preview window as formatted for message recipients.
4. When finished making changes, click Save. If you need to restore the entire template to its default, click the Reset to Default button.

File Preview

Enable users to preview files using the Kiteworks Web Application

You can allow end users in the Kiteworks Web application to preview specific file types from their folders and inboxes.

If a user is assigned the Viewer role, or if any user attempts to view a file that was sent to them as a view-only file, file previewing is allowed only if you also enabled watermarking for file previews.

Role: To turn file previewing on or off, your role must be System Admin. To enable watermarking, your role must be System Admin or Application Admin.

To enable users to preview files:

1. Go to Application Setup > Configuration > File Preview.
2. On the File Preview tab, turn on the "Enable File Previewing" switch, and then configure the settings.

Table 36. File preview settings

Maximum cache size	To manage disk space, specify the maximum percent of total storage that can be used for storing file previews. If the size is exceeded, cached file previews will be deleted according to the File Deletion setting.
Delete cached previews if not accessed in # of days	Delete cached file previews if not accessed by users within the specified number of days.
Cache deletion priority	The priority in which to delete cached file previews.

Table 36. File preview settings (continued)

Generate file previews when files are uploaded	Generate a cached preview of each file when it gets uploaded to the server. If the cached preview subsequently gets deleted, the server will generate a preview on demand, but will not cache the preview.
Apply watermark	Apply watermarks to files when they are previewed by users assigned the Viewer role, and when any user previews a view-only file. • Watermarks in text and image files are embedded in the text (PDF) and image preview files. • Watermarks in video files are overlayed on the preview file by the browser. **Exception:** Watermarking is not supported in Firefox and Safari browsers. If watermarking is enabled, video files opened in those browsers will not be viewable. • Watermarks are not applied to audio files.
Show on watermark	The information you want displayed in the watermark. • Timestamp - Display the date and GMT time the user received the file, either when the file was shared with them or was received in their inbox. • Viewer email address - When a user assigned the Viewer role previews the file, display the email address of the viewer in the watermark. • Sender email address - Display the email address of the user who shared or sent the file to the user who is previewing the file.
Custom text	Additional text you want to display in the watermark, such as "Do Not Distribute".
Allow users to download watermarked view-only documents	Allow users to download and save view-only files to their desktop. For some file types, such as Microsoft Office files, "[Watermarked]" will be appended to the downloaded file name.
Allow text search in view-only documents	When opening view-only files in the Kiteworks Web Application, enable end users to search for text within those files. **Note:** When this setting is enabled, there is risk of malicious users being able to extract the text from view-only documents. If you want to make the text layer full view-only, turn off this setting.

Table 36. File preview settings (continued)

Previewable file types	The types of files you want users to be able to view in the Kiteworks Web application. Each file can be up to 300 MB. **Exception:** Viewing text files is limited to 10 MB per file. • Microsoft Excel files • Microsoft PowerPoint files • Microsoft Word files • Image files (.pix, .tiff, .tga, .mvg, .svg) • CAD files (.dwg, .dxf) • Email files (.eml, .msg). **Note:** When end users open view-only email files, they will see only the email message body, not any file attachments. • Text/document files (.xml/.html)

Downloads and Guides

Enable users to download Kiteworks apps and plugins from the Kiteworks Web Application

For the Kiteworks apps and plugins you have deployed on your system, you can specify which apps and plugins end users can download and install from the Apps and Plugins link in the Kiteworks Web Application.

To enable users to download apps and plugins:

1. Go to Application Setup > Configuration > Downloads and Guides.

   Result: The Apps and Plugins section displays the items that you have deployed on your system.
2. To specify which items can be downloaded from the Kiteworks Web Application, click Edit.
3. (Optional) In the Help Text box, enter any text you want the user to read prior to downloading items.
4. Select which items you want users to be able to download.

   Result: As you select items, the Apps and Plugin screen updates to give you a preview of what end users will see in the Kiteworks Web Application.
5. Click Save, and then click the Close link at the top of the Apps and Plugin screen.
6. If you want to show a message at the top of the Kiteworks Web Application promoting the apps and plugins you selected, turn on the Enable Promo switch.

Enable users to download user guides from the Kiteworks Web Application

For those Kiteworks apps and plugins you have deployed on your system, you can specify which user guides end users can download from the Help link in the Kiteworks Web Application.

To enable users to access user guides:

1. Go to Application Setup > Configuration > Downloads and Guides.

   Result: The Help section displays the user guides that are downloadable from the Kiteworks Web Application.
2. To specify which guides can be downloaded from the Kiteworks Web Application, click Edit.
3. (Optional) In the Help Text box, enter any text you want users see prior to downloading documentation.
4. Select the guides you want users to be able to download.

   Result: As you select items, the Help screen updates to give you a preview of the user guide links that end users will see in the Kiteworks Web Application.
5. Click Save, and then click the Close link at the top of the Help screen.
6. The Kiteworks Web Application includes a getting started guide that you can make accessible to users from the application sign-in page. To display this link, go to the Enable Links on Login section and select the Kiteworks Getting Started Guide checkbox.

Upload custom user guides

If you customized or translated your own Kiteworks user guides, you can link to those guides instead of giving users access to the default guides.

If you customized or translated the Kiteworks Web User Guide, you can link to it or upload your own version of the guide in PDF format for users to download. Kiteworks also makes available this guide in Microsoft Word format for you to download and customize as needed.

To link to a custom user guide:

1. On the Downloads and Guides page, in the Help section, click Edit.
2. In the list of guides, click the edit icon for the custom you want to link to.
3. Enter the URL to the guide, and then click OK.

To download a Microsoft Word version of the Kiteworks Web User Guide:

1. On the Downloads and Guides page, in the Help section, click Edit.
2. For the Kiteworks Web User Guide, click the edit icon.
3. In the Default list, select Custom File, and then click the link for downloading the user guide.
4. Customize the guide as needed.

To upload a custom PDF version of the Kiteworks Web User Guide:

1. On the Downloads and Guides page, in the Help section, click Edit.
2. For the Kiteworks Web User Guide, click the edit icon.
3. In the Default list, select Custom File, and then click the Upload PDF button.
4. If you translated the guide into multiple languages, upload each PDF and then select which file associate with each language.

Authentication and SSO

LDAP

LDAP authentication

Kiteworks can be integrated with Lightweight Directory Access Protocol (LDAP) directories to streamline the user login process, allow for SSO implementations, and to automate administrative tasks such as creating users.

Kiteworks integrates with LDAP enabling the administrator to:

- Authenticate via LDAP
- Assign profiles based on LDAP
- Implement Repositories Gateway sources based on LDAP
  - Authenticate via LDAP/AD

    If Kiteworks is integrated with an LDAP, check Authenticate via LDAP/AD, so all internal users are checked against LDAP accounts during sign in.
  - Check against LDAP/AD

    If checked, database users will be checked against the LDAP server(s) every time they sign in to see if the Non-LDAP user has been promoted to an LDAP user. If unchecked, existing non-LDAP users will not be checked against LDAP and will remain non-LDAP users.
- First sign in only - Only users signing in for the first time will be checked against LDAP/AD.
- Every sign in - All users will be checked against LDAP/AD every time they sign in. In case a non-LDAP user is added, at the time of signing in the user will be marked as an LDAP user.
  - Allow Caching LDAP/AD Address Book on Kiteworks System

    On enabling this option, the LDAP/AD will be cached on Kiteworks and updated on a daily basis.

Sign in using a local password

You can log in and continue to administer the system if LDAP is down. You can request to create a local database password and use it to login when there is a LDAP outage. This event is logged and can be viewed in reports.

Once LDAP is down users cannot login. Users can login using database password only when LDAP is down.

Multiple LDAP support

Kiteworks provides multi-LDAP support. Kiteworks processes the configured LDAP servers in sequential order. If an LDAP server times out because of network issues, Kiteworks will process the next configured LDAP servers in order.

Note: If a user receives an error message that their username or password is invalid, their credentials may be on an LDAP server that is not reachable. To test this, click the LDAP server and Test user against configuration to test the LDAP settings.

Add LDAP servers

This section describes how to configure LDAP servers.

- Authenticate via LDAP/AD - You can turn this toggle switch off or on to authenticate via LDAP/AD.
- Search for User Account in LDAP/AD
  - First Sign in only - Only new users signing in for the first time will be checked against LDAP/AD.
  - Every Sign in - All users will be checked against LDAP/AD every time they sign in. In case a previous non-LDAP user is added to LDAP (at the time of signing in), the user will be marked as an LDAP user.
- Allow caching LDAP/AD address book on Kiteworks system - This feature is for the entire Kiteworks system and not for each LDAP server. When enabled, it stores all the LDAP address book information on the Kiteworks server from the other servers which speeds up the LDAP lookup. This information is synced daily so that the other servers do not need to be accessed. Only the servers displaying Connections OK in green are synced.

To add an LDAP server, click Add LDAP and then configure the server settings.

When multiple servers are added, you can drag the servers to re-order them. The LDAP servers are listed in the order that user's accounts will try to authenticate.

Table 37. LDAP server settings

Address book lookup	Enabling Address Book Lookup allows LDAP users to find other LDAP users with the User Filter. **Note:** LDAP Address Book lookup filter is separate from the User filter.
Active	Enable this checkbox for this server to be an active LDAP source.
Protocol	Choose LDAP, LDAPS (secure LDAP), or TLS from the drop-down menu. If TLS is selected, Kiteworks and the LDAP server use Transport Layer Security (TLS) to encrypt the connection, providing a secure channel.
Nickname	Set how this name is displayed to end users.
Domain filter	Domain filter for LDAP sources. If a user logs in using an email address, the system will only check against LDAP servers that specify the same email domain or where the Domain Filter is left blank.
Host	The Hostname or IP address of the LDAP server.
Port	The port that the LDAP server communicates on.
Base DN	Determines where in the LDAP tree structure the Kiteworks server will query for user identification. Typically, this is set to the root of the LDAP domain where the LDAP server is located, ex: DC=domain, DC=local.
Bind DN	This is the account the Kiteworks server will use when querying LDAP. Typically, this is a service account, with full read permissions to the LDAP tree, but no write or execute permissions. Ex: CN=Service Account, CN=Users,DC=domain,DC=local.
Bind password	The password for the account used in Bind DN.
Verify server certificate	If selected, Kiteworks will check the validity of the SSL certificate presented by the LDAP server. If not checked, Kiteworks will not perform this validation. You will only see this checkbox when the server is using TLS or LDAPS protocol.

Table 37. LDAP server settings (continued)

Use private internally signed certificate	Select this checkbox if the LDAP server is using a private internally signed certificate. Once this checkbox is selected the Certificate Chain of the Certificate field displays.
Certificate chain of the certificate	In this field enter the content of the Root Certificate or Certificate Chain of the Certificate Authority used to sign the certificate on the LDAP server.
Referrals	If checked, Kiteworks will allow referrals to alternate LDAP servers.
Network timeout	Wait time in seconds before the network times out when attempting to make queries. The maximum time is 600 seconds.
Repositories Gateway user attribute	Specifies which attribute will be used for authenticating Kiteworks users to Repositories Gateway sources. • DC\sAMAccountName: Domain Components (DC) of the User's DistinguishedName and the user's sAMAccountName are automatically retrieved. For example: CompanySharePoint.com\Art.Vandelay • sAMAccountName: This allows the administrator to manually enter the domain (e.g. company.com) instead of automatically retrieving it. This is useful if the users' DistinguishedNames on your network are different from the Domain or Workgroup they belong to. For example: test.user [admin types in a domain/workgroup name] • userPrincipalName: The name of a user in email address format. For example: test.user@CompanySharePoint.com
Repositories Gateway login domain	This field is applicable only when the LDAP attribute is specified as sAMAccountName.
Location attribute	Specify an attribute in LDAP to indicate a user's location. To map this attribute to a specific server, go to Locations Rules > Location Mapping.
Display Name attribute	Specify an attribute in LDAP that is indicative of a user's name.
Distinguished Name attribute	Specify an attribute in LDAP that is indicative of a user's unique identifier.
Email attribute	Specify an attribute in LDAP that is indicative of a user's email address, such as mail.
Groups attribute	Specify an attribute in LDAP that is indicative of a user's LDAP group(s), such as memberOf.

Table 37. LDAP server settings (continued)

User filter	Specify one or a list of valid LDAP filters to define how users are searched for. This specifies what attributes will be used to identify the user. This is in standard LDAP search format. Multiple attributes may be specified with an "or" symbol ("|"). Example: (&(objectClass=user)(|(mail=%%username%%)(sAMAccountName=%%username%%))). **Note:** For some LDAP setups to show Repositories Gateway sources properly and to access their Repositories Gateway shares and sites via Kiteworks, you can try using the following filter: (&(&(|(objectClass=user)(objectClass=inetOrgPerson))(|(objectClass=inetOrgPerson)(!(userAccountControl:1.2.840.113556.1.4.804:=18))))(|(distinguishedName=%%username%%)(mail=%%username%%)(sAMAccountName=%%username%%)(userPrincipalName=%%username%%)(uid=%%username%%)(proxyAddresses=SMTP:%%username%%))
Distribution list lookup	Enable this option to access the distribution list attribute fields listed below. These fields determine the lookup of the distribution list addresses only of the current server it is on. This is done individually for the other servers and they may have a different filter for the Mail Attribute and Member Attribute.
Distribution list filter	You can set a custom filter to define the distribution list entry in LDAP. The filter can contain a list of filters as defined by RFC 2254. For example, (|(objectClass=group)(objectClass=groupOfNames)).
Distribution list mail attribute	The attribute of the distribution list LDAP entry that stores the e-mail address of that list. For Active Directory, the value is "mail".
Distribution list member attribute	The attribute of the distribution list LDAP entry that stores the members of that list. For Active Directory, the value is "member".
Test user against configuration	Click the Test User Against Configuration checkbox to select it. The username and password fields displays. Enter a Username and Password, then click Test LDAP Settings to verify that a User can be authenticated against the selected LDAP. If the email address cannot be verified, the LDAP test result will display failed. If the email address is verified, the LDAP Test Result window displays a valid distribution list.
Test LDAP settings	This button can be used to test the LDAP connection.

LDAP Groups

Create LDAP groups

Kiteworks can be integrated with LDAP/MSAD so users can sign in with their network password. Additionally, Kiteworks allows administrators to add LDAP groups.

LDAP groups added to Kiteworks can be used as follows:

- LDAP group management is dynamic; in other words, as users are added and deleted from the LDAP groups, users are removed from or given access to folders automatically.
- The permissions for all members of an LDAP group are the same.
- LDAP groups are created by an administrator to make these groups available to end-users to be able to quickly share a folder with a group of users.
- You can also import LDAP groups into Kiteworks. This enables specific LDAP groups to be available to end-users so they can easily share folders with an entire group of users instead of adding individual users one at a time.
- These groups are not visible to end users unless they are added by the administrator.

Once an LDAP group is created in the Kiteworks Admin Console, the end user can search for that LDAP group in the Kiteworks Web Application by clicking the Invite button and searching for that specific LDAP group to share the folder.

To create an LDAP group:

1. Go to Authentication and SSO.
2. On the LDAP groups tab, click Add LDAP Group.
3. Search for the group you want to add.
4. Select the group, and then click Add.

Refresh LDAP groups

You can add an LDAP group to Kiteworks, which allows users to add these groups to folders (and set permissions). When a user logs in to Kiteworks, their group membership is checked. If the user belongs to an LDAP group, the user will have access to content that LDAP group can access.

Since users often belong to a subgroup of LDAP groups, Kiteworks periodically checks LDAP to see which subgroups belong to the LDAP groups. Once a day, Kiteworks automatically checks the LDAP groups to update the subgroups. A Refresh LDAP button is available in the administrator interface to manually recheck group permission.

Note: LDAP refresh checks and refreshes all the nested groups in the Active Directory. It does not check the actual membership.

To refresh an LDAP group:

1. Go to Authentication and SSO.
2. On the LDAP groups tab, click Refresh LDAP.

2FA

About two-factor authentication

Two-Factor Authentication (2FA) provides an additional security step when users sign in to Kiteworks. 2FA enhances the regular authentication by adding a "possession factor" (something the user has, such as a token, SMS-based phone or device, or email connection) with a "knowledge factor" (something the user knows, such as a password) into the authentication process.

2FA is limited to the Kiteworks idP. External SSO is required to fulfill all aspects of Authentication and Authorization which includes 2FA. Kiteworks, the Service Provider follows after Authentication and Authorization and does not currently utilize 2FA in post AAA capacity.

If 2FA is enabled for a user profile which also has SFTP turned on, 2FA will not apply to those users if they log in via SFTP. This is because most SFTP clients do not support 2FA.

Set up time-based one-time password authentication

Time-based one-time password (TOTP) is a standardized cryptographic algorithm for generating unique one-time passwords that remain valid for 30 seconds. Open integration in the Kiteworks Admin Console enables you to set up two-factor authentication with any app that implements TOTP to enforce an extra level of security when users sign in to the Kiteworks web application.

The following authentication apps have been tested, although you can use any app that supports the TOTP standard (RFC 6238):

- Microsoft Authenticator
- Google Authenticator
- FreeOTP Authenticator (Red Hat)
- Twilio Authy
- Duo Mobile
- LastPass Authenticator
- OneLogin Protect

Once you enable 2FA, you make it available to users through user profiles. Users will see the TOTP setup screen the next time they go to sign in to the Kiteworks web application. To set up TOTP, they use their phone to scan the barcode on the setup screen and enter the code returned by the authenticator app. After that, each time they sign in they'll need to enter a new passcode generated by their authenticator app. For faster sign in, you can choose to show the "Remember this device" check box on the 2FA screen so that they can temporarily add their computer or phone as a trusted device.

Setting up 2FA using TOTP consists of the following steps:

- Turn on two-factor authentication.
- Create a TOTP source.
- Enable TOTP settings in user profiles.
- Test two-factor authentication using TOTP.

Recommendation: Create a test user profile and user account for testing 2FA using TOTP. This enables you to ensure it's working correctly before impacting your users. Then you can enable the settings in user profiles to take effect the next time users sign in to the Kiteworks web application.

Turn on two-factor authentication

To turn on two-factor authentication:

1. Go to Application Setup > Authentication and SSO > 2FA.
2. On the 2FA tab, enable two-factor authentication and select additional settings you want to apply.

Table 38. 2FA tab settings

Setting	Description
Enable two-factor authentication	Require two-factor authentication when signing in to the Kiteworks web application.

Table 38. 2FA tab settings (continued)

Setting	Description
Apply two-factor authentication to admin logins also	Require two-factor authentication when signing in to the Kiteworks Admin Console. **Caution:** If 2FA isn't set up correctly, you may not be able to sign in to the Kiteworks Admin Console. Before selecting this option, set up two-factor authentication for end users first and verify it's working by signing in to the web application with a test account. If you make a mistake while configuring 2FA, you can fix it before enforcing the requirement for administrators.
Remember device for subsequent authentication	Display the "Remember this device" check box on the 2FA screen. Users can temporarily add their computer or device as a trusted device to bypass the verification code each time they sign in. Trust settings are revoked after 90 days, after which they'll need to choose to remember their devices again.
Mask two-factor authentication code	Hide passcodes as they are being entered on the 2FA screen.

Create a TOTP source

To create a TOTP source:

1. Go to Application Setup > Authentication and SSO > 2FA.
2. On the 2FA tab, click Add.
3. On the Add 2FA Source page, configure the source.

   Result: The source is added to the list on the 2FA tab. Two-factor authentication is also added as a setting on the Account tab in user profiles, but is off by default until you turn it on for the profile.

Table 39. 2FA Source settings

Setting	Description
Name	Type a name for the 2FA source.
Label (Optional)	The label that appears above the passcode box on the 2FA screen. Use the default label or enter a custom label. **Example:** One time passcode
Description text (Optional)	Type instructional text to help guide users through the process of entering one-time passcodes. This text will appear above the label. **Example:** Please enter your one-time passcode.
Module	Select "Time-based OTP". This also displays a new section on the page called TOTP Settings.

Table 39. 2FA Source settings (continued)

Setting	Description
Exclude IP (Optional)	Specify IP addresses or IP ranges from which 2FA will not be allowed. Use a comma between multiple entries. **Example formats:** 11.22.33.44, 11.22*, 11.22.33.44/55.
Backward time drift	To anticipate potential time differences between TOTP devices and the server, specify how far back time drift is acceptable. The default is 1 minute. Maximum is 3 minutes.
Forward time drift	To anticipate potential time differences between TOTP devices and the server, specify how far ahead the time drift is acceptable. The default is 1 minute. Maximum is 3 minutes.
Setup instruction 1	Instructional text that appears above the QR code on the TOTP setup screen. Use the default text or enter custom text.
Setup instruction 2	Instructional text that appears above the 6-digit code box on the TOTP setup screen. Use the default text or enter custom text.
Test 2FA settings	Test connection settings after initially setting up and testing TOTP. **Prerequisite:** Before you can test 2FA settings, you enable TOTP in a user profile and test it by signing in to the web application and setting up TOTP. Once set up, you can use this button to verify settings are working in the event of future connection issues.

Enable TOTP settings in user profiles

To enable TOTP settings in a user profile:

1. Go to Users > Profiles > *expand a profile* > Account tab.
2. In the Two-Factor Authentication list, select the 2FA TOTP source you just created, and then click Save.

Test two-factor authentication using TOTP

Prerequisite: Determine which authentication app you want to use and set it up. For instructions, refer to the app user documentation.

To test two-factor authentication settings using TOTP:

1. Sign in to the web application using a test account.

   Result: The TOTP setup page is displayed. If not, ensure that you turned on two-factor authentication.
2. When prompted to set up TOTP, open the authenticator app on your phone and scan the barcode to the app.
   - You may be able to use your device camera to scan the code to the app.
   - To manually get the code, click "Having trouble scanning the code?". Copy the secret key and enter it into your account in the authenticator app.
3. Enter the code from your authenticator app, and then click Submit.

   Result: A secret key is associated with your device and user account. If you signed in using TOTP successfully, your test is complete and you are ready to deploy TOTP to users.

4 If you created a test account for testing TOTP, you may want to delete it from the authenticator app. If not, whenever you open the app it will continue generating temporary passcodes for the test account.

Reset TOTP secret keys

When a user first signs into the Kiteworks web application using TOTP, a secret key is created for them. If a user changes their phone or needs to use a different authenticator app, they can reset their secret key in their profile account settings in the web application. This takes them through the TOTP setup process again so that they can associate a new key with their device and user account.

You can also reset their key for them from within the Kiteworks Admin Console. When you reset a user's secret key, they'll need to go through the TOTP setup process again the next time they sign in.

To reset a user's secret key:

1 Go to Users and click the user account you want to edit.
2 On the Time-based TOTP tab, click Remove Secret Key.

Exception: If you don't see the option to remove the key, the user has not yet signed in to the Kiteworks web application using TOTP.

Set up two-factor authentication for RADIUS

RADIUS is a client/server protocol. The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

Prerequisite: Open port 1812 for the RADIUS two-factor authentication server.

To set up two-factor authentication for RADIUS:

1 Go to Application Setup > Authentication and SSO > 2FA.
2 On the 2FA tab, click Add.
3 On the Add 2FA Source page, in the module list, select RADIUS Protocol.
4 Configure the source settings, and then click Save.

Table 40. RADIUS Protocol settings

Setting	Description
Name	Type a name for the 2FA source.
Label (Optional)	The label that appears above the passcode box on the 2FA screen. Use the default label or enter a custom label. **Example:** One time passcode
Description text (Optional)	Type instructional text to help guide users through the process of entering one-time passcodes. This text will appear above the label. **Example:** Please enter your one-time passcode.
Module	Select RADIUS Protocol.

Table 40. RADIUS Protocol settings (continued)

Setting	Description
Exclude IP (Optional)	Specify IP addresses or IP ranges from which 2FA will not be allowed. Use a comma between multiple entries. **Example formats:** 11.22.33.44, 11.22*, 11.22.33.44/55.
Server	Enter the IP address or hostname of the RADIUS server.
Secret	Enter the Secret, which is obtained from the RADIUS server.
Port	Enter Port 1812. This port for the RADIUS Two-Factor Authentication server must be opened.
Timeout	Time that the session between the RADIUS server and Kiteworks server(s) expires.
Maximum attempts	Number of times the Kiteworks server will attempt to connect to the RADIUS server. If connection attempts exceed this value, the user receives the error, "Authentication temporarily not available."
LDAP username attribute	• The LDAP/MSAD attribute the Kiteworks server uses to determine the user's RADIUS ID. This should map to the LDAP value used on the RADIUS server, if available. This option is only used when LDAP/MSAD has been set up on the Kiteworks server. The user's email address is used if no LDAP attribute it specified.
Authentication flow	Choose the authentication flow that is appropriate for your RADIUS server.
RADIUS attributes	Either a NAS-IP-Address or a NAS-Identifier must be present in an Access-Request packet. • NAS IP address - Specify the NAS IP Address of the RADIUS request. • NAS identifier - Specify the NAS Identifier of the RADIUS request.
Test 2FA settings	Test connection settings after initially setting up and testing TOTP. If successful, you can enable Apply Two-Factor Authentication to Admin Logins also. If not successful, verify your settings and test again. **Prerequisite:** Before you can test 2FA settings, you enable TOTP in a user profile and test it by signing in to the web application and setting up TOTP. Once set up, you can use this button to verify settings are working in the event of future connection issues.

Set up email-based one-time passcode authentication

To set up email-based one-time passcode authentication:

1. Go to Application Setup > Authentication and SSO > 2FA.
2. On the 2FA tab, turn on the "Enable Two-Factor Authentication" switch, and then enable one or more of the following settings as needed.

- Apply Two-Factor Authentication to Admin Logins Also - You can require that administrators also use this authentication method when signing in to the admin console.

  Caution: If you turn on this setting, you will also be required to use this authentication method when signing in to the admin console. Before enabling this option, it is strongly recommended that you set up the feature, apply it to a user profile, and then test the feature by signing in to the Kiteworks Web Application using two-factor authentication. Otherwise, if there is a problem with the setup configuration and you have turned on this setting, you may not be able to access the admin console again.
- Remember device for subsequent authentication - When a user is successful with signing in using two-factor authentication, temporarily add their device as a trusted device. The device will be remembered for 90 days after which the user will need to re-authenticate using two-factor authentication.
- Mask Two-Factor Authentication Code - Mask two-factor authentication passcode numbers.

3 To add an authentication source, on the 2FA tab, click Add.

4 On the Add 2FA Source page, in the module list, select Email-based OTP.

5 Configure the source settings, and then click Save.

Table 41. Email-based OTP settings

Setting	Description
Name	Type a name for the 2FA source.
Label (Optional)	The label that appears above the passcode box on the 2FA screen. Use the default label or enter a custom label. **Example:** One time passcode
Description text (Optional)	Type instructional text to help guide users through the process of entering one-time passcodes. This text will appear above the label. **Example:** Please enter your one-time passcode.
Module	Select Email-based OTP.
Exclude IP (Optional)	Specify IP addresses or IP ranges from which 2FA will not be allowed. Use a comma between multiple entries. **Example formats:** 11.22.33.44, 11.22*, 11.22.33.44/55.
Format	Select from a 6, 7 or 8 character decimal format.
Expiry	Enter the expiry duration in minutes.
Regenerate OTP label	Enter the label that will be shown for regenerating the one-time passcode link.
Regenerate OTP message	Enter the message that will be shown after the one-time passcode link is regenerated.

Table 41. Email-based OTP settings (continued)

Setting	Description
Test 2FA settings	**Prerequisite:** Before you can test 2FA settings, you enable email-based OTP in a user profile and test it by signing in to the Kiteworks Web Application and setting up email-based one-time passcodes. Once set up, you can use this button to verify settings are working in the event of future connection issues. Test connection settings after initially setting up and testing email-based one-time passcodes. If not successful, verify your settings and test again.

Set up SMS-based two-factor authentication

SMS-based 2FA allows use of SMS text messages as the 2nd factor in the Two-Factor Authentication (2FA) process. This method supports Twilio and Sinch as SMS providers. Existing Radius MFA integration and existing native 2FA using an email One Time Password (OTP) 2nd factor is still supported.

To use this feature, SMS-based 2FA, OTP settings and the SMS Service settings will need to be configured. The Application administrator can also configure the Kiteworks service to work with an external SMS service so that Kiteworks can send SMS messages to users or phone numbers.

To set up SMS-based two-factor authentication:

1. Go to Application Setup > Authentication and SSO > 2FA.
2. On the 2FA tab, click Add.
3. On the Add 2FA Source page, in the module list, select SMS-based OTP.
4. Configure the source settings, and then click Save.

Table 42. SMS-based OTP settings

Setting	Description
Name	Type a name for the 2FA source.
Label (Optional)	The label that appears above the passcode box on the 2FA screen. Use the default label or enter a custom label. **Example:** One time passcode
Description text (Optional)	Type instructional text to help guide users through the process of entering one-time passcodes. This text will appear above the label. **Example:** Please enter your one-time passcode.
Module	Select SMS-based OTP.
Exclude IP (Optional)	Specify IP addresses or IP ranges from which 2FA will not be allowed. Use a comma between multiple entries. **Example formats:** 11.22.33.44, 11.22*, 11.22.33.44/55.
Format	Select from a 6, 7 or 8 character decimal format.

Table 42. SMS-based OTP settings (continued)

Setting	Description
Expiry	Enter the expiry duration in minutes.
Regenerate OTP label	Enter the label that will be shown for regenerating the OTP link.
Regenerate OTP message	Enter the message that will be shown after the OTP link is regenerated.
SMS message template	In the SMS Message Template field key in the 2FA message that will be sent via SMS. For example, your one-time passcode (OTP) to sign in to your Kiteworks account is %%OTP%%. This OTP expires in %%EXPIRY_MINUTE%% minutes.
Test 2FA settings	Test connection settings after initially setting up and testing SMS-based OTP. If successful, you can enable Apply Two-Factor Authentication to Admin Logins also. If not successful, verify your settings and test again. **Prerequisite:** Before you can test 2FA settings, you enable SMS-based OTP in a user profile and test it by signing in to the web application and setting up SMS-based OTP. Once set up, you can use this button to verify settings are working in the event of future connection issues.

SMS-based 2FA allows use of SMS text messages as the 2nd factor in the Two-Factor Authentication (2FA) process. This method supports Twilio and Sinch as SMS providers. Existing Radius MFA integration and existing native 2FA using an email One Time Password (OTP) 2nd factor is still supported.

To use this feature, SMS-based 2FA, OTP settings and the SMS Service settings will need to be configured. The Application administrator can also configure the Kiteworks service to work with an external SMS service so that Kiteworks can send SMS messages to users or phone numbers.

SAML 2.0

Set up SAML authentication

SSO Setup

The server supports SAML and Kerberos SSO authentication so that users can authenticate via either method based on either who the user is or the user's location or client. The server supports multiple SSO providers to separate internal users and external users, which include, SAML 2.0 up to 5 idPs and Kerberos for Single Sign On use. Once it's set up, it shows in web UI sign-in page as a list of links.

The server leverages existing SSO resources for user authentication. If both SAML and Kerberos are enabled, you can set an IP redirection for either. Select the desired protocol to authenticate users with Single Sign On.

You can configure the authentication flow criteria based on:

- Pre-auth based on the user's email address (domain-based).
- Auto redirection based on the user's IP address.
- Users can choose an idP from the UI.

idP initiated SSO and service provider initiated SSO with SAML 2.0

In idP (Identity Provider) Initiated SSO (Unsolicited Web SSO) the Federation process is initiated by the idP sending an unsolicited SAML Response to the service provider. In the service Provider or Kiteworks initiated SSO, the service provider generates an AuthnRequest that is sent to the idP as the first step in the Federation process and the idP then responds with a SAML Response.

When using idP initiated login to the Kiteworks Admin Console, the RelayState parameter should be set to https://< Kiteworks server hostname>/admin/ for accessing the Kiteworks Admin Console. Always make sure that your URL ends with a "/". This does not apply to the service provider initiated login.

Setup SSO with SAML 2.0

Multiple idP signing certificates/keys are supported in SSO setup along with the ability to fetch remote idP metadata. You can configure SAML settings using metadata to import manually or automatically to get multiple idP signing certificates and URLs.

To set up SSO with SAML 2.0:

1. Go to Application Setup > Authentication and SSO.
2. On the SAML 2.0 tab, turn on the "Enable SAML" switch.
3. Configure the service provider settings, and then click Save.
   - Service provider entity ID: This ID is used by the service provider to refer to themselves during communications and to look up metadata for other entities. Typically it will be a URL, for example, https://sp.com.
   - Assertion consumer service: Location at a service provider that accepts <samlp:Response> messages (or SAML artifacts) for the purpose of establishing a session based on an assertion. For example, https://mobile.company.com/saml/saml2-acs.php.

Add multiples idPs

You can add up to 5 IdPs.

To add an identity provider (IdP):

1. In the Identity Provider (IDP) Settings section, click Add IdP.
2. Configure the IdP settings, and then click OK.

Table 43. SAML Settings tab settings

Authentication Request Settings	• Initiate AuthnRequest - There are various ways to connect to an identity provider, AuthnRequest is a SAML 2.0 supported method.
	  • NameIDPolicy Format - This is the format of the name identifier which will be requested to the idP (SSO server). The default requested format is "urn:oasis:names:tc:SAML:1. 1:nameid-format:unspecified". Select either unspecified or emailAddress.
	  • Force fresh authentication everytime - Check this checkbox to specify whether to force the user to authenticate on the idP, even if there is an existing idP session on the browser. This is useful if you do not want the SSO session to be shared across different service provider applications.
	  • SignAuthNRequest: Check this to specify whether to sign AuthNRequests are sent to this external idP.
	• Using ADFS 2.0 - Select this option if you are using Microsoft's Active Directory Federation Services (ADFS)
	  • ADFS 2.0 Rollup 2 installed - If you are using ADFS 2.0, check this box if ADFS 2.0 Rollup 2 patch is installed. Check the Microsoft support site for patch information at http://support.microsoft.com/kb/2681584.

Table 43. SAML Settings tab settings (continued)

Identity Provider (idP) settings	• Nickname - Specify a nickname for the idP.
	• Import idP metadata - Use a configuration from a remote metadata file to populate settings. Multiple IdP Signing Certificates are allowed.
	  • Remote IdP metadata URL - Specify the remote IdP metadata URL from where the metadata will be retrieved. This is the entity ID used by the idP to refer to themselves during communications and to look up metadata for other entities. Typically, it will be a URL, for example, https://auth.idp.com. You can:
	  • Retrieve IdP metadata - Select this option to manually retrieve the IdP metadata or select "Auto import IdP metadata periodically". Auto-import is separated in 2 parts: (1) auto-importing the IdP metadata (IdP entity ID, SSO URL, and SLO URL), and (2) auto-importing IdP certificates.
	• idP Entity ID - This is the ID that the idP uses to refer to themselves during communication, as well as metadata lookup for other providers. This is typically a URL.
	• Single sign-on service URL - The URL given by the idP to log the user into Kiteworks.
	• Initiate logout request - Auto-import the IdP certificate on a daily basis. The IdP settings will be replaced using the metadata information. You will need to provide the single sign-on service URL provided by the idP to be used to for logging out the user from the Kiteworks appliance. e.g. https://idp-logout.abc.com.
	• Single logout service URL - The URL given by the idP to log the user out from Kiteworks.
	• Logout landing page URL - Allow logout by providing a logout landing page URL.
	• IdP signing certificate - The RSA certificate (in PEM format) of the idP (SSO server) . This is used by the Kiteworks server (as Service Provider) to verify SAML response. Multiple certificates can be provided, i.e., for the cert rollover case. Click Add another IdP Signing Certificate to add additional certificates.
	• Auto create user - When a new user signs in to their Kiteworks system using SSO, the system automatically creates an account for them. Turn off this setting if you want to prevent this for the specific idPs.

Table 43. SAML Settings tab settings (continued)

SAML Attributes settings	• Display name attribute - Specify an appropriate attribute that is indicative of the user's display name. Otherwise leave blank to use LDAP display name attribute, or email when the LDAP display name attribute is not available. **Examples:** • http://schemas.microsoft.com/ws/2008/06/identity/claims/displayName • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name • Location attribute - Specify an appropriate attribute in the SAML assertion that is indicative of the user's location. If none is specified, "location" will be used. To map this attribute to an actual appliance location, see Configure location mapping **Examples:** • location • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country

Table 44. SSO Auto-Redirect tab settings

IP addresses	Specify IP addresses or IP ranges from which sign in requests will be auto-redirected to the configured SSO source. Leave this field blank to indicate no IP redirection. Use a comma between multiple entries. Supported format examples: 11.22.33.44, 11.22*, 11.22.33.44/55.
Exclude IP	Specify IP addresses or IP ranges from which sign in requests will not be auto-redirected to the configured SSO source. Leave this field blank to indicate no IP redirection. Use a comma between multiple entries. Supported format examples: 11.22.33.44, 11.22*, 11.22.33.44/55.
Email domain	You can setup email domain-based redirection to SSO so that internal users always use SSO-based authentication. The administrator will also be able to set up of a list of excluded email addresses separated by a comma for email addresses within the domains that will not be redirected to the idP but will follow the standard authentication route for their profile (password, 2FA, etc.)
Email domain inclusion regex	Specify a regular expression for email domains. Leave blank to indicate no redirection based on domain. If the user enters an email on the login prompt that matches the regular expression, then the user will be redirected to this SSO. If the user does not enter any domain in the email id, then also the user would be redirected to the SSO.
Email address exclusion list	Specify email addresses which will be excluded from auto-direction to the configured SSO. Leave blank to indicate no exclusions. Use a comma as a delimiter while specifying more than one email address. For example, aaa@abc.com, bbb@abc.com .

Table 45. Link Label tab settings

Login link label	The label you want to appear above the SSO redirect link. Use the default one or enter a custom label.
IP addresses for hiding SSO login link	IP addresses you want to prevent from seeing the SSO redirect link (and the associated server name or address of the idP) on the sign in page. You can enter a single address, or a range of addresses separated by commas, in the following formats: • Single IP address **Example:** 192.168.1.1 • IP address with wildcard **Example:** 192.168.* • Selection by subnet **Example:** 192.168.100.14/24 • Selection by range **Example:** 192.168.1.10-192.168.1.25, 192.168.1.10-192.168.1.25/24

Kerberos

Set up Kerberos authentication

Kerberos is a mature, widely used network authentication protocol which allow nodes in a non-secure network to authenticate to one another using tickets in a secure manner. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:

- It is secure: it never sends a password unless it is encrypted.
- Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
- The concept depends on a trusted third-party – a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

To set up Kerberos authentication:

1. Go to Application Setup > Authentication and SSO > Kerberos.
2. On the Kerberos tab, turn on the Enable Kerberos switch.
3. On the Kerberos Settings tab, enter the requested information:
   - Authentication realm - This is typically the Windows domain and MUST be in uppercase letters.
     Note: When this setting is modified, web services will restart on servers with the Web role.
   - Key distribution center (KDC) - Specify the IP address or hostname of the KDC that the Kiteworks server will use.
   - Realm replacement - Specify the replacement string that will replace the Authentication Realm if the Authentication Realm does not match the userPrincipalName domain.
   - Ignore realm - Drops realm and assumes username is sAMAccountname.

Note: LDAP user filter needs to be updated with an option to match against (sAMAccountName=%%username%%) in addition to normal login options.

- Keytab file - Click Upload File to upload the keytab file that will be used for decrypting Kerberos tickets. This file is normally generated with the ktpass tool on a Windows domain server.

  Note: When the keytab file is uploaded, web services will restart on servers with the Web role.

4 Click Save.

5 On the SSO Auto-Redirect tab, enter the requested information:

- IP addresses - Specify the IP addresses from which sign in requests will be auto-redirected to the configured SSO source. Use a comma to separate multiple entries in any of the following formats: 11.22.33.44, 11.22.*, 11.22.33.44/45.
- Exclude IP - Specify the IP address or IP address range from which sign in requests will not be auto-redirected to the configured SSO source (users will always have to sign in to Kiteworks). The exclusion range is always a subset of the auto-redirect range. If you do not specify IP Addresses for auto-redirect, you do not need to specify excluded IP addresses. Use a comma to separate multiple entries in any of the following formats: 11.22.33.44, 11.22.*, 11.22.33.44/45.
- Email domain - Set up email domain-based redirection to SSO so that internal users always use SSO-based authentication. The administrator will also be able to set up of a list of excluded email addresses separated by a comma for email addresses within the domains that will not be redirected to the idP but will follow the standard authentication route for their profile (password, 2FA, etc.)
- Email domain inclusion regex - Specify a regular expression for email domains. Leave blank to indicate no redirection based on domain. If the user enters an email on the login prompt that matches the regular expression, then the user will be redirected to this SSO. If the user does not enter any domain in the email id, then also the user would be redirected to the SSO.

  Example: ^(.*@kiteworks\.com)|(.*@kiteworks\.net)$
- Email address exclusion list - Specify email addresses which will be excluded from auto-direction to the configured SSO. Leave blank to indicate no exclusions. Use a comma as a delimiter while specifying more than one email address. For example, aaa@abc.com, bbb@abc.com.

6 Click Save.

7 On the Link Label tab, enter the requested information:

- Login link label - Enter a label for the link that redirects the user to the SSO system. Leave this field blank to use the default value.

8 Click Save.

Certificate-Based Authentication

Set up certificate-based authentication

In addition to authentication methods such as single sign-on, you can enable certificate-based authentication (CBA) as an alternate way for users to sign in using unique SSL client certificates installed in their browsers. When CBA is enabled, Kiteworks automatically signs users in after they select a certificate.

The identity of the authenticating user can be stored in the email part of the client certificate subject field, or in the Subject Alternative Name (SAN) field.

When a certificate nears expiration, the system notifies administrators 7 days in advance of expiration. Email notifications are sent daily to the default system notification email address, and contain links for signing in to the Kiteworks Admin Console to upload renewed certificates. An email notification is also sent when a certificate expires.

Certificate-based authentication sign in activity is tracked in the audit log.

Before enabling certificate-based authentication, keep the following requirements in mind:

- Certificate-based authentication can be used only for signing in to Kiteworks end user web-based applications. It can't be used to sign in to the Kiteworks Admin Console and SFTP shares.
- An uploaded certificate file can contain a single certificate or multiple certificates (unlimited) in a certificate chain. When uploading multiple certificates individually, they will be combined into a single certificate in the system.
- Certificate-based authentication is supported only on single tenant (standalone) Kiteworks systems. Multi-tenant systems don't contain certificate-based authentication configuration options in the Kiteworks Admin Console.
- Kiteworks validates certificates using OCSP or CRL, depending on the certificate contents. If the client (or intermediate CA) certificate contains only OCSP information, OCSP will be used to check for certificate revocation. If the certificate contains only CRL information, CRL will be used. If the certificate contains both OCSP and CRL information, or does not contain either protocol, the protocol selected in the admin console will be used.
- If a client certificate contains a new CRL, the CRL will be downloaded automatically.

Enable certificate-based authentication

To use certificates to authenticate Kiteworks users in your organization, you must upload a certificate and enable certificate-based authentication.

A certificate can be an issuer, intermediate, or root certificate authority (CA) certificate -- a special kind of X.509 digital certificate that can be used to issue user certificates. Supported file types are: .cer, .crt, .pfx, .p12, .spc, .p7b, .der

Important: Before enabling certificate-based authentication, select the preferred revocation validation mechanism and then upload certificates. Once you enable certificate-based authentication, the system will restart automatically. During this time, the system will be offline and this may take some time.

To select the preferred revocation validation mechanism:

1. Go to Application Setup > Authentication and SSO > Certificate-Based Authentication.
2. In the Preferred Revocation Validation Mechanism list, select the preferred protocol to check for certificate revocation.
   - OCSP - Use the OCSP URL in the client certificate to validate the certificate in real-time.
   - CRL - Validate the client certificate based on its current CRL database, as was downloaded from the CRL URL in the uploaded root certificates.

To upload certificates:

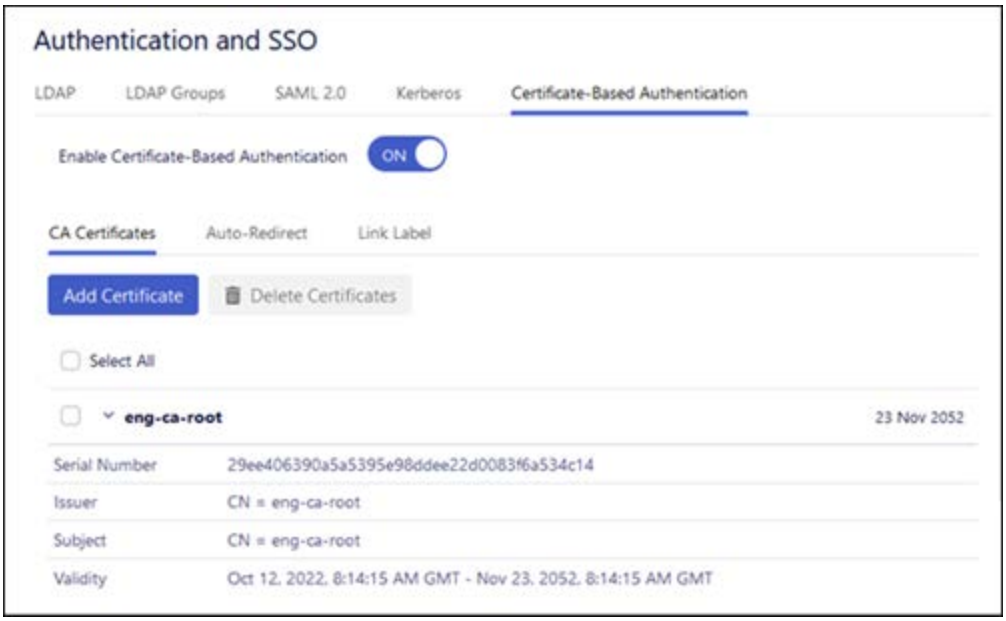
1. On the CA Certificates tab, click the Add Certificate button, and then select the certificate you want to upload.
2. Click Add Certificate.
3. Upload any additional certificates you want to add.

To enable certificate-based authentication:

Important: Enabling certificate-based authentication automatically restarts the system. During this time, the system will be offline.

1. At the top of the Certificate-Based Authentication tab, turn on Enable Certificate-Based Authentication.

Enabling certificate-based authentication automatically restarts the system. This may take a moment to complete.



2 Issue user certificates and send them (along with their encryption passwords) to your users for importing into their browser trust stores.

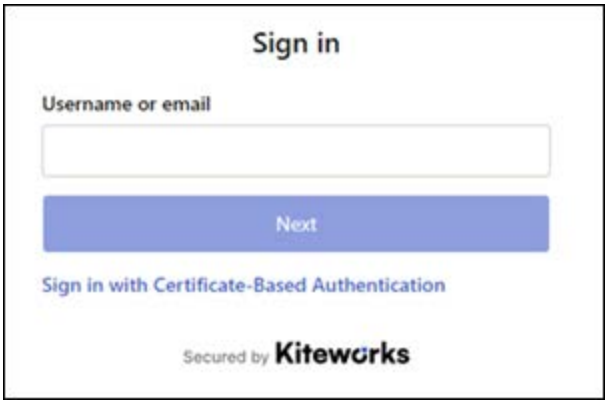
Customize the link for signing in using certificate-based authentication

By default, the certificate-based authentication link text that appears on the sign in page is "Sign in with Certificate-Based Authentication". You can customize the link text.

To customize the link text:

1 On the Certificate-Based Authentication tab, click the Link Label tab.

2 In the Login Link Label field, enter the text you want to use for the link on the sign in page. If you leave the field blank, the default "Sign in with Certificate-Based Authentication" text will be used.

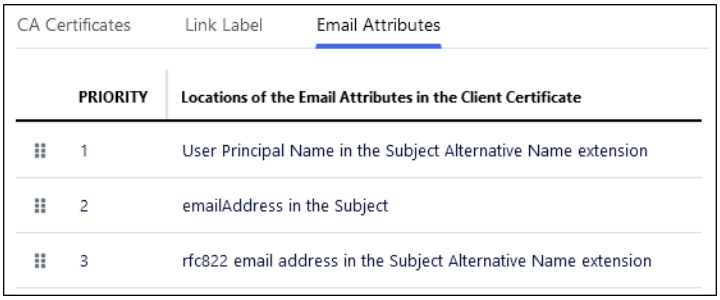


Specify certificate attribute priority for email addresses

You can decide the priority of certificate attributes by which certificate-based authentication will look for the user's email address. If a client certificate holds both the OCSP and CRL protocols, and OCSP is selected as the preferred protocol, failover to CRL occurs if the OCSP server times-out. If a CRL download fails, an email notification is sent to administrators.

To specify the certificate attribute priority for email addresses:

1. On the Certificate-Based Authentication tab, click the Email Attributes tab.
2. Drag to reorder the certificate attribute priorities as needed, and then click Save.



Turn off certificate-based authentication

When you turn off certificate-based authentication, users will need to use a different method for signing in to their Kiteworks applications, such as their username and password or single sign-on.

Important: Turning off certificate-based authentication automatically restarts the system. During this time, the system will be offline.

To turn off certificate-based authentication:

At the top of the Certificate-Based Authentication tab, turn off Enable Certificate-Based Authentication.

Delete certificates

When you delete a certificate, Kiteworks no longer trusts end user certificates signed by this certificate.

Prerequisite: If you have multiple certificates and you want to delete all of them, disable certificate-based authentication. Disabling certificate-based authentication automatically restarts the system. During this time, the system will be offline.

To delete a certificate:

1. Go to Application Setup > Authentication and SSO > Certificate-Based Authentication.
2. On the Certificate-Based Authentication tab, click the CA Certificates tab.
3. Select one or more certificates to delete, and then click the Delete Certificates button.

Logging

Activity

Set the audit log retention policy

The audit log retention policy lets you control how long event data in the audit log will be saved.

By default, event data is saved indefinitely to avoid potential data loss. You can adjust this setting to retain the data for a specific number of days, after which the data will be deleted from the audit log.

Recommendation: If you change the default setting, set a retention period of 365 days or more. A long retention period can give you enough data to find anomalies and avoid potential security incidents.

To configure the audit log retention policy:

1. Go to Application Setup > Logging.
2. On the Activity tab, enter the number of days you want to retain audit log data, and then click Save.

Tip: The number of file uploads and downloads displayed in the Activity Log section of the System Status page is derived according to the audit log retention policy.

Repositories Gateway

General Settings

Repositories Gateway sources

Kiteworks seamlessly connects to the following Repositories Gateway sources.

Table 46. Repositories Gateway sources

Source	Required server role	Note
Box	Repositories Gateway Cloud	End-users cannot add a new Box source; you must set this up for them to use.
Dropbox	Repositories Gateway Cloud	End-users cannot add a new Dropbox source; you must set this up for them to use.
File Share (CIFS / SMB / DFS)	Repositories Gateway On Premise	Content source is Windows File Shares/CIFS or Distributed File Systems (DFS).
Google Drive	Repositories Gateway Cloud	End-users cannot add a new Google Drive source; you must set this up for them to use.
Home Share	Repositories Gateway On Premise	The home directory of your operating system. End-users cannot add a new content source; you must set this up for them to use.
Manage Legal Content	Repositories Gateway On Premise	Content source is Manage Legal Content. Compatible with iManage.
OneDrive for Business	Repositories Gateway Cloud	End-users cannot add a new OneDrive for Business source; you must set this up for them to use.
SFTP Share	Repositories Gateway On Premise	Content source is an SFTP Share.

Table 46. Repositories Gateway sources (continued)

Source	Required server role	Note
SharePoint	Repositories Gateway On Premise	Content source is Microsoft SharePoint.
SharePoint Online	Repositories Gateway Cloud	Content source is Microsoft SharePoint Online.

Prerequisites

- Enterprise License.
- A server with an activated Repositories Gateway Cloud or Repositories Gateway On Premise role.

Kiteworks can support multiple servers with the Repositories Gateway role. This allows administrators to map each Repositories Gateway source to connect through a specific, perhaps dedicated, server with a Repositories Gateway role.

LDAP credentials are used on Repositories Gateway sources directly. When SSO or LDAP is turned on, Kiteworks database authenticated users are unable to see or use Repositories Gateway sources in the User View.

General settings

- Users can add Repositories Gateway sources.

  You can control users adding Repositories Gateway sources. This option, which is enabled by default, provides the flexibility of adding Repositories Gateway sources by both the administrator and the users. You can disable this setting if you want users to access only those Repositories Gateway sources which were added by the administrator. However, all existing Repositories Gateway sources will be accessible by end-users based on LDAP/SSO authentication or any other conditions set by the administrator.

  For large enterprises with hundreds of SharePoint sites and other Repositories Gateway sources, the end user self-service capability to set up connections to new sites saves a great deal of administrative overhead. However, for enterprises that want to tightly manage these connections, the ability to turn off this feature gives them the control they need.

- IP restrictions

  Set IP Address restrictions for both web users and mobile users.

  IP restrictions: Enter the IP addresses from which users have access to Repositories Gateway sources. The following formats are supported: 11.22.33.44, 11.22*, 11.22.33.44/24. Leave this field blank to indicate no restriction; use a comma between multiple entries.

  Apply restriction to mobile apps: When checked, the IP settings are also applied to mobile users.

Repositories Gateway SharePoint Online search setting

If your company uses Microsoft SharePoint Online for content sharing and collaboration, you can enable users to add their own links to SharePoint sites to their All Files page in the Kiteworks Web Application. You'll need to provide access to the SharePoint Online base URL from which users connect to SharePoint subsites.

When a user searches for a term in the Kiteworks Web Application, their search results will include the names of SharePoint Online sites containing a match for the term. The sites are listed under the SharePoint Sites tab on the search results page, along with options for adding or removing links to the sites.

Links appear as connections in the list of external sources listed on the All Files page and are visible only to the user who added them. When a user opens a connection, they'll be prompted to sign in unless they've already signed in to Office 365 or SharePoint.

Prerequisite: Enable the Repositories Gateway Cloud role on a node.

Rule: The ability to search SharePoint Online is available only to LDAP users. Non-LDAP users who perform a search won't see the SharePoint Sites tab at the top of the search results page.

To enable users to add links to SharePoint Online sites:

1. Go to Application Setup > Repositories Gateway > General Settings.
2. In the Repositories Gateway Search Setting section, configure the settings, and then click Save.

Table 47. Repositories Gateway Search settings

Setting	Description
Search center URL	The URL of the primary SharePoint Online site.
Token URI	The "OAuth 2.0 authorization endpoint (v1)" provided by the Office 365 configuration.
Auth URL	The "OAuth 2.0 token endpoint (v1)" provided by the Office 365 configuration.
OAuth Client ID	The Application ID provided by the Office 365 configuration.
Client secret	The "Key" provided by the Office 365 configuration.

Sources

Add Repository Gateway sources

The available Repositories Gateway sources are dependent on the Repositories Gateway roles you have in your deployment.

- Repositories Gateway Cloud role: Google Drive, Box, Dropbox, SharePoint Online, and OneDrive for Business.
- Repositories Gateway On Premise role: SharePoint, Windows Files Share, Home Share, and SFTP.

If the Repositories Gateway On Premise role is activated, end-users will be able to add their own Repositories Gateway On Premise sources. Repositories Gateway Cloud sources require configuration by an administrator for users to see these sources.

Notes:

- Google Drive and Box require the user's Kiteworks credentials to be the same as their credentials for Google Drive and Box. For the Dropbox, SharePoint Online, and OneDrive for Business, users are allowed to add only one personal/corporate account per Kiteworks account.
- In order for users to access Windows File Shares and Home Shares via Kiteworks, it is necessary for all users to have permission to traverse the top-level folder or mount point for the shares. Users need to traverse any root folders in order to access the subfolders or subshares containing their content.

To add a Repositories Gateway source:

1. Go to Application Setup > Repositories Gateway > Sources.
2. On the Sources tab, click Add Source.
3. On the Add Repositories Gateway Source page, select and configure the source you want to add.
   - Box
   - Dropbox
   - File Share (CIFS/SMB/DFS)
   - Google Drive
   - Home Share
   - Manage Legal Content
   - SharePoint
     - SharePoint Online and OneDrive for Business
     - Add OneDrive for Business to Kiteworks
     - Add SharePoint Online to Kiteworks
   - SFTP Share
4. Test the connection

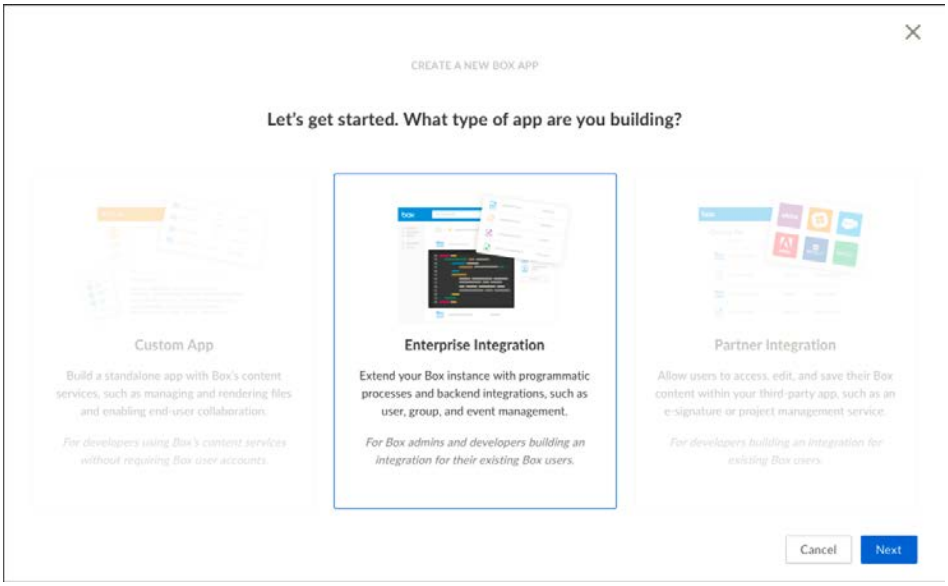
Box

Users can connect to their Box Business or Enterprise plans, but prior to doing this the administrator must create the app to enable connectivity.

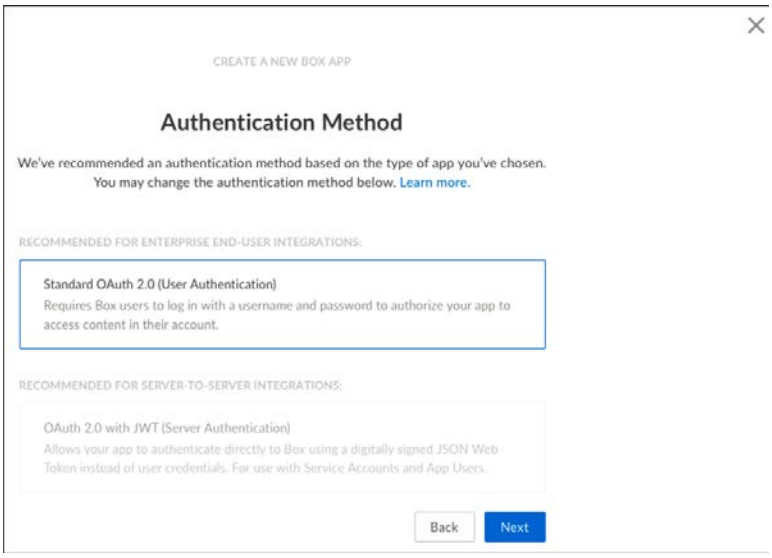
Note: Ensure that all the nodes with Repositories Gateway Cloud role in your cluster are able to reach www.box.com, api.box.com, upload.box.com and dl.boxcloud.com on destination port 443.

To configure the source in Box:

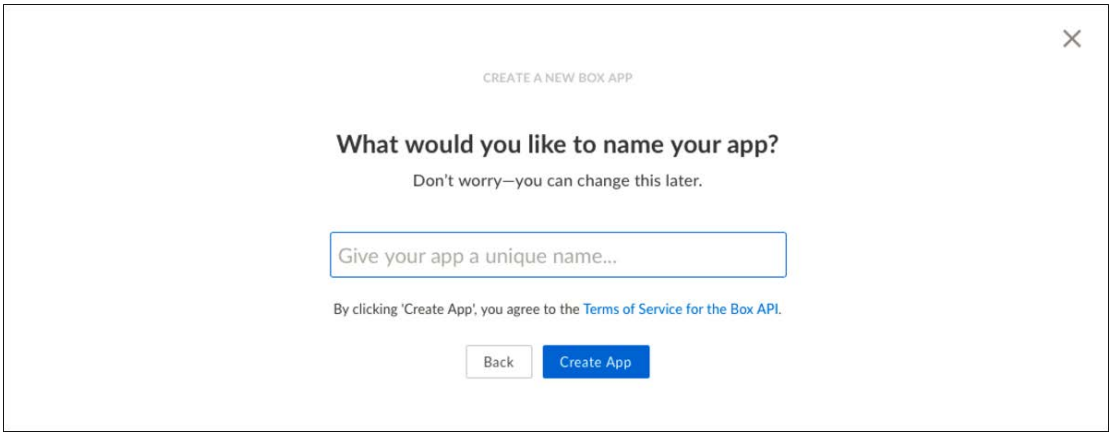
1. Go to https://app.box.com/developers/console/newapp in your web browser.
2. Choose Enterprise Integration and click Next.



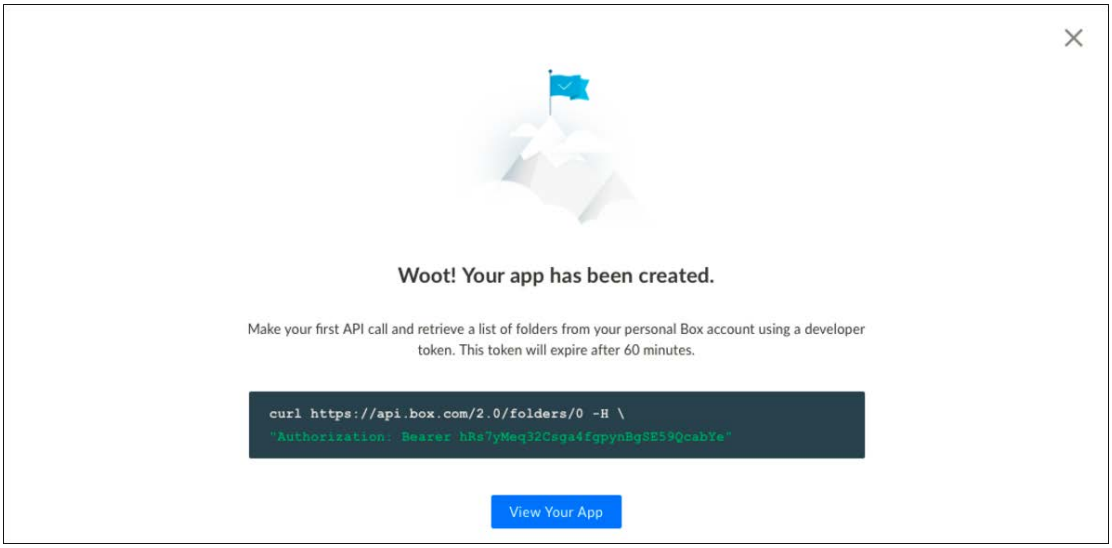
3. Choose Standard OAuth 2.0 (User Authentication) and click Next.



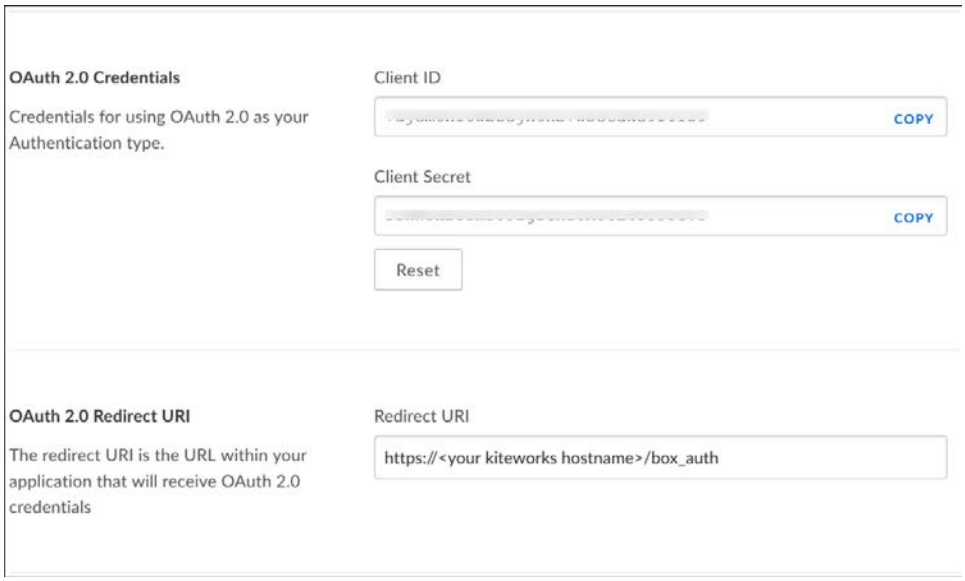
4 Type Kiteworks for <company name>, where <company name> is your company name in the App's name (it must be unique). Click Create App.



5 Click View Your App.

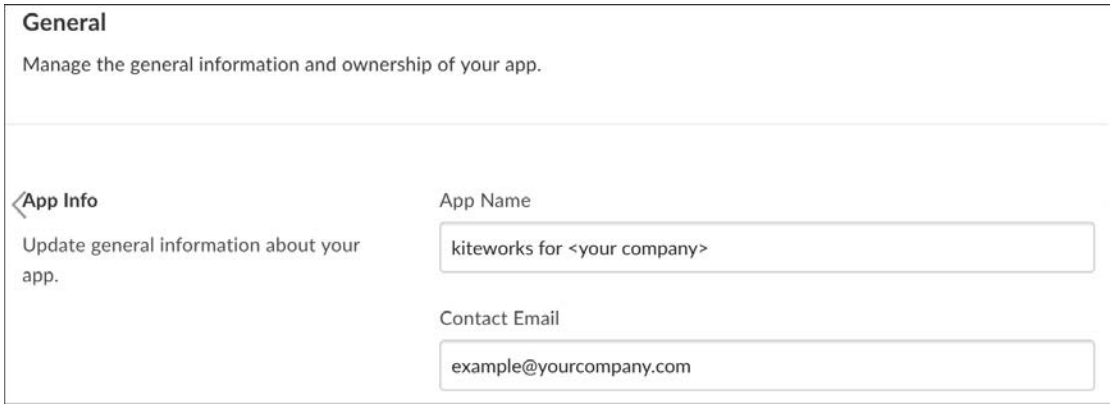


6 In the Configuration - OAuth 2.0 Redirect URI, in the Redirect URI field, enter https://<Kiteworks server address>/box_auth and click Save Changes.



7 Make a note of the Client ID and Client Secret fields. These codes will be used later.

8 In the General section, enter your support email address and click Save Changes.



To add the source in Kiteworks:

1 In the Kiteworks Admin Console, go to Application Setup > Repositories Gateway > Sources.

2 On the Sources tab, click Add.

3 Under Source Type, select Box. The following information must be added to the screen.

- Source Name – This name will be displayed on the Kiteworks Web Application for end-users, as well as the Repositories Gateway sources list on the Admin page.

  Note: The Site Name doesn't have to be identical to the Repositories Gateway sources name. For example, you can call it "Box", "Company's Box System", or anything you choose.
- OAuth Client ID – This information is what you collected previously.
- Client Secret — This information is what you collected previously.
- Description – This will display on the Repositories Gateway Source Admin page. It is used only to describe the connection.

4 Click OK.

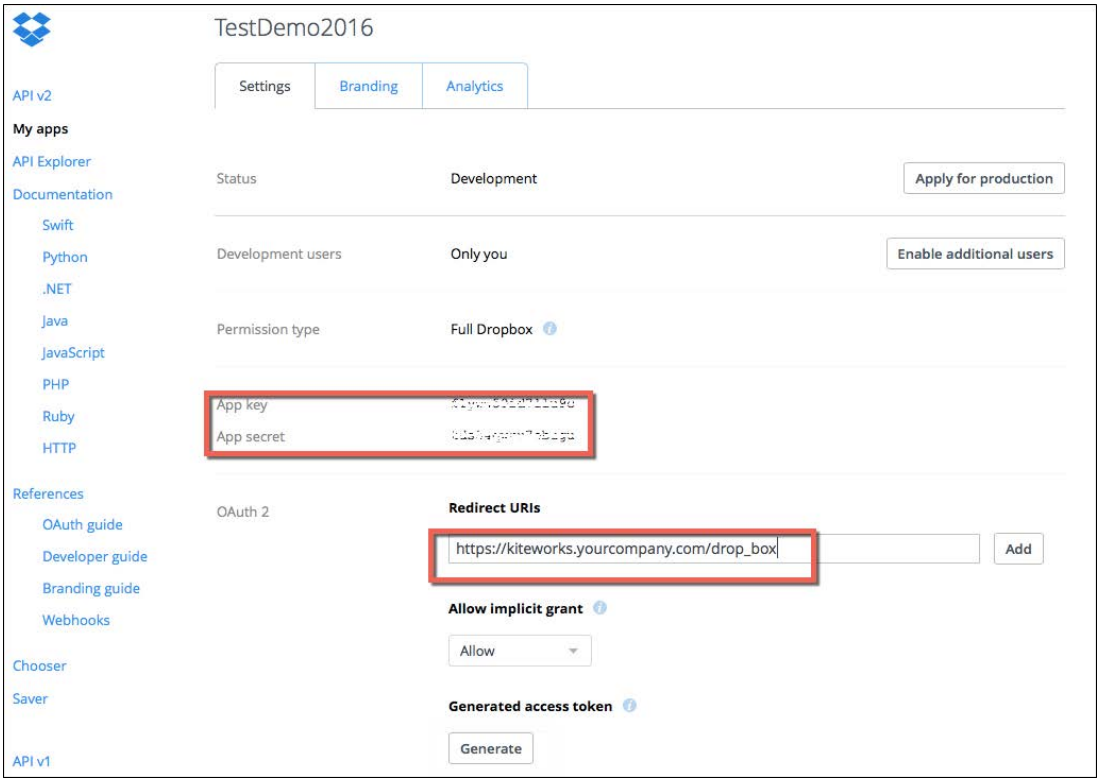
Dropbox

Before users can connect to Dropbox sources, you must create the Dropbox app and enable connectivity.

Prerequisite: Ensure all the nodes where the Repositories Gateway Cloud role is enabled are able to reach www.dropbox.com and api.dropbox.com on destination port 443.

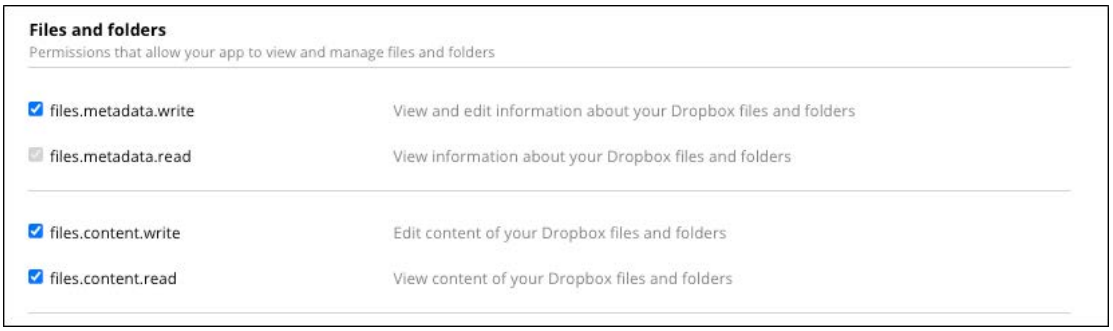
To configure the source in Dropbox:

1. Sign in to the DBX Platform developer portal at https://www.dropbox.com/developers.
2. In the portal, click "Create apps".
3. On the new app creation page, select "Scoped access", and then select "Full Dropbox" for the level of access you need.
4. Before entering a name for the app, review the naming guidelines in the developer branding guide to avoid any possible issues or conflicts. See https://www.dropbox.com/developers/reference/branding-guide.
5. Enter a name for the app, and then click "Create app".
6. On the next page, click Enable additional users. A popup displays informing you that 500 users can now connect with this client application. Click the link Learn more about production status requirements, if you need to add more users. Click Okay to continue.
7. On the Settings tab, under OAuth2, add the Redirect URI and click Add. The Redirect URI should be your Kiteworks URL followed by "drop_box".



Important: Make note of the App key and App secret. This information is required to continue with this procedure.

On the Permissions tab, ensure that all permissions in the Files and Folders section are selected.



To add the source in Kiteworks:

1. In the Kiteworks Admin Console, go to Application Setup > Repositories Gateway > Sources.
2. On the Sources tab, click Add Source.
3. From the drop-down list, select Dropbox.
4. Fill in the information as is prompted, including the App key and App secret.
5. Click OK. The source is now available to you in the Kiteworks Web Application.
6. Go to the Kiteworks Web Application, and then click the source created.
7. Sign in to Dropbox to authenticate to Repositories Gateway source.

   Notes:

   - You can select either App Folder or Full Dropbox, because both work.
   - Make sure that the popup blocker is not blocking the Dropbox login page. Safari does not inform the user that the popup blocker might be blocking a window. This could lead the user to believe that logging in is in process but the Login button remains grayed out and the user is unable to complete the setup process. Chrome and Firefox browsers notify if popups are blocked.

File Share (CIFS/SMB/DFS)

On the Add Repositories Gateway Source page under Source Type, select File Share. The following information must be added to the screen.

- Source Name – This name will be displayed on the Kiteworks Web Application for end-users, as well as the Repositories Gateway sources list on the Admin page.

  Note: The Source Name doesn't have to be identical to the Repositories Gateway sources name. For example, if the path is \\fileserver.example.local\Documents, the Source Name can be "Documents", "Corporate File Server", or anything you choose
- Source Path – The path to which this connection maps to the Repositories Gateway sources and retrieves the content; for example, \\ServerName\ShareName.
- Description – This will display on the Repositories Gateway Source Admin page. It is used only to describe the connection.

Notes:

If the connections from Kiteworks to your File Share is slow, a potential reason is the Windows server hosting the share is not able to resolve the hostname of the Kiteworks Repositories Gateway On Premise server. This can be fixed by adding an entry either in your DNS or in the hosts file on the Windows server. The hostname of the Repositories Gateway On Premise server can be seen on the System Setup > Locations page in the Kiteworks Admin Console.

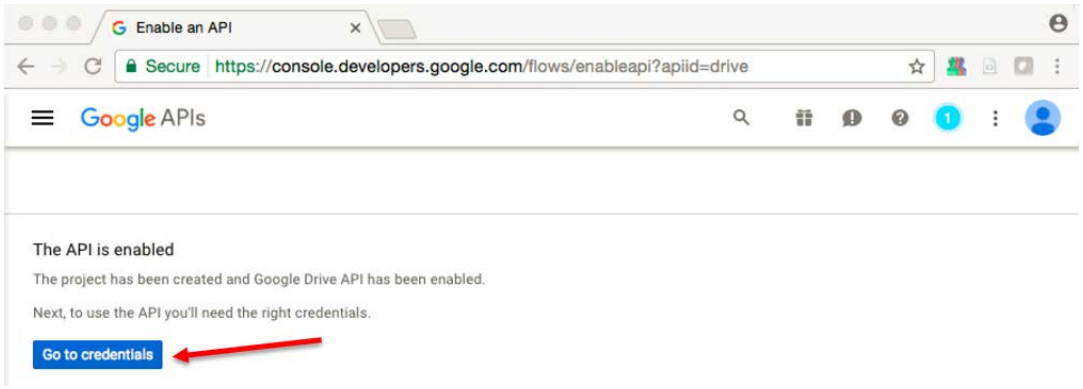
The Microsoft Search Center is only available with SharePoint, and to search a CIFS share these files need to be hosted locally in that SharePoint server.

Google Drive

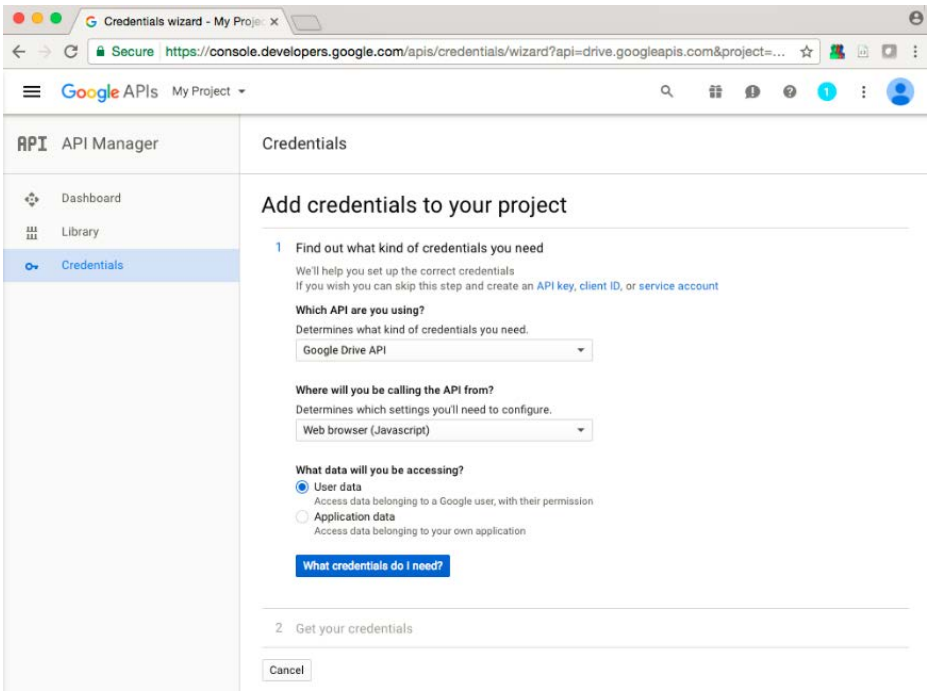
Users can connect to their Google Drive, but before they can do this, you must create the client app to enable connectivity.

To configure the source in Google Drive:

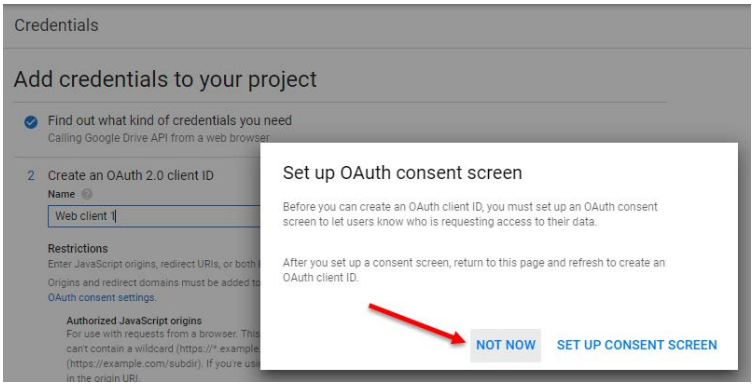
1. Go to https://console.developers.google.com/start/api?id=drive in your web browser.
2. Click the Create a project dropdown menu to select an existing project or create a new one. Click Continue.
3. Google Drive API will be automatically enabled for your project. Click Go to credentials.



4. On the Add credentials to your project page, the first step is to find out what kind of credentials you need. From the Which API are you using? dropdown menu, select Google Drive API. From the Where will you be calling the API from? dropdown menu, select Web browser (JavaScript) and from the What data will you be accessing? options, select the User data radio button. Click What credentials do I need?



5 A Set up OAuth Consent Screen displays. Click NOT NOW. Do not click SET UP CONSENT SCREEN in this window as you will need to Add credentials to your project.

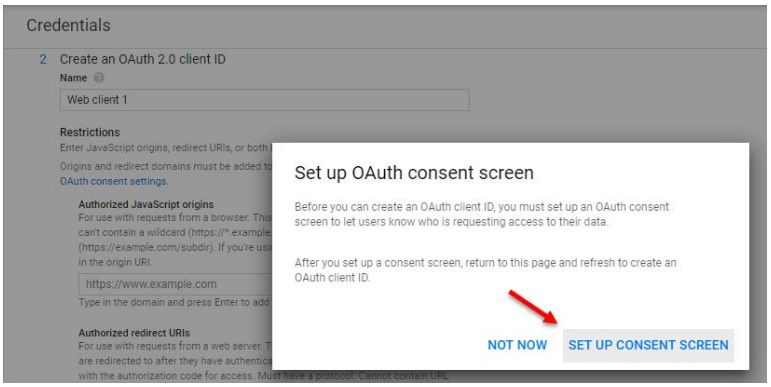


6 The Add credentials to your project page displays. Populate the Name, Authorized JavaScript origins and Authorized redirect URIs (which is the domain of your Kiteworks server) fields. Click Refresh.

For example: Authorized JavaScript origins: https://kiteworks.example.com

Authorized redirect URIs: https://kiteworks.example.com/gdrive_auth

7 On clicking Refresh, the Set up OAuth Consent Screen displays again. Click SET UP CONSENT SCREEN to go to the OAuth Consent Screen.



8 On the OAuth Consent Screen configure the following fields. Some of the fields are optional and can be left blank. Click Save. All the fields are explained on the OAuth consent screen page.

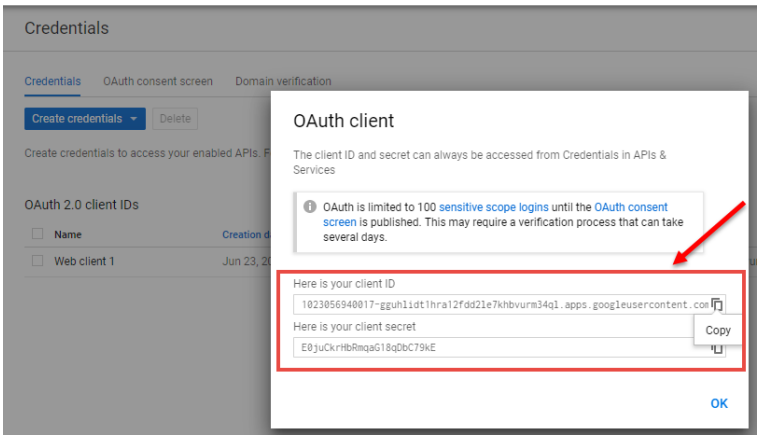
- Application type - Public or Internal
- Application Name
- Support email - (optional)
- Authorized domains - This domain needs to be a Top Private Domain.
- Application Homepage link - This link must be on an Authorized Domain.

9 The APIs Credentials window displays. Click the down arrow on the Create Credentials button and select OAuth Client ID.

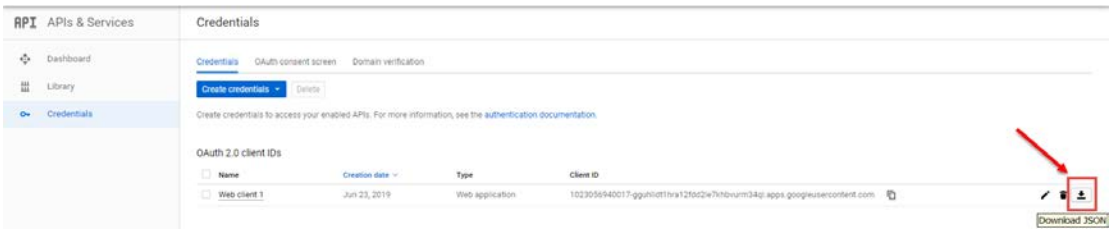
10 The Create OAuth client ID page displays. Populate the following fields and click Create.

- Application Type
- Name
- Authorized JavaScript origins: For example, https://kiteworks.example.com
- Authorized redirect URIs: For example, https://kiteworks.example.com/gdrive_auth\

The OAuth client ID and client secret are displayed. Copy both the IDs. These IDs can always be accessed from the Credentials page in APIs & Services. Click OK.



The Credentials page displays with the OAuth 2.0 client IDs listed. Click the download button to download the JSON file.



To add the source in Kiteworks:

1. In the Kiteworks Admin Console, go to Application Setup > Repositories Gateway > Sources.
2. On the Sources tab, click Add Source.
3. From the drop-down list, select Google Drive.
4. Next to "Config JSON File", click the "Choose file" button and then upload the JSON file you downloaded which contains all of the relevant information. The Token URI, Auth URI, OAuth Client ID, and Client Secret fields will be automatically populated. Etner the custom Source Name and Description.
5. Click OK.

Home Share

On the Add Repositories Gateway Source page under Source Type, select Home Share.

The following information must be added to the screen.

- LDAP – Select the required LDAP server from the drop-down list.
- User Home Directory Attribute – Enter the Home Directory Attribute within your LDAP setting, for example, `homeDirectory`.
- Click Save Changes.

Note: If users experience slow connections from Kiteworks to the Home Share, a potential reason is the Windows server hosting the share is not able to resolve the hostname of the Kiteworks Repositories Gateway On Premise server. This can be fixed by adding an entry either in your DNS or in the hosts file on the Windows server. The hostname of the Repositories Gateway On Premise server can be seen on the System Setup > Locations page of the Kiteworks Admin Console.

Manage Legal Content

Manage Legal Content Repositories Gateway source is compatible with iManage.

Requirement:

In order to make a successful connection, Kiteworks needs the iManage APIs to be available through "WorkSite Mobility Server for iOS". Version 9.3 R2 and 9.4 R2 of Worksite Server have the Mobility component built-in. Other versions (9.0 and above) need the Mobility server installed separately. To verify that the Mobility component is installed and running, please go to: http://<SERVERNAME>/Mobility2/MobilityService.svc/TestConfiguration?user=testuser

in your web browser, where <SERVERNAME> is the hostname/IP address of your Mobility server. You should get a success response similar to "TestConfiguration from testuser : SUCCEEDED".

On the Add Repositories Gateway Source page under Source Type, select Manage Legal Content.

The following information must be added to the screen.

- Source Name — This name will be displayed to Kiteworks end-users on web and mobile devices. It is recommended to set a name which is already familiar to the end-users.
- Source URL — URL to the iManage server where the mobility component is running. The format should be http://<hostname or IP address>/
- Description — Optionally used to describe the source.

SharePoint

On the Add Repositories Gateway Source page under

- Source Type, select SharePoint.

  The following information must be added to the screen.
- Source name — This name will be displayed on the Kiteworks Web Application for end-users, as well as the Repositories Gateway sources list on the Admin page.

  Note: The Source Name doesn't have to be identical to the Repositories Gateway source name. For example, if the path is http://sharepoint.example.com/marketing the Source Name can be "Marketing" or "SharePoint Marketing Site" or any other name you choose.
- Source URL — The URL to which this connection maps to the Repositories Gateway source and retrieves the content.

  For example, for the SharePoint site http://sp2010-demo/marketing/default.aspx the Connection URL should be http://sp2010-demo/marketing/default.aspx
- Description — This will display on the Repositories Gateway Source Admin page. It is used only to describe the connection.

Note: Make sure that the SharePoint server's full URL containing FQDN is added to the Alternate Access Mappings. To do this, go to the SharePoint Central Administration > System Settings > Configure alternate access mappings > Add Internal URL, and add the full URL containing FQDN of their SharePoint server as the internal URL.

SharePoint Online and OneDrive for Business

Before you can add SharePoint Online or OneDrive for Business sources via the Kiteworks Admin Console, a client application needs to be set up on Office 365. This client application allows Kiteworks users to authenticate their SharePoint Online sites and OneDrive for Business using OAuth authentication. The next section Configuring Client Application on Office 365 applies to both SharePoint Online and OneDrive for Business. Only one client application is sufficient to add both source types.

For the SharePoint Online and OneDrive connector to work, connectivity to the api.office.com services endpoint is required.

Access to login.microsoftonline.com is required for the SharePoint Online, OneDrive connector to work.

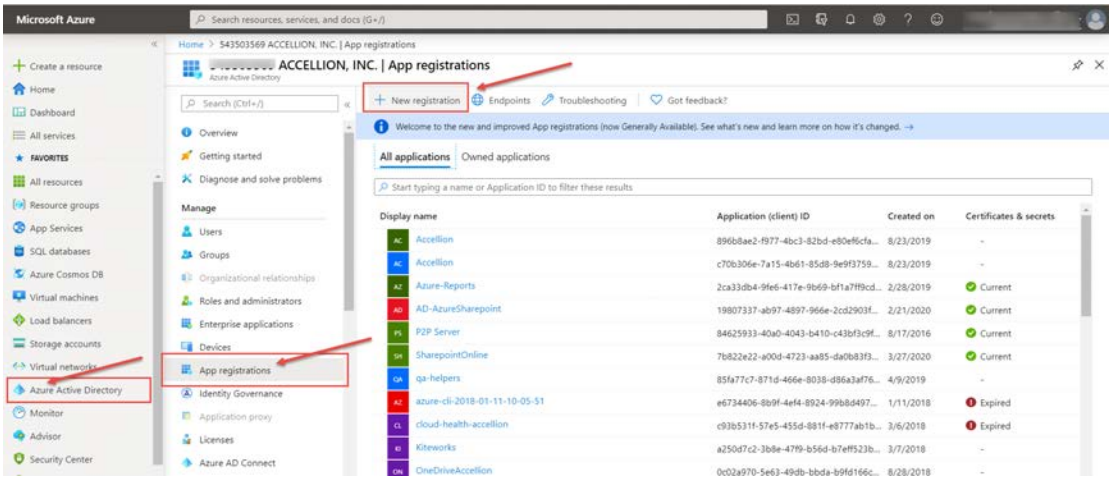
Configure Client Application on Office 365

Note: This section applies to the new "Microsoft Azure Portal" (https://portal.azure.com/).

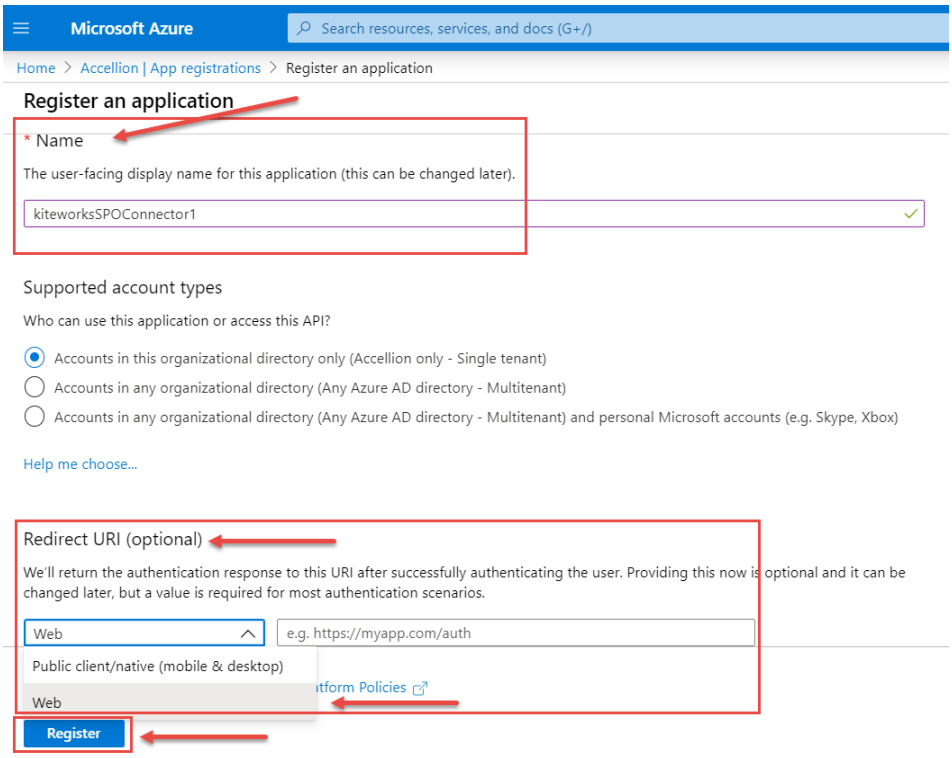
Perform the following steps to set up the App in the Azure AD:

1. Go to the Microsoft Azure Portal at https://portal.azure.com/
2. In the leftmost panel, click the Azure Active Directory service. If you do not see it on the panel, click More Services at the left bottom to look for it.
3. Make sure that the directory that has your SharePoint Online or OneDrive for Business users is selected. Click Switch directory and pick the right one if that is not the case.
4. Click App registrations in the panel that opens.

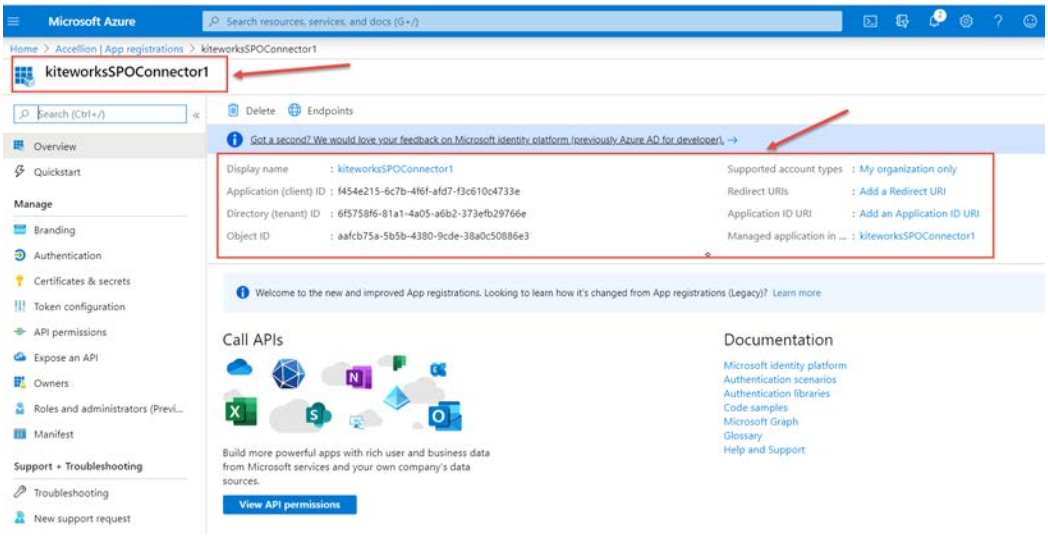
5 Click Azure Active Directory > App registrations > + New registration.



6 Name the application in the Name field and click Register.



7 The app is created and displays on the page. Configure the different fields of the app, such as, Supported account types, add a Redirect URI, or add an Application ID URI, etc.

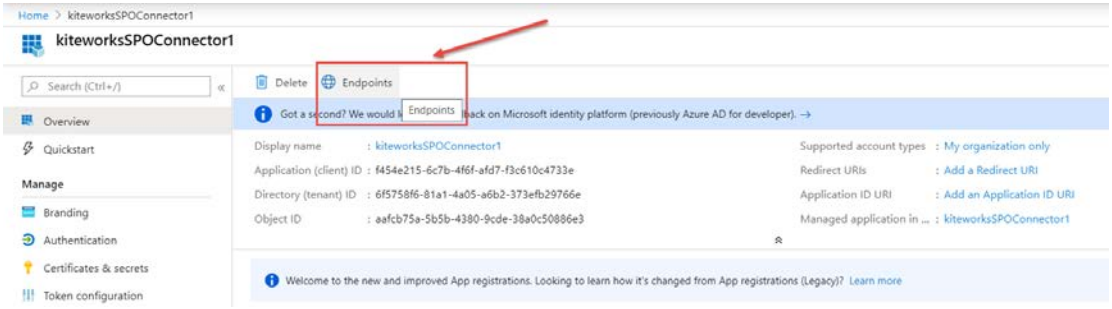


8 Go to the Kiteworks Admin Console and make sure Authenticate Via LDAP/AD is ON in the Authentication and Authorization > LDAP page.

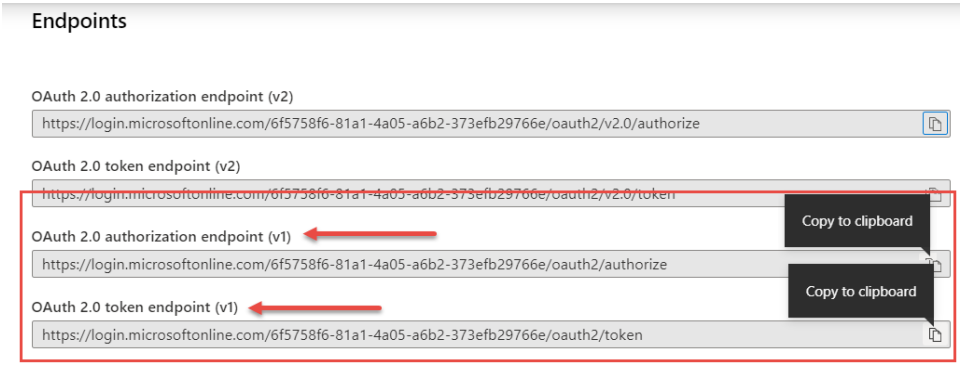
9 Go to Repositories Gateway > Sources , and then click Add Source to add an Repositories Gateway source. On the Add Repositories Gateway Source page, select a Source Type and type a name in the Source Name.

10 Enter the name of the URL of the SharePoint Online site, for example, https://kiteworksdemo-my.sharepoint.com/.

11 Go to the Microsoft Azure page and click Endpoints.

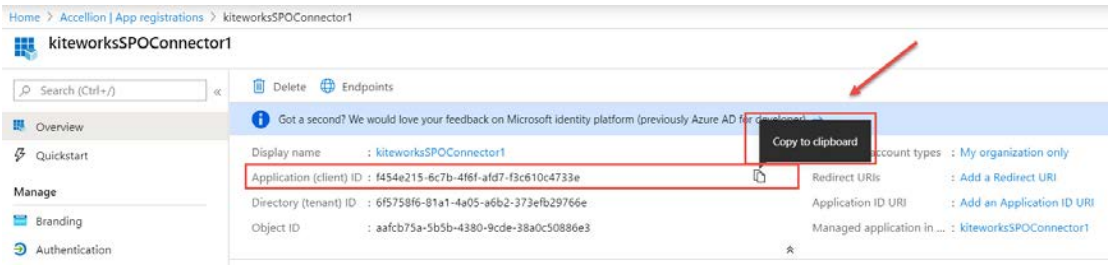


12 The Endpoints display. Copy the OAuth 2.0 authorization endpoint (v1) and OAuth 2.0 token endpoint (v1).

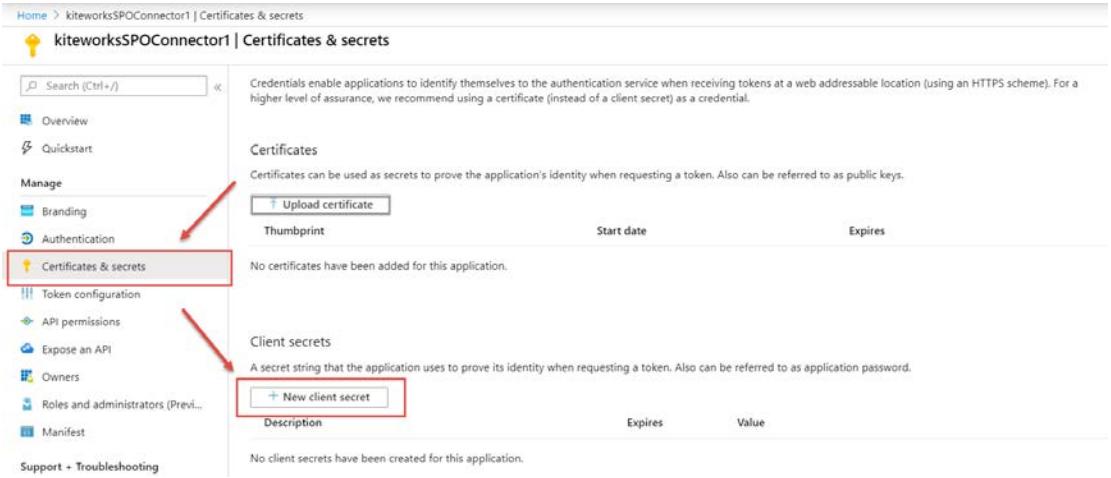


13 In the Kiteworks Admin Console, go to the Repositories Gateway source and paste the endpoints into the Token URI and Auth URI fields respectively.

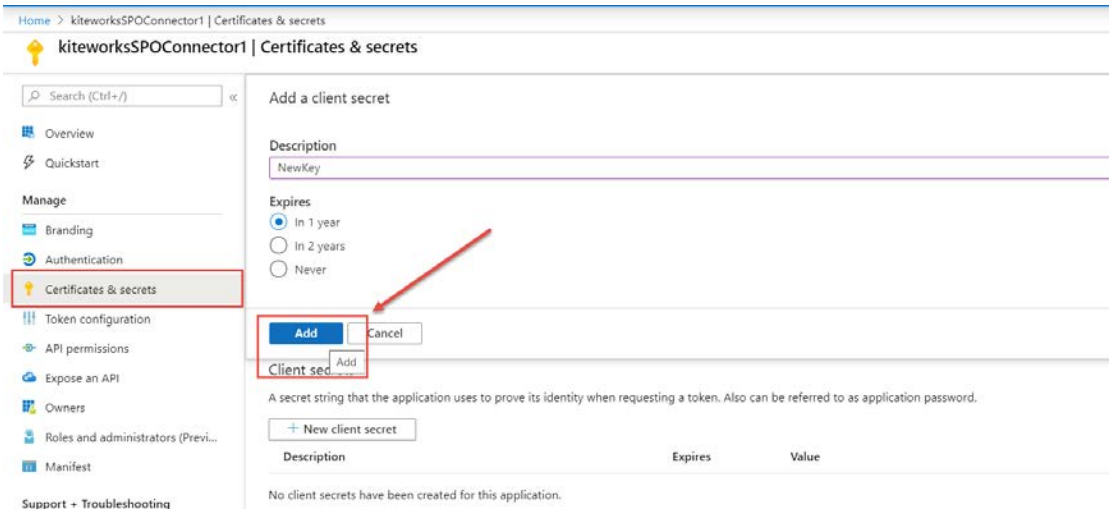
14 From the SSO connector, copy the Application Client ID. In the Kiteworks Admin Console, go to the Repositories Gateway source and paste it into the OAuth Client ID field.



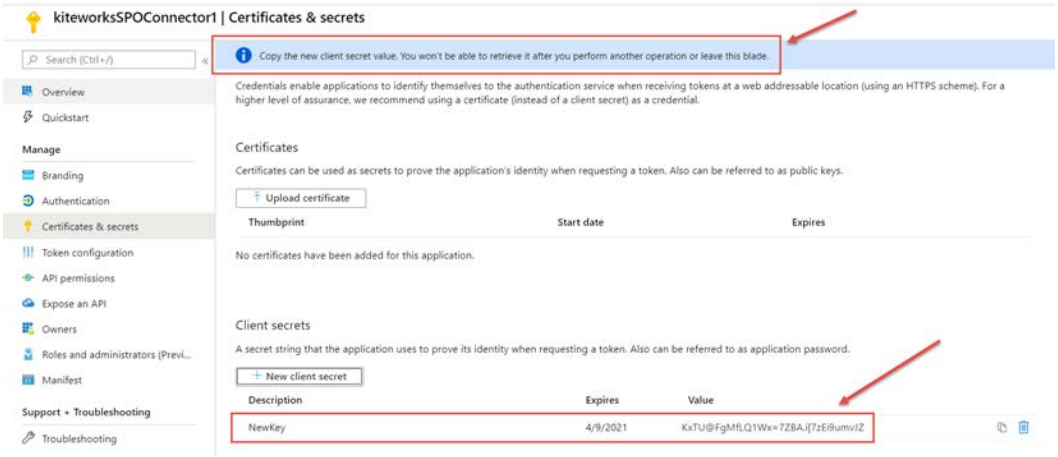
15 Next click Certificates & secrets and click New client secret



16 Enter the key Description and select the Duration. Click Add.

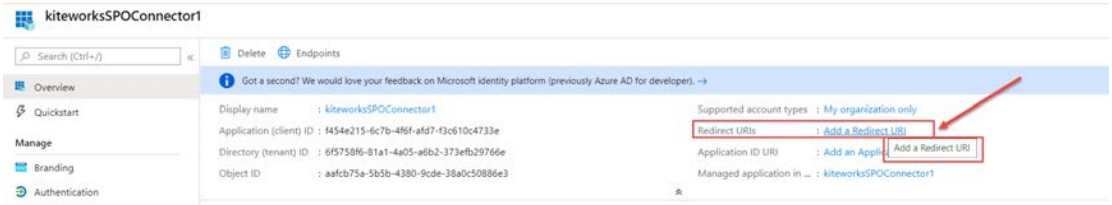


17 Copy the key value right after you save and paste it in a text file on your computer.

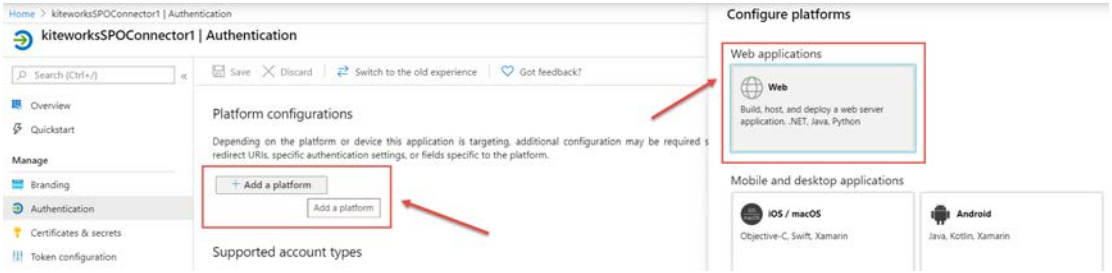


18 Paste the key in the Kiteworks Admin Console Client Secret field

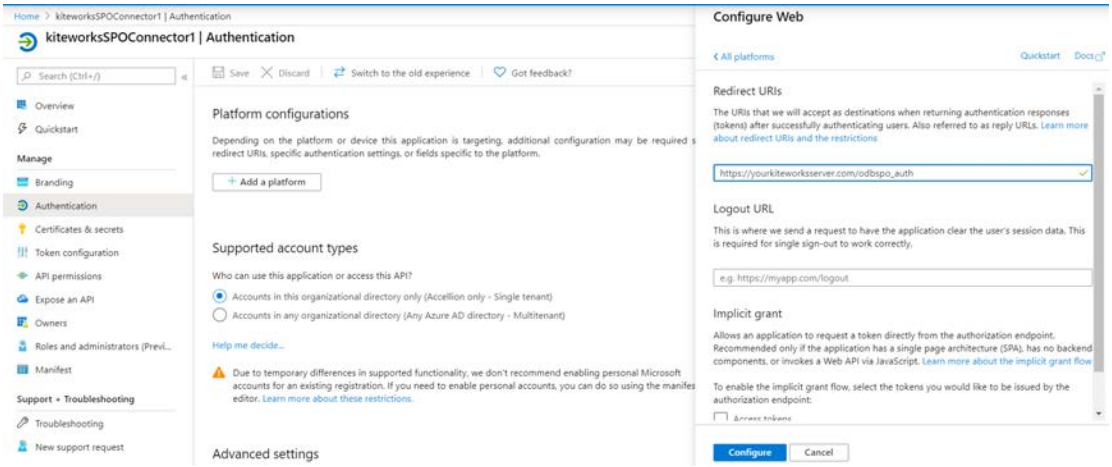
19 To configure the redirect URI, click Redirect URI.



20 Click Add a platform, and then click the Web button.

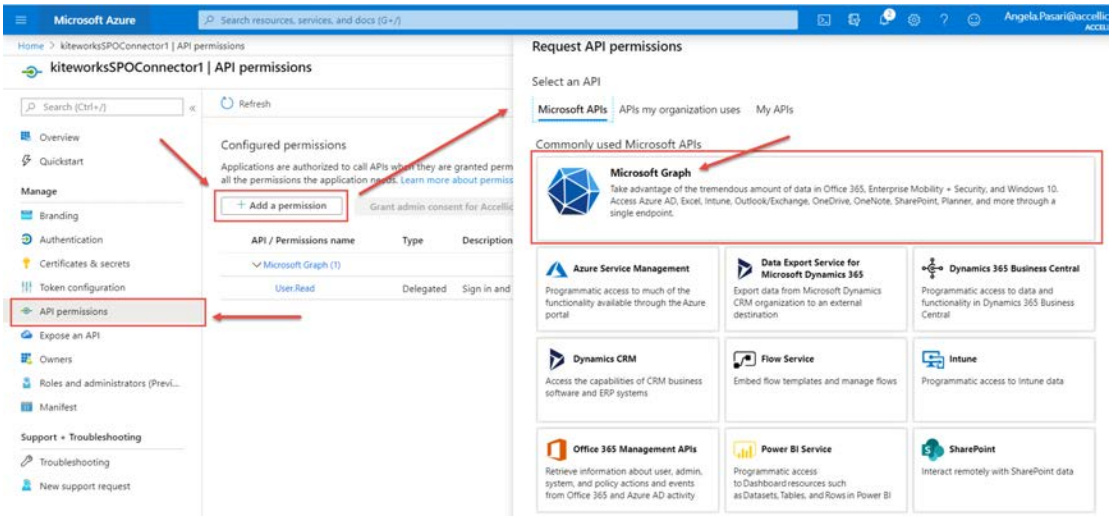


21 In the Redirect URI field, enter your URL to https://< Kiteworks server address>/odbspo_auth. Click Configure.

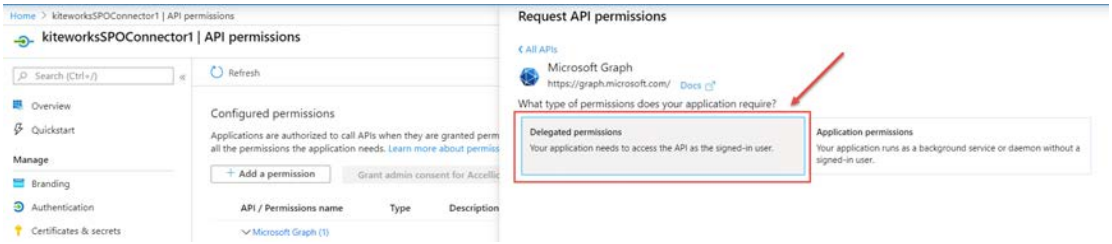


You will be notified that you have successfully updated the server.

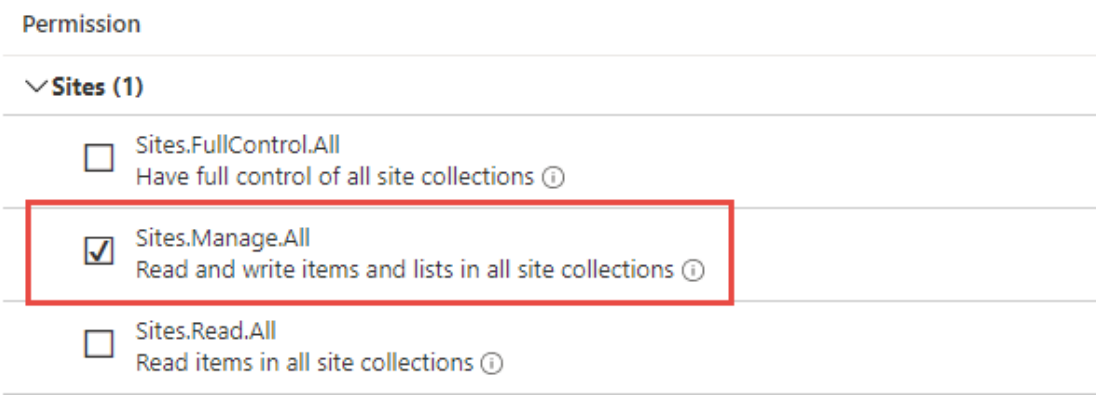
22 To add permissions, click Add permission > + Add permission. The Request API permissions panel displays. Click Microsoft Graph.



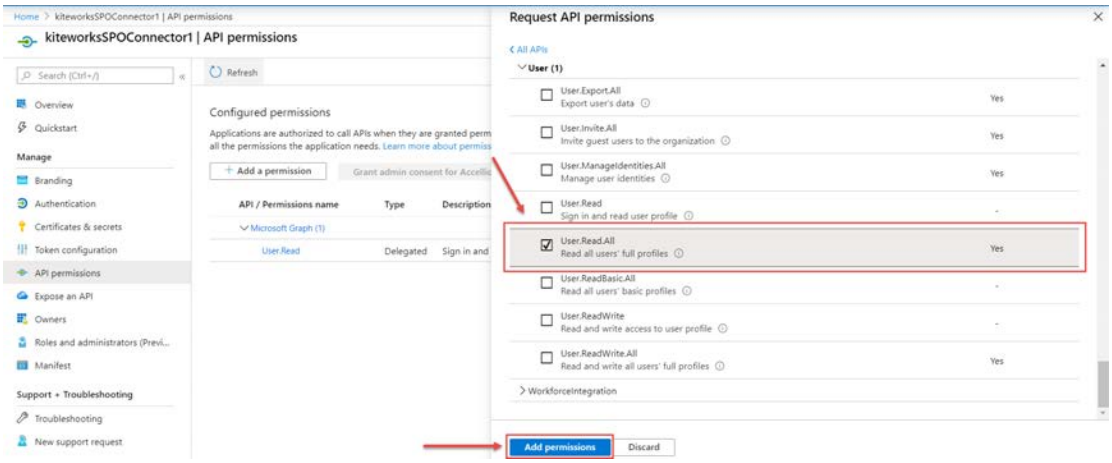
23 Click Delegated permissions.



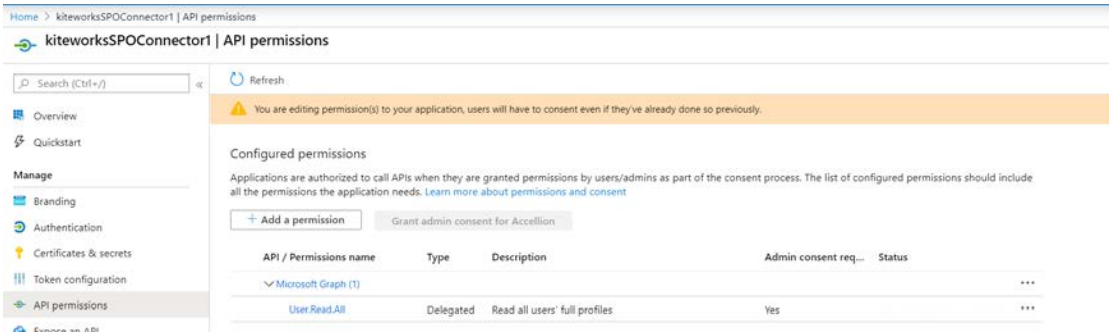
24 Select AllSites, and then click the Sites.Manage.All checkbox.



25 Click Users and check the User.Read.All checkbox. Click Add Permissions.



26 You will be notified that you are editing permissions.



Add OneDrive for Business to Kiteworks

In the Add Repositories Gateway Source window under Source Type select OneDrive for Business.

The following information must be added to the screen:

- Source Name – This name will be displayed on the Kiteworks Web Application for end-users, as well as the Repositories Gateway sources list on the Admin page.
- Source URL – Enter the OneDrive for Business URL.
- Token URL – Enter the "OAUTH 2.0 TOKEN ENDPOINT" copied from Office 365 configuration.
- Auth URL – Enter the "OAUTH 2.0 AUTHORIZATION ENDPOINT" copied from Office 365 configuration.
- Auth URI – Enter the "OAUTH 2.0 AUTHORIZATION ENDPOINT" copied from Office 365 configuration.

  Note: Make sure you use OAuth 2.0 authorization endpoint (v1).

- OAuth Client ID – Enter the "Application ID" copied from Office 365 configuration.
- Client Secret — Enter the "Key" copied from Office 365 configuration.
- Description – This will display on the Repositories Gateway Source Admin page. It is used only to describe the connection.

Notes:

- Access to the following URL:

  https://api.office.com/discovery/v1.0/me/services is required for the OneDrive connector to work.
- You are allowed to add multiple OneDrive for Business sources as long as they have different Source URLs.

Add SharePoint Online to Kiteworks

In the Add Repositories Gateway Source window under Source Type select SharePoint Online.

The following information must be added to the screen:

- Source Name – This name will be displayed on the Kiteworks Web Application for end-users, as well as the Repositories Gateway sources list on the Admin page.

  Note: The Source Name doesn't have to be identical to the Repositories Gateway sources name. For example, if the path is http://SPOnline.example.local, the Site Name can be "SPOnline, "Enterprise Workspace", or anything you choose.
- Source URL – Enter the URL of the SharePoint Online site.
- Token URI – Enter the "OAUTH 2.0 TOKEN ENDPOINT" copied from Office 365 configuration.
- Auth URI – Enter the "OAUTH 2.0 AUTHORIZATION ENDPOINT" copied from Office 365 configuration.

  Note: Make sure you use OAuth 2.0 authorization endpoint (v1).

- OAuth Client ID – Enter the "Application ID" copied from Office 365 configuration.
- Client Secret — Enter the "Key" copied from Office 365 configuration.
- Description – This will display on the Repositories Gateway Source Admin page. It is used only to describe the connection.

Note: The Microsoft Search Center is only available with SharePoint, and to search a CIFS share these files need to be hosted locally in that SharePoint server.

SFTP Share

An SFTP Share can be added to Repositories Gateway sources providing connectivity to SFTP data sources using the Repositories Gateway On Premise role. The connector is added and provisioned by the administrator. You can select one or more User Profiles and make the SFTP share available to the chosen user profile(s). One the connector is available to a user the SFTP source type displays as a menu option and the user can access it without entering any credentials since the administrator configures either Password or SSH Key based authentication for the user to sign into their SFTP shares and access content.

In the Add Repositories Gateway Source window under Source Type select SFTP Share.

The following information must be added to the screen.

- Source Name — This name will be displayed to Kiteworks end-users on web UI as well as in the Repositories Gateway sources list. It is recommended to set a name which is already familiar to the end-users. In this example the Source Name is demo_sftp.
- Description — Optionally used to describe the Repositories Gateway source.
- Source URL — URL of the SFTP server. The format should be sftp://<hostname or IP address>/
- Authenticate Using Password — For authentication using the password, the user name and password to access the SFTP Connector is set by the administrator. This set user name and password is shared by the selected User Profile group and is not your LDAP credentials.
  - Username — The user name set by the administrator for selected User Profiles.
  - Password — The password set by the administrator for selected User Profiles.
- Authenticate Using SSH Key — Add the SFTP Share and select SSH Key based authentication. Copy the private key into the text area provided for the key. The key must be in PEM (Privacy Enhanced Mail) format.
  - Username — Enter the user name of the person.
  - SSH Key — Enter the SSH key in this field. You can copy and paste the private key that is set for the SFTP server. The public key must first be copied to the SFTP server. If the server is non-Kiteworks,

use the `ssh-copy-id` utility to copy the public key. If the server is a Kiteworks SFTP server, copy the SFTP public key on User's Settings page.

- Passphrase — Type the passphrase associated with the SSH key. This can also be given while generating the key. This is optional field which is set by the administrator.

- User Profiles — Click Choose User Profiles to select the user profiles you would like to access the SFTP Connector. See the Clients and Plugins tab to enable SFTP access for a user profile.

Configure all the fields and click Save. Switch to the web application and refresh the page. The SFTP Share by the name of demo_sftp will be added.

Note: The SFTP Connector requires the Repositories Gateway On Premise role to be enabled. If the role is not activated, a message displays asking you to enable it: Please activate a Repositories Gateway role in the cluster at the Locations page.

Test the connection

Follow these steps to test the connection between Kiteworks and the Repositories Gateway source.

1. From the list of sources click the Repositories Gateway sources that was just added.
2. Enter the username and password. This is used to test the new Repositories Gateway source connection.
3. Click Test to test the connection. If the connection is successful, the following message is displayed:

   If there are errors, check if your account has access to the Repositories Gateway source and if the username and password are correct.

Troubleshooting

Connection Issues – If a user reports a problem connecting, or that SharePoint resources are not available, check the following:

- Verify the account they're using has access to those SharePoint resources. It could be they have multiple accounts, and the account they're signing in with doesn't have access to those resources.
- Check their user account via the Admin dashboard, Repositories Gateway sources. Click the source and enter that user's credentials in the test section to verify that the connection succeeds.

Integrations

Microsoft

Kiteworks integration with Microsoft

Kiteworks supports integration with Office Web Application on-premise. An administrator can integrate Kiteworks with Office Web Application systems running on-premise allowing users to open and edit Microsoft Office documents in Office Web Application on the Web, mobile devices and the desktop.

To configure the Web, mobile and desktop integrations, go to Application Setup > Integrations.

Web integration with Microsoft Office Online

Web integration with Office Online enables users to view and edit Microsoft Excel, Microsoft PowerPoint, and Microsoft Word files directly in the browser. Two types of integration are available for Office Online:

- Office 365
- Office Online Server (WOPI) or Office Web Application (OWA)

Mobile integration with Office Online

Mobile integration with Office Online enables users to use Microsoft Office mobile applications to create new documents or edit and save documents back from Kiteworks on iOS and Android devices.

Files downloaded, as well as those created on the device, are encrypted while at rest with iOS 256-bit AES.

Turning on the "Enable iOS (Document Provider)" option enables iOS8 and above-based devices to use third-party applications such as Microsoft Excel, Microsoft PowerPoint, and Microsoft Word to view Kiteworks as a source and to view, edit, and save back files.

Desktop integration with Microsoft Office Desktop

Desktop integration with Office Online enables users to use Microsoft Office desktop applications to create new documents or edit and save documents back from Kiteworks using MS Office applications installed on the desktop.

Integration with Microsoft Office Online

To integrate with Office 365, Kiteworks uses a proxy server. This server redirects traffic to Office 365 and does not cache or capture user data.

Prerequisites:

- The Kiteworks installation must be publicly accessible via its application URL.
- The Kiteworks configuration for Microsoft integrations must be enabled.
- Users expecting to use the functionality must be licensed with an Office365 online account with online editing.

Enabling Office 365

To enable Office 365:

1. Go to Application Setup > Integrations > Microsoft/WOPI > Web.
2. In the Integration Type list, select Office365.
3. Turn on the Enable O365 switch, and then click Save.

   Result: The configuration is complete and stored in database, and the Discovery URL for O365 is activated. If the O365 connection is successful, the connection status indicator displays "OK". If the server is not reachable by O365, or if there are any other issues with the server, the O365 Connection Status displays "ERROR".

Once properly configured, Kiteworks Web Application users have the option to edit Microsoft Office files using Microsoft Excel, Microsoft PowerPoint, and Microsoft Word on the web. If the option is not available to users, either O365 was not configured properly or there is a connection issue.

Note: Kiteworks needs to use a proxy server configured for productivity.kwpubservices.com to route traffic to O365 for online editing. This is necessary to provide a single URL to O365 for whitelisting.

A license is needed for users to be able to use Office 365 which enables them to edit documents online with Office 365.

Enabling Office 365 On-Premise

Prerequisites:

- A functioning OWA server with a valid domain and SSL certificate.
- A functioning Kiteworks server with a valid domain and a valid SSL certificate.
- Access from all browsers that need to access this feature to the OWA domain.
- Access from the OWA server to the Kiteworks domain.

To enable Office 365 On-Premise:

Perform the following steps to configure the Kiteworks installation with an on-premise OWA server.

1. Go to Application Setup > Integrations > Microsoft/WOPI > Web.
2. In the Integration Type list, select Office Web Application (OWA).
3. In the Discovery URL box, enter the domain name of the OWA server "/hosting/discovery". For example, http://acc.blue/hosting/discovery.
4. Click the Test URL button. If the test is successful, a "Discovery URL test successful" message is displayed.
5. Click the Save button to activate the feature for all users.

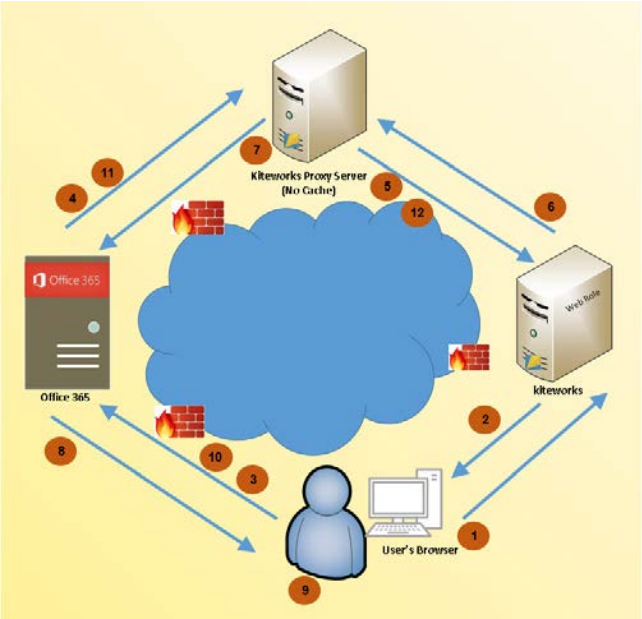
Note: DNS entries can be whitelisted for HTTPS traffic from the Kiteworks proxy. Whitelisting IP addresses are subject to change.

How Office 365 works in Kiteworks

The following steps give a high-level flow of how a document is accessed, edited and saved in the Kiteworks Web Application using Office 365. All connections are done through HTTPS using Port 443.

1. In the Kiteworks Web Application, a user browses to a Microsoft Word file.
2. The user selects the file, clicks Edit Content, and then selects the Microsoft Word for the Web.
3. Kiteworks responds to redirect to O365 Web Edit URL + a one-time use token.
4. The user's browser redirects to O365 Web Edit URL in the cloud.
5. O365 requests the Microsoft Word file using a token from the Kiteworks proxy. For example, productivity.kwpubservices.com.
6. The Kiteworks proxy relays the request to the Kiteworks instance.
7. The Kiteworks instance responds with the Microsoft Word file requested from O365 in the cloud.
8. The Kiteworks proxy relays the Microsoft Word file to O365.
9. O365 responds to the user with Web Editor + the Microsoft Word file.
10. The user edits the Microsoft Word file.
11. The Microsoft Word fileis automatically sent via O365.
12. O365 sends the Microsoft Word file to the Kiteworks proxy. For example, productivity.kwpubservices.com.
13. The Kiteworks proxy relays the saved Microsoft Word file to the Kiteworks instance.

When the user closes the Microsoft Word editor, the Microsoft Word file is saved one last time.



Note: DNS entries can be whitelisted for HTTPS traffic from the Kiteworks proxy. Whitelisting IP addresses are subject to change.

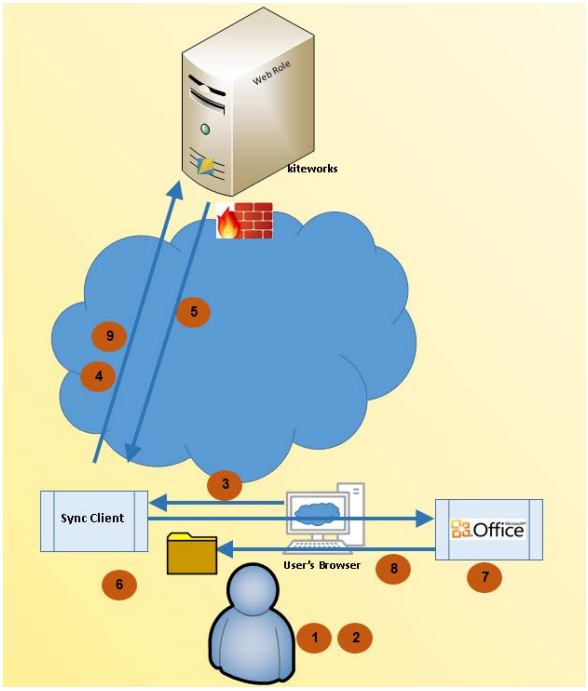
How Desktop Edit works

Desktop Edit integration with Kiteworks requires the sync client to be installed on the desktop but it does not require any server integration.

Requirement: If a proxy server on the end user computers is set up for Desktop Edit then it needs to be configured to exclude "desktopedit.kwlocalhost.com" and "127.0.0.1".

The following steps give a high-level flow of how a document is accessed, edited and saved in Kiteworks using Desktop Edit. All connections are done through HTTPS using Port 443.

1. The user browses to a Word file in Kiteworks. The browser gets a one-time User Token and a File ID from kiteworks.accellion.com.
2. The user invokes Desktop Edit of file from the web application.
3. The web browser calls the Desktop Edit/Sync Client. This Sync Client takes the request, the one-time User Token and the File ID and makes the request to download the file and opens it with MS Office.
4. Desktop Edit calls to Kiteworks for the file.
5. The file is downloaded.
6. Desktop Edit invokes the Microsoft Office product.
7. The user makes edits.
8. The edited file is saved. When the file is saved, it is saved back to the Sync Client.
9. The Sync Client uploads the file back again to kiteworks.accellion.com



Kiteworks Office Online Server (On-Premise)/Office Web Application (OWA)

The following steps are required to configure a Kiteworks on-premise deployment to connect to Office 365 on-line:

1. The Kiteworks system should be exposed to the outside world via a URL that's publicly accessible and addressable enabling anyone from anywhere with a with public Internet connection to connect to that Kiteworks system.
2. The Kiteworks system should be able to communicate with the end-users and the office online server.
3. A legitimate SSL certificate is required for both the Office Online Server and the Kiteworks server.

You will need to provide a Discovery URL of your Office Web Application server to configure the Web integration with Kiteworks. After populating the field, click Test to make sure the URL provided is correct. An error will display if the URL provided is not correct.

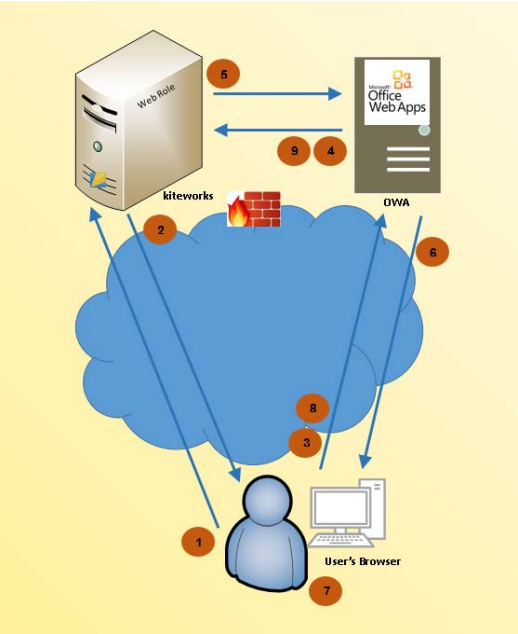
Note: The connectivity to an on-premise Office Online server needs to be accessible from the WEB servers.

How Kiteworks Office Online Server (On-Premise) or OWA Works

The following steps give a high-level flow of how a document is accessed, edited and saved in Kiteworks using OOS and Office Web Apps server. All connections are done through HTTPS using Port 443.

1. The user browses to a Word file in Kiteworks. A request is made to Web-edit a document. For example, "Document XYZ" from the user to Kiteworks.
2. Kiteworks responds to redirect to Office Web Apps server Web Edit URL to access the Kiteworks document + a one-time use Token.
3. The user's browser redirects to Office Web Apps server Web Edit URL.
4. Office Web Apps server requests document data using token from Kiteworks.
5. Kiteworks responds back with document content.
6. Office Web Apps server responds with Web Editor + Document XYZ

7 The user makes edits.
8 Document XYZ is saved.
9 Office Web Apps server saves Document XYZ to Kiteworks.



SMS Service

Configure SMS services

The Application administrator can configure the Kiteworks service to work with an external SMS service so that Kiteworks can send SMS messages to users or phone numbers.

Note: SMS Service changed events are logged in Activities

You can select from the following SMS Service Provider options:

- Twilio
- Sinch
- Other (any other SMS service)

Configure Twilio and Sinch SMS services

Perform the following steps to configure Twilio or Sinch SMS service settings:

1 Go to Application Setup > Integrations > SMS Service.
2 Select the SMS Service Provider for sending SMS messages.
3 Configure the settings.
   - Twilio Account SID/Sinch Service Plan ID: Enter the Account SID or the Service Plan ID.
   - Twilio Auth or Sinch Token: Enter the token.
   - From Number: Enter the sender's phone number.
4 Click Save to save the settings.

5 Click Test SMS Service to test the SMS settings. The Test SMS Settings window displays. Enter the Recipient Number and the Message. Click Send SMS to test the service.

6 Click Save to save the settings.

Configure other SMS services

Besides Twilio and Sinch, other SMS gateway providers are supported. Select Other from the dropdown menu of SMS Service Provider to configure any other SMS service. The parameters are explained below.

Table 48. SMS service settings

SMS service settings	SMS configuration template: A list of tested configuration templates are available which can be used by the administrator to populate the configuration. Select any one template from the dropdown menu options.
SMS service account	Account ID - Enter the Account ID. This is your account identifier as registered at your SMS service provider. This value will be used to replace all occurrences of %%account_id%% string placeholders. Account key/token/password - Enter the account key or token or a password. This is your account key, or token or password as found at your SMS service account configuration. This value will be used to replace all the occurrences of %%account_key%% string placeholders. Sender number/name - Enter the sender's phone number or name. Your SMS service provider may not need this setting. This value will be used to replace all occurrences of %%sender%% string placeholders. Some SMS service providers, for example, Sinch and CM Telecom/SMS Trade expect a (string) sender name instead of a sender phone number.
HTTP settings	HTTP request method - The HTTP method to use for calling the SMS service API. Select POST and GET from the dropdown menu options. API URL - The URL for calling the SMS service API. You can use the following placeholders which will be replaced with the correct values before the API request is made: • %%account_id%% • %%account_key%% • %%sender%% • %%recipient%% • %%message%% HTTP authentication header - The HTTP authentication header to use when calling the SMS service API. If you enable this, the value of the account ID and account Key, token or password will be used as the HTTP user name and password. HTTP request header- The HTTP authentication header to use when calling the SMS service API. If you enable this, the value of the account ID and account key, token or password will be used as the HTTP user name and password. Select None, Basic Authentication or Digest Authentication.

Table 48. SMS service settings (continued)

HTTP request content	Successful response detection - Specify the Content type of the HTTP request. • If you choose Form, a Content-Type header application/x-www-form-urlencoded will be added to the request body with the proper encoding. • If you choose JSON, a Content-Type header application/json will be added to the request header and the content data will be added to the request body with the proper encoding. For the JSON type, all content data value must be a simple scalar value. For a complex JSON structure, please use Other instead. • If you choose Other, please fill in the content template and add a correct Content-Type header at the HTTP Request Header section. Content Data - Data to be included in the request body, example: name: value. You can use the following placeholders which will be replaced with the correct values before the API request is made: • %%account_id%% • %%account_key%% • %%sender%% • %%recipient%% • %%message%%
HTTP response handling	Successful response detection: Specify a method to use for detecting a successful API response.
Additional options	Country code prefix - A prefix to be added to the country code of the recipient number, for example, some SMS service providers expect only '00' instead of '+' as a country code prefix. If you leave this blank, the default '+' prefix will be used. Disable server certificate verification - Check this box to disable the SSL certificate verification while connecting to an SMS gateway.

Error reporting for SMS messages

When the SMS Service fails to send SMS messages, an alert is posted on the Admin Dashboard indicating the number of failed messages. The audit log displays the SMS service error and once the SMS service setting is fixed, the log shows that the SMS message(s) was sent and the notification on the Admin Dashboard disappears.

Licenses

View and upload licenses

The Kiteworks Licenses page displays information about your license including your license package, license key, and license expiration date. It also lists the features that are enabled on the system and the corresponding number of allocated user licenses.

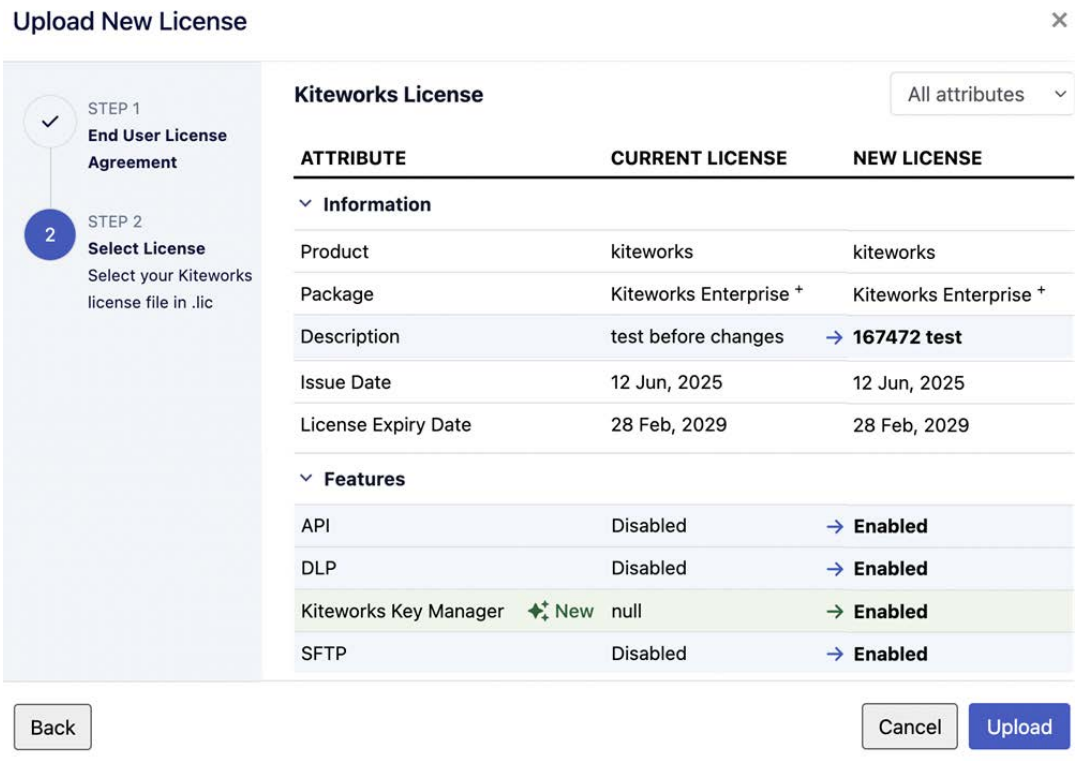
- To view your Kiteworks license, go to Application Setup > Licenses > Kiteworks License.
- To view the list of third party libraries shipped with Kiteworks applications and plugins, go to the Third Party Licenses tab.

Upload new licenses

When uploading a new license, you will need to review and sign the End User License Agreement (EULA). During the upload process, a comparison table shows the differences between the current and new license, highlighting differences such as feature changes or capacity adjustments.

To upload a license:

1. Go to Application Setup > Licenses > Kiteworks License, and then click Upload New License.
2. Review the End User License Agreement.
3. Enter your first and last name to sign the license agreement, and then click Accept.
4. On the Upload New License page, select the license file, and then click Upload.
5. Review the license attribute comparison table showing differences between the current and new license, and then click Upload.



Result: The license gets uploaded to the server and relevant information is extracted for display on the license page.

5005LC and 422LC license error codes

5005LC: This error code is returned when the license expires.

422LC: This error code is returned when there are insufficient licenses available.

The 5005LC License Error Code also displays if the following two scenarios occur:

- If Self Registration or LDAP Integration is enabled, and a new user who does not have a license tries to self-register, then the user will see the following error code and message.
- If an existing user tries to invite a user or send files to a user that would need a license and if licenses have run out, then the user will see the error message "There was an internal error (5005LC)".

The other license error codes are:

- 5001: License Expired
- 5002: Feature Expired
- 5003: Licensing Restriction Exceeded
- 5004: Feature not licensed
- 5005: Licensed User Limit Exceeded

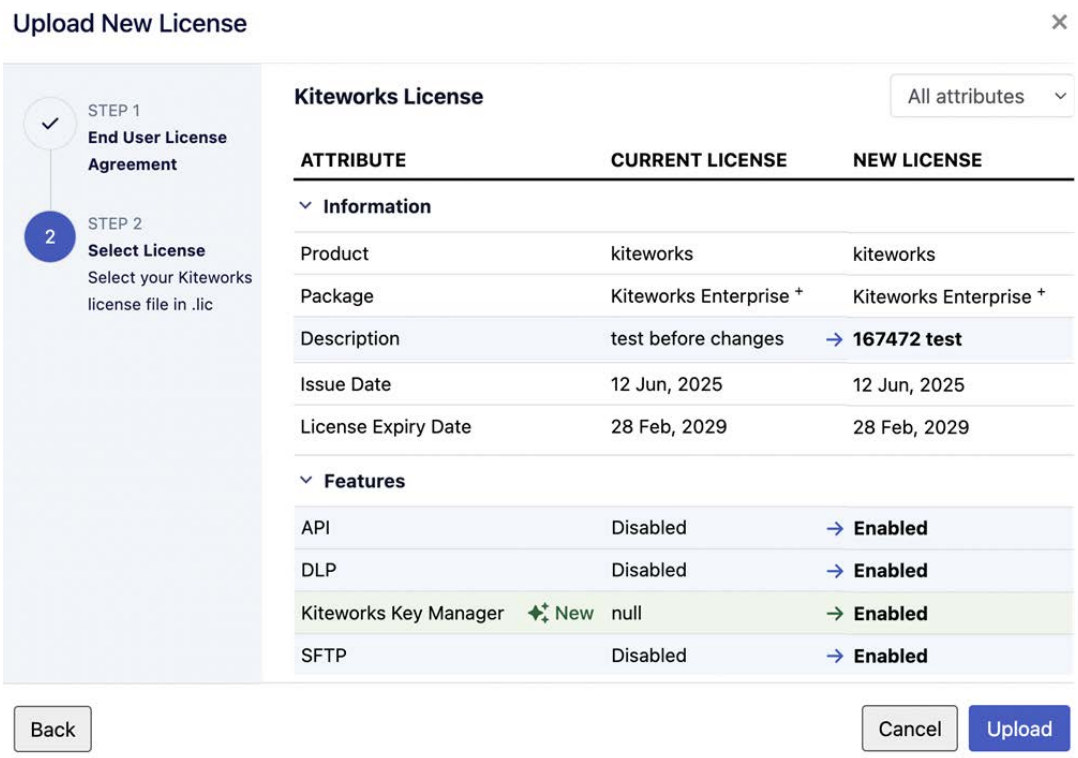
Renew licenses

Kiteworks will start sending email notifications to system administrators 14 days before a license is set to expire.

Prerequisite: To request a new license, please contact your Kiteworks account representative. They will email you the new license for uploading to the server.

To upload a license:

1. Go to Application Setup > Licenses > Kiteworks License, and then click Upload New License.
2. Review the End User License Agreement.
3. Enter your first and last name to sign the license agreement, and then click Accept.
4. On the Upload New License page, select the license file, and then click Upload.
5. Review the license attribute comparison table showing differences between the current and new license, and then click Upload.



Result: The license gets uploaded to the server and relevant information is extracted for display on the license page.

Clients and Plugins

Apps

Kiteworks Desktop Client

Kiteworks Desktop Client (also called "Kiteworks for Desktop") synchronizes files between a user's computer and the Kiteworks server. It allows them to easily access, share, and collaborate on desktop files within your organization's Kiteworks secure file sharing platform.

Key features and benefits

- Keeps users local files in sync with the Kiteworks server, ensuring they always have the latest versions.
- Enables users to access and work with files from their local computers without needing to constantly download and upload files.
- Provides seamless collaboration with others who are also using the Kiteworks platform, fostering a streamlined workflow.
- Leverages Kiteworks security features, including encryption and access controls, to protect sensitive data.

After deploying the app you can make the *Kiteworks for Desktop User Guide* available for users to download from the Kiteworks Web Application. See Enable users to download user guides from the Kiteworks Web Application.

Download an installation file for silent installation

You can push and install the appropriate Microsoft Software Installer (.MSI) file and the configuration file to silently install the desktop client to the end user's computers.

To download the installation file:

1. Go to Application Setup > Clients and Plugins > Apps.
   - To access the installation file for Mac, click Kiteworks Desktop Client for Mac.
   - To access the installation file for Windows, click Kiteworks Desktop Client for Windows.
2. On the Downloads tab, download the installation file.

Perform a SCCM installation for Windows

You can push and install the Microsoft Software Installer (.MSI) file and the desktop client installation/config file to user computers via Group Policy or SCCM or any software deployment tools used in your organization. Once pushed, when the user starts the Kiteworks Desktop Client application, they only need to authenticate to begin using the application.

To perform an SCCM installation:

1. Go to Application Setup > Clients and Plugins > Apps > Kiteworks Desktop Client for Windows.
2. On the Downloads tab, download the installation file.
3. When the download completes, double-click the installation file.
4. The Opening Kiteworks desktop app for Win.exe dialog box displays. Click Save File to save the file.

5 The file downloaded is called: kiteworks_desktop_app_for_Win-<version#>.exe

6 Create a new folder and extract the contents of this file in the newly created folder.

7 Select the 64-bit or 32-bit .msi files based on Microsoft Windows Operation System that your enterprise uses.

Note: The kiteworksInstall file is the Windows Installer Package for limited user only. Use this file to install the Windows Desktop application if you would like to install it for limited user only.

8 From the unzipped files Kiteworks folder, edit the file called kiteworks.config.
Modify line <Auth />
Replace with <Auth> your Application Host Name of your Kiteworks system </Auth>
Example: <Auth>MyCompany.com</Auth>

Note: If you would like to install or force the Secure Desktop Container installation on a selected drive, edit <DriveLetterToStartSearchWith>F</DriveLetterToStartSearchWith> (in this example the "F" drive is selected.

9 Use Group Policy, SCCM or a similar tool to install the Kiteworks desktop client and the kiteworks.config file on an end user's computer. The kiteworks.config file needs to be saved as "C:\ProgramData\Accellion\kiteworks\kiteworks.config" on the user's computers.

You can also deploy the Kiteworks Desktop Client/Secure Desktop Container .msi or .exe as a software payload, using Microsoft Group Policy/GPO.

Kiteworks Desktop Client 2.0

Kiteworks Desktop Client 2.0 is available alongside the existing Kiteworks Desktop Client application. This version offers enhanced performance and additional features, including more granular syncing capabilities such as optimized workflows for folders exceeding a specified size threshold.

Key features

- Cross-platform compatibility - Supports installation on Linux systems, expanding accessibility.
- Virtual file system (Windows only) - Introduces a Virtual File System feature for Windows users, allowing all files and folders to be visible within the app without occupying local storage space until accessed. This approach optimizes local disk usage by downloading files on-demand.
- Multi-server and multi-account syncing - Enables synchronization with multiple servers and/or accounts, providing flexibility for users managing diverse environments.

For instructions on how to deploy the app, refer to the *Kiteworks Desktop Client 2.0 Administrator Guide* available from the Help menu in the Kiteworks Admin Console. You can also make the new *Kiteworks Desktop Client 2.0 User Guide* available for download from the Kiteworks Web Application. See Enable users to download user guides from the Kiteworks Web Application.

Kiteworks mobile apps

Apps for iOS and Android for mobile and tablets are packaged together in the Mobile Apps link listed under Mobile Apps. You can enable or disable the Mobile Apps for all users by clicking on the ON/OFF button in the Status column. The default is ON.

Table 49. Mobile App settings

Setting	Description
Access token lifetime	The token lifetime duration, which specifies the validity duration of an access token from the time it is granted. The default is 720 hours. Maximum is 1440 hours.
Force authentication	Set this field to Never or Always. If set to Never, users will not have to authenticate every time they launch the app after signing in. If set to Always, users will have to authenticate every time they launch the app. Touch ID or Face ID (on iOS) and Fingerprints (on Android) can be used to authenticate.
Allow clipboard	When viewing files, You can allow users to copy content to the clipboard by selecting On. This option is enabled by default.
App "Allow List"	Approved Bundle ID Search Strings of 3rd party apps for mobile and tablet iOS and Android users. For example, com.domain.appname. A comma separator is used to separate the strings. Enter an asterisk to allow all apps that open files and are installed on mobile and tablet devices.
Push notifications	You can enable or disable notifications. Users will receive mobile notifications about important events, such as, when they receive new messages or when files are added to subscribed folders, if this option is turned on. Users can turn off Push Notifications on their mobile device under Settings. This option is enabled by default

Get the mobile app

When the Mobile Apps is enabled (which is the default), end-users will see a Get the Mobile App window on the right bottom corner of the web application page. Click either the "AppStore" or the "GooglePlay" button to go to the respective sites to download the mobile app.

Note: If the end user closes the Get the Mobile App window displayed on the right, it will not display again, but you can get the app by clicking the Get the Mobile App button on the top banner.

Plugins

Manage Kiteworks plugins

Kiteworks provides the following plugins:

- Kiteworks for Google Docs
- Kiteworks for Google Drive
- Kiteworks for iManage Work
- Kiteworks for One Outlook
- Kiteworks for Outlook Desktop
- Kiteworks for Salesforce Lightning

Support for automatic updates

With Auto Update the system will automatically check if a new version is available. If a new version is available, users will be notified and prompted to manually install a new version when it is available. This feature is enabled by default for the following plugins ensuring that users always have the most up-to-

date clients and security patches. To disable this feature, go to Application Setup > Clients and Plugins > Plugins, and for the following plugins uncheck the Auto Update checkbox.

- Kiteworks for iManage Work
- Kiteworks for Outlook Desktop

Kiteworks for Google Docs

Create and configure Google Cloud Platform (GCP) projects

Configure the Google Cloud Platform project for to make the Editor Add-on available on the G Suite marketplace. As publishing on the Chrome Web Store also publishes it to the G Suite Marketplace, only a few fields specific to the G Suite Marketplace have to be configured in the GCP console.

After creating and configuring the script, a Google Cloud Platform project will need to be created for each script at this site https://console.developers.google.com.

Create three separate projects with the following names:

- Kiteworks GDocs Add-on
- Kiteworks GSlides Add-on
- Kiteworks GSpreadsheets Add-on

Important: All the steps described in this section need to be performed for each project individually. Some fields and settings will vary for each project so values for each project are given below. Ensure that you configure each project with its own settings and values.

Create a GCP project

Perform the following steps to create a new GCP project:

1. Go to the Google console to create your project at http://console.developers.google.com or http://console.cloud.google.com.
2. Click the dropdown menu at the upper left corner.
3. A pop-up window displays. Select the Domain where you want the project to be located and click NEW PROJECT.
4. Set the fields.
   - Project name
   - Kiteworks Google Docs. (Gdocs project)
   - Kiteworks Google Sheets (GSheets project)
   - Kiteworks Google Slides (Gslides project)
   - Location (this was already set when you selected the domain from previous step)
5. Click the CREATE button.
6. Click the breadcrumb menu in the upper left corner and go to IAM & Admin > Settings.
7. Save the Project number (this will be used as the associated GCP project number in the AppScript Project which will be used later).

Enable the required APIs and services

Perform the following steps to enable the required APIs and services:

1. In the GCP Project Dashboard click ENABLE APIS AND SERVICES.
2. Search the following APIs. Follow the instructions on the screen and enable these APIS and Services:
   - Google Drive API

     Perform the following steps to enable the Google Drive API from the library:
     - Select Kiteworks GDocs Add-on.
     - Select API & Services.
     - Select Library.
     - Search for Google Drive API.
     - Select Enable API.
     - Configure G Suite Marketplace SDK after adding it and the Google Drive API.
   - Chrome Web Store API
   - G Suite Marketplace SDK

Configure OAuth consent screen

The credentials for OAuth consent screen need to be configured. The consent screen tells your users who is requesting access to their data and what kind of data is being accessed.

On the Google Cloud Platform Console select the project created for the Add-on at: https://console.developers.google.com

The OAuth Consent screen will need to be configured for each project.

1. In the OAuth consent screen, configure the following fields
   - Application Type: Internal
   - Application Name:
   - Kiteworks GDocs (GDocs project)
   - Kiteworks GSheets (GSheets project)
   - Kiteworks GSlides (GSlides project)
   - Application logo: <use provided assets>
   - Support Email: <company support email>
   - Authorized domains: <Kiteworks server domain>
2. Click Save.

Configure credentials

For Kiteworks Google Editors Credentials are automatically created after associating the App Script project with the GCP Project.

This concludes the setup for the GCP Project.

See Chrome Web Store deployment and or G Suite Marketplace deployment.

Note: Kiteworks for Google Editors is required to be Published in Chrome Web Store.

Google App Script project creation and configuration

This section describes how to create and configure a Google App Script project.

1. Go to https://script.google.com.
2. Make sure the Google App Script API is turned on. You can turn it on by clicking Settings > Turn on Google App Script API.
3. Click New project located at the upper left corner of the page.
4. Name your project based on the current Kiteworks Google Editors naming:
   - Kiteworks GDocs
   - Kiteworks GSheets
   - Kiteworks GSlides
5. Enable the Manifest file by going to View > Show manifest file (this will show in the appscript.json file)
6. Update Code.js based on the target Editors

Kiteworks document

Add the following code to this Code.js script for Kiteworks GDocs.

Code.js

```
//-------------------------------------------------------------------------------
// Accellion for Google Editors (GDocs)
// <Code.gs>
// Version 1.0.0
//
// Do not make changes to this script unless you know what you are doing.
// Contact Kiteworks technical support for more details.
//-------------------------------------------------------------------------------

// Creating Menu Buttons using Respectate UI API of the App.
function onOpen(e) {
var addonMenu = DocumentApp.getUi().createAddonMenu()
addonMenu
.addItem('Send using Accellion', 'sendViaAccellion')
.addToUi();

addonMenu
.addItem('Share copy using Accellion', 'shareViaAccellion')
.addToUi();
}

// This is a trigger function, which gets called every time the Google Doc is opened and the Addon menus are added.
function onInstall(e) {
onOpen(e);
}

function getRedirectionTemplate(activity) {
```

```
var googleToken = ScriptApp.getOAuthToken();
var docId = DocumentApp.getActiveDocument().getId();
var scriptProperties = PropertiesService.getScriptProperties();
var domain = scriptProperties.getProperty('accellion_domain');
var redirectionURL = domain + '/gdrive/'+ activity +'?state={"ids":["'+ docId +'"],"action":"open","access_
token":"'+ googleToken +'","action_by": "gdoc"}';
var encodedURL = encodeURI(redirectionURL);
var html = "<script>window.location.href='"+ encodedURL +"';</script>"
var template = HtmlService.createTemplate(html);

return template;
}

function sendViaAccellion() {
var pageData= getRedirectionTemplate('send').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Send using Accellion');

DocumentApp.getUi().showSidebar(pageData);
}

function shareViaAccellion() {
var pageData= getRedirectionTemplate('copy').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Share copy using Accellion');

DocumentApp.getUi().showSidebar(pageData);
}
```

Add the following code to appscript.json for Accellion GDocs.

```
{
"timeZone": "Asia/Hong_Kong",
"oauthScopes": [
"https://www.googleapis.com/auth/documents",
"https://www.googleapis.com/auth/userinfo.email",
"https://www.googleapis.com/auth/drive.file",
"https://www.googleapis.com/auth/drive.metadata",
"https://www.googleapis.com/auth/drive",
"https://www.googleapis.com/auth/script.container.ui"
],
"dependencies": {
```

```
},
"exceptionLogging": "STACKDRIVER",
"webapp": {
"access": "DOMAIN",
"executeAs": "USER_ACCESSING"
}
}
```

Kiteworks spreadsheet

Add the following code to this Code.js script for Kiteworks GDocs.

Code.js

```
//-------------------------------------------------------------------------
// Accellion for Google Editors (GSheets)
// <Code.gs>
// Version 1.0.0
//
// Do not make changes to this script unless you know what you are doing.
// Contact Kiteworks technical support for more details.
//-------------------------------------------------------------------------
function onOpen(e) {
var addonMenu = SpreadsheetApp.getUi().createAddonMenu()
addonMenu
.addItem('Send using Accellion', 'sendViaAccellion')
.addToUi();

addonMenu
.addItem('Share copy using Accellion', 'shareViaAccellion')
.addToUi();
}

// This is a trigger function, which gets called every time the Google Doc is opened and the Addon menus are added.
function onInstall(e) {
onOpen(e);
}
function getRedirectionTemplate(activity) {
var googleToken = ScriptApp.getOAuthToken();
var docId = SpreadsheetApp.getActiveSpreadsheet().getId();
var scriptProperties = PropertiesService.getScriptProperties();
var domain = scriptProperties.getProperty('accellion_domain');
var redirectionURL = domain + '/gdrive/'+ activity +'?state={"ids":["'+ docId +'"],"action":"open","access_token":"'+ googleToken +'","action_by": "gsheet"}';
```

```
var encodedURL = encodeURI(redirectionURL);
var html = "<script>window.location.href='"+ encodedURL +"';</script>"
var template = HtmlService.createTemplate(html);

return template;
}

function sendViaAccellion() {
var pageData= getRedirectionTemplate('send').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Send using Accellion');

SpreadsheetApp.getUi().showSidebar(pageData);
}
function shareViaAccellion() {
var pageData= getRedirectionTemplate('copy').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Share copy using Accellion');
SpreadsheetApp.getUi().showSidebar(pageData);
}
```

Add the following code to appscript.json for Accellion GSpreadsheets.

```
{
"timeZone": "Asia/Hong_Kong",
"oauthScopes": [
"https://www.googleapis.com/auth/spreadsheets",
"https://www.googleapis.com/auth/userinfo.email",
"https://www.googleapis.com/auth/drive.file",
"https://www.googleapis.com/auth/drive.metadata",
"https://www.googleapis.com/auth/drive",
"https://www.googleapis.com/auth/script.container.ui"
],
"dependencies": {
},
"exceptionLogging": "STACKDRIVER",
"webapp": {
"access": "DOMAIN",
"executeAs": "USER_ACCESSING"
}
}
```

Kiteworks slide

Add the following code to this Code.js script.

Code.js

```
//---------------------------------------------------------------------------
// Accellion for Google Editors (GSldies)
// <Code.gs>
// Version 1.0.0
//
// Do not make changes to this script unless you know what you are doing.
// Contact Kiteworks technical support for more details.
//---------------------------------------------------------------------------

// Creating Menu Buttons using Respectate UI API of the App.
function onOpen(e) {
var addonMenu = SlidesApp.getUi().createAddonMenu()
addonMenu
.addItem('Send using Accellion', 'sendViaAccellion')
.addToUi();

addonMenu
.addItem('Share copy using Accellion', 'shareViaAccellion')
.addToUi();
}

// This is a trigger function, which gets called every time the Google Doc is opened and the Addon menus are added.
function onInstall(e) {
onOpen(e);
}

function getRedirectionTemplate(activity) {
var googleToken = ScriptApp.getOAuthToken();
var docId = SlidesApp.getActivePresentation().getId();
var scriptProperties = PropertiesService.getScriptProperties();
var domain = scriptProperties.getProperty('accellion_domain');
var redirectionURL = domain + '/gdrive/'+ activity +'?state={"ids":["'+ docId +'"],"action":"open","access_token":"'+ googleToken +'","action_by": "gslide"}';
var encodedURL = encodeURI(redirectionURL);
var html = "<script>window.location.href='"+ encodedURL +"';</script>"
var template = HtmlService.createTemplate(html);

return template;
```

```
}

function sendViaAccellion() {
var pageData= getRedirectionTemplate('send').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Send using Accellion');

SlidesApp.getUi().showSidebar(pageData);
}

function shareViaAccellion() {
var pageData= getRedirectionTemplate('copy').evaluate()
.setSandboxMode(HtmlService.SandboxMode.IFRAME)
.setXFrameOptionsMode(HtmlService.XFrameOptionsMode.ALLOWALL)
.setTitle('Share copy using Accellion');

SlidesApp.getUi().showSidebar(pageData);
}
```

Add the following code to appscript.json for Accellion GSlides.

```
{
"timeZone": "Asia/Hong_Kong",
"oauthScopes": [
"https://www.googleapis.com/auth/presentations",
"https://www.googleapis.com/auth/userinfo.email",
"https://www.googleapis.com/auth/drive.file",
"https://www.googleapis.com/auth/drive.metadata",
"https://www.googleapis.com/auth/drive",
"https://www.googleapis.com/auth/script.container.ui"
],
"dependencies": {
},
"exceptionLogging": "STACKDRIVER",
"webapp": {
"access": "DOMAIN",
"executeAs": "USER_ACCESSING"
}
}
```

To set Script Properties, go to File > Project Properties > Script Properties.

- Property Name: accellion_domain
- Property Value: {Kiteworks server address}. (Complete URL example: https://kiteworks.com)

To save the changes and create aversion, go to File > Manage Version. Add a brief description and click Save new version.

Associate the App Script Project with the GCP Project.

1. Go to Resources > Cloud Platform Project.
2. Enter the Project Number of the GCP Project.
3. Click Set Project.

This will create an App Script Credential for the associated GCP Project.

This concludes the setup for the App Script Project.

Chrome Web Store deployment

Prerequisite: Make sure the Chrome web store is enabled before performing these steps.

1. In the App Script Project, go to Publish > deploy as add-on.
2. Populate the fields accordingly.
   - Title
     - Kiteworks GDocs
     - Kiteworks GSheets
     - Kiteworks GSlides
   - Short Description-Give a short description of the project.
   - Add-on Type
   - Docs-for GDoc
   - Sheets -for GSheets
   - Slides-for GSlides
   - Version-Specify the version you created in last steps of the App script project.
   - Help URL-Optional
   - Report Issue URL-Optional
   - Post-install tip
3. Click Create web store draft or Update web store draft.
4. Click Edit in Chrome Web Store.
5. Fill or upload required files and or assets:
   - Detailed Description-Kiteworks GDocs Add-on
   - Icon-128x128 pixels
   - Screenshot-604x400 pixels or 1280x800 pixels
   - Promotional Tile Images-Small tile 440x280 pixels
   - Category-Utilities
   - Region-Enter the region
   - Visibility-My Domain
6. Click Publish.

Once published you will be redirected to the add-in's page. Click the free button and the add-in will be installed for the user.

This concludes the publishing in the chrome web store .

Configure the G Suite Marketplace SDK deployment (domain wide)

Perform the following steps to deploy the G Suite Marketplace SDK:

1. Go to Resources > Cloud Platform project in the App Script Project.
2. Click the GCP Project ID associated with the App Script Project. The administrator will be redirected to the GCP Project dashboard.
3. Locate the G Suite Marketplace SDK towards the lower end of the dashboard, and then click it. If you cannot locate it you can search for G Suite Marketplace SDK.
4. Click Configuration from the side menu option.
5. Fill and upload the required fields and assets:
   - Language-Enter the language
   - Application Icon-Use provided assets
   - Support URL-Enter the support URL
   - Extensions - Select Editor
     - Docs add-on extension
       - Script ID - This ID can be found in the App Script project properties
       - Version
   - Sheet add-on extension
     - Script ID - This ID can be found in the App Script project properties
     - Version
   - Slides add-on extension
     - Script ID - This ID can be found in the App Script project properties
     - Version
   - Visibility-My Domain
6. Click Save.
7. Go to the top of the page and click Integrate With Google.
8. Go to https://gsuite.google.com/marketplace/?pann=gam.
9. From the left panel list, select <Domain Name> Apps.
10. From the list of Domain published app select Kiteworks Editors Addins:
    - Kiteworks GDocs
    - Kiteworks GSheets
    - Kiteworks GSlides
11. Click DOMAIN INSTALL.

Publish

For Kiteworks Google Editors Publish setup is not required.

This concludes the G Suite Marketplace domain wide deployment.

Note: Add-ins will take some time before appearing in the G Suite Market Place.

Enable the Kiteworks server to communicate with the Google Cloud APIs

One the settings are configured for all the projects, you will need to enable the Kiteworks server with the Google cloud APIs.

To do so, go to Application Setup > Clients and Plugins > Plugins and make sure Kiteworks for Google Docs, Kiteworks for Google Sheets and Kiteworks for Google Slides status is turned ON.

Deploy the Google Editor Add-on in Kiteworks

You can deploy the Google Editor add-ons and add Google Client IDs for each of the following components into Kiteworks:

- Google Docs add-on
- Google Sheets add-on
- Google Slides add-on

From your Kiteworks server Kiteworks Admin Console and click Application Setup > Clients and Plugins > Kiteworks for Google Docs > Client ID.

Enter the Client ID for each project which is generated from the Google APIs > APIs & Services > Credentials page of each project and click Save.

To control the Google Editors (Docs, Slides and Sheets) Add-on independently, you will need to create a separate Google Cloud Console project for Google Editor Add-on.

Kiteworks for Google Drive

The Kiteworks Google Drive App is a business workflow that can be integrated into Google Drive. The app simplifies and secures any data sharing from Google Drive. Without leaving the Google Drive environment you can send, share copy and add from Kiteworks via the app.

To enable the app in Google Drive, you need to follow a few steps as a G Suite administrator. Every menu option in Google Drive, for example, send, share/copy and add, is considered a "project".

For instructions on how to deploy the plugin, refer to the *Kiteworks for Google Drive Administrator Guide*. You can access the guide from the Help menu in the Kiteworks Admin Console. After deployment, you can also make the *Kiteworks for Google Drive User Guide* available for download from the Kiteworks Web Application.

Kiteworks for iManage Work

The Kiteworks for iManage Work plugin provides a secure way to send and share iManage DMS files from within iManage Work for the Web. The plugin simplifies and secures any data that is attached to an iManage workspace and ensures that it resides in Kiteworks when users send or share files. It provides access to Kiteworks with the ability to view a list of files, download and delete files in a folder and without leaving the secure Kiteworks environment you can send and receive files via the plugin.

For instructions on how to deploy the application, refer to the *Kiteworks for iManage Administrator Guide*. You can access the guide from the Help menu in the Kiteworks Admin Console. After deployment, you can also make the *Kiteworks for iManage Web User Guide* available for download from the Kiteworks Web Application.

Kiteworks for Office

Kiteworks for Office enables you to extend Office clients such as Word, Excel and PowerPoint to save files to Kiteworks and Repositories Gateway sources. Additionally, the application provides the ability to

send files securely via Kiteworks.

Using Kiteworks as the conduit, you can use Kiteworks for Office to:

- Open, Save, Save as, and Send Kiteworks files directly from within Microsoft Office Word, Excel or PowerPoint applications.
- Extend the Microsoft Office native UI by creating two Kiteworks custom buttons for Save and Send.
- Open a Kiteworks file in Word, Excel or PowerPoint, edit it and send the file from the Office application directly.

Kiteworks for Office is available to the client through the Kiteworks license when it is purchased. Once available, the add-in is enabled by the administrator in the Kiteworks Admin Console for end users. Once enabled Kiteworks for Office displays on the Application Setup > Clients and Plugins > Plugins tab.

Supported versions

Windows 11, Windows 10, Windows 8.1.

MS Office 2019, 2016, 2013, 2010.

Kiteworks for Office only works with the desktop version of Microsoft Word, Microsoft Excel, and Microsoft PowerPoint. 32-bit and 64-bit

Minimum requirements

Target Framework: NET Framework version 4.6.2 is used.

MS Office 2010 or newer version must be installed

Visual Studio Tools for Office (VSTO)

Deployment

Kiteworks for Office can be deployed using the MSI installer for GPO deployment (automatic deployment or silent installation using msiexec). The MSI installer does not have the VSTO deployment package so the "VSTO Runtime Redistributable" will need to be downloaded and installed manually. The Visual Studio Tools for Office Runtime can be downloaded from Microsoft Website.

The EXE installer includes the VSTO Runtime Redistributable, but it cannot be deployed using Microsoft GPO Management (GPO only supports MSI). The link to Visual Studio 2010 Tools for Office Runtime: https://www.microsoft.com/en-us/download/details.aspx?id=54251

Error messages

Net 4.5 not found: This setup requires the .NET Framework 4.6.2 to be installed. Install the .NET Framework then run this installer again.

If VSTO Runtime not found: Visual Studio 2010 Tools for Office Runtime 10.0.60825 or greater is required.

Download the Kiteworks for Office for Desktop plugin

Go to Application > Client Management > Kiteworks for Office to download the installer. There are two options of the installer to choose from:

1. .exe Package - The .exe package combines the vstor_redist.exe (VSTO Runtime Redistributable) into the installer. Using this installer will result in an additional step for the administrator if Kiteworks for Office is deployed via GPO. See the following website for instructions on how to install VSTO Runtime with Group Policy. https://social.msdn.microsoft.com/Forums/vstudio/en-US/208e6d9d-d084-4d45-af40-9351d08902e9/how-to-install-vsto-runtime-with-group-policy?forum=vsto

   Note: The VSTO Runtime Redistributable development tool will not be uninstalled if Kiteworks for Office is uninstalled.
2. .msi Package - The .msi package includes the VSTO Runtime Redistributable development tool in the installer. The VSTO Runtime Redistributable development tool will be uninstalled when Kiteworks for Office is uninstalled.

   After deployment, you can make the *Kiteworks for Office User Guide* available for download from the Kiteworks Web Application.

Kiteworks for One Outlook

Kiteworks for One Outlook is available for use with the new version of Outlook for Windows released by Microsoft. In this initial release of the plugin, users can compose messages, configure message security settings, and attach files to send to others. Recipients who receive these messages click the Access Message button in their email notifications to access the message in the Kiteworks Web Application or mobile app. Current Microsoft behavior is to store messages sent using the plugin in an automatically-created "Kiteworks Sent" folder in the user's email client and to identify those messages as draft messages.

This release of the Kiteworks for One Outlook plugin contains functionality limited to sending and receiving files securely through Kiteworks. The Kiteworks for Outlook Desktop plugin continues to be supported. If your users require additional Kiteworks integration with Outlook, they should continue to use the Kiteworks for Outlook Desktop plugin.

Register the application in Azure

To register the application in Azure:

1. Sign in to the Microsoft Azure portal with administrator credentials for the Microsoft 365 tenancy.
2. In Azure, search for "App registrations".

   Alternative: Under Azure Services, click App Registrations.
3. On the App Registrations page, click New Registration.
4. On the "Register an application" page, set the following values:
   - Name - The user-facing display name for the application, such as "Kiteworks for One Outlook".
   - Supported account types - Select "Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)."
5. Click "Register".

   Result: The "Kiteworks for One Outlook" application is created.
6. Copy the following IDs and save them to a file. You'll need them later in the deployment process.
   - Application (client) ID
   - Directory (tenant) ID

Add a client secret

To add a client secret:

1. At the top of the page, go to Home > App Registrations > Kiteworks for One Outlook.
2. In the left pane, go to Manage > Certificates & Secrets.
3. On the Client Secrets tab, click "New client secret.
4. Enter a description to uniquely identify the secret from other secrets.
5. Select the expiration date for the secret or specify a custom lifetime.
   - Client secret lifetime is limited to two years (24 months) or less.
   - Microsoft recommends that you set an expiration value of less than 12 months.

   Result: Azure updates the application credentials and shows the details of the client secret you created.
6. Copy the client secret value to a secure place. You'll need it later in the deployment process.

   Reminder: Be sure to copy the secret value. Once you close this page, you won't be able to access it again.

Configure the application to expose the web API

To configure the application to expose the web API:

1. In the left pane, go to Manage > Expose an API.
2. Next to the Application ID URI, click Add to generate the ID.

   Result: The section for setting the application ID URI appears with a generated URI in the form of api://*<app-id>*.
3. In the Application ID URI box, insert the fully-qualified-domain-name of the Kiteworks server between the "api://" prefix and the application ID (GUID).

   Example: api://*<your-kiteworks-url.com>*/*<app_id>*
4. Click Save.

Add a scope

To add a scope:

1. On the "Expose an API" page, click Add a Scope.
2. In the Add a Scope pane, configure the Scope form settings.

Table 50. Add a Scope form settings

Setting	Description
Scope name	Enter "access_as_user". This is the value that's called when access to this API is requested, and in access tokens when the scope has been granted to the client application.

Table 50. Add a Scope form settings (continued)

Setting	Description
Who can consent	Select "Admins and users".
Admin consent display name	Enter "Read/write permissions to user mail. Read permissions to user profiles."
Admin consent description	Enter "Allow Office to have read/write permissions to all user mail. Office can call the app's web APIs as the current user."
User consent display name	Enter "Read/write permissions to your mail. Read permissions to your profile."
User consent description	Enter "Allow Office to have read/write permissions to your mail, and read permissions to your profile."

3 For the State, click Enabled, and then click Add Scope.

Result: The new scope you defined displays in the pane.

Authorize client application IDs

Perform the following steps to authorize each Microsoft application ID:

- Microsoft Office application endpoints - ea5a67f6-b6f3-4338-b240-c655ddc3cc8e
- Microsoft Office - d3590ed6-52b3-4102-aeff-aad2292ab01c
- Office on the web - 93d53678-613d-4013-afc1-62e9e444a0a5
- Outlook on the web - bc59ab01-8403-45c6-8796-ac3ef710b3e3

To authorize the client application IDs:

1. On the "Expose an API" page, under Authorized Client Applications, click Add a Client Application.
2. For the Client ID, input a Microsoft application ID.
3. Under Authorized Scopes, select the "api://<*fully-qualified-domain-name*>/<*app-id*>/access_as_user" checkbox.
4. Click "Add Application".
5. Repeat the steps above until you have authorized each Microsoft application ID.

Add Microsoft Graph permissions

To add Microsoft Graph permissions:

1. In the left pane, go to Manage > API Permissions.
2. Under Configured Permissions, click Add a Permission.
3. On the "Request API permissions" page, click the Microsoft APIs tab.
4. In the Commonly Used Microsoft APIs list, click Microsoft Graph.
5. On the Microsoft Graph page, click Delegated Permissions.
6. In the "Select permissions" search box, search for the permissions as follows: profile, openid, Mail.ReadWrite.
7. If the unnecessary User.Read permissions is listed by default, remove it.
8. Select the checkbox corresponding to each permission as it appears.

   Note: The permissions will not remain visible in the list as you select each one.
9. After selecting the permissions your add-in needs, click Add Permissions.
10. Under Configured Permissions, click "Grant admin consent for <*tenant name*>".

Define the access token version

To define the access token version:

1. In the left pane, go to Manage > Manifest.
2. For the accessTokenAcceptedVersion property, change the value from "null," to "2,".
3. To update the manifest, click Save.

Enable Kiteworks for One Outlook on the Kiteworks server

Role: (missing or bad snippet)

To enable the app on the Kiteworks server:

1. On the Kiteworks server, sign in to the Kiteworks Admin Console.
2. Go to Application Setup > Clients and Plugins > Plugins.
3. On the Plugins tab, turn on Kiteworks for One Outlook.
4. Expand the Kiteworks for One Outlook section.
5. On the Configuration tab, enter the following values you saved when deploying on Azure, and then click Save.
   - Application ID - This is the "Application (client) ID" you saved to a file.
   - Tenant ID - This is the "Directory (tenant) ID" you saved to a file.
   - Application Secret - This is the client secret value you saved to a secure place.
6. Click the Manifest tab and download the manifest file to be uploaded in Office 365 Centralized Deployment.

   Result: The OneOutlook_Manifest.xml file is downloaded.

Upload Kiteworks for One Outlook to Office 365 Centralized Deployment

To upload Kiteworks for One Outlook to Office 365 Centralized Deployment:

1. Sign in to the Microsoft 365 admin center with your Global Administrator account.
2. Go to Settings > Integrated Apps.
3. On the Integrated App page, go to the Deployed Apps tab, and then click Upload Custom Apps.
4. On the Upload Apps to Deploy page, in the "App type" list, select "Office Add-in".
5. In the "Choose how to upload app" list, select "Upload manifest file (.xml) from device".
6. Find and upload the OneOutlook_Manifest.xml file, and then wait for the file to be validated.
7. Once the validation is completed, click Next.
8. On the "Add users" page, in the "Assign Users" section, select an option, and then click Next.
9. On the "Accept permissions requests" page, review the app permissions and capabilities, and then click Next.
10. On the "Review and finish deployment" page, review the information, and then click Finish Deployment.
11. Click "Done".

    Note: Microsoft states that it can take up to 24 hours for a newly deployed add-in to appear on the app ribbon in Outlook user mailboxes. Your users may need to close and reopen Office to view the add-in icon on the app ribbon.

Add the Kiteworks for One Outlook app to Outlook

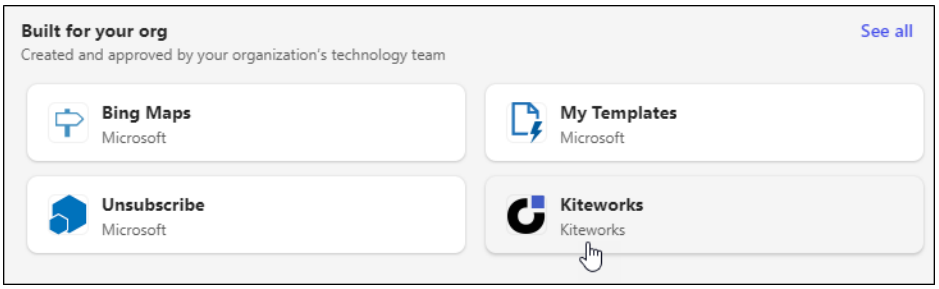
- Install Kiteworks for One Outlook using Classic Outlook
- Install Kiteworks for One Outlook using Outlook on the web

Install Kiteworks for One Outlook using Classic Outlook

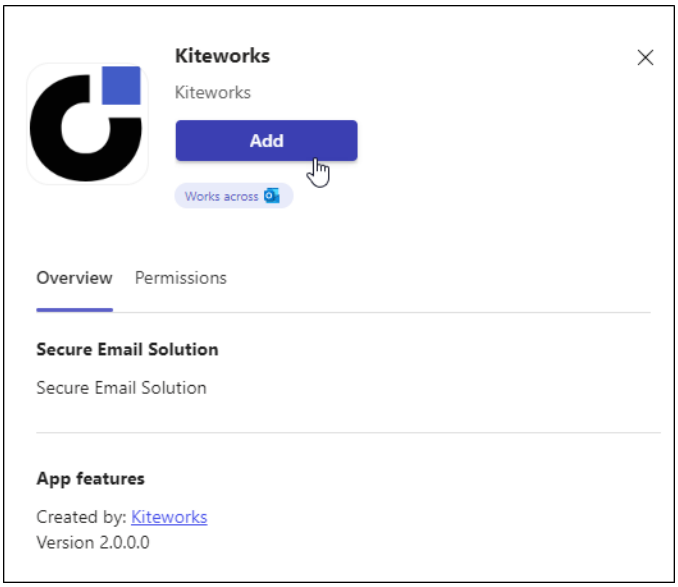
To install Kiteworks for One Outlook using Classic Outlook:

1. In Outlook, navigate to the ribbon.
2. If you're reading a message, select the Home tab. If you're composing a message, select the Message tab.
3. In the Apps section of the ribbon, click All Apps.

4. Perform one of the following actions:
   - In the apps list, click Kiteworks.
   - If you don't see the Kiteworks app in the apps list, click Add Apps. On the App Store page, in the "Built for your org" section, click Kiteworks.



5. On the Kiteworks app page, click Add.



Install Kiteworks for One Outlook using Outlook on the web

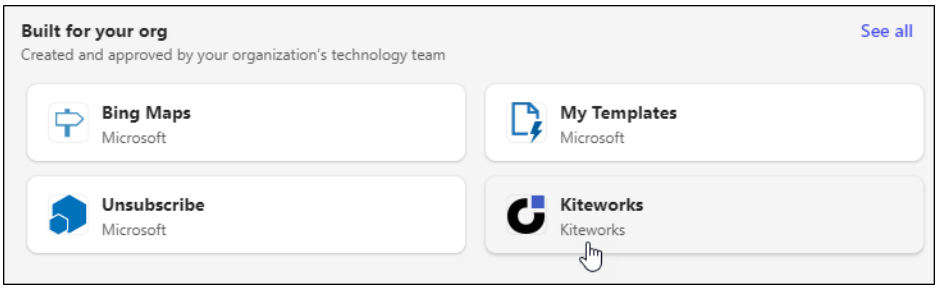
To install Kiteworks for One Outlook using Outlook on the web:

1. In Outlook, navigate to the app bar on the left side of the page.
2. On the app bar, click More Apps.

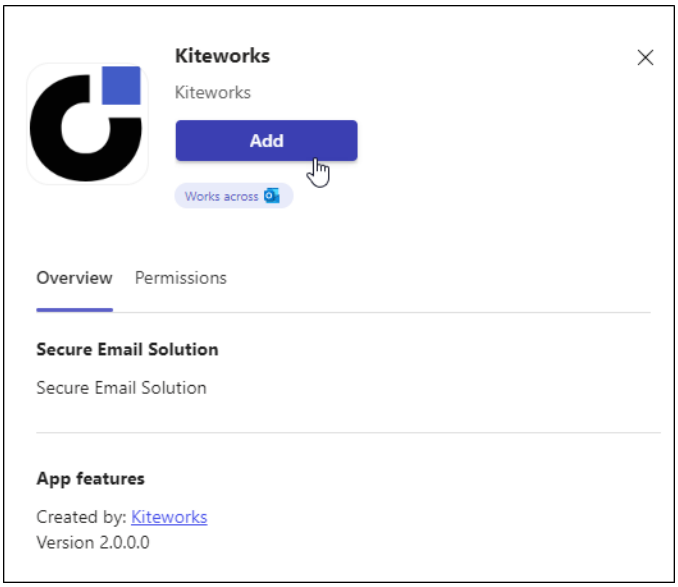
Alternative: In a new message, click the Apps button.

3 Perform one of the following actions:

- In the apps list, click Kiteworks.
- If you don't see the Kiteworks app in the apps list, click Add Apps. On the App Store page, in the "Built for your org" section, click Kiteworks.



4 On the Kiteworks app page, click Add.



Kiteworks for Outlook Desktop

The Kiteworks for Outlook Plugin is enabled through the Kiteworks license when it is purchased.

For the Outlook Plugin installation, you can push and install the appropriate Microsoft Software Installer (.MSI) file and the registry keys to the end user's computers via Group Policy or SCCM or any software deployment tools used in the organization. Once pushed, when the user starts the Outlook Plugin, the user only needs to authenticate to start using the plugin.

Download and install Kiteworks for Outlook Desktop

Administrators will be notified when a new release of the Outlook Plugin installer files is available for the desktop. You can upload a custom Outlook desktop client installer to the system which will replace the original installers enabling ease of distribution. The original installer files can still be restored, if needed. This configuration is available for each tenant for a multi-tenant system.

Note: If Auto Update is enabled, auto-update will update the newer version installed on the system.

Kiteworks for Outlook Desktop settings

Settings tab

Table 51. Settings tab

Setting	Description
Access token lifetime	The token lifetime duration, which specifies the validity duration of an access token from the time it is granted. The default is 720 hours. Maximum is 1440 hours.
Refresh token lifetime	Issued together with the access token, the refresh token can be used to renew the access token. Refresh token lifetime specifies the validity duration of a refresh token since it was granted. The default is 1440 hours. Maximum is 1440 hours.
Auto update	Automatically update the app on end user computers when a new version of the app is available.

Downloads tab

Kiteworks works seamlessly with the Outlook Desktop plugin, allowing users to securely send files using Outlook. To use the Kiteworks for Outlook Desktop Plugin you must install the software onto your system. Click the Download button, or click the Upload Installer link and choose a file to upload newer client installer files to replace the current (GA) version. You will still be able to restore to the GA version if needed.

Silent install registry key

You can push and install the appropriate Microsoft Software Installer (.MSI) file and the registry keys to the end user's computers via Group Policy or SCCM (which is referred to as "Silent Install" here), or any software deployment tools used in the organization. Once pushed, when the user starts the Outlook Plugin, the user only needs to authenticate to start using the plugin.

Table 52. Registry keys and what they control

Key Name	Possible Value	Description
AccellionActivation	If set to 0: Plugin will auto-prompt login If set to 1: User must manually click the login button	Outlook Plugin Activation feature: If set to 0: The user will be prompted to log in (if the user has not already logged in) during: • Outlook start-up • Triggering new mail • Click the login button in the side-bar If set to 1: The user will not get prompted to log in, except when the user manually clicks on the login button in the Outlook plugin's side-bar.
AccellionAutoReadMode	If set to 0: Disabled If set to 1: Enabled	Auto read mode
AccellionDebugLevel	If set to 1: Enables low level debug mode If set to 2: Enables high level debug mode	Debug Level
AccellionForcedStop	If set to 0: Disabled (plugin is activated) If set to 1: Enabled (plugin is deactivated)	Turn off the Outlook Plugin
AccellionHostName		
AccellionMultiAccount	If set to 0: Disabled If set to 1: Enabled	Allows users to add multiple accounts.
AccellionUsername	<string>	Username for silent installation

To download the Silent Install Registry Key, click the Download button and click Save File in the pop-up window to save the reg file to your desktop. Use Group Policy, SCCM, or a similar tool to install the Kiteworks Outlook Plugin and registry keys on end user's computers.

Once the installation is complete the Kiteworks Activation icon displays in place of Kiteworks Attach and Security Options. The plugin will not prompt the user to log in until the user has chosen to activate the plugin.

Note: Once the registry keys are installed the user will not need to enter the Kiteworks the host name manually.

Once the plugin is activated, the Send Secure option displays for an authenticated user in the "Microsoft Outlook Quick Access Toolbar".

Outlook automation policy

At the user profile level, you can enforce a set of policies for all emails being sent using the Kiteworks for Outlook Desktop plugin. Any policy setting combination set by the Kiteworks administrator will be followed and applied automatically to an Outlook email being composed by end users. See Create and edit user profiles.

Multi-language support

The Kiteworks for Outlook Desktop plugin will localize based on the language in Outlook.

Kiteworks for Outlook Desktop plugin activation feature

Registry keys and what they control

- ActivationFeature (in HKLM): If set to 0 or missing, OLP will not care about the ChooseToInstall value in HKCU.
- ActivationFeature (in HKLM): If set to 1, OLP will check the value of ChooseToInstall value in HKCU.

Table 53. Sample of DWORDS written to the registry

Sample of Install
[HKEY_LOCAL_MACHINE\Software\Accellion\AccellionOutlook] "AccellionActivation"=dword:00000001

Table 54. Basic sanity check

Task	Expected Behavior
Install the Microsoft Software Installer (.MSI) file available with the Activation feature Launch Outlook, open a New Email window.	The user will see the Activate button and the tooltip when the mouse is hovered over.
Registry key ActivationFeature in HKLM is set to 0.	This is an old behavior of the Kiteworks for Outlook Plugin (you will need to login from Start > Kiteworks for Outlook Plugin).
Registry key ActivationFeature in HKLM is missing.	This is an old behavior of the Kiteworks for Outlook Plugin (you will need to login from Start > Kiteworks for Outlook Plugin).

Table 54. Basic sanity check (continued)

Task	Expected Behavior
Previous Plugin already installed. Do Not Set ActivationFeature in HKLM. Update to the latest. Run sanity test.	No change, This is an old behavior. Outlook Plugin behaves as before.
Previous Plugin already installed. Set ActivationFeature in HKLM to 0. Do not update. Run the sanity test. Update to latest.	No change, This is an old behavior. Outlook Plugin behaves as before since in HKCU ChooseTo Install=1.
Previous Plugin already installed. Set the ActivationFeature in HKLM to 1. Do not update. Run the sanity test. Update to the latest.	No change, This is an old behavior. Outlook Plugin behaves as before since in HKCU ChooseTo Install=1.
Previous Plugin already installed. Update to the latest. Set ActivationFeature in HKLM to 0.	No change, This is an old behavior. Outlook Plugin behaves as before since in HKCU ChooseTo Install=1.
Previous Plugin already installed. Update to the latest. Set ActivationFeature in HKLM to 1	No change, This is an old behavior. Outlook Plugin behaves as before since in HKCU ChooseTo Install=1.

Outlook may disable the Kiteworks for Outlook Desktop plugin add-ins. If this happens contact Kiteworks technical support at https://community.kiteworks.com to enable add-ins.

Kiteworks for Salesforce Lightning

The Kiteworks for Salesforce Lightning plugin is a business workflow integrated in the Kiteworks Enterprise package and requires a new license. It is not available for the Kiteworks Business package. It enables you to send, share, and request files to folders in Salesforce, while keeping your data in Kiteworks. In the plugin, you can utilize other Salesforce objects, such as Support Cloud, Sales Cloud, and Customer Experience Cloud. You can expand on cases to view the activities in that case. For more information on how to use the Kiteworks for Salesforce Lightning plugin, refer to the *Kiteworks for Salesforce User Guide*.

The Kiteworks for Salesforce Lightning plugin also enables you to customize your deployment. For example, you can limit the plugin to only sending files or requesting files to folders.

Key features of Kiteworks for Salesforce Lightning

- It is deployed by an administrator with permission to deploy to a subset of users in the organization.
- It is enabled by the administrator using a new Client ID (an identifier for the application -- for example, a 32-character hex string) and a Client Secret (known only to the application and the authorization server) so that end users can install and use the plugin.
- Works with a variety of Salesforce objects: Account, Case, Contact, Opportunity, Task, and custom Salesforce objects
- Folders are created under the Case Owners. Users who are Case Owners in Salesforce are assigned the Collaborator role in Kiteworks.
- It is disabled by default.

Minimum requirements

- For users to access Kiteworks for Salesforce Lightning, you must have uploaded a Salesforce license.
- Salesforce user account: A profile that can create a case with the appropriate Case ID.
- Kiteworks user account: Can be tied to a Salesforce user account. The connection between a Salesforce user account and a Kiteworks user account is determined by matching email addresses.

End user sign-in scenarios

There are three scenarios when a user signs in:

- If the user has a Kiteworks account and a Salesforce account with the same email, they can sign into Kiteworks or the Kiteworks for Salesforce Lightning plugin seamlessly. Once signed into Salesforce, Kiteworks displays in an object page.
- If the user does not have a Kiteworks account, but does have an internal domain email on Salesforce, signing in will also be seamless because the user account will be created automatically on the Kiteworks system.
- If the user has an external email domain, the "External users are not supported." error message will display. Contact Kiteworks technical support at https://community.kiteworks.com to create a Kiteworks account.

For additional end user information, refer to the refer to the *Kiteworks for Salesforce User Guide*.

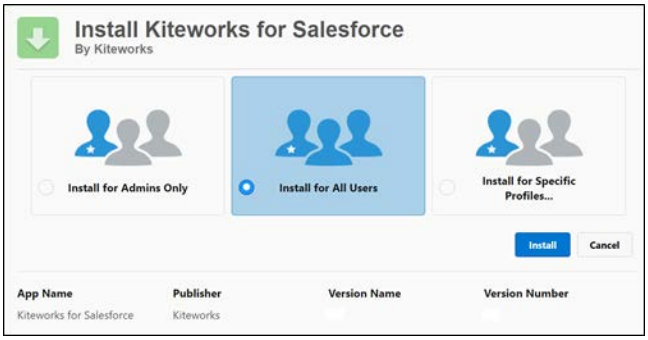
Install Kiteworks for Salesforce Lightning

To install Kiteworks for Salesforce Lightning:

1 Request the installation URL from Kiteworks technical support at https://community.kiteworks.com.

Rationale: You install Kiteworks for Salesforce Lightning using a package installation URL or an AppExchange private listing URL. Both links can be provided to you by Kiteworks technical support.

2 Choose the options you want to install.

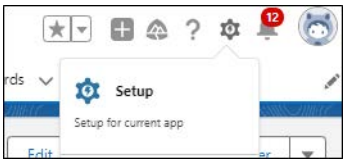


3 Click Install and follow the installation instructions.

Add the plugin to the Salesforce layout

To add the plugin to the Salesforce layout:

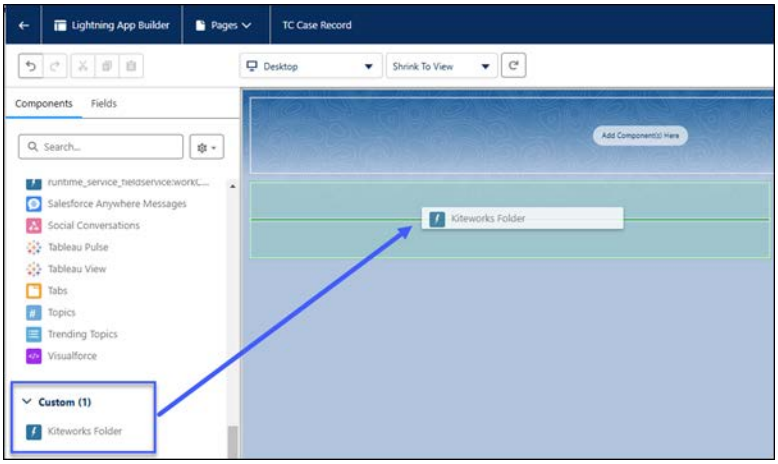
1. In Salesforce, click the Setup icon on the toolbar, and then click Setup.



2. On the Setup page, search for "Lightning App Builder".

   Alternative: In the navigation pane, go to Platform Tools > User Interface > Lightning App Builder.

3. In the Lightning App Builder, go to the row containing the object in which to add the plugin, and then click Edit.
4. In the left pane, click the Components tab and expand the Custom section.
5. From the Custom section, drag the "Kiteworks Folder" component to where you want to place it on the page.



6. In the top right corner of the page, click Save.

   Result: Kiteworks for Salesforce Lightning is added to the object page.

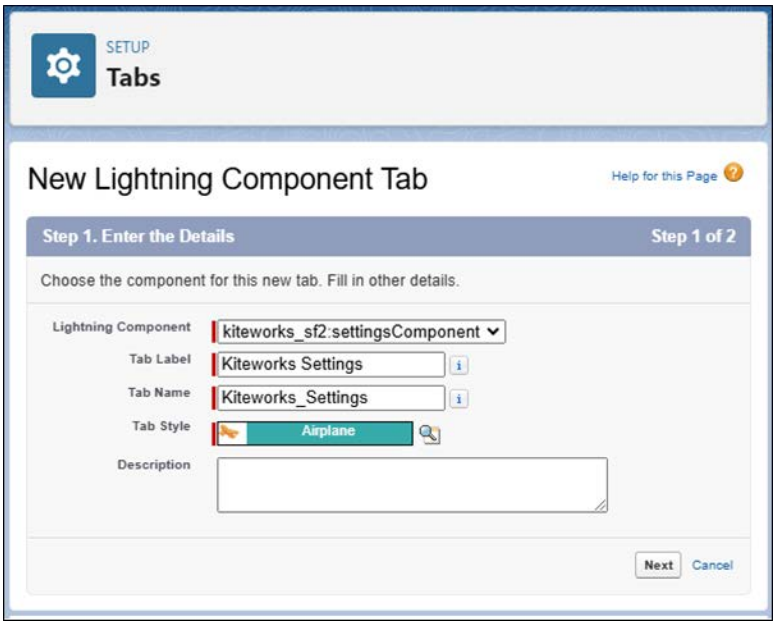
Add the plugin to the Custom Tabs list in Salesforce

To create a custom tab for the plugin:

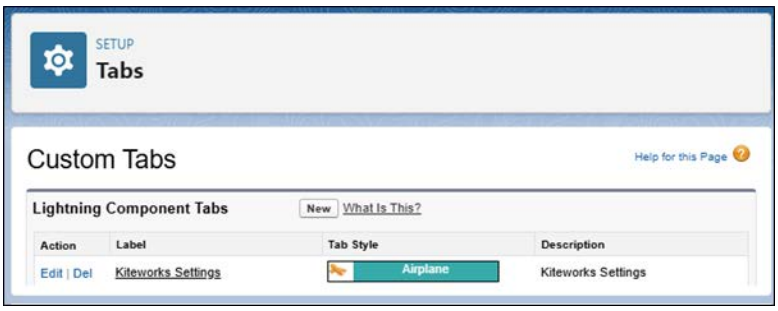
1. On the Setup page, search for "Tabs".

   Alternative: In the navigation pane, go to Platform Tools > User Interface > Tabs.

2. On the Tabs page, in the Lightning Components Tabs section, click New.
3. On the New Lightning Component Tab, fill in the component details.
   - Lightning component - Select "kiteworks_sf2:settingsComponent".
   - Tab label - Enter "Kiteworks Settings". This label appears as the Lightning Component tab name in the Salesforce app navigation menu.
   - Tab name - The unique name used by the API and managed packages.
   - Tab style - Select or create a tab style.

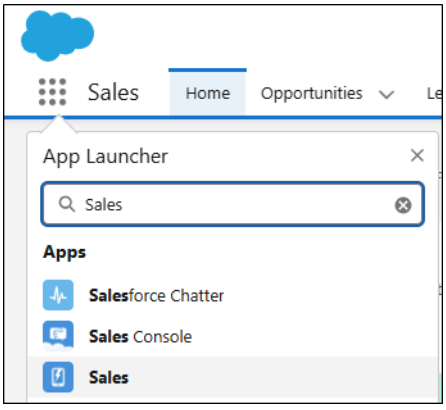


4 Click Next > Save.



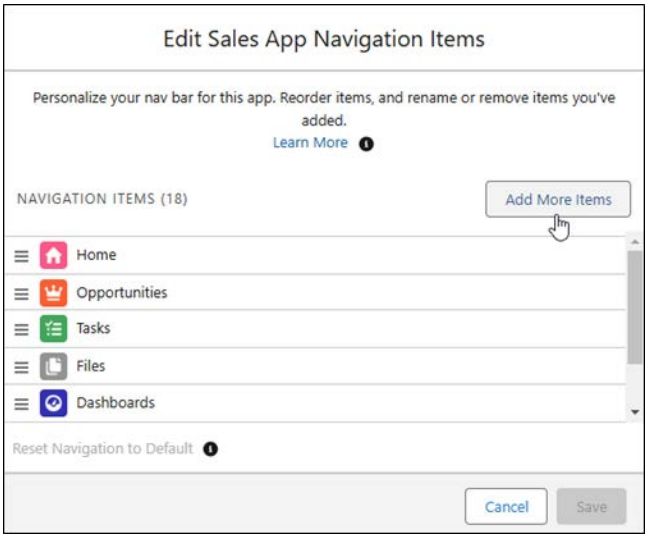
To add the Kiteworks Settings tab to Salesforce:

1 From the App Launcher, go to the Sales home page.



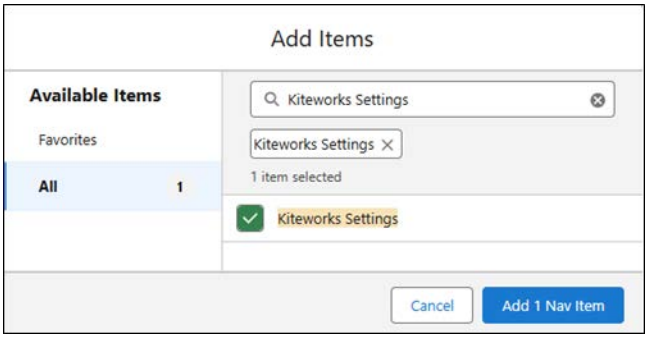
2 In the top right corner of the page, under your profile icon, click the pencil icon and select "Personalize your nav bar".

3 Click "Add More Items".



4 In the navigation pane on the Add Items page, click All.

5 In the list of items, click the plus (+) sign next to "Kiteworks Settings", and then click "Add 1 Nav Item".



Result: Kiteworks Settings is added to the list of available app navigation items. You can use drag and drop to reorder the list.

6 Click Save.

Register the Kiteworks server as a remote site in Salesforce

To register the Kiteworks server as a remote site in Salesforce:

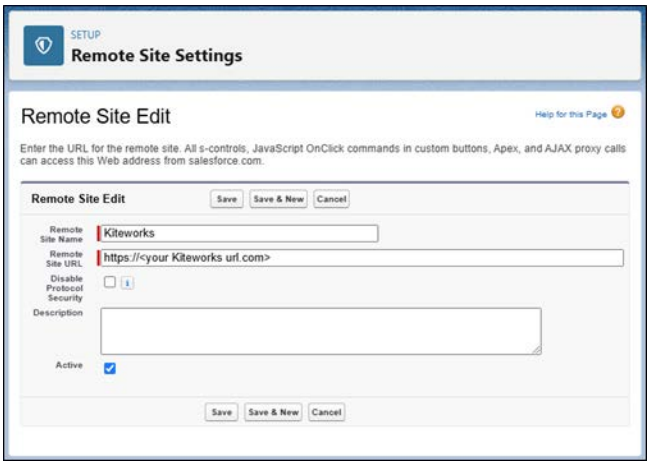
1 On the Setup page, search for "Remote Site Settings".

Alternative: In the navigation pane, go to Settings > Security > Remote Site Settings.

2 On the Remote Site Settings page, click New Remote Site.

3 On the Remote Site Edit page, enter a name for the site, such as "Kiteworks".

4 Enter the Kiteworks URL for the site, such as https://*<your Kiteworks url.com>*.



5 Enter a description for the site.

6 Click Save.

Make the Kiteworks server a Trusted URL in Salesforce

To make the Kiteworks server a Trusted URL in Salesforce:

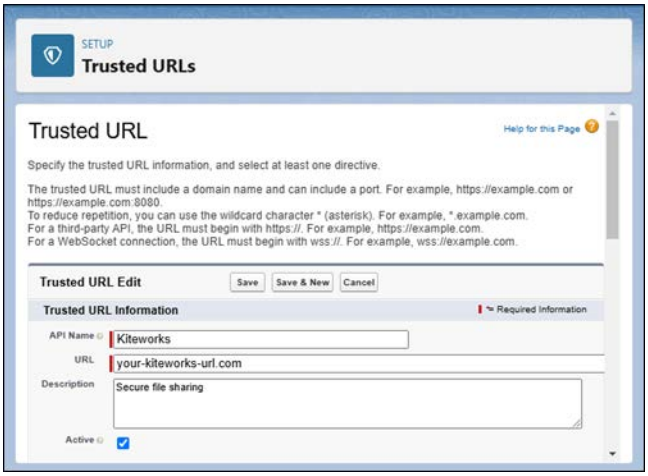
1 On the Setup page, search for "Trusted URLs".

Alternative: In the navigation pane, go to Settings > Security > Trusted URLs.

2 On the Trusted URLs page, click New Trusted URL.

3 On the Trusted URL page, configure the Trusted URL Information.

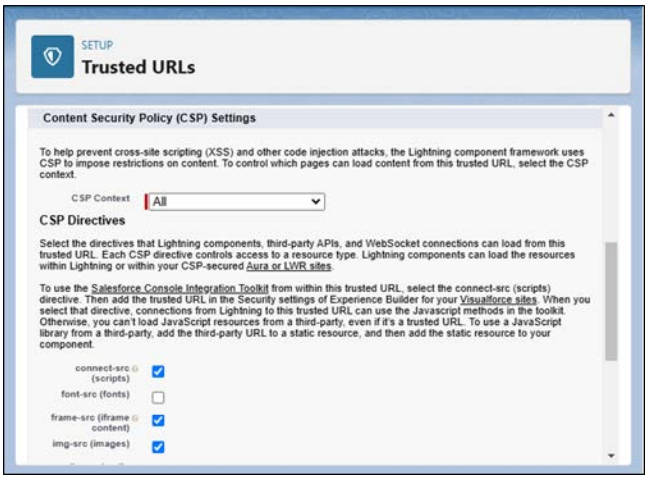
- API Name - Enter the API name for the trusted URL, such as "Kiteworks".
- URL - Enter the Kiteworks server URL, for example https://*<your-kiteworks-url.com>*.
- (Optional) - Enter a description for the trusted URL.



4 Configure the Content Security Policy (CSP) Settings.

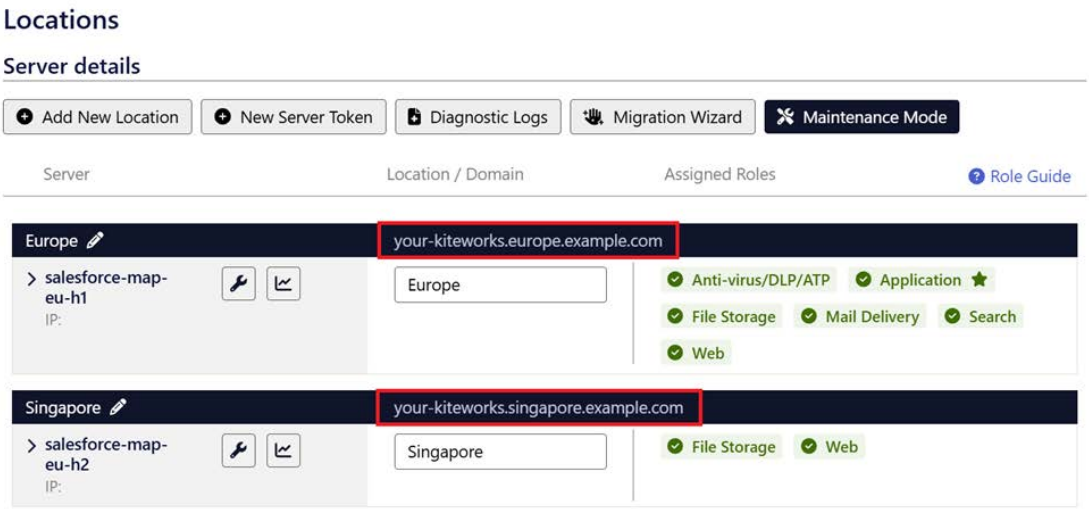
- CSP Context - Select "All".
- CSP Directives - Select the following checkboxes:

- connect-src (scripts)
- frame-src (iframe content)
- img-src (Images)



5 Click Save.

6 If you have multiple locations configured in the Kiteworks Admin Console, repeat the steps above to add a Trusted URL for each location. The example image below shows two locations in the Kiteworks Admin Console that would need to be added: *https://your-kiteworks.europe.kiteworks.com* and *https://your-kiteworks.singapore.kiteworks.com*.



Enable Lightning Web Security in Salesforce

Enabling Lightning Web Security allows Kiteworks for Salesforce Lightning to download Kiteworks files since the plugin uses iFrame to perform download operations.

To enable Lightning Web Security in Salesforce:

1 On the Setup page, search for "Session Settings".

Alternative: In the navigation pane, go to Settings > Security > Session Settings.

2 On the Session Settings page, select the "Use Lightning Web Security for Lightning Web Components and Aura components" checkbox.

3 Click Save.

4 Clear your browser cache.

Enable the plugin in the Kiteworks Admin Console

Prerequisite: So that users can access Kiteworks for Salesforce Lightning, upload a Salesforce license to the Kiteworks Admin Console.

To upload a license:

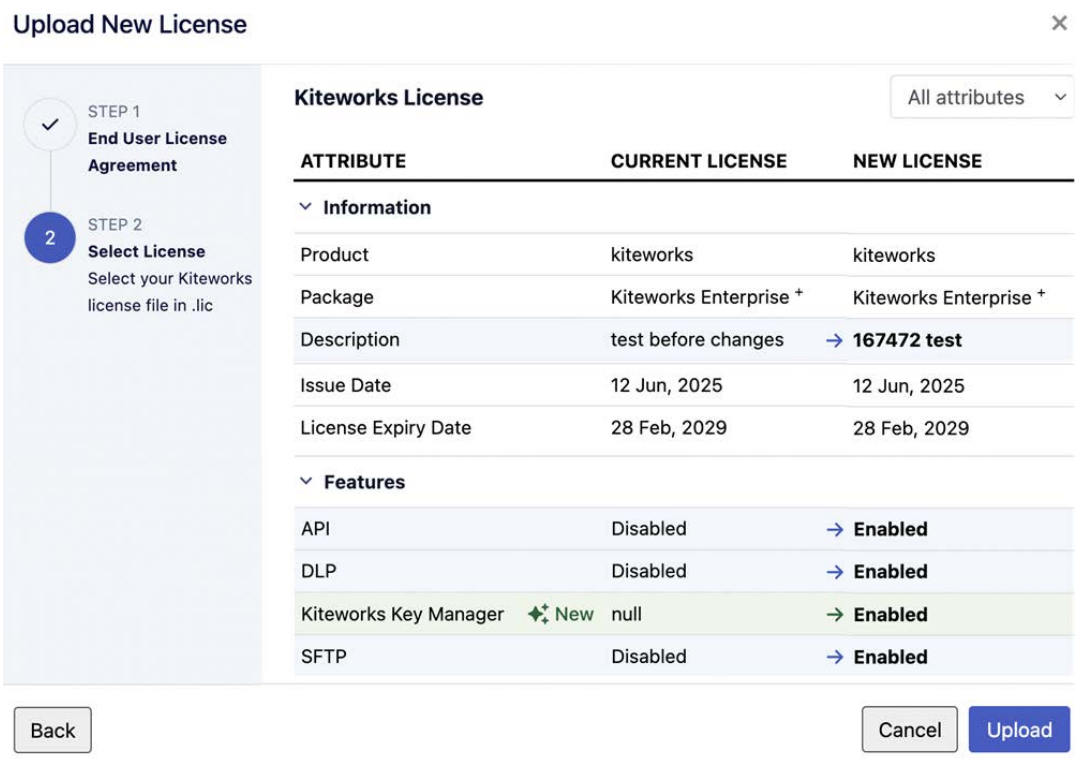
1 Go to Application Setup > Licenses > Kiteworks License, and then click Upload New License.

2 Review the End User License Agreement.

3 Enter your first and last name to sign the license agreement, and then click Accept.

4 On the Upload New License page, select the license file, and then click Upload.

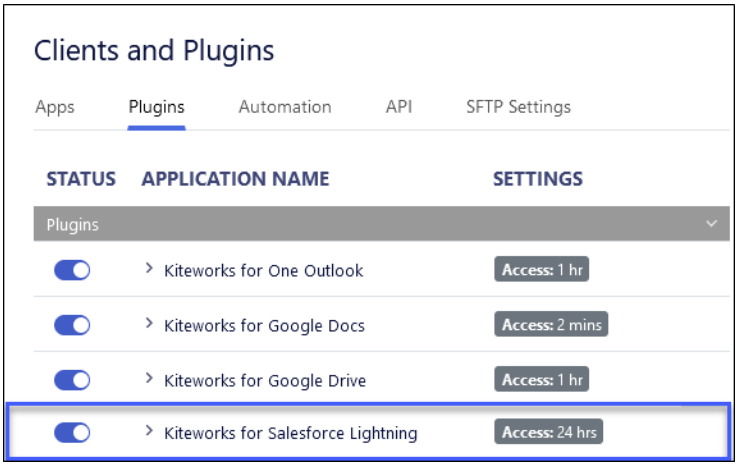
5 Review the license attribute comparison table showing differences between the current and new license, and then click Upload.



Result: The license gets uploaded to the server and relevant information is extracted for display on the license page.

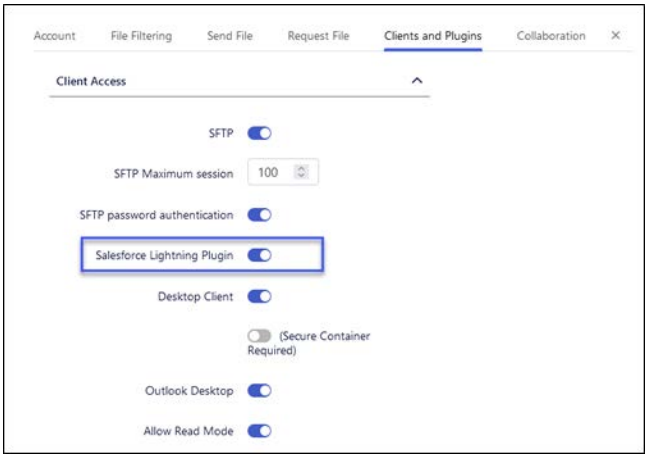
To enable the plugin:

1. Go to Application Setup > Clients and Plugins > Plugins.
2. Turn on Kiteworks for Salesforce Lightning.



To provide user access to the plugin:

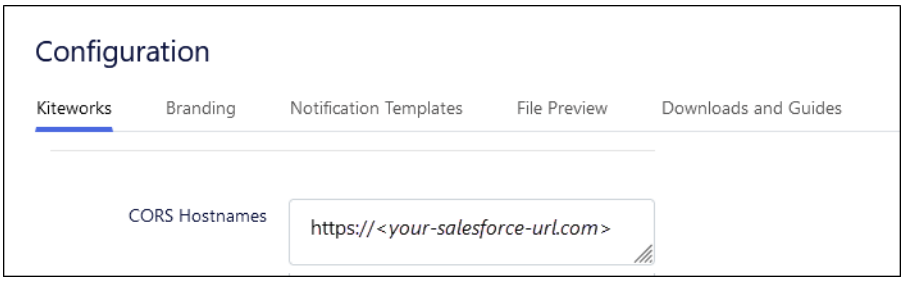
1. Go to Users > Profiles > *expand a profile* > Clients and Plugins.
2. Under Client Access, turn on Salesforce Lightning Plugin.



To configure the CORS hostname:

1 Go to Application Setup > Configuration > Kiteworks.

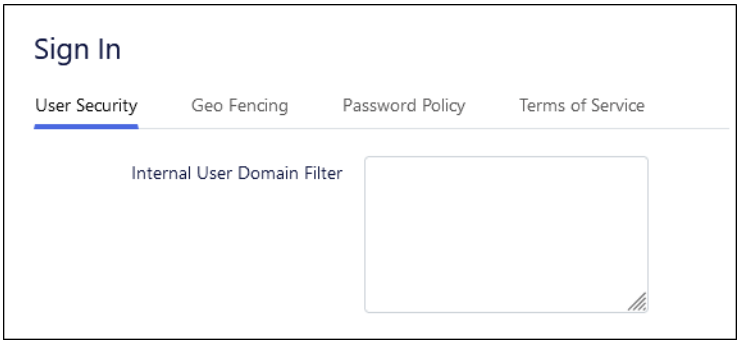
2 In the CORS Hostnames box, enter the Salesforce URL starting with https://. For example: https://<*your-salesforce-url.com*>.



To add the domain for the plugin:

1 Go to Security Policies > Sign In > User Security.

2 In the Internal User Domain Filter box, enter the domain.

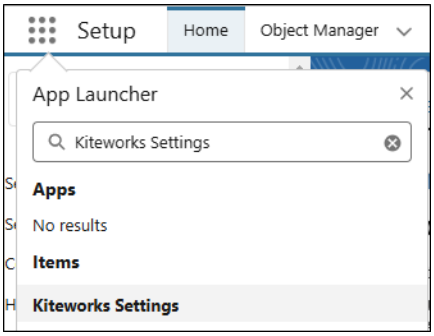


3 Click Save.

Generate a Consumer ID, Client Secret, and Private Key

To generate a Consumer ID, Client Secret, and Private Key:

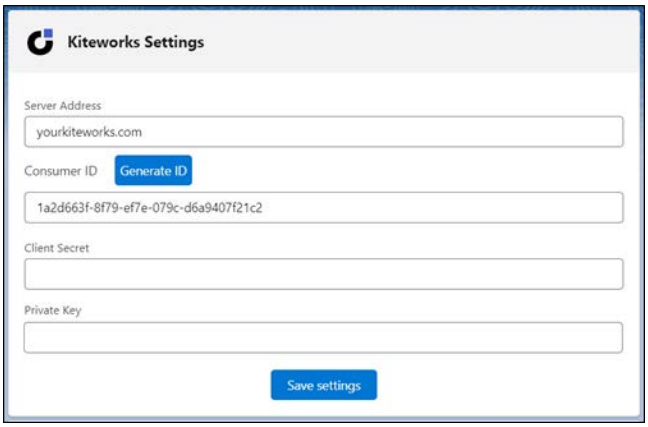
1 In Salesforce, from the App Launcher, search for "Kiteworks Settings".



2 On the Kiteworks Settings page, in the Server Address box, enter the host name of the Kiteworks server.

3 Next to Consumer ID, click Generate ID. Save a copy of the Consumer ID for configuring Kiteworks for Salesforce Lightning in the Kiteworks Admin Console.

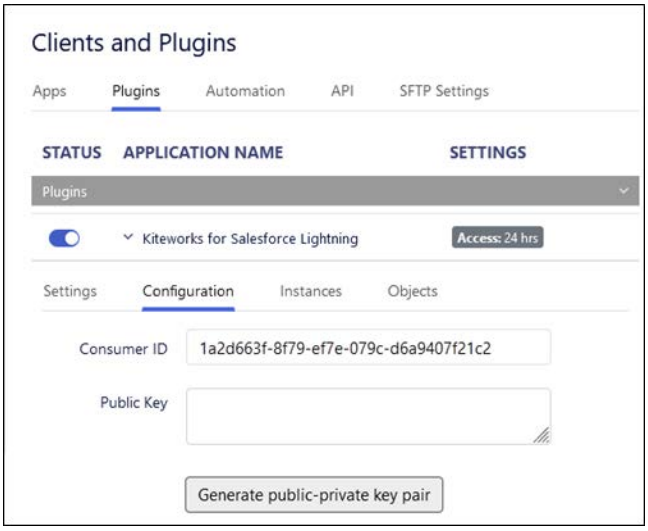
4 Click Save Settings.



5 In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Plugins.

6 Under Kiteworks for Salesforce Lightning, click the Configuration tab.

7 In the Consumer ID field, paste the consumer ID you generated in Salesforce.

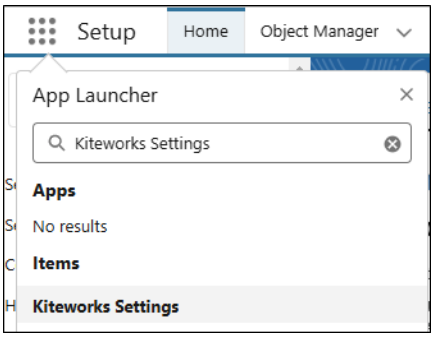


8 Click "Generate public-private key pair", and then save a copy of the generated key to finish configuring the "Kiteworks Settings" in Salesforce.

9 Click "Generate client secret", and then save a copy of the generated key to finish configuring the "Kiteworks Settings" in Salesforce.

10 Click Save.

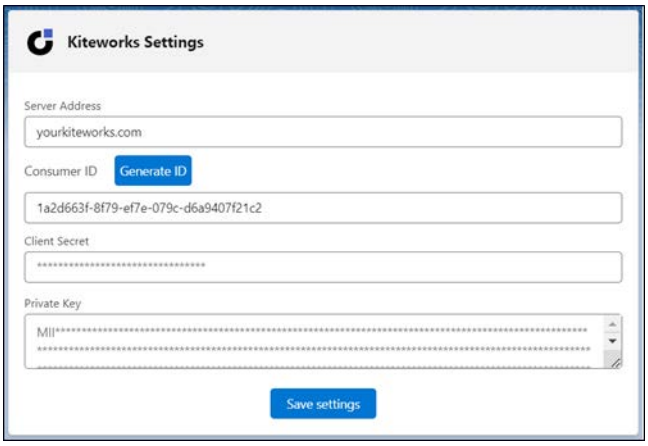
11 In Salesforce, from the App Launcher, search for "Kiteworks Settings".



12 On the Kiteworks Settings page, in the Client Secret field, paste the client secret you generated in the Kiteworks Admin Console.

13 In the Private Key field, paste the key you generated in the Kiteworks Admin Console.

14 Select the Apex Trigger on Case Creation checkbox, and then click Save Settings.



Enable custom objects in Salesforce

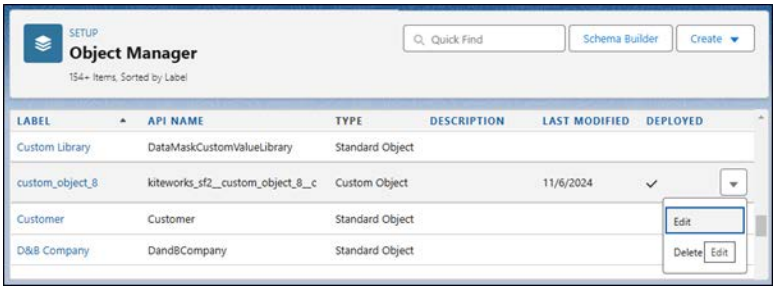
If you use custom objects in Salesforce, enable them in Salesforce.

To enable custom objects in Salesforce:

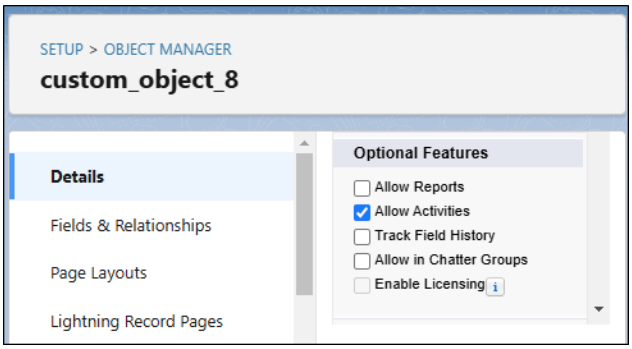
1 On the Setup page, search for "Object Manager".

Alternative: In the navigation pane, go to Platform Tools > Objects and Fields > Object Manager.

2 Select the custom object, and then click Edit.



3 In the Optional Features list, select the Allow Activities checkbox.



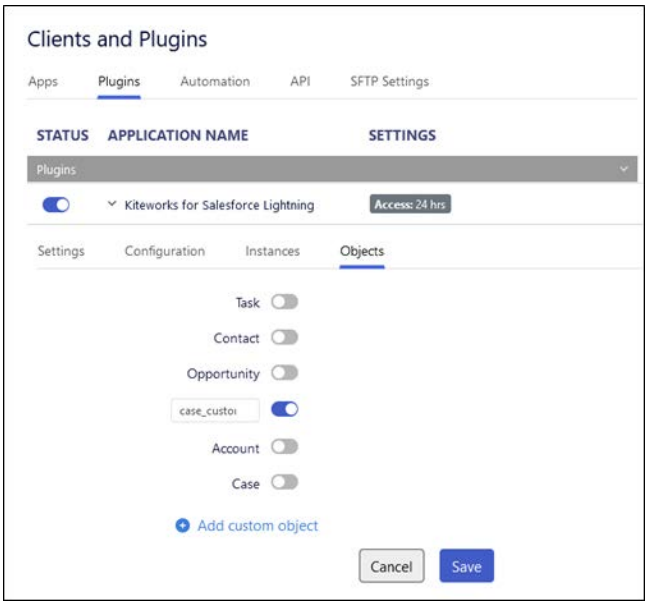
Add custom Salesforce objects to the Kiteworks Admin Console

If you enabled custom objects in Salesforce, add them to the Kiteworks Admin Console.

To add custom Salesforce objects to the Kiteworks Admin Console:

1 In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Plugins.
2 Under Kiteworks for Salesforce Lightning, click the Objects tab.
3 On the Objects tab, click Add Custom Object.
4 Enter the name of the Salesforce custom object you want to add.
5 Turn on the object switch, and then click Save.

Result: The custom object is added and is also available to select in user profiles that can access Salesforce objects.

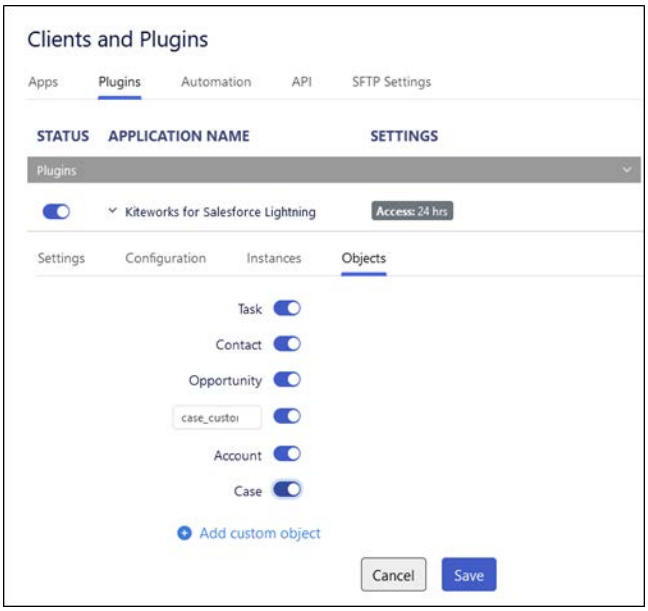


Enable Salesforce objects in the Kiteworks Admin Console

To enable Salesforce objects in the Kiteworks Admin Console:

1 In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Plugins.
2 Under Kiteworks for Salesforce Lightning, click the Objects tab.

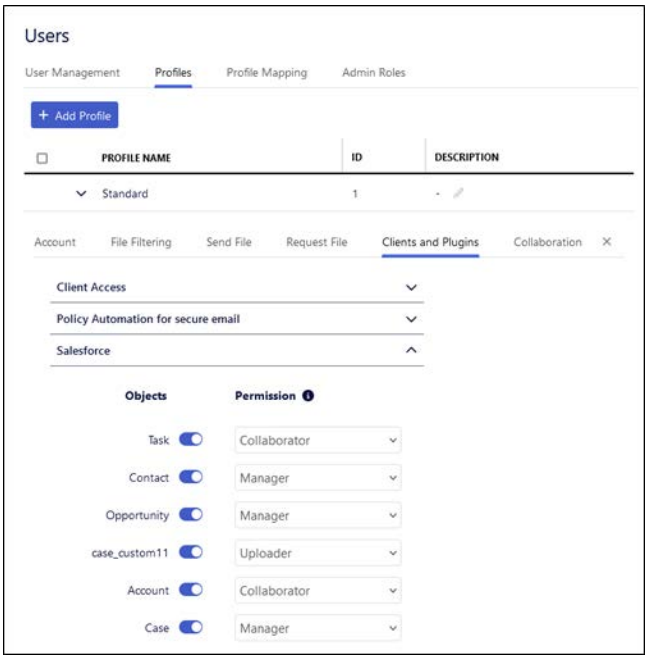
3 Turn on all object switches, and then click Save.



Grant user profile access to Salesforce objects

To grant user profile access to Salesforce objects:

1 Go to Users > Profiles > *expand a profile* > Clients and Plugins.
2 Under Salesforce, turn on the objects you want to be accessible to users assigned the profile.
3 Assign permissions (Kiteworks end user roles) to objects, and then click Save.

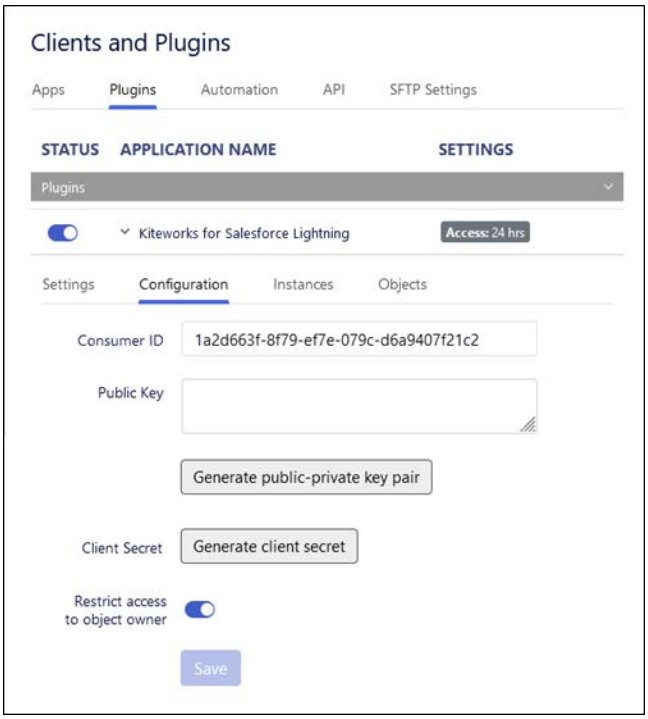


Allow only object owners to access Kiteworks for Salesforce Lightning in Salesforce objects

By default, all Salesforce users have access to Salesforce objects where the Kiteworks for Salesforce Lightning plugin has been added. To allow only the object owners to be able to access objects containing the Kiteworks for Salesforce Lightning plugin, you can enable object owner restriction.

To allow only object owners to access Kiteworks for Salesforce Lightning in Salesforce objects:

1. In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Plugins.
2. Under Kiteworks for Salesforce Lightning, click the Configuration tab.
3. Turn on "Restrict access to object owner", and then click Save.



Configure Kiteworks for Salesforce Lightning to use multiple instances of Salesforce

By default, deploying Kiteworks for Salesforce Lightning creates a single Salesforce instance. You can configure the plugin to support more than one Salesforce instance, allowing the plugin to properly distinguish between Salesforce instances.

Warning: Once you add more than one instance, you can't revert to a single instance. You also can't delete the additional instances. It is strongly recommended that you take a snapshot of each node on the Kiteworks system to preserve its state and data prior to adding multiple instances. If you experience an issue, you can revert each node to its prior state. For on-premises deployments, refer to snapshot instructions corresponding to your virtual machine. If your system is hosted by Kiteworks, contact Kiteworks technical support at https://community.kiteworks.com to request that they take a snapshot of each node for you. Provide the date and time of your planned maintenance window, the name of each node you want to back up, and the time you want the snapshots to be taken. Technical support will notify you once the snapshots have been taken.

To Kiteworks for Salesforce Lightning to use multiple instances of Salesforce, perform the following tasks:

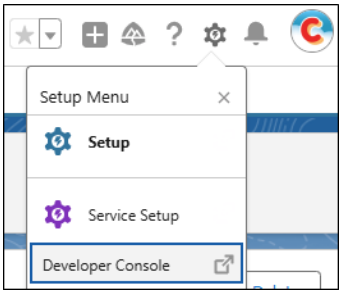
- Find your Salesforce Organization ID.
- Add another Salesforce instance to the Kiteworks Admin Console.
- Provide user access to a new Salesforce instance.

Find your Salesforce Organization ID

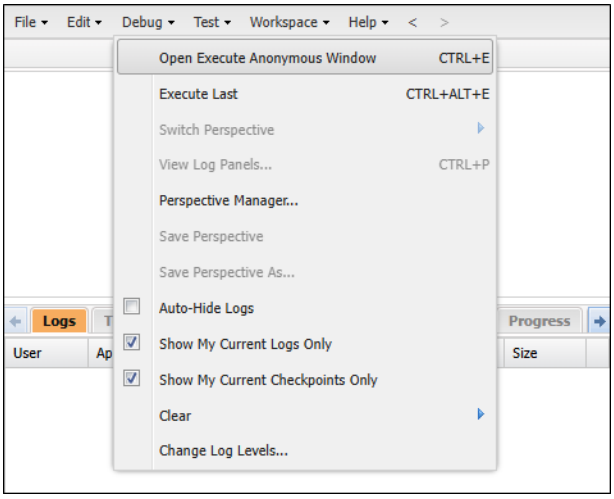
Your Salesforce Organization ID is the unique identifier for your Salesforce identity. You will need it to add a new Salesforce instance to the Kiteworks Admin Console.

To find your Salesforce Organization ID:

1 In Salesforce, click the Setup ⚙ icon on the toolbar, and then click Developer Console.

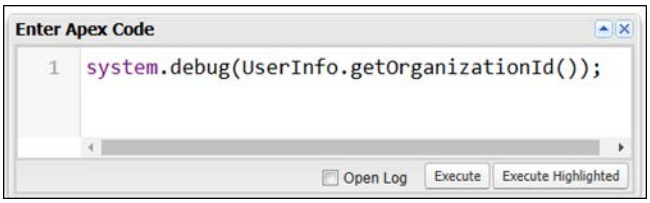


2 In the Developer Console, click Debug > Open Execute Anonymous Window.



3 In the Enter Apex Code box, enter the following code to get your Salesforce Organization ID:

```
system.debug(UserInfo.getOrganizationId());
```

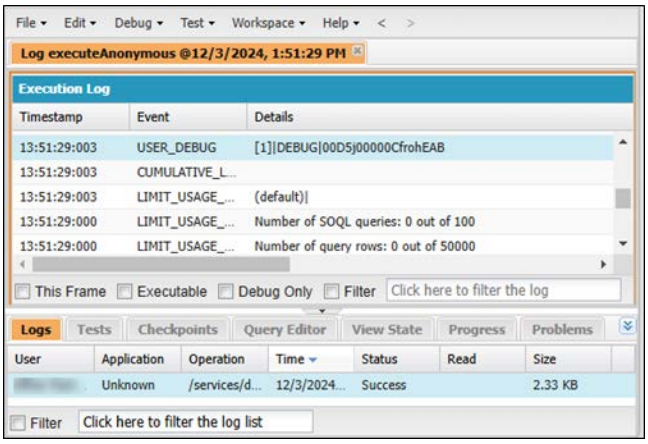


4 Click Execute.

5 In the Logs section, click the log you just generated.

6 In the log, go to the USER DEBUG event row and write down the 18 character ID.

Example: In "DEBUG|00D5j00000CfrohEAB", the 18 character ID is 00D5j00000CfrohEAB.



7 Save a copy of the ID to add a new Salesforce instance to the Kiteworks Admin Console.

Add another Salesforce instance to the Kiteworks Admin Console

Warning: Once you add multiple instances, you can't revert to a single instance.

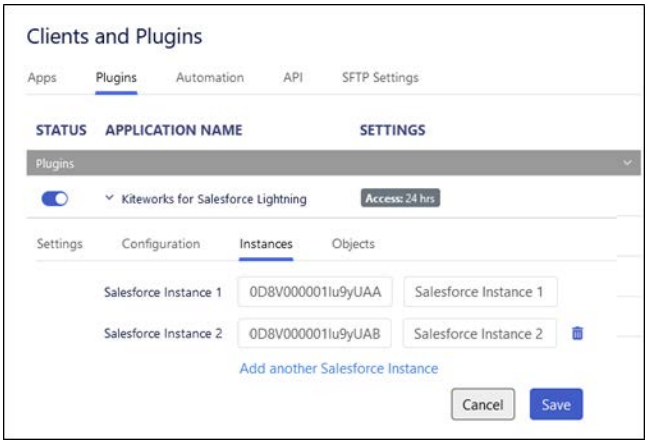
To add another Salesforce instance to the Kiteworks Admin Console:

1 In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Plugins.

2 Under Kiteworks for Salesforce Lightning, click the Instances tab.

3 Click "Add another Salesforce instance", and then enter the 18 character Salesforce Organization ID you copied from the Salesforce Developer Console.

4 Provide a name for the new instance, and then click Save.



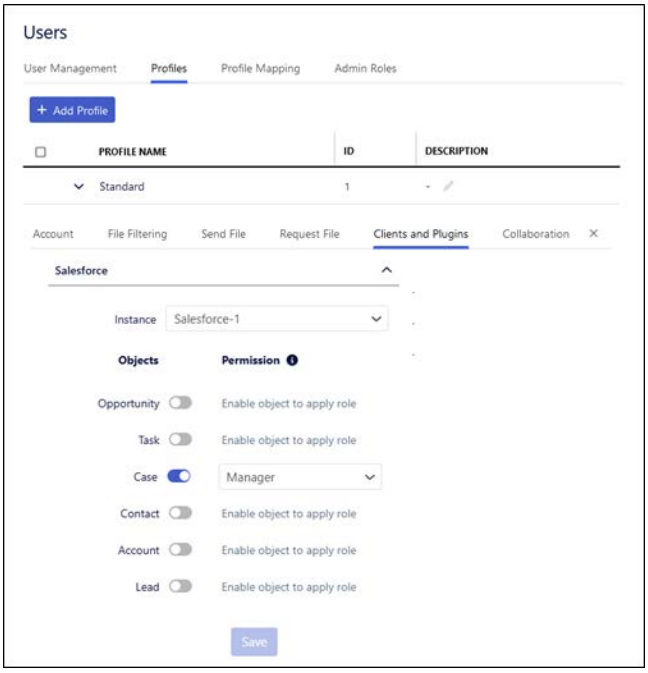
5 Confirm that you want to add the new instance.

Provide user access to a new Salesforce instance

You provide user access to a new Salesforce instance through a user profile in the Kiteworks Admin Console.

To provide user access to a new Salesforce instance:

1. In the Kiteworks Admin Console, go to Users > Profiles > *expand a profile* > Clients and Plugins.
2. Under Salesforce, select the instance you want to be accessible to users assigned the profile.
3. Turn off any enabled object switches and then turn them on again.
4. Assign or update permissions (Kiteworks end user roles) for the objects in the new Salesforce instance, and then click Save.

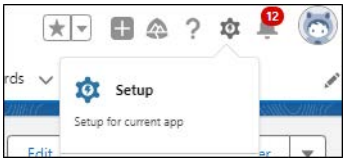


Set up the Salesforce Experience Cloud Community

If you want to use Kiteworks for Salesforce Lightning in Experience Cloud, set up your Salesforce Experience Cloud Community. Enabling this feature will allow Kiteworks for Salesforce Lightning to be available in Experience Cloud Community environment and serve its functionalities to the community. Salesforce Experience Cloud is available in Salesforce Enterprise, Performance, Unlimited, and Developer editions.

To set up the Salesforce Experience Cloud Community:

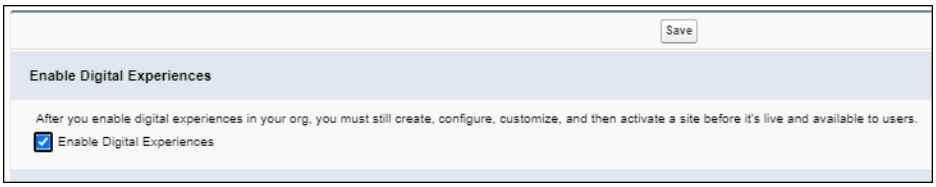
1. In Salesforce, click the Setup icon on the toolbar, and then click Setup.



2. On the Setup page, search for "Digital Experiences".

   Alternative: In the navigation pane, go to Platform Tools > Feature Settings > Digital Experiences.

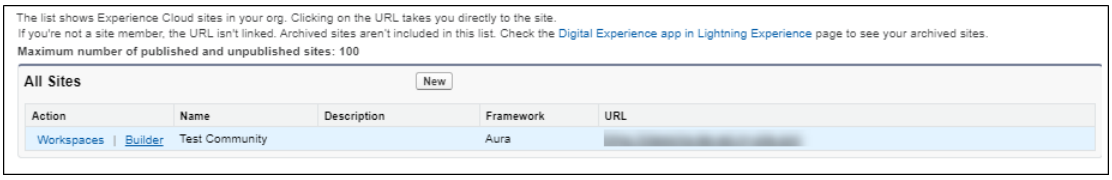
3 Select the Enable Digital Experiences check box, and then click Save.



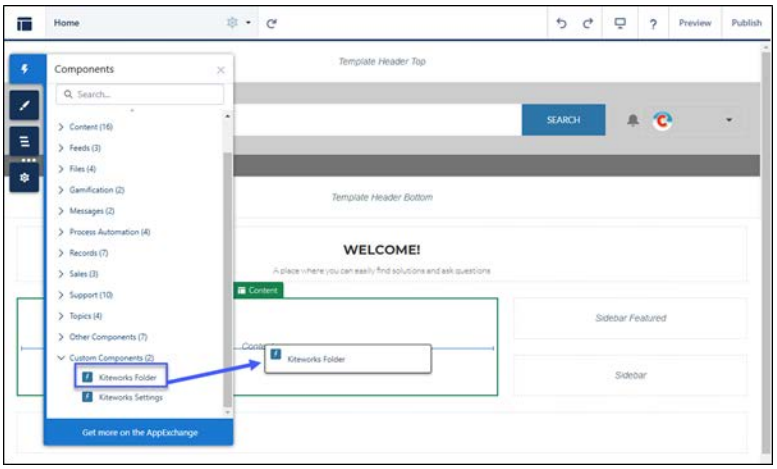
4 In the Digital Experience section, click All sites.

5 On the All Sites page, in the row of your organization's website, click Builder and customize the website as needed.

Note: If there are no websites, click New, and then select a suitable template with your desired URL. Once added, click Builder and customize the website as needed.

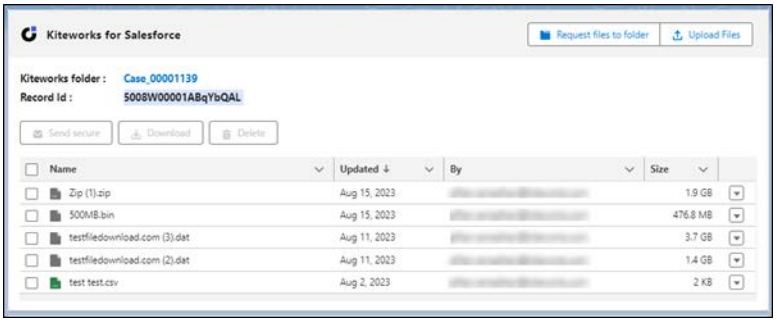


6 In the Experience Builder, click the Custom Components button, and then drag the "Kiteworks Folder" component to the layout.



7 In the layout, click "Kiteworks Folder" and configure the Object Name and Record ID fields.

- Object Name - Case, Contact, or Opportunity.
- Record ID - The Record ID of the Salesforce Object ID, such as Case ID, Contact ID, or Opportunity ID.



8 In the top right corner of the Experience Builder, click Publish.

Result: The Kiteworks Folder and Kiteworks Settings are added to the Experience Cloud page.

Apex Trigger on Case Creation

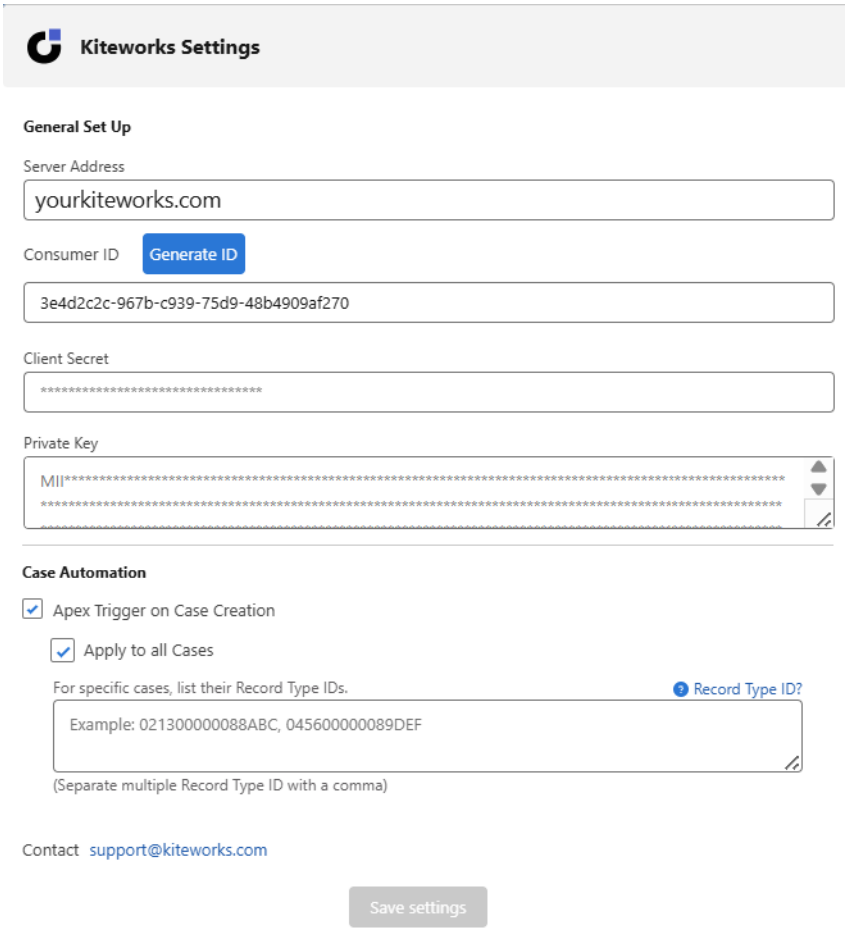
Apex Trigger on Case Creation automatically creates a corresponding Case folder in Kiteworks when a new case is created in Salesforce. It also sends a file request from Kiteworks to the recipient's email address in the Contact field for external domains.

Note: This feature does not currently support multi-instances.

To enable Apex Trigger on Case Creation:

1. Go to Kiteworks Settings in Salesforce.
2. In the Kiteworks Settings box, select the Apex Trigger on Case Creation.

   Result: An "Apply to all Cases" checkbox and text field for specifying Record Type IDs is displayed.
3. Perform one of the following actions:
   - If you want to apply the Apex Trigger to all cases, select the Apply to All Cases checkbox.
   - If you want to apply the Apex Trigger to only specific cases, enter the Case Record Type ID corresponding to each case. You can add up to 13 Record Type IDs.



4. Contact Kiteworks technical support at https://community.kiteworks.com to request enabling this feature on the Kiteworks side.

Automation

Kiteworks Automation Agent

The Automation Agent is a Command Line Interface (CLI) utility that extends and automates enterprise secure file transfer capabilities. It automates Send File (Upload) and Download of files, folders, email notification of file transfer activities and status, and scheduled file transfers.

kAA license

The Kiteworks Automation Agent is enabled through the Kiteworks license when it is purchased. With the latest Kiteworks release none of the following packages are included by default. You have to purchase the Enterprise Addon suite and upload a new license in addition to purchasing a Kiteworks system to use the following packages:

- SFTP
- APIs
- Automation Agent for Windows, Mac and Linux
- Kiteworks Secure MFT Client

Notes:

- Existing Kiteworks systems that are already using SFTP, APIs and the Automation Agent will be allowed to use these packages without disruption.
- Additionally, after a software update, if none of the above packages were previously being used, then a new license with the Enterprise Addon suite will need to be uploaded to enable these packages.

Get started with the Kiteworks Automation Agent

To use the agent, perform the following steps:

1. Upload the License to enable the functionality of the agent for your Kiteworks setup.
2. Go to Application Setup > Clients and Plugins > Automation.
3. On the Automation tab, enable the automation agent for the target platform (Windows, Linux or Mac) that you would like the agent to run on. This can be done by turning the toggle switch to ON in the Status column.
4. To download the agent, download the installer for the target platform. Optionally, you can download the *Kiteworks Automation Agent User Guide*.
5. Send the installer and the guide to the end user that needs to use the agent.

See the *Kiteworks Automation Agent User Guide* for more information on installing, uninstalling and using the Kiteworks Automation Agent.

Kiteworks Secure MFT Client

The Kiteworks Secure MFT Client enables users to automate tasks or entire processes using Node-RED.

Node-RED provides an editor for wiring together flows using a wide range of nodes that you can deploy to runtime in a single-click. Node-RED includes extensive documentation to help you learn how to use the tool. You can access the Node-RED documentation at https://nodered.org/docs/.

Once you've enabled the application on the server, you can make it available for users to download from the Kiteworks Web Application. You can also make the *Kiteworks Secure MFT Client User Guide* available for download from the web application.

Enable Secure MFT Client on the Kiteworks server

The Kiteworks Secure MFT Client is available if you purchased the Kiteworks Automation Agent license. Once you've installed the license, you need to enable the application on the Kiteworks server.

To enable the application in the Kiteworks Admin Console:

1. In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Automation.
2. In the Automation section, turn on Kiteworks Secure MFT Client.
3. To ensure that the Secure MFT Client application stays up to date with the latest features and security updates, ensure that automatic updates are enabled by default on the Secure MFT Client configuration page. When a new version is available, end users will be notified and prompted to install the update.

To make an installer available from the Kiteworks Web Application:

1. In the Kiteworks Admin Console, go to Application Setup > Configuration > Downloads and Guides.
2. In the Apps and Plugins section, click Edit.
3. Select the applications you want users to be able to download, and then click Save.

To make user documentation available from the Kiteworks Web Application:

1. In the Kiteworks Admin Console, go to Application Setup > Configuration > Downloads and Guides.
2. In the Help section, click Edit.
3. Select the documents you want users to be able to download, and then click Save.

Install Secure MFT Client

You install Secure MFT Client as a Windows service where it runs in the background on your computer even if you close the application. Flows continue to run in the background unless you stop the service.

Installing Secure MFT Client also installs Node.js. This adds a palette manager to the Node-RED editor main menu so that you can install new nodes from both the Node-RED library as well as the wider community.

Prerequisites: If you plan to run the service using a non-default user account, your account needs the following permissions to run the service and its application files:

- Permission to run a service.
- Read permissions on the installation directory and its sub-directories.
- Write permission on the Kiteworks Secure MFT (Windows Service) folder. When you create flows, they are stored in the flows.json file in this folder. The client will need to be able to update this file.

As an administrator, you can download and install the application directly from the Kiteworks Admin Console. End users download and install the application from the Kiteworks Web Application. For end user installation and use instructions, refer to the *Kiteworks Secure MFT Client User Guide*.

To download Secure MFT Client from the Kiteworks Admin Console:

1. In the Kiteworks Admin Console, go to Application Setup > Clients and Plugins > Automation > Kiteworks Secure MFT Client.
2. On the Downloads tab, download Kiteworks Secure MFT Client (Windows Service).
3. Click the installation file you downloaded and follow the instructions on the screen.
4. In the Service Settings dialog box, specify how you want to run the service.

- To run the service using your default local system account, leave the service settings blank.
- To run the service using a different local user account, enter the user name and password for the account.

Rule: The service can run using only a local user account, not a domain user account.

5 Specify where you want to install the application.

6 The default installation location is: C:\Program Files (x86)\Kiteworks Secure MFT (Windows Service).

7 Complete the installation.

Result: The Kiteworks Secure MFT Client service starts automatically in the background on your computer. You can open the Windows Services app to verify that service is running.

To open the Secure MFT Client:

You can open the application in the following ways:

- On your desktop, click the Kiteworks Secure MFT Client (Windows Service) shortcut.
- In a web browser, enter the following address: http://localhost:1881/red

Uninstall Secure MFT Client

Recommendation: If you want to preserve your flows, export them to save as backups. If you reinstall the application, you can import the flows for use again. In the *Kiteworks Secure MFT Client User Guide*, refer to "Export flows".

To uninstall the Secure MFT Client:

1 Open Windows "Services" app and stop the Kiteworks Secure MFT Client Service.

2 Browse to the installation folder.

3 The default installation location is: C:\Program Files (x86)\Kiteworks Secure MFT (Windows Service).

4 Double-click the uninstall.exe file.

5 Delete the Kiteworks Secure MFT Client (Windows Service) folder.

Kiteworks Secure MFT Server

The Kiteworks Secure MFT Server provides a management console that provides secure automated data transfers to and from Kiteworks. It has the ability to create, schedule, manage, monitor and control automated content transactions in the following content firewall scenarios:

- B2B, Kiteworks to Kiteworks
- SFTP to Kiteworks
- Kiteworks to SFTP

Listed below are some key features of the Secure MFT Server:

- The Secure MFT Server is based on Apache Airflow.
- More than one Secure MFT Server can be enabled on a Kiteworks cluster as long as the connected Kiteworks server has the Secure MFT Server license.
- Once the Secure MFT Server is deployed, only the MFT service runs on that server.
- The default roles are, Admin, DAG Manager, Operator, and Public.
- In the management console the user can create a DAG (workflow) which is a collection of all the tasks you want to run, organized in a way that reflects their relationships and dependencies.

To enable the Secure MFT Server to work from a Kiteworks instance, go to the Kiteworks Admin Console, and then click Application Setup > Clients and Plugins > Automation. Click the ON/OFF switch in the Status column to turn it on.

Once enabled, you can enter you Secure MFT Server URL, for example, https://<airflow server domain/ip>:8080, to get redirected to the server. The user will need to have an account for the server in order to log in.

API

Create custom applications

Custom applications can be used to automate business workflows, such as on-boarding new Kiteworks users to access relevant folders automatically. Kiteworks APIs are used to develop custom applications. The Custom Application page lists all custom applications that already exist on the system.

To create a custom application:

1. Go to Application Setup > Clients and Plugins > API, and then click Create Custom Application.
2. Enter the following information:
   - Name: Enter a name for your custom application.
   - Description: Enter a description for your application.
   - Flows: Select the authorization flow that your application will use to obtain an access token.
     - Authorization code: Standard OAuth 2.0 authorization-code grant type consists of authorization, consent, and code redemption process.
     - Signature authorization: Use this flow when the registered client can verify the identity of the user, and only for trusted applications. You can generate a random signature key or manually enter the key.
     - User credential: Use this flow to allow the registered client to obtain the access token by providing their user name and password. This flow should be used only for trusted applications that cannot use a web form-based login, but require the user to authenticate with their user name and password (any command line based utilities). This flow follows the Resource Owner Password Credentials Grant specified in RFC 6749.
   - Enable refresh token: If enabled, when an access token expires, a new access token can be obtained using a refresh token without re-initiating the authorization process.
   - Redirect URI: Specify a redirect URI for securely passing authorization requests. The Redirect URI can contain custom schemes like a server URL (such as https://) or an app URL (such as myapp://). For example, myapp://127.0.0.1/path. Or it could contain %%HOST%% which will resolve the hostname of the current Kiteworks instance. For example, https://%%HOST%%/oauth_ callback.php.
   - Access token lifetime: Set the duration for a token lifetime.
   - Refresh token lifetime: If "Enable Refresh Token" is enabled, set the duration that an access token can be refreshed.
3. Click the APIs you plan to use for your custom application.

   Scopes are defined limits to client applications for accessing data. By selecting the appropriate scopes for the application, you allow or restrict certain tasks from being performed by a user or on behalf of a Kiteworks user. Each custom application that is created can have server-side authorization scopes. You can define on the server which endpoints the custom application is allowed to use and how they can be used.

4. Click Add Application, and then copy the Client Application ID, Client Secret Key, and the Signature Secret to a secure location for safe-keeping.

   Caution: The Client Application ID and Client Secret Key cannot be changed and should be protected since these credentials could be used to access Kiteworks systems, potentially exposing the systems to loss or theft of critical information. You are responsible for keeping these credentials safe and sharing them with only trusted individuals.
5. Confirm that you copied the Client Application ID, Client Secret Key, and the Signature Secret.
6. Click the custom application you just created and customize additional settings as needed.
   - Settings: You can make changes to the initial settings you already configured.
   - Scopes: You can add or remove API scopes.
   - Security:
     - Remote wipe enabled: Enable remote wipe functionality for the application.
     - Pin enabled: Specify whether a PIN should be enabled for the application. This is recommended for mobile applications.
     - White listed apps: List any third-party mobile applications that can be used to open files via the "Open-In" menu. Use comma-separated ID search strings (for example, com.domainname.appname, *).
7. Click Save.
   - To test the custom application, go to https://<*hostname of your Kiteworks deployment*>/rest/index.html.
   - To prepare the application for distribution, click the Distribution tab. Export the application package and submit it for certification at developer.kiteworks.com.

Enable the Kiteworks API Playground UI

The Kiteworks API Playground contains sample Python code and instructions for parameters. Code can be copied and pasted into your integrated development environment (IDE). The sample code library is accessible from the admin console as part of the API license or when participating in the Kiteworks Secure API free 60-day trial.

To enable the Kiteworks API Playground:

1. Go to Application Setup > Clients and Plugins > API.
2. In the top right corner of the page, turn on the Enable Kiteworks API Playground button.

To get started using the Kiteworks API playground:

1. Create a custom application and ensure that Signature Authorization is enabled.
2. Go to the playground at https://<hostname of your Kiteworks deployment>/rest/index.html.
3. On the Kiteworks API Documentation toolbar, click "Get a Token".
4. In the Request OAuth Token dialog box, select Signature-based Access Token from the grant list.
5. Fill in the information based on the application you just created in the Kiteworks Admin Console.
6. Test all the API endpoints through the playground.
7. Register the application at https://developer.kiteworks.com.

SFTP Settings

Configure SFTP

To configure SFTP settings:

1. Go to Application Setup > Clients and Plugins > SFTP Settings.
2. Configure the settings, and then click Save.

Table 55. SFTP settings

Setting	Description
Maximum SFTP sessions in system	The maximum number of open SFTP sessions allowed on the system. When a user tries to sign in using SFTP, the system will check to see if there are sessions available. The default is 10000. Maximum is 50000. You can also control the number of SFTP sessions per user profile. To specify the number of SFTP sessions per user profile: Go to Users > Profiles > *expand a profile* > Clients and Plugins. Specify the maximum number of sessions. The default is 10000. Maximum is 50000.
SFTP sessions idle timeout	How long SFTP control connections can be idle before they time out. The maximum is 86400. The default is 600 seconds (10 minutes). Minimum is 60 seconds. Maximum is 86400 seconds (24 hours).
Access token lifetime	The token lifetime duration, which specifies the validity duration of an access token from the time it is granted. The default is 720 hours. Maximum is 1440 hours.
Refresh token lifetime	Issued together with the access token, the refresh token can be used to renew the access token. Refresh token lifetime specifies the validity duration of a refresh token since it was granted. The default is 1440 hours. Maximum is 1440 hours.

Software Update

Back up the database

Back up the Kiteworks database prior to updating Kiteworks. Backing up the database backs up all application data. This enables you to restore the database in the event of data corruption or loss during a software update. Only one backup is stored at a time. When you back up the database, the old version is replaced with the current backup.

You don't need to turn on maintenance mode to perform a Kiteworks database backup.

If you've taken a virtual snapshot of the database, you don't need to back up the database. If you have multiple servers, be sure to take a virtual snapshot of each server.

EPG Database Backup

Back up the EPG database prior to updating Kiteworks.

Note: The option to back up the EPG database is available if you've also deployed a cluster with the EPG Database role enabled on one or more nodes.

Backing up the database backs up all application data. This enables you to restore the database in the event of data corruption or loss during a software update. Only one backup is stored at a time. When you back up the database, the old version is replaced with the current backup.

Prior to backing up the database, you may be prompted to activate maintenance mode.

If you've taken a virtual snapshot of the database, you don't need to back up the database. If you have multiple servers, be sure to take a virtual snapshot of each server.

Update Kiteworks

Get early access to software updates

You can opt-in to receive early access software update which will require a new test license to test new features and capabilities before the update is released for general availability (GA). An early access software update includes major planned features for the next GA release. When this option is enabled, the system will check for an early access version in addition to the GA versions of the software updates.

Note: Once you have updated to an Early Access version you will not be able to revert back to the prior version on your system. To opt in to early access software updates, go to System Setup > Software Update > Settings.

Things to consider before installing a software update

Disk space required and time taken for the software update

Due to different sizes of organizations, data, and databases, it is not possible to confirm whether a specific amount of available disk space will be enough for an update. This can only be confirmed by Kiteworks Technical Support.

Most software updates range between 400 MB to 1 GB. When performing a software update, it is recommended to download the update and perform the update when convenient. This can reduce the time it takes to complete the update. The speed at which the files are downloaded depends on the WAN connection. A slow connection could take hours for the update to complete.

After the packages have been downloaded to all the servers and the update starts, the main application server will run through a series of database processes, which can take between 5 to 90 minutes depending on the resources of the system and the size of the database.

Update availability

If you receive an alert of a software update, but the system is reporting no new updates are available, or an update version that does not match the software update alert, you can clear the update cache for each server. Go to Software Update. To clear the update cache, go to System Setup > Software Update > Settings. In the Host table on the Update tab, expand each server node, and then click Clear Cache. After clearing all caches, go to the blue panel at the top of the page and click Check Again to check for the latest update.

Database backup

Prior to a software update, it is recommended you take a snapshot of each node in the cluster.

- Do not shut down multiple servers with Application roles assigned to them at the same time. Only one Application role can be down at any given time. You will need to shut down the single server with the Application role, take the snapshot, start the server and wait until the dashboard has reported that the server has recovered and displays in green. Depending on how fast the connection is to the other application servers and how large the database is will determine how long it takes to recover. This process could take up to 90 minutes. Do not shut down any subsequent servers that have the Application role assigned to them until all Application servers are green and available. After the server has recovered, you can move onto the next Application server.
- Servers that do not have an Application role assigned to them can be shut down at any time. You can choose to shut down, take a snapshot, and start the servers one by one like what is required with the Application role server, or choose to shut down all servers that have no Application role assigned to them at the same time, take a snapshot of all of them and then start them.

Alternatively you can back up the Kiteworks database prior to updating Kiteworks. Backing up the database backs up all application data and enables you to restore the database in the event of data corruption or loss during a software update. Only one backup is stored at a time. When you back up the database, the old version is replaced with the current backup. You don't need to turn on maintenance mode to perform a Kiteworks database backup. If you've taken a virtual snapshot of the database, you don't need to back up the database. To back up the database, go to System Setup > Software Update > Update. In the blue panel at the top of the page, click Generate Backup.

The system is offline during a software update

During a software update, the entire platform will be offline in maintenance mode and will automatically restart several times. Services will be restarted and unavailable as well. Users trying to connect to the system will see a message informing them that the system is in maintenance mode and to try again later.

Note: To minimize down time, Kiteworks uses the closest geographic mirror to obtain the software update.

Troubleshooting network connectivity

Each node must be able to reach update.kiteworks.co and resolve the IP address of that hostname and any hostname it may redirect to, such as update01.accellion.net, update4.accellion.net, update5.accellion.net, or update6.accellion.net. To resolve a hostname/IP address using the configured DNS server, go to System Setup > Locations. Next to the server name, click the wrench icon, and on the DNS Lookup tab configure and test the hostname/IP address.

Port 443 connectivity to the IP address of the server is required unless a proxy is required. To test port connectivity, go to System Setup > Locations. Next to the server name, click the wrench icon, and then click the Check Connectivity tab.

- If the test succeeds, but the software update page reports an issue with connecting to the update server, ensure that a software update proxy is not misconfigured on the node. See Configure proxy servers.
- If no proxy is set and port 443 is open to the update server, and the software update page is still reporting a connection issue, check with your network team and confirm no filtering devices are filtering the SSL/TLS connections. Although port 443 connectivity may be available, the SSL/TLS handshake could be filtered by a network security application.
- If a proxy is configured perform a DNS Lookup check to confirm the Kiteworks appliance is able to resolve the hostname of the proxy if a hostname is configured. Also ensure that the Kiteworks appliance is able to connect to the proxy on the specified port.
- If the Kiteworks appliance is able to resolve and connect to the software update proxy, contact your proxy administrator and make sure the Kiteworks appliance and update servers are in an allow list so that the connection is allowed, and investigate any logs that report the HTTP requests to the update server.

Update Kiteworks

To install a software update:

1. Go to System Setup > Software Update > Update.
2. On the Update tab, if a new version of the software is available the information is displayed in the blue panel at the top of the page. You can also click Check for online update to check for updates.
3. If an update is available, the System Pre-Check panel shows whether the system passed all prechecks for installing the update. You can also click Show Details to view the result of each pre-check.
4. In the Update Mode list, select the type of update to install.
5. If you only want to download the update file for future use, click Download Only, and then click Download Update. Once the download is complete, the page will be updated to notify you that the software update package is ready for installation.
6. When you are ready to install the update, perform one of the following actions:
   - If you are performing an online software update, click Download & Run Update.
   - If you downloaded a software update, once the download is complete, click Run Update.

Apply patches

When you apply a patch the entire platform will be offline in maintenance mode and will automatically reboot several times. Services will be restarted and unavailable.

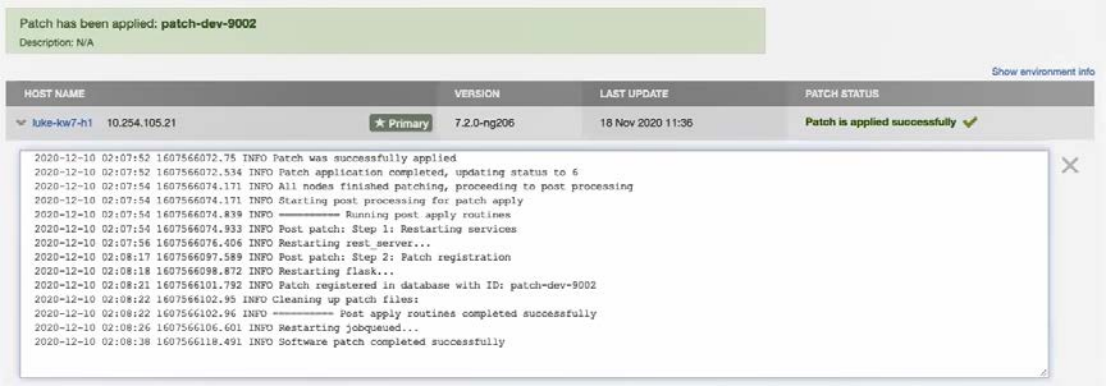
To apply a patch:

1. Go to System Setup > Software Update.
2. On the Update tab, in the Update Mode list, click Patch Update.

3 On the update page, activate the patch or upload a patch received from Kiteworks technical support.

4 Click Apply Patch.

Result: As the patch is applied, the system performs several pre- and post-installation checks. Once the process is complete, the Software Update page indicates that the patch was installed.



Revert patches

You can revert only the latest patch that was applied. When you revert a patch, the patch is deregistered from the system. The entire platform will be offline in maintenance mode and will automatically reboot several times. Services will be restarted and unavailable. To revert a patch, click the Revert Patch link under the patch name.

Locations

Server roles

- Anti-virus/DLP/ATP role
- Archival role
- Application role
- Email Protection Gateway roles
- File Storage role
- Key Manager role
- Mail Delivery role
- Repositories Gateway Cloud role
- Repositories Gateway On Premise role
- SafeEDIT role
- Search role
- SFTP role
- SMTP Automation role
- Web role

Anti-virus/DLP/ATP role

Provides anti-virus, data loss prevention (DLP), and advanced threat protection (ATP) services by scanning files for viruses or sending files to a third-party DLP and ATP server for scanning.

This role is CPU intensive and should be on the same node as the Storage role for direct access to the files for scanning.

Archival role

Performs journaling and archiving of emails sent through Kiteworks. This role requires a license and can only be enabled on a dedicated node, with no other roles enabled on that node.

Application role

Provides the business logic for Kiteworks and contains the database for system configuration, user information, and file metadata. All metadata of the information in Kiteworks cluster is stored here. All LDAP queries come from the Application role.

This is a mandatory role. When using an LDAP/AD server for authentication, the firewall rules must allow communication from all servers with Application roles to the LDAP/AD server.

One server in a Kiteworks deployment must be running the primary Application role.

If you need to disable the Application role on a server set as "Primary", first move the Primary designation as follows:

To designated a different Application role as the primary Application role:

1. Go to System Setup > Locations, and then click to expand the server with the primary Application role (designated with a "star").
2. Next to the primary Application role, click the arrow and then click Reassign Primary.
3. On the Assign Primary Application page, select another server with an Application role to move the primary designation to, and then click Reassign.

   Note: Only eligible servers will be displayed.
4. Turn off the old primary Application role on the initial server.

Reassign an unavailable primary application server

If the Primary Application server is unavailable, the Kiteworks system will continue to operate as long as a quorum of Application servers are available. However, as the Primary Application server is responsible for sending emails, the Kiteworks system will not be able to send emails until another server is promoted to the Primary Application role.

Important:

- In the case of reassigning the Primary Application server, the administrator needs to configure the Application servers to use the mail relay (firewall and correct routing information). Kiteworks recommends that the mail relay be configured for all Application servers to save time in a disaster situation.
- We strongly recommend that you contact Kiteworks technical support at https://community.kiteworks.com in a disaster situation. However, you will want to bring back the failed Application server as soon as possible. If there are not enough Application servers to form a quorum, users will no longer be able to access Kiteworks content until a majority of the Application servers become available again.

For example:

If the Primary Application server goes down in a three-Application server cluster, you can:

1. Detect that the Primary Application server has gone down.
2. Reassign the Primary Application server to one of the remaining two Application servers (service restart may be necessary).
3. When the old Primary Application server is powered on, it will rejoin the cluster.
4. Once the old Primary Application server comes back up, the database will be updated from the other Application servers and it will know it is no longer the Primary Application server.

Email Protection Gateway roles

Kiteworks Email Protection Gateway (EPG) simplifies sending encrypted, compliant messages and attachments from the web or mobile, in Microsoft 365, or other email systems or enterprise applications. Centralized policy controls and rules automation ensure sensitive messages are encrypted while allowing users to work with their standard clients and without the need for plugins or training.

EPG requires two different Kiteworks roles:

- Email Protection Gateway role
- Email Protection Gateway Database role

Enabling the Email Protection Gateway role assigns the EPG functions to the node. Backend changes are made to enable the EPG Admin console (https://<external hostname or IP>/mailadmin) and the EPG Webmail console (https://"IP address"/responsiveUI).

Before enabling the Email Protection Gateway role on a node, review the requirements below. For more detailed information, refer to the Kiteworks Email Protection Gateway Deployment Guide and Kiteworks Email Protection Gateway Administrator Guide.

Note: EPG is a license-enabled feature. If your Kiteworks license does not include this feature, you will not see the option to turn on the Email Protection Gateway role.

Multi-node deployments

When deploying EPG, you must turn on the Email Protection Gateway role and the Email Protection Gateway Database role. You can deploy several Email Protection Gateway roles and up to three Email Protection Gateway Database roles. Kiteworks recommends deploying EPG in a multi-node configuration, with two or more EPG nodes connected to a 3-node EPG database cluster. This configuration provides redundancy for EPG operations to ensure that a failure on one node in the cluster does not impact the others. In a 3-node EPG database cluster, the system is protected against database failure and data loss.

While the Email Protection Gateway role and the Email Protection Gateway Database role can be enabled on the same node, no other Kiteworks roles should be enabled on a node with either the Email Protection Gateway role or the Email Protection Gateway Database role.

Firewall requirements

Each EPG node requires the following ports open for proper communication. For detailed port configuration information, refer to the "Network configuration" section in the Kiteworks Email Protection Gateway Deployment Guide.

- 25
- 80
- 389
- 443
- 636
- 3316
- 33160
- 33161

Turn on the Email Protection Gateway Database role

Enabling the Email Protection Gateway role requires that the Email Protection Gateway Database role be enabled before the Email Protection Gateway role.

When enabling the Email Protection Gateway Database role, consider the following:

- You can deploy multiple Email Protection Gateway roles and up to 3 Email Protection Gateway Database roles in a cluster (three are recommended for resiliency and fault toleration).
- In a cluster environment, the Email Protection Gateway Database role and Email Protection Gateway Database role can coexist on a node, but no other Kiteworks roles should be enabled on that node.
- Port 3316 must be open between each Email Protection Gateway node and Email Protection Gateway Database node.
- When an EPG database cluster is used, ports 3316, 33160, and 33161 must be open between all Email Protection Gateway Database nodes. On all Email Protection Gateway Database nodes, ports 3316 and 33160 must be open to all EPG nodes as well.
- You can enable the same Kiteworks anti-virus on an Email Protection Gateway node. Kiteworks recommends enabling EPG Anti-virus on the same node as the Email Protection Gateway role for the best performance. Kiteworks does not recommend enabling the EPG Anti-virus on the same node as the Email Protection Gateway Database.
  Important: When the EPG Anti-virus is enabled, it consumes a general Anti-virus license.

To turn on the Email Protection Gateway Database role:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure, and then turn on the Email Protection Gateway Database role.

Turn on the Email Protection Gateway role

Prerequisite: Turn on the Enterprise Protection Gateway Database role.

To turn on the Email Protection Gateway role:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure, and then turn on the Email Protection Gateway role.

File Storage role

The File Storage role stores all user files. You can move the storage role from one Kiteworks server to another. Physical files can be moved from one storage (source server) to another target server, which means copying files and content over the network and removing the source.

The following three points must be noted while performing a Move Storage operation:

- During a move operation, files can still be downloaded from the source server (the server that is being moved).
- During a move operation, files cannot be uploaded to the source server (the server that is being moved). However, files can still be uploaded to the destination server or a third storage server if one is available in your location.
- The move storage operation can only be performed within a location. If an organization has two locations, for example, in Netherlands and Germany, the move storage operation can only be performed among the servers in Germany or among the servers in Netherlands. The move storage

operation cannot be performed from a Germany location to a Netherlands location.

- Folders and users are not moved during a move storage.

You can click the role to reassign the role.

If you would like to reassign the File Storage role, for example, reassign the role as a Sync File Storage, a prompt will display asking to move the File Storage (users, files and folders) to another location before reassigning the role in this location.

Click Move to move file storage. The Move File Storage window displays asking the user to choose an eligible destination host with available space along with how much space is available and whether a move to that location is allowed or not.

The Move Storage progress is displayed in the role manager and can be paused, resumed, and cancelled. If you choose to cancel you will be asked to confirm the process.

When Move Storage in progress it will still allow to assign or unassign other roles, except the Application role. It will also prevent any other big tasks, for example, another move storage, software update, shutdown, etc.

Once the move is complete, any files that could not be moved will be listed on the screen. You can view and download the files, and also choose whether to retry, skip, or delete the files from the move process.

Note: The states are currently tracked only in the Kiteworks Admin Console.

Key Manager role

Key Manager is a server role that enhances the security of internal encryption keys on file storage nodes in a cluster. It acts as an internal Hardware Security Module (HSM) by keeping and serving encryption secrets. It takes encryption keys currently stored on file storage nodes, encrypts them, and then saves the keys in the Key Manager.

Requirement: To access the Key Manager role, the Key Manager feature needs to be activated in your Kiteworks license. To view the features included with your license, see View and upload licenses. If the Key Manager license is included, it is listed in the Features section. To request this feature, please contact your Kiteworks account representative.

Turn on the Key Manager role

You can enable the Key Manager role on any server node. During the process you must provide a passphrase to protect the storage keys in the cluster. Then you can link the file storage nodes you want to protect. Linking a file storage node to the Key Manager host node automatically configures Key Manager as the HSM on those nodes.

Warning: The passphrase used to protect the storage keys in the cluster is not recoverable. It is strongly recommended you take a virtual snapshot of the entire system before enabling the Key Manager role. If necessary, you can restore the snapshot to return the file storage node encryption keys to their original formats for reuse again.

To turn on the Key Manager role:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure, and then turn on the Key Manager role.
3. On the Key Manager Configuration page, enter and confirm the passphrase you want to use, and then click Save.
4. **Rule:** Password rules are set by the password policy configured for the system. To edit the password policy, see Set the password policy.
5. Link the file storage nodes you want to protect using the Key Manager.

Recommendation: Link all file storage nodes to ensure that all stored data receives the additional layer of encryption provided by the Key Manager. If you don't link all file storage nodes, an alert will display on the dashboard listing the unlinked nodes in case you want to link them. You can click the alert to return to the Locations page for linking the additional nodes.

Results:

- The Locations page shows the Key Manager role enabled on the host node.
- On each linked node, a lock icon is added to the File Storage label indicating that the Key Manager HSM settings are configured for protecting the data stored on those nodes.

Link additional file storage nodes to the Key Manager

To link additional file storage nodes to the Key Manager:

1. On the Locations page, expand the server node where the Key Manager role is enabled.
2. Next to the Key Manager role, click the arrow and then click Manage Storage Node.
3. Next to each file storage node you want to protect using Key Manager, click the Link button.

If a node status is listed as Unavailable, another HSM has been configured on that node. To make the node available, you'll need to remove the current HSM configuration on the node, and the repeat the steps above to link the node. To remove HSM settings on a node, expand the server node, click the External Services tab, and then clear the "Enable HSM" checkbox.

To unlink file storage nodes from the Key Manager:

1. Click the node where the Key Manager role is enabled. Next to the Key Manager role, click the arrow and then click Manage Storage Node.
2. On the configuration page, unlink the nodes you want.

Change the Key Manager role passphrase

When you change the Key Manager role passphrase, a new master key pair is generated and encrypted using the new passphrase.

To change the Key Manager role passphrase:

1. Click the node where the Key Manager role is enabled. Next to the Key Manager role, click the arrow, and then click Manage Storage Node.
2. On the reset page, enter and confirm the new passphrase, and then click Save.

Unlock the Key Manager role

The Key Manager role gets locked when you restart the host node individually or as part of a complete system reboot. Once the node restarts, file storage nodes linked to the Key Manager won't apply the additional layer of encryption until you unlock the Key Manager role. When the Key Manager role is locked, you're notified in the following ways:

- An alert on the Kiteworks Admin Console dashboard. Click the alert to access the role.
- Next to the role, a lock icon is added next to the Key Manager switch.

To unlock the Key Manager role:

1. In the roles section, next to the Key Manager switch, click the lock icon.
2. On the Unlock Key Manager Service page, enter the passphrase, and then click Unlock.

Turn off the Key Manager role

To turn off the Key Manager role:

1. In the roles section, turn off the Key Manager role.
2. On the Key Manager Deactivation page, enter the passphrase, and then click Continue.
3. Unlink all of the nodes, and then click Deactivate.

   Results:

   - The Locations page shows the Key Manager role is off on the node.
   - The lock icon is removed File Storage label on any nodes that were linked to the Key Manager node, indicating that the Key Manager HSM settings are not configured on those nodes.

Mail Delivery role

The Mail Delivery role sends emails sent by end-users, administrators, system notification emails, etc., from a Kiteworks cluster. This role is different from the SMTP Automation role, which is responsible for receiving emails, replacing attachments with secure Kiteworks links and sending these modified emails to the intended recipients. The Mail Delivery role can be enabled on multiple hosts in the cluster. This gives the administrator more flexibility and ensures failover and load balancing.

After first time set up (FTS), Kiteworks automatically assigns the Mail Delivery role on the existing Primary Application host.

Note: If the server does not have an Application role, it is recommended to turn on the Application role. For better performance, enable the Mail Delivery role on hosts that have an Application role.

To configure the Mail Delivery role, see Configure mail relay settings.

Repositories Gateway Cloud role

Provides access to Repositories Gateway sources, such as DropBox, Box, and Google Drive. Allows Kiteworks to integrate with Repositories Gateway systems or file stores.

This role requires a license.

Repositories Gateway On Premise role

Provides connectivity to content sources, such are SharePoint, Home Drives, and File shares (CIFS).

This role requires a license and is not available in multi-tenant systems. Requires a separate designated server and must be deployed on-premises, regardless of Kiteworks being on-premises or hosted. Place this role as close to the Repositories Gateway source as possible on the network.

SafeEDIT role

SafeEDIT next-generation digital rights management (DRM) enables possessionless editing of shared files by internal and external users in a browser-based virtual UI, while the files stay protected in the Kiteworks server cluster.

SafeEDIT requires a SafeEDIT license for the subset of seats for those who will use the feature. Keep the following in mind:

- The first time a user edits a file in SafeEDIT mode, they are assigned and retain a SafeEDIT license.
- You can monitor SafeEDIT license usage from the System Status page and also filter by SafeEDIT account type on the Users > User Management page.
- If you have a limited number of available SafeEDIT licenses, periodically releasing licenses from inactive users will free up licenses for other users. To release a user's SafeEDIT license, go to Users > User Management, select the user whose license you want to release, and then click the Release SafeEDIT License button.

When deploying SafeEDIT you need to ensure that application editors corresponding the file types you want accessible for SafeEDIT are installed on the server. You also need to edit the relevant SafeEDIT configuration files on the Windows server to map the required file types to the relevant applications. For instructions on how to deploy SafeEDIT, refer to "Appendix C - Deploy SafeEDIT" in the *Kiteworks Deployment Guide*. You can access the guide from the admin console help menu.

Turn on the SafeEDIT role

Prerequisite: Ensure the Kiteworks cluster has TCP 443 connectivity to safeedit-license.kiteworks.co.

To turn on the SafeEDIT role:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure, and then turn on the SafeEDIT role.
3. Next to the SafeEDIT role, click the arrow, and then click Configure.
4. On the SafeEDIT Configuration page, configure the host settings, and then click Save.
5. Ensure the server has TCP 443 connectivity to *safeedit-license.kiteworks.co*.

Table 56. SafeEDIT host settings

Setting	Description
Session time limit	The amount of time after which an active session will automatically end, regardless of inactivity. The session time limit ensures that users do not leave sessions open indefinitely, preventing another user from starting a new session. You can specify a value from 3600 seconds (1 hour) to 7200 seconds (2 hours).
Watermark opacity	Adjust the watermark opacity and preview the watermark that is displayed to Kiteworks web application users editing files in SafeEDIT mode.
Number of concurrent sessions per server	The number of concurrent sessions each SafeEDIT Windows Server can support at any given time.

To add a SafeEDIT Windows Server:

1. On the SafeEDIT Configuration page, click Add Servers.
2. Configure the connection settings, and then click Save.

Table 57. SafeEDIT Windows Server connection settings

Setting	Description
IP/hostname	The IP address and hostname of the Windows server.
Remote Desktop Protocol (RDP) port	The port that will be used for the server with the SafeEDIT role to connect to the Windows server. The default is port 3389, but you can enter a different port number. This port number must be open between the Kiteworks node and the static servers used for SafeEDIT. Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel.

Search role

The Search role is on by default and enables searching within the Kiteworks Web Application. Users can search for folder names, file names, message attachment file names, and content within message subject lines and body text. If you turn off the Search role, users can search only for folder and file names, and email addresses of message senders and recipients.

If you want to give users the ability to search for content in file and message file attachments, you can turn on search indexing. Keep the following in mind:

- The time it takes to perform content search indexing depends on the number and size of files to be indexed. Full content searching in the Kiteworks Web Application is not available until all files have been indexed.

- Every three minutes the system searches for new or updated files to index. If there are a large number of files to index, the Kiteworks Admin Console may experience resource issues while indexing is in progress. The Search role is a resource-intensive role and requires high usage of CPU, memory (RAM), and disk space. CPU is heavily used by the extraction library during file indexing.
- The size of a full content search index can take up to 85 percent of total storage space on the disk. If there is not enough disk space, indexing will stop.
- While indexing is in progress, you can hover your mouse over the Search role to view the status.
- Once indexing is complete, Kiteworks Web Application users will see an additional "Include content" filter option when viewing their search results. They can use this option to expand their results to include content found in files and message file attachments.

To turn on the Search role:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure, and then turn on the Search role.

To turn on search indexing:

1. Go to System Setup > Locations.
2. Click to expand the server containing the activated Search role.
3. Next to the Search role, click the arrow, and then click Configure.
   Note: After expanding the node containing the Search role, it may take a moment for the arrow to appear next to the role.
4. On the Index Content page, turn on search indexing.

SFTP role

Enables users to store and deliver files transparently over SFTP using any available client that supports SFTP.

This role requires a license and is not available in multi-tenant systems. Enable this role on all servers with an active Web role that are in the DNS for the application domain name. This role must be publicly accessible to access SFTP client from the outside. By default, port 22 must be accessible by all end users for all servers assigned the SFTP role.

SMTP Automation role

SMTP Automation is an easy way for scanning devices or other applications to send out secure emails via Kiteworks. It provides the ability to share data and reports securely using the existing built-in SMTP service. SMTP Automation accepts an email with attachments over SMTP protocol, replaces the attachments with secure Kiteworks links and then relays the email to the recipient.

The SMTP Automation role can be on multiple servers and can exist together with other roles on the same server.

Click SMTP Automation to enable it.

Note: SMTP Automation works on only single tenant (standalone) Kiteworks systems. Multi-tenant systems will not be able to see this role or its settings.

Important: SMTP Automation is part of the Kiteworks Automation Suite but will require a new license file for the SMTP Automation feature to be enabled. The Automation Suite also includes the Automation Agent, REST API and SFTP. Just like SMTP Automation, each of these individual features has to be included separately in the license file to be enabled.

Click the Configure icon to configure the SMTP Automation settings.

The SMTP Automation Settings window displays.

- Port - You can modify this field. The default value is set at 12525. The SMTP Automation will listen to incoming emails on this port on all network interfaces.
- Allowed Incoming IP Range - Specifies the IP ranges of your applications or devices that can send emails to this server's SMTP Automation.
- Enforce TLS - You can check or uncheck this box. It is checked by default. Enforcing TLS ensures that emails are sent to the SMTP Automation securely. If enabled, non-TLS connections will be rejected by SMTP Automation.
- Bounce Relay - Bounce Relay is an optional setting. If hostname or IP address is entered entering a Port value is mandatory.
- Port - SMTP Automation will use this server to send bounce notifications (non-delivery reports).
- Enable SMTP Automation Role - If the SMTP Automation role is already on, an Update button displays if any changes are made to the settings.

Send File settings

The emails relayed by SMTP Automation follow most of the Send File settings of the sender's user profile. These settings can be accessed by the administrator at Users > Profiles > *select a profile* > Send File.

Web role

Provides access to the web browser, API's, mobile apps, desktop clients, and other plugins. The Web role is an endpoint that the DNS points at to serve web requests to end users.

This is a mandatory role. To use the Web role internally, the internal DNS needs to point to this server and users must have access to the server.

Group servers by location

System administrators define Locations, which are logical groupings for servers; these logical groupings will be used by application administrators for replication and user upload mapping rules.

Use this screen to:

- Create a Location.
- Assign, add, or reassign servers to a Location, using drag and drop.
- Configure Location Proximity to optimize data traffic. Optional: Assign a DNS entry for a Location.
- Manage Storage, Network Settings, and Security settings for individual servers.

Create a location

When set, the DNS settings for Locations will allow Kiteworks to route a user's activities, including file upload and download, to the closest Kiteworks server. A URL domain needs to be specified that can be used to access the servers in this location, for example, location.domain.com. In addition, the domain should be registered in a DNS to point to the servers and an SSL certificate should support the domain that is being set.

For example, if a European user is traveling to the United States, their upload/download traffic will be routed to the server closest to them.

Edit a location

Use this screen to set up storage service for the selected Location: Virtual Disk.

Virtual disks

Virtual disks are the default native file storage for Kiteworks servers. This does not require any setup.

Enable storage failover

When a file is uploaded and there is not enough storage in the most proximate location, the administrator has an option to enable or disable Storage Failover to be able to use an alternate upload location.

You can enable or disable upload failover if the upload location is derived by the location of the Web server. Upload failover will not occur if the upload location is the user's preferred location. Enable Storage Failover is enabled by default.

Configure location proximity

The Location Proximity feature optimizes data traffic by routing data uploads to an end user's nearest Kiteworks location.

Kiteworks offers an Enable Location Proximity Feature option which when enabled optimizes performance for users around the world by routing requests to servers closest to the user's location. Locations can be created throughout an organizations' business premises, such as, state locations, country locations, continent locations to optimize the network traffic with minimal drag on performance inside a multi-location cluster. For example, if a request is made to an organization in Chicago with the Location Proximity feature enabled, the client will be directed to the closest location in Chicago for that session. If the information is not available in that location, the system will retrieve it from the next closest location and continues this process till the information is located.

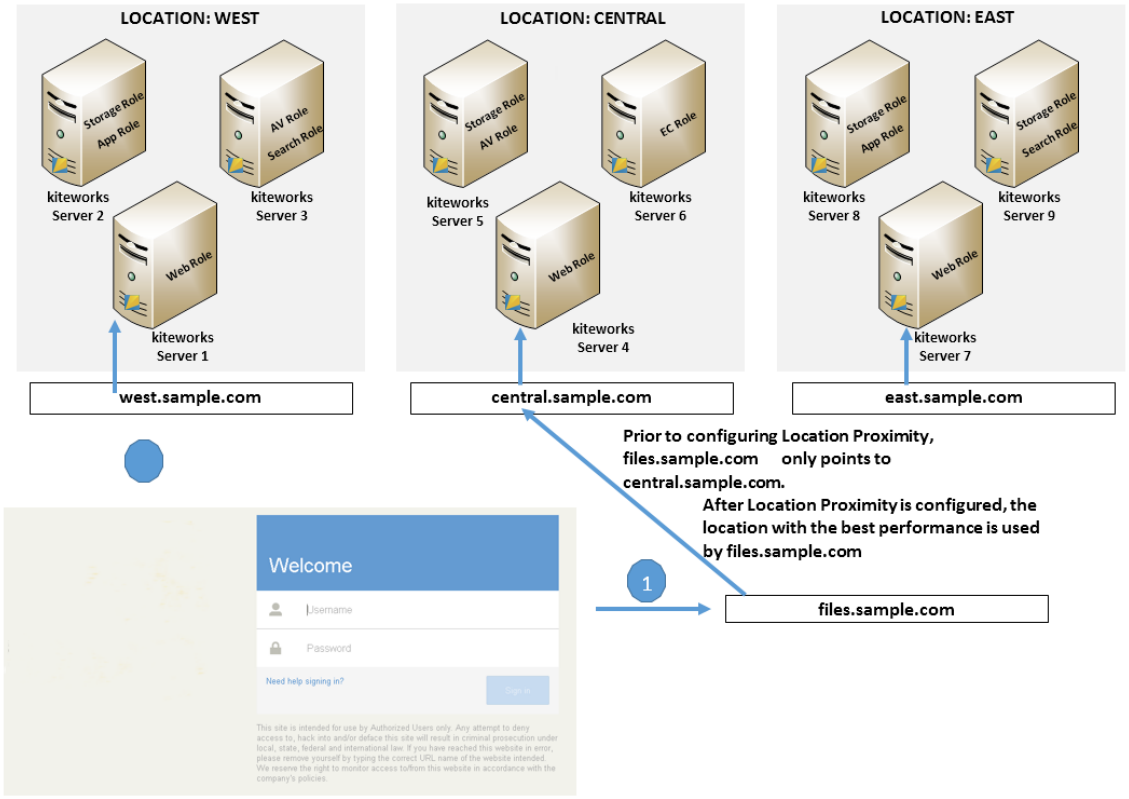
Enable (check) the Location Proximity Feature. A green indicator is displayed when the DNS configuration is set correctly. To enable Location Proximity, the location domain must be defined for every location.

Note: When Location Mapping and Location Proximity are enabled, all uploads for mapped users will go straight to the mapped server, not through the Proximity Server.

Location optimization

The following diagram shows a geographically distributed Kiteworks cluster. There are three locations labeled East, West and Central with Kiteworks servers in each location. The cluster has four separate DNS entries to manage if Location Proximity is enabled, files.sample.com is the primary DNS name for the cluster. In order for Location Proximity to work properly, the administrator need to add an individual DNS name that points to at least one server in each location.

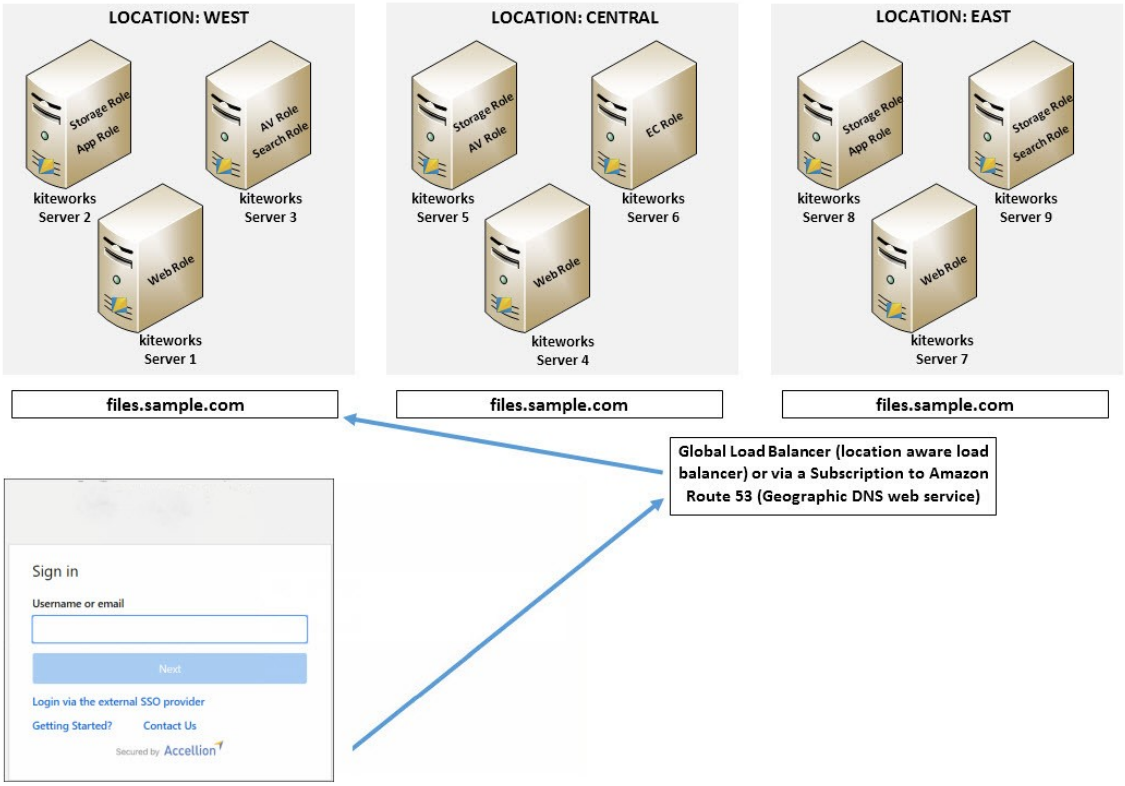
In this example, west.sample.com is pointing at Kiteworks server 1, central.sample.com is pointing at Kiteworks server 4 and east.sample.com is pointing at Kiteworks server 7. Prior to configuring location proximity, if any of these location names are accessed from a browser, the user will be redirected to files.sample.com which only points to Kiteworks server 4 in the central location. After location proximity is configured, end-users will be able to take full advantage of this feature in Kiteworks. When initially files.sample.com is accessed from their browser, a user will be directed to Kiteworks server 4. This is where the user will log in. After successfully logging in, the user's browser will determine which location performs the best and is the closest. In this example the browser will try east.sample.com, central.sample.com, west.sample.com as well as, files.sample.com. The location with the least drag in performance is then used by the browser for the remainder of the session for information requests from Kiteworks. All this works transparently to redirect the user to the best performing closest location.



Note: If the administrator has mapped the server to a specific location the request will go to the location mapped.

Using a Geographic DNS Web Service or a Global Load Balancer Appliance

Kiteworks location proximity feature can also be supplemented using a geographic DNS web service or a global load balance appliance. In the following diagram, Kiteworks is configured to be geographically distributed in the West, Central and East U.S. In this example, it is more optimal for the customer to not enable the Location Proximity feature in Kiteworks but instead have access to either a geographically aware DNS service (subscription to Amazon Route 53) or a global load balancer (location aware load balancing appliance), configured to point the application URL (in this case files.sample.com) at a web role or a set of web roles in each location. This setup will route end-users to the closest Kiteworks cluster at all times.



Generate diagnostic logs

You can generate system diagnostic logs for troubleshooting server issues. You can generate logs for multiple servers in bulk and automatically upload them to Kiteworks technical support. When uploading logs, the upload page displays the full URL of the destination server where the logs will be uploaded.

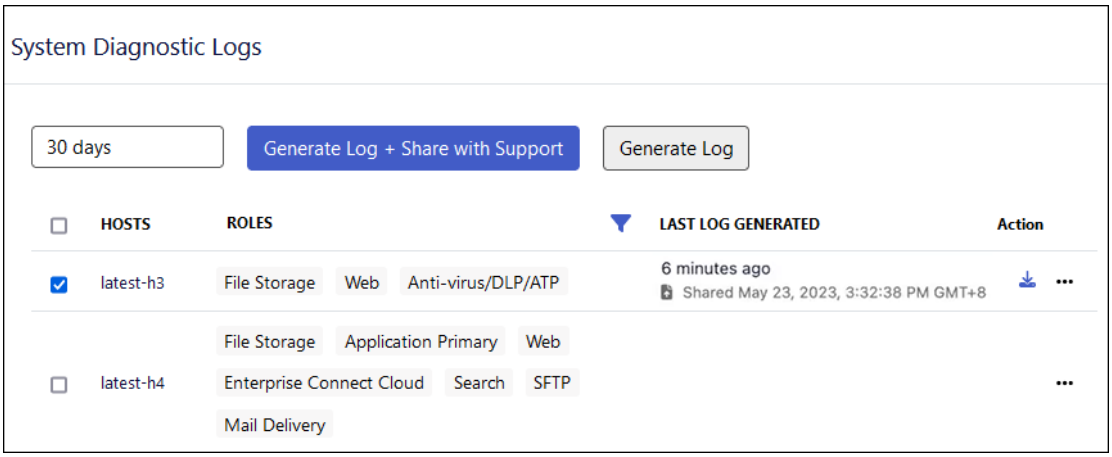
Prerequisites:

- If you plan to automatically upload system logs to Kiteworks technical support, have a copy of the share token that was sent to you in the email request from technical support. You will need to provide it prior to uploading the logs.
- Ensure that port 443 is open for bidirectional server-to-server communication.

To generate system diagnostic logs:

1. Go to System Setup > Locations.
2. On the Locations page, in the Server Details section, click Diagnostic Logs.
   Alternative: Next to the server containing the logs, click the wrench icon. On the Server Tools page, go to the System Logs tab.
3. On the System Diagnostic Logs page, select the servers containing the logs you want to generate, and then perform one of the following actions:
   - To generate the logs for download, click Generate Log.
   - To generate the logs for download and automatic upload to Kiteworks technical support, click Generate Log + Share with Support. When prompted to upload the generated logs, provide the share token that was sent to you in the email request for logs, and then click Submit.
4. After generating the logs, you can download them from the System Diagnostics Logs page. In the

Action column, click the Download icon.



Check network connections

Used to determine if a clear path exists to other network resources. For example, if a new LDAP connection is failing, see Check Connectivity to verify the route to the LDAP server is open on the specified port.

To check network connections:

1. Go to System Setup > Locations.
2. Next to the server name, click the wrench icon.
3. On the Check Connectivity tab, specify the settings, and then click Check Connectivity.

DNS lookup

Resolves a hostname/IP address using the configured DNS server. Can be used to test whether DNS is resolving correctly.

To perform SNS lookup:

1. Go to System Setup > Locations.
2. Next to the server name, click the wrench icon.
3. On the DNS Lookup tab, specify the settings, and then click DNS Lookup.

Test the email server

Test that the mail server is accepting mail from the Kiteworks server.

To test the email server:

1. Go to System Setup > Locations.
2. Next to the server name, click the wrench icon.
3. On the Sent Test Email tab, specify the settings, and then click Send Test Email.

Migrate nodes using the migration wizard

The Migration Wizard provides a controlled and guided process for migrating nodes between environments (on-premises to cloud, cloud to on-premises, or between similar environments). Once the transfer of node roles and data is complete, the existing nodes are no longer usable.

The wizard performs a series of pre- and post-migration checks and verifications to ensure system stability throughout the migration process, making it a versatile tool for infrastructure management.

Note: Nodes with the following roles can't be migrated using the Migration Wizard. For assistance migrating these nodes, please contact Kiteworks technical support at https://community.kiteworks.com.

- Email Protection Gateway
- Email Protection Gateway Database
- SafeEDIT

Role: To migrate nodes, your role must be the System Admin role.

- Run the Node Migration Prerequisite Report.
- Get the latest image files from Kiteworks technical support.
- Create the new destination virtual machine.
- Generate the node migration token.
- Add the new destination node to the cluster.
- Allocate disks on the new destination node.
- Update the system to the latest version of Kiteworks.
- Run a system precheck.
- Start the migration.
- Test the new destination node.
- Turn off roles on the migrated source node.
- Take a snapshot of the migrated source node.
- Decommission the migrated source node.
- Shut down the migrated source node.

Run the Node Migration Prerequisite Report

Run the Node Migration Prerequisite Report to prepare the system for migrating a source node to a new destination node. The report lists the system specifications, network requirements, and storage requirements for configuring the destination node. You can also download the report for future reference.

To run the Node Migration Prerequisite Report:

1. In the Kiteworks Admin Console, go to System Setup > Locations, and then click Migration Wizard.
2. On the Planning tab, in the Available Source Nodes section, select the source node you want to migrate.
3. Click the Node Migration Prerequisites Report button to generate the report.
4. Review the requirements and firewall changes you'll need to implement on the new destination node to ensure the node functions properly after migration.

Get the latest image files from Kiteworks technical support

To get the latest Kiteworks image file for the new destination node, please contact Kiteworks technical support at https://community.kiteworks.com. You will need to provide your current Kiteworks software version, FIPS certification, and information about the environment in which the virtual machine is hosted.

Create the new destination virtual machine

Create the destination virtual machine according to the specifications in the Node Migration Prerequisites Report. This step is performed outside of the Kiteworks Admin Console.

Generate the node migration token

When adding the new destination node to the cluster, you need to provide a node migration token to join the cluster without impacting the number of currently allocated licenses until the new node is activated.

To generate a node migration token:

1. In the Migration Wizard, click the Migration tab.
2. On the System Tokens page, click the Migration Token tab, and then click Generate Token.
3. Copy the token to use in the First Time Setup process.

Alternative: You can also create a migration token outside of the Node Migration Wizard. Go to System Setup > Locations > Migration tab.

Add the new destination node to the cluster

Use the First Time Setup process to add the new node to the cluster. For assistance, please contact Kiteworks technical support at https://community.kiteworks.com.

Allocate disks on the new destination node

On the new destination node, allocate disks to partitions as specified in the Node Migration Prerequisites Report. To allocate storage, go to the Locations page, expand the node, and then go to Storage > Manage Storage. See Manage server storage.

Update the system to the latest version of Kiteworks

Update the Kiteworks system to ensure that all nodes are running the latest software version. See Update Kiteworks.

Run a system precheck

Using the Migration Wizard, run a system precheck on the source and destination nodes. This does not lock the migration process. Whether prechecks pass or fail, you can always click Go Back to return to the previous tab or click Cancel to end the system precheck.

To run a system precheck:

1. Go to System Setup > Locations, and then click Migration Wizard.
2. On the Migration tab, select the new destination node.

   Rule: The destination node can't have any roles assigned to it.
3. To run the system precheck, click Continue to Precheck.

4. If a precheck does not pass, review the explanation in the Action column and fix the issue. Run the precheck again to verify that your changes were successful. You can continue to review and rerun prechecks until all processes display the "Passed" status.
5. Once all prechecks have passed, click Continue to start the migration.

Start the migration

When all prechecks have passed, you can start the node migration process. As the migration proceeds, you can monitor the status and troubleshoot any issues. Review the expandable log in the Migration Wizard. You can also minimize the wizard to run in the background.

After migration, all migrated roles will become active on the destination node, which will assume all traffic sent previously to the source node. At that time, you must turn off all roles on the source node.

Warning: Once the migration process starts, it can't be stopped or undone.

To start the migration:

1. On the Transfer Roles and Data page, review and verify the selected source and destination nodes.
2. When ready, click Start Transfer.
3. On the Confirmation page, review the information. When ready, select the "Yes, I am ready to transfer roles and data" checkbox, and then click Transfer Roles and Data.

Test the new destination node

After migrating the source node, test the new destination node to ensure that transferred roles are functional on the node. This test also checks for any post-migration issues on the destination node and verifies that the node is stable and working efficiently.

To test the new destination node:

1. On the Transfer Roles and Data page, click Continue to move to the Node Test page.
2. Click Test Node to verify that the system is functioning properly.
3. If the source node contained the Web, SFTP, or Mail Delivery role, further testing is required. In the Next Steps section, review and complete the manual tests.
   - Web role - Unassign the Web role from the source node and verify that the web browser traffic is going to the new destination node. If the new node is not receiving traffic, ensure that DNS records or load balancers point to the correct IP address of the new destination node.
   - SFTP role - Unassign the SFTP role from source node and verify that SFTP clients can connect to the new destination node. If the new node is not receiving traffic, ensure that the firewall is not blocking ports configured with the SFTP role.
   - Mail Delivery role - Verify that the Mail Relay Server is configured to accept email from the destination node. Go to System Setup > Locations and expand the new destination node. Open the Mail Delivery role settings and send a test email. If the test email is received successfully, the Mail Delivery role is functioning properly.

     If the test email is not successful, review the Mail Delivery role settings to ensure that the Mail Relay Server is configured to accept email from the new destination node. Send another test email to confirm.
4. Once post-migration testing is successful, select the "I have completed all testing provided above" checkbox.

Turn off roles on the migrated source node

After verifying that the system is functioning properly, turn off all roles on the migrated source node.

To turn off roles on the migrated source node:

1. Go to System Setup > Locations and expand the source node.
2. Turn off all roles on the source node.

Take a snapshot of the migrated source node

Take a snapshot of the migrated source node so that you can revert it to its prior state if you experience an issue.

- For on-premises deployments, refer to snapshot instructions corresponding to your virtual machine.
- If your system is hosted by Kiteworks, please contact Kiteworks technical support at https://community.kiteworks.com to request that they take a snapshot of the node for you. Provide the date and time of your planned maintenance window, the name of the node you want to back up, and the time you want the snapshot to be taken. Kiteworks technical support will notify you when they take the snapshot.

Recommendation: Keep the snapshot for 1 week in case of unforeseen issues with the migration.

Decommission the migrated source node

After turning off all roles on the migrated source node, decommission the source node.

Warning: Decommissioning a node can't be undone.

To decommission the migrated source node:

1. Go to System Setup > Locations, and expand the source node.
2. On the Decommission tab, click Decommission.

Shut down the migrated source node

After decommissioning the migrated source node, shut down the virtual machine for the migrated source node.

Storage

Manage server storage

As storage disks fill, you can add storage in the following ways:

- Add new disks to the server.
- Expand the existing disk.

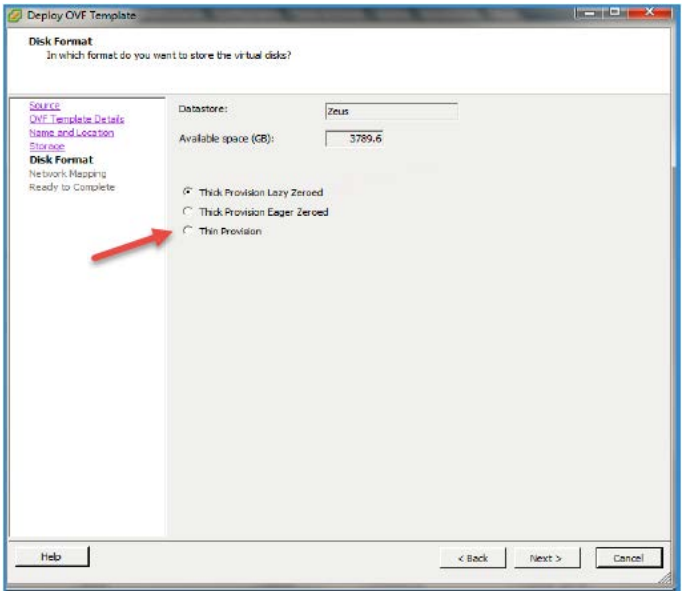
After adding or expanding storage, configure Kiteworks to use this new allocated storage.

Add a new disk versus expand storage on an existing disk

When you add a physical hard drive to your existing Kiteworks cluster it will be a new disk drive.

When you expand existing available storage, more space is allocated on an existing disk.

Recommendation: For virtual disks, do not deploy with the Thin Provision option to avoid risk of data loss and corruption.



Add a hard disk or virtual hard disk

To add an additional new disk to your Kiteworks cluster, you will need to first locate the Storage server on your cluster. Once the storage server is located, add the new physical drive.

To add a hard disk or virtual hard disk:

1. Go to System Setup > Locations, and then click to expand the server on which to add storage.
2. On the Storage tab, click Manage Storage.
3. On the Manage Storage page, attach a new disk, and then click "Refresh the list".
4. To add storage, click Add.
5. On the confirmation page, click "Add as Data Storage".

   Result: Once the disk is added, the total disk space is allocated to increase data storage and all existing data on the disk will be erased.

Enable the Search role if you would like to add this disk as Search Index Storage.

The progress of the new disk addition is displayed while it is being added.

Please contact Kiteworks technical support at https://community.kiteworks.com to assist with the expansion of the root partition as this will require the server to be offline. A separate Linux server for expanding Linux partitions in the system and Root drives will be needed.

Once the disk is added, the Manage Storage page displays the new disk.

Expand an existing disk for additional data storage

To expand a disk for additional storage:

1. Go to System Setup > Locations, and then click to expand the server on which to add storage.
2. On the Storage tab, click Manage Storage.

3 On the Manage Storage page, next to the storage disk you want to expand, click Add.
4 In the "Storage to be increased" list, select the type of storage you want to add.
5 Click Add Storage.

Result: On the Storage tab, the expanded disk space is increased according to the additional storage you added.

Expand a virtual disk

When you expand the size of a virtual hard disk, the sizes of partitions and file systems are not affected.

When you expand a virtual hard disk, the added space is not immediately available to the virtual machine. To make the added space available, you must use Manage Storage tool in Kiteworks.

To expand a virtual disk:

1 Turn off the virtual machine.
2 Verify that the virtual disk is not mapped or mounted. You cannot expand a virtual disk while it is mapped or mounted.
3 Verify that the virtual machine has no snapshots.
4 Verify that the virtual machine is not a linked clone or the parent of a linked clone.

Expand the System Storage disk

You can expand the system and root partitions only if you have added virtual disk storage first.

Exception: Expanding the system storage for systems in AWS and Azure is not supported.

Prerequisite: Expand the virtual disk storage on the virtual machine. One the storage is expanded, the ability to expand the system storage disk will be available for that machine.

To expand the system storage disk:

1 Go to System Setup > Locations, and then click to expand the server you want to configure.
2 On the Storage tab, click Manage Storage.
3 On the Manage Storage page, under System Storage, click Expand.
4 Review the confirmation message, and then click OK.

Add new storage to System storage

Prerequisite: Expand the virtual disk storage on the virtual machine. One the storage is expanded, the ability to add storage will be available for that machine.

To add new storage to System storage:

1 Go to System Setup > Locations, and then click to expand the server you want to configure.
2 On the Storage tab, click Manage Storage.
3 On the Manage Storage page, under System Storage, click Add.
4 On the Add Storage page, click the down arrow to increase storage.
5 Select System Storage, and then click Add Storage.
   Result: The new total storage is displayed on the System Storage bar.

Add or expand System Tmp storage

The System Tmp storage is a /tmp location for system services or processes to cache temporary data, such as database processing or system clock synchronization. It is different from the "Tmp storage" in that it is only used by the Kiteworks application. The minimum size you can add is 20 GB.

To add or expand a System Tmp storage:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Storage tab, click Manage Storage.
3. On the Manage Storage page, next to the storage you want to add, click Add.
4. In the "Storage to be increased" list, select System Tmp Storage.
5. Click Add Storage.

Result:

- If you added System Tmp storage, after restarting the server the new storage is listed on the Storage tab.
- If you expanded System Tmp storage, the disk space is increased to the additional storage you added.

Direct mounting of an NFS Volume

Kiteworks provides the capability to add NFS volumes and create ACFS on them. Storage can be added that is not part of a Kiteworks server enabling the administrator to increase Data Storage easily. This function provides the following features:

- Only Data Storage is supported.
- You can use the disk encryption scheme. However, Kiteworks will use file level encryption when writing files to a NFS volume.

Set up the NFS mounted volume

For an NFS mounted volume to work with Kiteworks, you will need to set up the NFS server where the volume is present. The NFS server is outside the Kiteworks cluster and is managed by an administrator. The client-side setup is managed through the Kiteworks Admin Console.

Requirement: You can only mount NFS volumes to servers where the File Storage role is enabled.

To set up the NFS server:

1. Install the NFS server-side components.
2. Create a user with ID 500 and group with ID 501.
3. Create a mount point directory for storage and export it through /etc/exports file.
4. Make sure the mount point directory is owned by the user/group created in step 2 above.
5. Mount the NFS volume from the Kiteworks Admin Console. Kiteworks works as an NFS client.

To mount the NFS volume:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Storage tab, click Manage Storage.
3. On the Manage Storage page, click Mount NFS Volume.
4. Configure the settings.

- NFS Host - Specifies the host name or an IP address of the remote NFS server. Only IPv4 protocol is supported.

- Remote NFS Path - Specifies the path of the remote directory used for the NFS mount point. This should be the same directory as configured in the /etc/exports file.
- Mount Option - Enter the mount options separated by a comma. Available options: [defaults,soft,hard,timeo,retrans,rsize,wsize,ac,noac,retry,intr,nointr,vers,lock,nolock,local_lock]. For example: "soft,timeo=600". Enter "defaults" or leave it empty to set the default mount options: "hard,timeo=600,retrans=2,rsize=32768,wsize=32768,ac,retry=10000,nointr,vers=3,lock".

5 To mount the NFS volume, click Mount NFS.

Result: The new volume is tested. If the test passes, the NFS volume appears under Data Storage with the size and connection status.

6 You can also test the volume once you have added it or test mounting a new volume by clicking Test NFS Connection to test the connectivity to the NFS server. If the test fails you will be notified that the NFS volume failed to mount.

Remount the NFS volume

You can remount the existing NFS volume if a new host name or new mount option is given by clicking Remount. The new host name will point to the existing NFS server.

Expand and display of additional storage panels

You will see additional storage panels, such as, TMP Storage (temporary storage), Database Storage and Log Storage based on when the Kiteworks system was created.

Encryption key - rotate key

Kiteworks native storage (Virtual Disks) use AES256 bit encryption to encrypt data at rest. You can secure this encryption with an additional encryption key. An encryption key is automatically generated when virtual disks are formatted.

To update or rotate the encryption key:

1 Go to System Setup > Locations, and then click to expand the server you want to configure.

2 On the Storage tab, click Rotate Key.

3 Click Generate New Key. You can accept the auto-generated key or you can enter your own encryption key.

Note: The key must be exactly 64 characters and contain number 0-9 and/or letters a-f.

Add data storage and search index storage

If necessary, add storage for data first, then create the Search Index Storage. You will receive a system alert if storage is low.

Requirement: You can only add search index storage to servers where the Search role is enabled.

Prerequisite: Calculate how much storage you will need for the Search Index. For a single node setup, the index requires up to 85% of the total amount of storage the user files use.

To add data storage and search index storage:

1 Go to System Setup > Locations, and then click to expand the server you want to configure.

2 Calculate approximately 85% of the total storage used.

3 Click the Storage tab, and then add the calculated amount of storage to the server.

Migrate data storage disks

You can initiate the migration of disks on a specific host. All the disks will be migrated in one operation.

If any data storage that uses the old encryption technology needs to be migrated, the system will display an alert. Clicking on the alert will take you to the server's Storage tab.

To migrate data storage disks:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Storage tab, click Manage Storage.
3. On the Manage Storage page, next to the disk with the old encryption software, click Migrate. .

   Note: Disks displayed in grey have the older encryption software version.

   Result: The system performs a precheck process before migration to ensure that the migration occurs successfully.
4. Once the precheck passes, click Start Migration.

   Result: Once the migration starts, it initializes, migrates data, finalizes, and then notifies you when the process is done.

   - If there is an error in the migration process, the progress bar lets you know if the error occurred while initializing, migrating or finalizing the disk. An Operation failure displays in the progress bar. You can click Cancel to stop the migration. On the Activity and Reports page, check the audit log for any errors and retry the migration. If the issue still persists contact Kiteworks technical support.
   - If the migration completes successfully, the Manage Storage window displays the Data Storage disk with the updated encryption software.

Migrate Tmp Storage

If you have Tmp Storage configured with an older image, it will also need to be migrated to the newer encryption software version. The system will display an alert. Clicking on the alert will take you to the server's Storage tab.

Note: You may not need to do the Tmp migration since it is needed only for older images when there is no dedicated disk for Tmp storage because it is part of the System storage.

To migrate Tmp Storage:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Storage tab, click Manage Storage.
3. On the Manage Storage page, if additional storage is required the system will notify you how much additional storage is needed to migrate Tmp Storage to the newer encryption software. Click Add.
4. On the Add Storage page, click the down arrow to increase storage.
5. Select Tmp Storage, and then click Add Storage.
6. When prompted, turn on maintenance mode to ensure system integrity.

   Result: The process of adding the first Tmp storage disk starts with initializing the disk. It is then formatted and the data is moved on the formatted disk. Once all the data is moved the disk is mounted. Additional disks only need to be initialized and then they are mounted. Once the disk is added the progress bar displays Done.

   - If there is an error in adding the disk, the progress bar lets you know if the error occurred while initializing, formatting, moving data or mounting the disk. An Operation failure displays in the progress bar. Click Close in the Manage Storage window to cancel the current migration process. On the Activity and Reports page, check the audit log for any errors and retry the migration. If the issue still persists contact Kiteworks technical support.

- If the migration completes successfully, the Manage Storage window displays the Tms Storage disk with the updated encryption software.

Security

Configure SSH and SFTP access

In Kiteworks, SSH and SFTP use port 22 by default. SSH is used by Kiteworks technical support to provide remote system maintenance and support. SFTP is used when transferring to and from Kiteworks over the SSH protocol.

Depending on your security policies, you may want to limit access to port 22. You can change the default SSH and SFTP port numbers, host Key Exchange Algorithms (Kex), and Message Authentication Codes (MAC).

You can use the same port number, Kex, and MAC settings for both SSH and SFTP or configure the settings separately.

This feature is available for on-premise nodes only.

To configure SSH and SFTP access:

1. Access SSH or SFTP settings in one of the following ways:
   - To access SSH settings, go to System Setup > Locations, and then click to expand the server you want to configure. On the Security tab, next to "SSH Access for Kiteworks Support", click the wrench icon.
   - To access SFTP settings, go to System Setup > Locations, and then click to expand the server you want to configure. Expand the SFTP role, and then click Configure.
2. Select whether to use the same settings for both SSH and SFTP.
3. Specify the port, algorithms, and codes you want to use.
   - The default port is 22. If you change it, update your firewall policies to access the new port number.
   - Key Exchange Algorithms and Message Authentication Codes that are grayed out are custom algorithms and codes that were added for you by Kiteworks technical support. If you disable these customizations, they will be removed completely. To add them back again, contact technical support.
4. Click Save.

Reset remote management passwords

Kiteworks ships with a default remote management password for Kiteworks technical support to remotely access a server and assist with maintenance and troubleshooting.

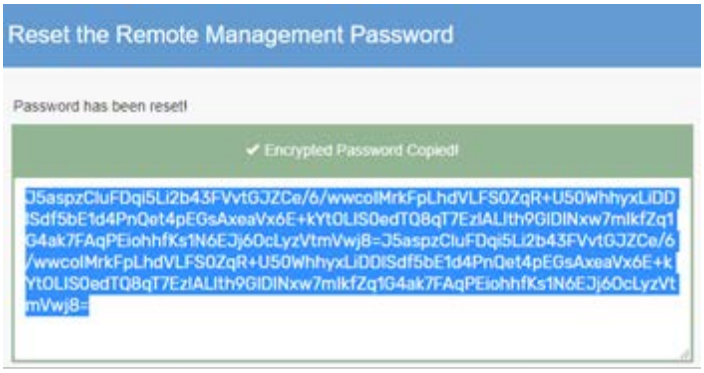
You can reset the default password to prevent access to the system. If you need assistance from technical support, you'll need to send them a new password so that they can access the server. When assistance is no longer needed, you can reset the password again to restrict access.

You can reset the remote management password using the Kiteworks Admin Console. However, if your support representative needs root access to the server you'll need to send them a set of encrypted remote management keys consisting of the remote management password and an elevated permission password. You generate this set of keys using a command-line interface.

Remote management password keys use asymmetric (RSA 2048) encryption to securely transfer of information between clients and servers.

To reset the remote management password using the Kiteworks Admin Console:

1. Go to System Setup > Locations, and then click to expand the server for which to allow remote access.
2. On the Security tab, next to Remote Management Password, click Begin Reset.
3. Follow the prompts to confirm that you want to reset the default password, and then click Reset.
4. Copy the new encrypted password to a secure place.



5. If necessary, send your support representative the encrypted password so that they can access the server using SSH.

   Recommendation: When finished working with technical support, generate a new password to prevent further access to the server. You can copy the new encrypted password to a secure place for future use or just generate a new password when you want to allow remote access again.

To reset the remote management password using a command-line interface:

1. Using the vSphere command-line interface, sign in with your user name and password for accessing the server.
2. Go to Configuration > User > Generate Remote Management Password.

   Result: Two QR codes are generated due to the size of the new encryption key.
3. Take a screen capture of each QR code and save the files to a secure place.

   Recommendation: When naming the files, indicate the sequence in which the codes were generated. Your support representative will need to upload them in the correct sequence for decryption. For example:

   - remote_management_password_1.png
   - remote_management_password_2.png

To reset the elevated permission password using a command-line interface:

1. Go toConfiguration > User > Generate Elevated Permission Password..

   Result: Two QR codes are generated due to the size of the new encryption key.
2. Take a screen capture of each QR code and save the files to a secure place.

   Recommendation: When naming the files, indicate the sequence in which the codes were generated. Your support representative will need to upload them in the correct sequence for decryption. For example:

   - elevated_permission_password_1.png
   - elevated_permission_password_2.png

The WAF rules version

Enables an embedded Web Application Firewall (WAF) to inspect all web interface traffic on the Kiteworks system to detect and/or block HTTPS attacks, such as cross-site scripting (XSS) or SQL injection. No administrator interaction is needed to define or alter the rules. The WAF is automatically configured with an industry best practice ruleset optimized for the Kiteworks application.

The WAF:

- Logs all events and makes them available via alerts, administrative reporting, the CISO Dashboard, the syslog, and the Splunk forwarder.
- Is tuned to minimize false positive indications.
- Protects only the Kiteworks deployment, not other parts of your enterprise, but is compatible with any external WAF in your architecture.

File integrity monitoring

Kiteworks offers file integrity monitoring (FIM) with Open Source Host Intrusion Detection Security (OSSEC).

Email alerts are generated for rootkit issues or file integrity issues, for example change in size, checksum, permissions, owner, or group of a file. If these file modifications are detected, a warning displays with the exact time the file modification was detected. The Syslog also shows the activity, before and after the modification of the file. The email alerts usually notify administrators to contact Kiteworks technical support. For examples of events, including the alert name, alert trigger, activity shown in the Kiteworks Admin Console, and an example of the JSON that gets exported to the syslog, see Alerts and notifications

In addition to reporting file integrity and rootkit alerts, the File Integrity Monitoring service also reports system level events in the Syslog. One example is an alert generated when the Tcpdump utility is started on a network interface, causing the interface to go into promiscuous mode.

File integrity monitoring is on by default as a security best practice. You will be warned if any irregularity is detected on the system. To clarify or resolve such issues, contact Kiteworks technical support at https://community.kiteworks.com.

The email daemon also sends an email to the administrator.

The Activities report also displays the alert with the details of the activity.

The HIPAA Compliance Report also displays the file integrity monitoring warning.

To enable or deactivate file integrity monitoring:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Security tab, turn the File Integrity Monitoring switch on or off.

Configure intrusion detection and prevention

Kiteworks provides an on-board Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that supports two modes of operation:

- Zero Trust
- Dynamic IP Banning (default)

In Zero Trust mode, all IP addresses are automatically blocked unless they are explicitly listed in the Allowed IP List. It is important to note that in this mode, IP addresses in the Allowed IP List will never get banned, regardless of their actual behavior.

In the Dynamic IP Banning mode, the system monitors IP addresses that display suspicious or malicious behavior. Once an IP address crosses a certain threshold withing a specified time frame, the system will automatically enter the IP address into the Blocked IP List.

You can manually add IP addresses or ranges to the Allowed IP List so that they do not get blocked automatically, or manually add IP addresses or ranges to the Blocked IP List so that they are permanently blocked.

To configure intrusion detection and prevention settings:

1. Go to System Setup > Locations, and then click to expand the server you want to configure.
2. On the Security tab, go to Intrusion Detection and Prevention and specify whether to implement zero trust intrusion prevention or dynamic blocking of IP addresses.
   - Zero Trust - Automatically block all IP addresses, except addresses in the Allowed IP List.
   - Dynamic IP Banning - Automatically block offending IP addresses.
3. If you choose Dynamic IP banning, configure ban trigger and duration settings.

   To configure ban trigger and duration settings:

   1. Click Configure.
   2. On the Configure Ban Settings page, specify the ban trigger and duration settings.
      - Ban trigger - Block IP addresses after the specified number of consecutive failed sign in attempts.
      - Ban duration - Ban IP addresses for the specified duration (in minutes) after Fail2Ban detects the specified number of failed sign-in attempts.
   3. Click Save.

To allow or block IP addresses:

1. In the Allowed IP List or Blocked IP List, click Add.
2. Enter the IP addresses you want to allow or block from accessing the server.

   Enter a single address or a range of addresses separated by commas in the following formats:
   - Single IP address

     Example: 192.168.1.1
   - IP address with wildcard

     Example: 192.168.*
   - Selection by subnet

     Example: 192.168.100.14/24
   - Selection by range

     Example: 192.168.1.10-192.168.1.25/24
   - IPv6 format

     Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
3. Click Add.

To remove an IP address from the allowed or blocked list:

To remove an IP address from the allowed or blocked list, select the checkbox next to the IP address, and then click Delete.

Dynamic IP Banning precedence

When you add IP addresses to the allowed or blocked list, and the same IP addresses (or overlapping IP address range) is present in the other list, Dynamic IP Banning operates in the following ways:

- If an IP address is present in the blocked list and the same IP address is added to the allowed list, that IP address is removed from the blocked list and an alert is sent to the administrator.
- If an IP address range is in the blocked list and an IP address from the range (or an overlapping IP address range) is added to the allowed list, then the operation is not allowed and an alert is sent to the administrator.
- If an IP address (or a range of IP addresses) is present in the allowed list, and the same IP address (or range of IP addresses or overlapping IP address range) is manually added to the blocked list, the operation succeeds and an alert is sent to the administrator. In this case, the Blocked IP List takes precedence.

Notes:

- Dynamic IP Banning will ban IP addresses after a number of failed SSH/SFTP login attempts that happen within a 10-minute time window. Both duration and number of failed sign in attempts are configurable, but the 10-minute time window is currently not configurable.
- Dynamic IP Banning will ban IP addresses for the same duration as above after receiving too many web requests within a short period of time (preventing DDOS). The rate limit is 30 requests/second and is not configurable.
- Dynamic IP Banning will ban IP addresses that have sent malicious web requests for the same duration as above. The threshold of malicious behavior and time-window is not configurable.
- Banning using the wildcard character is not supported.
- Manually banned IP addresses are permanently banned. The ban duration setting does not apply to these IP addresses.

External Services

Configure NTP settings

NTP (Network Time Protocol) is the Internet protocol used to synchronize clock times for all connected servers in a network. All servers that have Kiteworks installed, regardless of the role run NTP. For the NTP settings you want to make sure that all your servers are pointing to the same NTP server(s). You can also point your cluster to an external NTP server as long as there is no time drift between servers.

You can set the NTP server per node in the Locations page in External Services tab for each node. Enter the Host name or IP Address of the NTP server that Kiteworks will use for time synchronization. Setting this field to blank will disable time synchronization. For redundancy, up to five NTP servers can be configured for a Kiteworks deployment.

Note: If the system time on the Kiteworks server drifts too far from local time, users may receive errors of expired sessions due to incorrect times set in the cookies.

NTP checks all servers that are configured when it syncs. It is recommended to configure at least four up-stream servers in case one server is unreachable, NTPD will have three servers to choose from. This configuration provides some redundancy.

Configure syslog settings

The Syslog Server, if specified, defines where all servers in the Kiteworks cluster will send their syslog messages. Once the Syslog server is specified, the activities are captured in that server. Please see Appendix G: JSON and single line syslog examples for a list of activities, keywords, explanation, examples and related information.

Enter the host name or IP Address of the Syslog Server. Select the Protocol and Port. Check Use TLS if appropriate for your deployment.

Note: It is required that the Syslog be enabled on all the Application servers so that activities are written to the Syslog on the Application server where the activity occurs, but it is also recommended that Syslog should be enabled for all Kiteworks servers so that all the activities are logged.

You can set up the syslog to point a Kiteworks server to multiple syslog servers. Multiple syslog streams are supported and you can choose a different format for each server with either JSON format or Single Line with comma separator format.

- Comma-separated format. Example: Jul 10 14:36:45 my-server-h1 rest_server.py: user@email.com id=1 (internal), 192.101.0.10,

Activity Type: user_logged_in, Activity Group: admin, Activity: Logged in

- JSON format.

Example:

{
"event_name": "admin_logged_in",
"event_description": "Logged into Admin Interface",
"user_id": 10,
"username": "user@email.com",
"user_type": "internal",
"user_ip": "10.2.3.4",
"host": "myserver-h1",
"user_agent": "Mozilla/5.0 (Macintosh...",
"successful": 1,
"client_name": "my service name",
"client_id": "kw_admin",
"client_device": "My-Device",
"endpoint": "POST /rest/users/actions/login?",
"endpoint_version": "13",
"flag": 1,
"data": {}
}

You have the option to add another syslog server. The Add another Syslog Server link enables you to add multiple syslog servers. Enter the remote server information, port and choose either Comma-separated format or JSON format. If multiple syslog servers are configured, the server will send syslog information simultaneously to each configured server. If the connection to one or more servers goes down, the Kiteworks server will cache the syslog information until the server responds (up to 1GB). When the connection is back online, Kiteworks will send the pending syslog information for that server.

To remove a server, click the delete icon to remove the server.

Check the Apply the same "Syslog Settings" to all hosts option to apply these settings to the entire cluster before saving.

The following messages are available for export: Kernel messages, Emergency messages, Activity Report messages, Nginx messages, and Audit messages.

Configure mail relay settings

You can improve mail delivery and increase the performance and security of your email delivery from Kiteworks by enabling DomainKeys Identified Mail (DKIM), adding host names to your Sender Policy Framework (SPF) record, configuring Pointer (PTR) records and enforcing Transport Layer Security (TLS)

for all hosted customers. SPF works by a Domain Name System (DNS) record that specifies the servers that are authorized to send emails on behalf of a domain.

A notification is sent if the system detects that SPF is not configured for a specified internal domain. All systems hosted by Kiteworks are also alerted to use Kiteworks mail relay servers.

Hosted systems

If Kiteworks is hosting your system, update your SPF records to include the following Kiteworks mail relay servers for hosted customers:

- dnsma.accellion.com
- dnsus1.accellion.com
- dnsus2.accellion.com

Non-hosted systems

When editing server settings, you can access mail relay settings by configuring the Mail Delivery role or by going to the External Services tab. It is recommended you configure mail relay settings by configuring the Mail Delivery role. This enables you to also test the mail relay settings to ensure that the Mail Delivery role is functioning normally. After testing, if you want to apply the mail settings to all hosts on the system, you can do this from the External Services tab.

To configure mail relay settings:

1. Go to System Setup > Locations.
2. Click to expand the server containing the Mail Delivery role you want to configure.
3. Next to the Mail Delivery role, click the arrow and then click Configure.
4. On the Male Delivery Settings page, configure the mail relay settings.

Table 58. Mail Settings tab

Enforce TLS	Ensure that mail transactions are sent via a secure channel. If TLS is unavailable at the receiving mail server, the system will treat those emails as undeliverable.
Mail relay server	The host server for mail relay. The Mail Delivery role requires mail relay to prevent emails from being treated as spam or sent to a black hole.
Port	The port that you want to use for the mail relay server.
Use authentication	Authenticate all mail transactions using a user name and password. When you turn on this settings, you will be prompted to enter the user name and password to use.

Table 58. Mail Settings tab (continued)

Enable DKIM	Enable DKIM for all mail transactions to ensure that domain name matching the filter can receive the email. If TLS is unavailable at the receiving mail server, the system will treat those emails as undeliverable. **To configure DKIM settings:** 1 Click the Add button. 2 On the Add DKIM Settings page, enter the following information: • Domain name - The signing domain of the DKIM signature. **Example:** domain.com • Selector - The name to use for locating the DNS TXT record to be looked up for querying the DKIM public key. The selector name will need to be used to create the appropriate DNS record on your DNS server. **Example:** dkim • Private key - To automatically generate a private key, turn on the "Use auto generated key" switch. Later you will be able to download the corresponding public key to be published on your DNS server. **Alternative:** Upload your own private key to be used for the DKIM signature. • Upload private key - Use a private key for the DKIM signature. Click "Upload private key" and then upload the key. 3 To save the DKIM settings, click Add.

5 To test the mail settings, click the Send Test Email tab. Enter the information, and then click Send Test Email.

Result: The test email is sent to the recipient address. If the email is received, the Verify Role tab displays a message stating that the Mail Delivery role is functioning normally. If the recipient does not receive the test email, review the mail settings and ensure that the mail relay server is configured to accept emails from the host.

To apply the mail settings to all hosts:

1 If you want to apply the settings to all hosts on the system, while the server is expanded, click the External Services tab.

2 On the Mail Settings tab, click "Apply the same "Mail Settings" to all hosts".

Configure SNMP settings

When SNMP is enabled on your host system it allows monitoring from another system via the SNMP protocol.

SNMP identifies objects like with an Object Identifier, or OID. Both SNMP concepts OIDs and MIBs (Management Information Base) can be used. Run the following command from a Linux endpoint to test if SNMP is working:

snmpget -v1 -c Testing 192.168.0.222 sysDescr.0

Change testing to equal the SNMP community string entered on the appliance's Admin GUI and the IP address of your appliance. This should provide a response.

System Health Monitoring

Kiteworks provides a system health monitoring service for system maintenance and operation control. This service provides alerts to the administrator for processes, such as NTP (Network Time Protocol), Fail2Ban, job queue, etc., which are monitored by SNMP.

The following fields can be configured on the SNMP settings page:

- Enable SNMP: Enables/disables SNMP.
- System Contact: The contact email address for the system in case there is a problem.
- System Locations: The address or locations of the system.
- Allowed Incoming IP range: Specifies the IP or IP ranges (in comma separated CIDR notation) of your applications/devices that can communicate with this server's SNMP.
- SNMP Version: Specifies the SNMP version, you can select a version from the drop-down menu. SNMP v1, v2c and v3 are supported.
  - v1/ and v2c are simple and only require a plain text community string to restrict access.
  - v3 is more secure. It requires authentication to restrict access and allows encryption during data transmission.
- Community String: Plaintext user ID or password that should be sent along with a Get-Request to access SNMP on this host. The string 'public' is not allowed as a community string because of security reasons.
- Apply the same "SNMP Settings" to all hosts: Check this before saving if you want to apply the same settings from this section to all hosts.
- SNMP Version: If version 3 is selected a user name, authentication password and a privacy password will be used:
- User Name : User name will be used to authenticate access to SNMP on this host.
- Authentication Password: An authentication password will be used to authenticate access to SNMP on this host.
- Privacy Password: Password which will be used to encrypt the data transmission sent from SNMP on this host.

Configure HSM settings

Luna HSM (Hardware Security Module) is integrated into Kiteworks for improved data storage security by introducing an additional layer of encryption where the key is stored in a network-attached HSM. The Thales Luna HSM Client software is preinstalled on all servers and the client software handles the certificate management and authentication with the HSM. Each server in a cluster has its own HSM settings.

To enable the HSM integration, go to System Setup > Locations, and then click to expand the server you want to configure. On the External Services tab, configure the following settings:

- Enable HSM - Enabling integration with the HSM Server will encrypt the key to mount data storage in HSM.
- HSM Provider - Luna is the default HSM vendor provider.
- HSM Server Host - Hostname or the IP address of the HSM server.
- HSM Server Certificate - The certificate generated by the HSM server.
- Partition Slot ID- The Partition slot ID that will be used by the server (1-100).
- Partition Password- The password of the Partition Slot ID.
- HSM Client Certificate - If the HSM Client certificate has not been generated, click the refresh icon to generate the certificate. Once generated, click Download Client Certificate and then upload the

certificate to the HSM server.

- Apply these "HSM Settings" to all hosts - Once all the settings have been configured, click this option to apply these setting to all hosts.

Use AWS KMS as an HSM in Kiteworks

Kiteworks also integrates with the AWS (Amazon Web Services) Key Management Service (KMS) to let you create and manage your cryptographic keys and control their use across a variety of Amazon Web Services WS services. AWS KMS is a SaaS that provides key management to all other Amazon and 3rd party services.

The AWS KMS integration with Kiteworks lets administrators choose AWS KMS as an HSM (hardware security module) provider to protect file storage keys. The integration with AWS KMS HSM improves data storage security by introducing an additional layer of encryption because the key is stored in a network-attached AWS KMS HSM.

Note: Luna HSM is another supported option as an HSM.

By default, AWS KMS stores keys in a shared environment that uses HSMs that have been validated under FIPS 140-2 or are in the process of being validated to protect your keys. AWS KMS can also provide you with logs of all key system usage to help meet your regulatory and compliance needs.

The data that is protected by the AWS KMS HSM includes:

- All dmcrypt passphrases used for ACFS storage
- All file-level-encryption volume master keys and passphrase

The data not protected by the AWS KMS HSM includes:

- All passphrases used for /kw/tmp partition
- All ecryptfs passphrases

AWS KMS also supports custom key stores which are backed by CloudHSM. You might consider creating and using a custom key store if you have any of the following requirements:

- Key material cannot be stored in a shared environment.
- Key material must be subject to a secondary, independent audit path.
- HSMs that generate and store key material must be certified at FIPS 140-2 Level 3.

In this integration, Kiteworks uses a Customer Master Key (CMK). This is provided by the customer and is stored by AWS. The CMK can be generated from the AWS Management Console or by code using the AWS API. Only an identifier is needed to use this key in API calls. An example of an identifier could look something like this:

key_id = 'arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

This CMK is used to encrypt and decrypt the data keys used for encrypting/decrypting data. Data keys are not stored by AWS KMS but are used and managed outside of AWS KMS - in this case, in Kiteworks. Kiteworks only uses AWS KMS to decrypt the data key.

Configure the Kiteworks/ AWS KMS integration

This HSM integration can be enabled and configured by an administrator in the Kiteworks Admin Console.

To enable and configure HSM integration:

1. Go to System Setup > Locations.
2. Click to expand the server you want to configure.
3. Click the External Services tab, and then click HSM Settings.

4. In the HSM Provider list, select AWS Key Management Service (KMS), and then select the Enable HSM checkbox.
5. Configure the HSM settings.
   - AWS Access Key ID - See the detailed onscreen field help on the right of the panel for the complete details on this setting. A link is also provided to Amazon AWS documentation for additional assistance.
   - AWS Secret Access Key - See the detailed onscreen field help on the right of the panel for the complete details on this setting. A link is also provided to Amazon AWS documentation for additional assistance.
   - Customer Master Key ID - See the detailed onscreen field help on the right of the panel for the complete details on this setting. A link is also provided to Amazon AWS documentation for additional assistance.
   - Default AWS Region - AWS uses the concept of a Region. This is a physical location around the world where data centers are clustered. Each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. Select the best region for your configuration needs.
6. Once all your HSM settings have been configured, click Save.

Configure Splunk Universal Forwarder settings

The Splunk Universal Forwarder forwards Kiteworks audit log (syslog) data produced using Splunk elements to the Splunk CISO Dashboard. You can configure multiple hostnames for the indexers (Splunk servers) and enable TLS to ensure secure communication between the Kiteworks server and the Splunk server.

You can configure Splunk Universal Forwarder to forward data using Splunk servers or the Kiteworks syslog server.

Recommendation: Use the Splunk Universal Forwarder on all servers in the cluster to ensure that all audit log and syslog data is forwarded. You can configure the forwarder on one server and then apply the settings to multiple servers.

For instructions on how to install and configure the CISO Dashboard, including the Splunk Universal Forwarder, see Install and configure the CISO Dashboard.

Configure the Splunk Universal Forwarder to use Splunk servers

To configure the Splunk Universal Forwarder to use Splunk servers:

1. In the Kiteworks Admin Console, go to System Setup > Locations, and then click a server you want to edit.
2. On the External Services tab, click Splunk Universal Forwarder Settings.
3. In the Platform list, select Enterprise or Cloud.

   To configure Splunk to forward data to a Splunk Enterprise instance:

   1. In the Splunk Server field, enter the host names and port numbers of the Splunk servers where you want to forward logs.

      Example when forwarding to multiple Splunk servers: hostname1:port1,hostname2:port2
   2. To secure communication over a secure channel, turn on the Enable TLS switch.

      Result: The Verify Server Certificate switch displays.
   3. To verify the Splunk server certificate, turn on the Verify Server Certificate switch.

4. Check the common name of the certificate.
5. Upload the client certificate that will be used to connect to the Splunk servers. This is required for the Splunk server to verify the client.

To configure Splunk to forward data to a Splunk Cloud instance:

1. Obtain the Splunk Search Processing Language (SPL) credentials package file (splunkclouduf.spl).
2. Upload the SPL file.

4. If you want to apply the settings to all servers in the cluster, turn on "Apply the same Splunk Universal Forwarder Settings to all hosts" switch, and then click Save.

   Result: The log forwarding process starts and data starts appearing in the Splunk environment.

Notes:

- Only one Splunk server is configurable, so whenever a new host and port is received from system the previous server will be disabled and new one will be set.
- Universal Forwarder licenses are included with Splunk. You do not need to purchase them separately.

Configure the Splunk Universal Forwarder to use the Kiteworks syslog server

To configure the Splunk Universal Forwarder to use the Kiteworks syslog server:

1. In the Kiteworks Admin Console, go to System Setup > Locations, and then click the server you want to edit.
2. On the External Services tab, click the Syslog Settings.
3. In the Splunk Server field, enter the server IP address.

   Example: <your_localhost_ip_address>
4. For the Protocol, select TCP.
5. For the Port, enter 514.
6. To secure communication over a secure channel, turn on the Use TLS switch.
7. For the Format, select "JSON format".
8. To apply the settings to all servers in the cluster, turn on "Apply the same Splunk Universal Forwarder Settings to all hosts" switch, and then click Save.

   Result: The log forwarding process starts and data starts appearing in the Splunk environment.

Proxy Settings

Configure proxy servers

In the Proxy Settings tab, you can configure the following types of proxy servers:

- Software Update Proxy
- Anti-Virus Proxy
- Proxy Server for Box
- Login Proxy for Repositories Gateway Cloud

Software Update proxy

The Software Update Proxy specifies a web proxy to be used for software updates.

Go to System Setup > Locations. Click the server you want to configure, and then click Proxy Settings > Software Update Proxy.

Click Use Authentication to configure the Username and Password.

Select the Apply these "Software Update Proxy" settings to all hosts before saving to apply the same settings to all hosts.

Anti-Virus proxy

The Anti-Virus Proxy specifies a web proxy to be used for anti-virus.

Go to System Setup > Locations. Click the server you want to configure, and then click Anti-Virus Proxy.

Enter an Anti-Virus Server URL or IP address that will be used for anti-virus via a proxy server.

Click Use Authentication to configure the Username and Password.

Select the Apply these "Anti-Virus Proxy" settings to all hosts before saving to apply the same settings to all hosts.

Proxy server for Box

This is a feature which allows Kiteworks to connect to Box via your proxy server in cases where direct connectivity between the Repositories Gateway Cloud role and Box is not possible.

Enter a Proxy Server for Box URL or IP address that will be used to connect to Box via a proxy server.

Click Use Authentication to configure the Username and Password.

Select the Apply these "Proxy Server for Box" settings to all hosts before saving to apply the same settings to all hosts.

Note: The Proxy Server for Box and the Login Proxy for Repositories Gateway Cloud sources can be used together and based on the request connections will be made between these two proxy servers.

Login proxy for Repositories Gateway Cloud

The Login Proxy for Repositories Gateway Cloud is a Kiteworks service which can be configured in environments where users cannot directly access Repositories Gateway Cloud sources from their network. This proxy service which runs on Kiteworks only allows users to connect to Repositories Gateway Cloud sources in order to authenticate and set up a secure Repositories Gateway session with Repositories Gateway Cloud sources.

This requires two (2) DNS servers:

- The first DNS server should direct all Repositories Gateway Cloud sources, for example, *.dropbox.com.com traffic to the proxy server for Repositories Gateway Cloud sources IP address. This will be the IP address you assign to the Kiteworks Repositories Gateway Cloud proxy.
- The second DNS server is for Kiteworks. The Kiteworks cluster (specifically the Repositories Gateway Cloud proxy role, Application roles, and the Repositories Gateway Cloud role) need to be able to go to all Repositories Gateway Cloud sources, for example,*.dropbox.com directly. Since the Repositories Gateway Cloud sources proxy service only allows user authentication with Repositories Gateway Cloud sources, the Kiteworks cluster cannot use the proxy to reach Repositories Gateway Cloud sources. You need to make sure only your users are being forwarded to the proxy and Kiteworks is allowed access to Repositories Gateway Cloud sources.

Firewall Changes for the Repositories Gateway Cloud sources Proxy:

- The Repositories Gateway Cloud proxy IP needs to connect to all Repositories Gateway Cloud sources, for example, dropbox.com on Port 443.
- The Kiteworks roles - Dropbox proxy, Repositories Gateway Cloud, and App roles - need to be able to connect to all Repositories Gateway Cloud sources, for example, dropbox.com, api.dropbox.com, api-content.dropbox.com, and api-notify.dropbox.com, all on Port 443.

Note: The server cannot have multi-tenant setup.

- Repositories Gateway Proxy IP: Specify a virtual IP address for this host, for example 192.168.99.98. If users in your network cannot access Repositories Gateway Cloud sources (e.g. Dropbox) directly, you can use a Kiteworks node as the proxy between the user and the cloud Repositories Gateway source

  The DNS must redirect all Repositories Gateway Cloud sources, for example, dropbox.com or www.dropbox.com traffic to this virtual IP address. This proxy will only activate every time a user is needed to do an authentication to Repositories Gateway Cloud sources. Ensure that the authentication URIs are redirected to this virtual IP address in your DNS.
- Subnet Mask: Enter the subnet mask for the proxy IP, for example, 255.255.0.0.
- IP Range: Specify the IP addresses from which the proxy can be used. If the user signs in while coming from any matching IP, the proxy will be used. Leave blank if the proxy is to be used for users coming from any IP. The following formats are supported: 192.168.10.34, 192.168.*, 192.168.1.0/24.

Configure Repositories Gateway Cloud Proxy Settings

1. Go to System Setup > Locations.
2. Click the server you want to configure, and then click Proxy Settings > Login Proxy for Repositories Gateway Cloud.
3. Specify a Virtual IP Address for the Repositories Gateway Proxy IP.
4. Specify a Subnet Mask.
5. Specify an IP Range. Traffic coming from outside the specified range will not have their Repositories Gateway sources connections proxied.
6. Click Save.

Shutdown

Shut down and restart servers

To shut down and restart a server:

1. Go to System Setup > Locations.
2. Click to expand the server you want to shut down or restart.
3. On the Shut Down tab, perform one of the following actions:
   - To shut down the server, click Shut Down.
   - To restart the server, click Restart.

Decommission

Decommission servers

Warning: Once you decommission a server, you cannot add it back to the cluster.

To decommission a server:

1. Go to System Setup > Locations.
2. Click to expand the server, and then turn off all roles on the server.

3 Click the Decommission tab., and then click Decommission to remove the server from the cluster.

4 Click to expand the server you want to decommission, and then click Decommission.

Network Settings

Configure Internet Protocol (IP)

You can configure up to two network interface cards (NICs) for Kiteworks. NIC1 can have both an external IP address and an internal IP address to enable hosts that are in a LAN to communicate with servers in the cloud or other networks. NIC2 can have internal IP address only and can be used to shape internal traffic like file replication.

Minimum setup requirements

One server per location with all three core roles activated: Web, Application, and File Storage. DNS must be configured to point to a server with an activated Web role.

Recommended setup requirements

For each location, at least one server with all three core roles activated: Web, Application, and File Storage. DNS must be configured to point to a server with an activated Web role.

Network routing diagram

Up to 10 hosts are displayed in the Network Routing Diagram. For information about a particular host and to Edit Routing, click the host name in the diagram.

The External IP for NIC1 is the NAT IP obtained from your network administrator.

Auto Discovery: To find the best connections and fix existing connections, click Auto-Discovery.

Test Connection: Testing connections is checked via port 443.

Note: The Network Routing Diagram shows a maximum of ten (10) hosts.

IPv4

IPv4 (Internet Protocol Version 4) and IPv6 protocols are used to identify devices on the network. These protocols are designed for use in interconnected systems of packet-switched communication networks. The IPv4 IP used to identify devices on a network through an addressing system.

To deploy the network using IPv4, go to System Setup > Network Settings. In the Host table, expand the host and then click the IPv4 tab.

Click any of the servers, for example, h1, h2, h3 or h4 or click the Cluster Routing button to view the cluster routing details of that server as seen by others and IP addresses of other hosts connected to that server.

Enter the IP addresses in all the fields to configure IPv4 for that server.

External IP: Specifies the External IPv4 for NIC1 is the NAT IP obtained from your network administrator. Your system will be accessible from the Internet using this IP address. For example, 54.244.231.235.

Configure Static Routing: If you have specific routes that needs to be added to the system and specific gateways the system needs to take, those static IP addresses can be added here as well as which interface will be used.

Cluster Routing: Click this option, and then click the down arrow and select the IP address from the IP ADRESS OF OTHER HOST TO CONNECT FROM column to select which route should be taken to

communicate with which system. It is possible to use 2 network interfaces and segregate traffic, if needed for each system, if 2 network interfaces are attached to the system.

DNS Server: Specifies the Domain Name System server IP address. It is recommended to use at least 2 DNS servers in case the primary DNS server goes down. You can use up to three servers.

IPv6

Benefits of IPv6:

- More Efficient Routing - IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical.
- More Efficient Packet Processing - IPv6's simplified packet header makes packet processing more efficient.
- Directed Data Flows - IPv6 supports multicast data flows rather than broadcast data flows.
- Simplified Network Configuration - Address auto-configuration (address assignment) is built into IPv6.
- Support for New Services - By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services.
- Security - IPSec, which provides confidentiality, authentication and data integrity, is built into IPv6. The IPv4 ICMP packets are often blocked by corporate firewalls as they potentially carry malware. The ICMPv6 implementation of the Internet Control Message Protocol for IPv6 could be permitted because IPSec is applied to the ICMPv6 packets.

To deploy the network using IPv6, go to System Setup > Network Settings. In the Host table, expand the host and then click the IPv6 tab.

Enable IPv6 using the following steps:

1. Slide the IPv6 Enabled switch to enable it.
2. Enter the IPv6 Address for NIC1 for this server.
3. Select the Prefix Length for NIC1. This will be the number of bits from 1 to 128 which determines the network portion of the IPv6 address for NIC1.
4. Enter the IPv6 Gateway address.
5. Click Save.

Using a load balancer in front of Kiteworks

If the Kiteworks Web role is behind a load balancer or proxy, Kiteworks will record the IP address of the load balancer or proxy when logging end user activities. To log the actual client IP address that makes the call, you will need to configure the load balancer or proxy to send an X-Forwarded-For HTTP header that includes the original client IP. You will also need to configure Kiteworks to accept the X-Forwarded-For header from specific servers. This will need to be configured for each server in the network. To enable this, populate the Allowed Proxy IP field on the Network Settings page to set the proxy IP to restrict which proxies are allowed to forward requests to the server.

Examples:

192.168.1.1

10.7.8.9

0.0.0.0/0

192.168.0.0/16

127.0.0.0/8

Cluster Configuration

System Services

Monitor system services

The Systems Services tab provides a visual display of the status of key Kiteworks services. From this page, you can restart system services.

The System Service table displays information on the services. For multi-node deployments, the service status is displayed for each node along with the option to restart that service for all nodes.

You can expand the service to view service information for each node and to restart the service on a node. You can also enable or disable email notifications for a service.

- Heartbeat Service - A CRON-like scheduling service that runs periodic tasks based on a defined schedule. Problems with the heartbeat service will result a multitude of important monitoring and notification scripts not running.
- JWT Service - Generates and validates JSON Web Tokens (JWT) for authenticating internal communications between Kiteworks server nodes.
- NGINX Service - Manages the internal routing of API requests.
- Jobqueue Service - Schedules and manages tasks, such as file uploads and sending mail, on the Kiteworks server. The server manages multiple job queues, with each queue being assigned a priority that the job scheduler uses to determine which jobs in which queue get evaluated for processing first.

  Jobs are typically processed without issue, but if a problem arises the job queue service restarts automatically to resolve it. If the system can't determine why a job is stuck in queue, you may need to restart the job queue service yourself to resolve the issue.
- Memcache Service - Decreases data access latency, increases throughput, and eases the load off of back-end systems. It provides the sub-millisecond latency and scale required to manage session data, such as user profiles, credentials, and session state.

  If you experience persistent problems with web pages not being displayed on the server, clear the contents of the memcache service to see if this resolves the issues.
- API Service - Manages all Kiteworks API requests and responses.
- Internal API - Manages all internal API requests.
- Legacy API Service - Legacy PHP service that serves Kiteworks API requests.
- Messaging Queue Consumer - Processes messages in the queue.

  Note: This service is displayed only when the CFDB role is enabled on a server.
- Subscription Monitoring Service - Monitors permission changes to folders subscribed to by the MFT server.
- Search Service - The Apache search platform used to enable searching for files, folders, and emails in the Kiteworks Web Application.

  Note: This service is displayed only when the Search role is enabled on a server.
- Search Indexer - Periodically submits objects to the search service for indexing.

  Note: This service is displayed only when the CFDB role is enabled on a server.
- Storage Service - Manages file operations, such as uploads and downloads.
- File Encryption Service - Manages the encryption and decryption of files.
- PHP CGI - Allows the web server to run PHP code.
- Replication Service - Finds and replicates files between locations according to defined rules.

  Note: This service is displayed only when the ACFS role is enabled on a server.

- MongoDB - A NoSQL database used by the Content Firewall Database (CFDB) role. Enabling the CFDB role changes the database to which events are logged in Kiteworks. When enabled on a node, a new MongoDB database is created on that node.

  Note: This service is displayed only when the CFDB role is enabled on a server.
- Internal API Service for MongoDB - Serves all internal API requests that read or write to the MongoDB.

  Note: This service is displayed only when the CFDB role is enabled on a server.
- Intrusion Detection Service - Bans IP addresses after failed SSH/SFTP login attempts or too many web requests within a short period of time.
- FIM Alert Service - Polls for events emitted by file integrity monitor (FIM) and triggers alerts.
- Legacy Storage Service - Legacy PHP service for supporting streaming uploads.
- MariaDB - SQL database used by the Kiteworks system.
- Mail Daemon - Manages sending and receiving emails.
- NTP Daemon - Synchronizes the server clock with remote NTP servers.
- RabbitMQ Service - Open source messaging broker that acts as an intermediary for messaging. It gives applications a common platform to send and receive messages, and messages a safe place to live until received.
- File Integrity Monitor - Monitors the integrity of system files and sends alerts when triggered.
- Splunk Forwarder - Forwards all event logs to a configured Splunk server.

  Note: This service runs only when the Splunk forwarder is enabled.
- SSH Service - Allows external clients (such as SFTP) to connect using the Secure Shell (SSH) protocol.
- SNMP Service - Receives, authenticates, and processes Simple Network Management Protocol (SNMP) requests from external applications.

Get notified when services are down

Email alerts are sent when one or more services is detected as being down. Emails are sent to the email address entered in the Support Email field (Application Setup > Kiteworks).

Email notification is enabled by default for all services.

To disable mail notification:

1. Go to System Setup > Cluster Configuration > System Services.
2. On the System Services tab, click the row for the service you want to disable email notification.
3. Clear the "Send email alert when the service is down to <email> checkbox.

Restart services

Restarting a service may be necessary to resolve performance issues or to bring up a down service. In most cases, system administrators will receive email notification, but mail notifications may be affected by one or more services being down (the mail daemon, for example).

To restart a service:

1. Go to System Setup > Cluster Configuration > System Services. Alternatively, click the link in the notification email.
2. On the System Services tab, find the service you need to restart.

3. To restart the service on all nodes, click Restart All.
4. To restart a service on one node, click the row for the service you need to restart. Find the row for the desired node and click Restart.
5. Verify the restarted service returns to normal operation. A service restart may take up to a minute depending on the number of nodes restarted. For best results, refrain from taking any other action until the service has restarted.

System Configuration

Clean up storage

To reclaim storage space, each day the system runs a cleanup_expiry script on each server node to remove expired content and stray files. This includes quarantined files older than 90 days. The cleanup process runs at 3:00 AM GMT time. You can schedule a different time for the process to run. You can also manually start the cleanup process as needed. The process can run while the system is in maintenance mode, unless the system is undergoing a software update. When manually cleaning up storage, the Nginx cache is also cleared to free up space issues that result when large files uploaded from Repositories Gateway sources consume excessive temporary storage.

When you clean up storage, a cleanup script runs a collection of cleanup functions on each node. On the application server, it deletes expired folders and files, and permanently deleted files. If you've enabled secure delete (Security Policies > Files and Folders > Retention tab > Advanced Settings), purged files are deleted securely by overwriting the file encryption keys with random bits. On server nodes, the cleanup script clears the local cache and deletes temporary files.

Before the cleanup script runs, the following prechecks are run on each node. If a precheck fails, the process is not started.

- Cleanup is not already in progress.
- The database is accessible.
- No software updates are in progress.
- The cleanup schedule time is consistent between the database and the local cron file. If different, the value in the local cron file is updated to match the value in the database.

To clean up storage:

You can reschedule the automated cleanup or manually start the process.

- To reschedule cleanup, go to System Setup > Cluster Configuration > System Configuration. In the Storage Cleanup section, enter a new GMT time for the cron job to begin.
  - For hours, enter a value from 0-23.
  - For minutes, enter a value from 0-59.

  When you change the time, a "system_setting_changed" event is tracked in the audit log.
- To clean up storage immediately, click Run Cleanup Now.

  Alternative: You can also manually clean up storage from the Files and Folders page. At the bottom of the page, click Clean Up Storage.

As the cleanup process runs, the overall percent complete for all nodes is shown. To view the percent complete for each node, click Show Progress Log.

When you view the progress log, it shows the details of the cleanup. For example:

- For each cleanup function:
  - How long it took to perform the cleanup.
  - The details of any errors that may have occurred.
- The total time it took to perform cleanup.

Other details are listed for each server node. For example:

- "completed_tasks": 1,
- "total_tasks": 3,
- "completed_percent": 33,
- "failures": 0

Log data is retained for 30 days.

Configure storage alerts

Administrators assigned the System Admin role can set up more precise notifications for when storage is running low. There a five distinct storage alert categories (Database Storage, System Storage, Log Storage, File Storage, and Other Storage) with customizable thresholds based on both percentage and absolute gigabyte values. Choose whether to trigger an alert when either condition is met or only when both conditions are met. This granular control helps prevent unexpected system downtime by providing early warnings when storage resources are running low, allowing for proactive management of system resources.

Important: Regardless of configured settings, if available storage falls below the following critical thresholds, maintenance mode will be turned on to prevent potential data loss or a system crash. While in maintenance mode, the system will not be accessible to end users.

- Database storage falls below 2.5 GB.
- System storage falls below 2.5 G.
- Log storage falls below 1 GB.

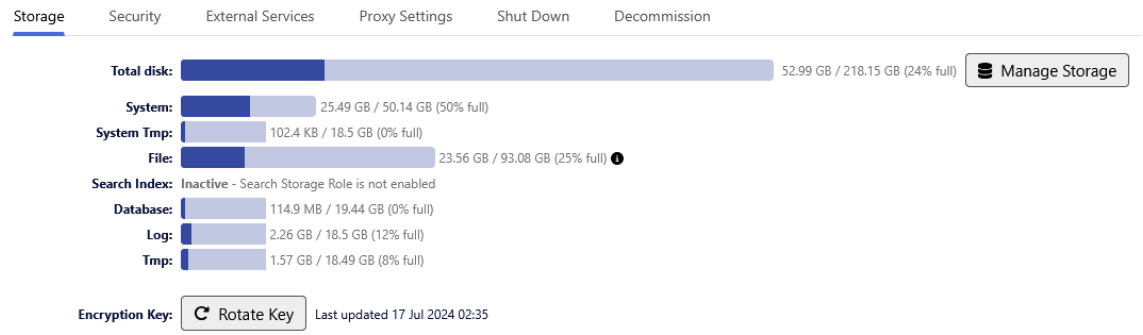
Low storage notifications appear via the alert (bell) icon in the top right corner of the Kiteworks Admin Console and are also emailed to administrators with a recommendation to increase storage on partition as soon as possible.

To configure storage alerts:

1. Go to System Setup > Cluster Configuration > System Configuration.
2. Configure each storage alert category with your preferred thresholds.
3. Set percentage values (minimum 1%, maximum 99%).
4. Choose "OR" to indicate either condition can be met or "AND" to require both conditions be met. For each alert type, you can leave one value blank to omit that condition, but at least one condition must be specified.

To monitor storage levels:

Go to System Setup > Locations, and then click to expand the server you want to monitor. The Storage tab displays the storage information.



If you need to add or expand disks, click Manage Storage. See Manage server storage.

Reduce network latency

If you deployed two or more servers in different locations (countries) that have high network latency, you can optimize database performance by changing the default configuration setting for the cluster from LAN to WAN. This adds higher tolerance to reduce the number of times the system may slow down or timeout as a result of network interruptions.

When you change the setting, the process takes approximately one minute for each application node. Each node will be restarted in sequence. During this time you can leave or refresh the page, or even sign out and return later to view the status.

To reduce network latency:

1. Go to System Setup > Maintenance Mode and turn on Maintenance Mode.
2. Go to System Setup > Cluster Configuration > System Configuration.
3. In the Application Role Configuration section, select WAN.
4. Click Apply.

Token

Generate tokens for server setup

Two ways to do this:

System Setup > Locations > New Server Token.

System Setup > Cluster Configuration > Token.

For system administration, use this screen to generate tokens for server setup.

To generate tokens for server startup:

1. Go to System Setup > Cluster Configuration > Token.
2. Click Generate token. This token is used to configure a new server into the server cluster.
3. Copy the token displayed (the green text).
4. Copy the generated token from this page, switch to the page where you are setting up the additional server in the browser, paste it in the Application Token field.

The system administrator can view the status when adding a new server to a cluster. If necessary, You can cancel the operation. See the *Kiteworks Deployment Guide* for more details on deploying a server.

SFTP

Configure the SFTP session banner

You can customize or turn off the informational banner that users see when starting a new SFTP session prior to login. Kiteworks provides a customizable informational banner for communicating information such as security and compliance requirements. This is a system-wide banner that applies to all nodes on which the SFTP role is enabled.

Note: Some external clients may not support the display of SFTP banners.

To customize or turn off the SFTP session banner, go to System Setup > Cluster Configuration > SFTP.

SSL Settings

Configure SSL

On the SSL Configuration tab, you can access all the SSL information. A publicly signed SSL Certificate must be renewed annually. The SSL Certificate format is a .pem file for the Apache-Mod format. Go to System Setup > SSL Settings.

Note: A publicly signed SSL wildcard or Subject Alternative Names (SAN) certificate can be used for Kiteworks.

View SSL certificates

View Certificate information for who issued the certificate and when the certificate expires.

An alert displays on the SSL Configuration page when the Application URL does not match the SSL certificate.

Note: This enforces SSL certificate checks for calls within the Kiteworks cluster. This security measure is switched on only if the system has a wild card SSL certificate. This alert also displays on the Kiteworks Admin Console dashboard.

Configure the Transport Layer Security (TLS) protocol

Transport Layer Security (TLS) is a critical security protocol used to protect web traffic. It provides confidentiality and integrity of data in transit between clients and servers exchanging information. TLS versions 1.2 and 1.3 are supported.

As best practice, it is recommended you enable TLS 1.3 over TLS 1.2. You can also enable TLS 1.2 and 1.3 together.

Configure SSL ciphers

You can choose Ciphers from the list provided to enable or disable them.

Cipher Suite algorithms that can be used by the server to communicate with the clients. Some ciphers are recommended based on their cryptographic strength and good support from a wide range of clients.

In general, more enabled ciphers means that the server can communicate with more types of clients, for example, to support older browsers but relatively less secure. While fewer enabled ciphers may mean more secure but may limit the server to communicate with some clients that do not support the enabled ciphers.

For Ciphers ECDHE-ECDSA-AES256-GCM-SHA384 and ECDHE-ECDSA-AES128-GCM-SHA256 to work, upload an EC certificate.

Note: IE11 requires at least ECDHE-RSA-AES256-SHA384 enabled in optional ciphers if Kiteworks is using an RSA certificate.

Generate a Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is required by the Certificate Authority (CA) to issue your SSL certificate.

To generate a Certificate Signing Request:

1. Go to System Setup > SSL Settings > Generate CSR.
2. Enter the requested information.
3. Click Generate CSR.

4 Click Download the CSR.

5 Click Download the SSL Private Key.

Important: This SSL Private key should be saved and stored securely.

Upload an SSL certificate

To upload an SSL certificate:

1 Go to System Setup > SSL Settings > Upload Certificate.

2 Select the SSL Certificate file.

3 Select the SSL Private Key file.

4 Select any Intermediate Certificates to upload. Multiple intermediate certificates should be concatenated in either chain direction.

5 Click Upload.

Satellite Servers

Register MFT Servers as a satellite servers

Before you can use the Kiteworks Secure MFT Server to transfer files to and from a Kiteworks server, you need to register the Secure MFT Server as a remote satellite on the Kiteworks server. This consists of the following steps:

- Generate a license key on the Secure MFT Server.
- Register the license key on the Kiteworks server.
- Activate the license key on the Secure MFT Server.

Prerequisites: To register the Secure MFT Server on the Kiteworks server, you need the following:

- An administrator role on the Secure MFT Server with permission to access the Admin menu.
- The host name (domain name) or IP address of the Kiteworks server.
- An administrative user account on the Kiteworks server for accessing the server's Kiteworks Admin Console.

Generate a license key on the Secure MFT Server

To generate a license key on the Secure MFT Server:

1 On the Secure MFT Server navigation bar, click Admin > Setup > Activate.

2 Under "Generate a license key for this server", enter the host name (domain name) or IP address of the Kiteworks server.
Example: server.example.com

3 Click Generate License Key.
Result: The license file is downloaded to your computer and a link to the Kiteworks server is activated in the next step.

Register the license key on the Kiteworks server

To register the license key on the Kiteworks server:

1 Under "Register the license key on the Kiteworks server", right-click the System/Satellites link to open a new browser tab, and then sign in to the Kiteworks server.
Result: On the Kiteworks server, the Kiteworks Admin Console opens to the System Setup > Satellite

Servers page.

2. On the Kiteworks server, sign in to the Kiteworks Admin Console.
3. Go to System Setup > Satellite Servers.
4. On the Satellites Servers page, click Add.
5. In the Add Satellites dialog box, enter the name you want to identify the Secure MFT Server.
6. Upload the license key file you generated from the Secure MFT Server.
   Result: The server is registered as a satellite on the Kiteworks server. The status remains Off until you return to Secure MFT Server and activate the license key.

Activate the license key on the Secure MFT Server

To activate the license key on the Secure MFT Server:

1. On the Secure MFT Server navigation bar, click Admin > Setup > Activate.
2. Under "Activate the license key on this server", click Activate.
   Result: The server is activated as a satellite on the Kiteworks server.
3. Return to the Kiteworks server. On the Satellites page, verify that the Secure MFT Server satellite is turned on. You may need to refresh the Kiteworks Admin Console to see the status change.

Manage backup and disaster recovery of MFT Servers

Kiteworks provides capabilities for MFT server backup and disaster recovery (DR) to ensure continuous operation of workflows. From the Satellites page you can assign an MFT satellite server to be the primary server for processing workflows, and assign other servers to act as secondary, backup servers in case the primary server fails.

The primary server is automatically backed up every minute or whenever a change occurs in the Kiteworks Secure MFT Server application on that server. The backup file is uploaded to the Kiteworks server and then all secondary servers download and restore the backup file. The amount of time required to complete a restore operation depends the processing involved to replicate the primary server (number of workflows, tasks, and so on).

Here are some things to keep in mind:

- The default role for an MFT satellite server is Unassigned, which excludes it from DR.
- Assigning the Secondary role to a server stops the worker service on that server. Workflows can no longer be run on the server since it's being used to replicate the primary server. If you want to run workflows on a secondary server, assign it as the new primary server. The most recent backup downloaded to that server will be used as the starting point on that server.
- Server backup and restoration status is tracked in the Kiteworks audit log.

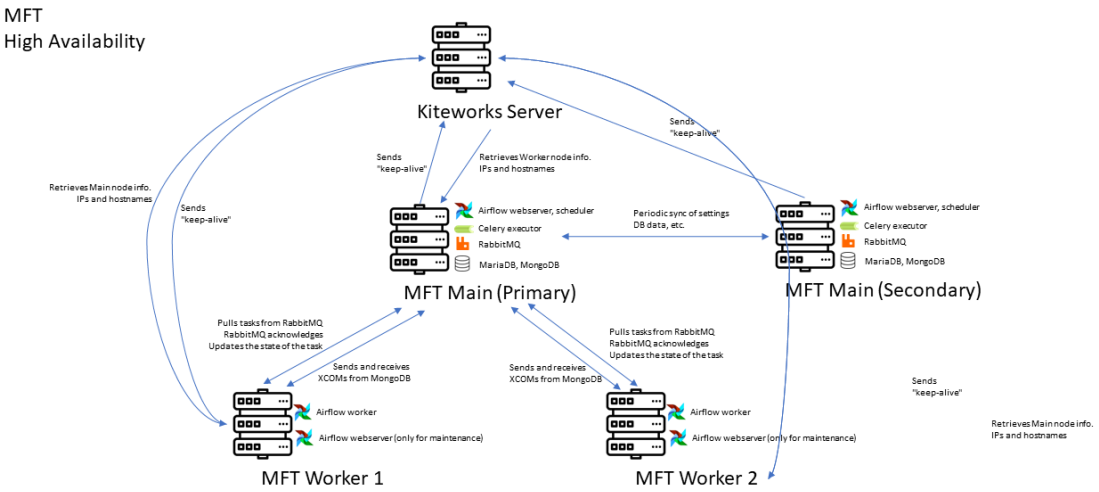
To designate an MFT satellite server as a primary or secondary server:

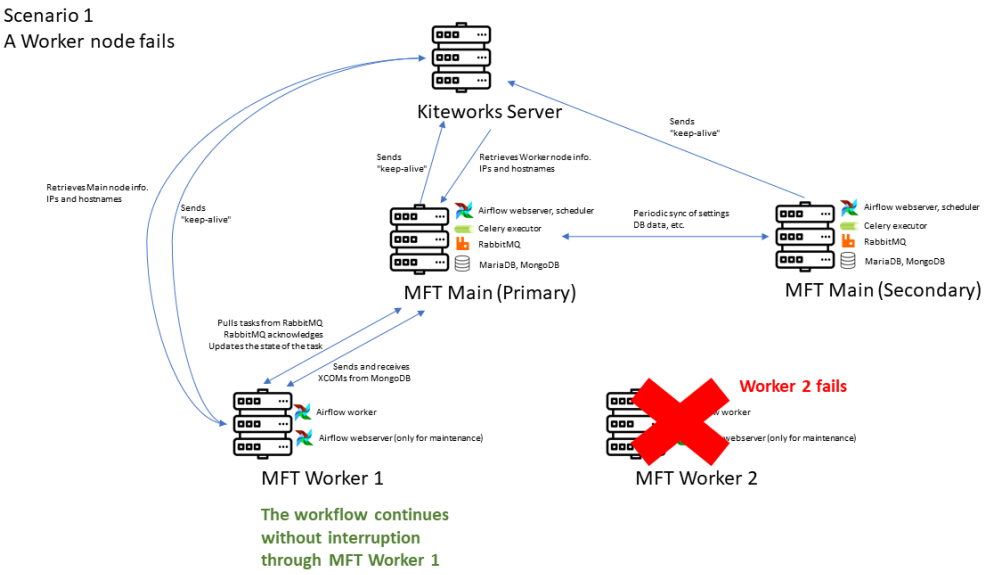
1. Go to System Setup > Satellite Servers.
2. For the server you want to use as the primary server for processing workflows, change the role to Primary.
3. For each server you want to use as a backup server, change the role to Secondary.

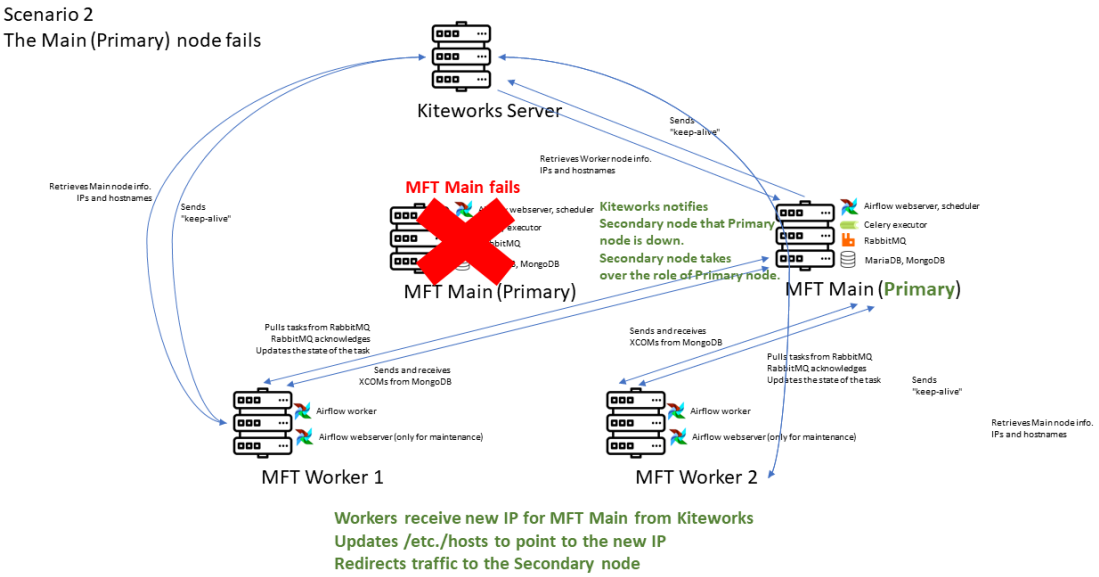
Configure high availability and load balancing of MFT Servers

In addition to assigning Primary and Secondary roles to MFT satellite servers, you can designate additional satellite servers to act as worker nodes for processing workflows. If a worker node fails or is taken offline, a second worker node takes over processing workflows and tasks. This ensures that the

cluster remains operational (high availability). Worker nodes in a cluster also distribute tasks across themselves to prevent overloading a single node with tasks and time-intensive workflows (load sharing).





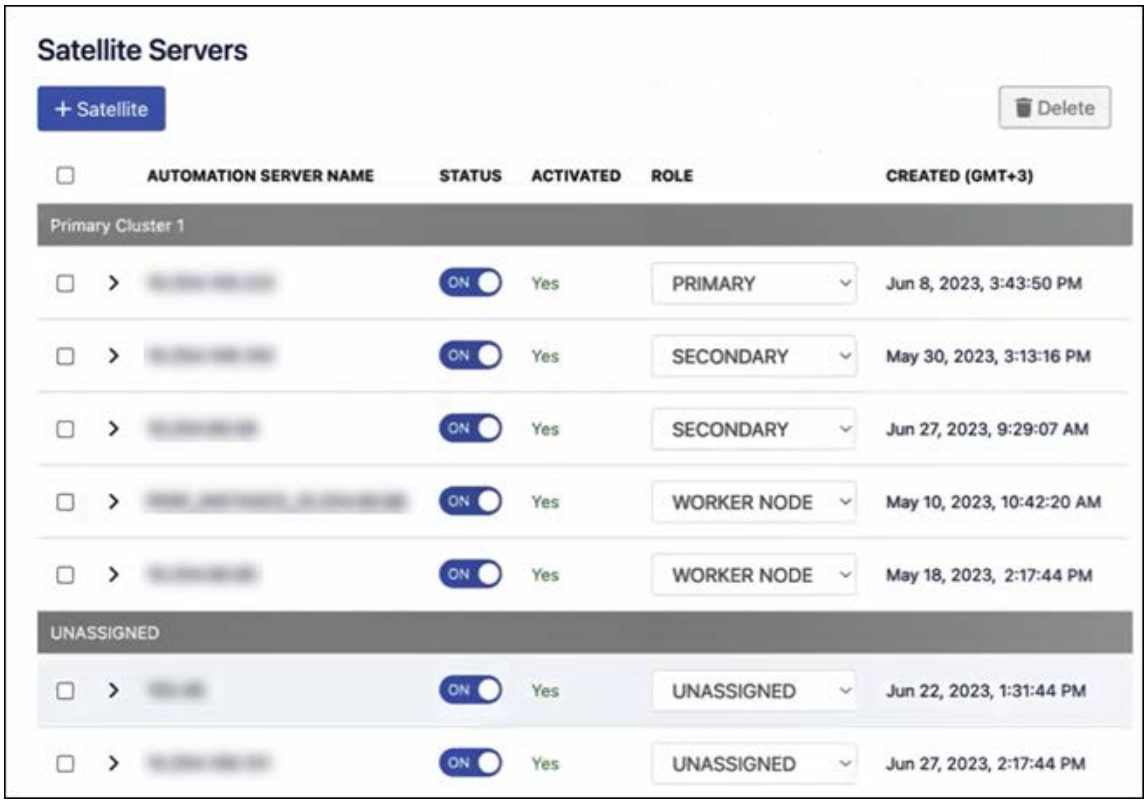


Here are some things to keep in mind:

- When worker nodes are added to the cluster, the primary server no longer executes the workflows, but instead delegates workflow processing to the worker nodes. The primary server then performs only management tasks such as creating workflows, scheduling runs, hosting the admin application, and creating connections.
- Only worker nodes have automatic high availability. A minimum of two worker nodes is recommended to ensure that if a worker node fails an additional node can continue processing workflows.
- Synchronization of workflows between worker nodes can take from 1-2 minutes.
- Worker nodes have the same hardware requirements primary/secondary nodes.

To designate MFT satellite servers as worker nodes:

1. Go to System Setup > Satellite Servers.
2. For each server you want to use as a worker node, change the role to Worker Node.
3. If you have deployed multiple server clusters, select the cluster for the worker node.



Switch to a backup server in the event of a failure

Each minute, the primary server communicates its health status to the Kiteworks server. If the primary server is unreachable or its service fails 5 consecutive times, an email notification is sent to the email address designated for receiving system notifications. To configure this address, go to click Application Setup > Configuration > Notification Email.

The email notification describes the issue and provides a link for accessing the Satellite Server page. From there you can sign in to the Kiteworks Admin Console and switch to a backup server to resume running workflows.

To switch to a backup server:

On the Satellite Server page, make a secondary server the new Primary server. This starts the worker service on that server and uses the last successful restoration to resume running workflows.

The role on the failed primary server is automatically changed to Unassigned. To resolve the issue, refer to the reason listed in the email notification and also check the audit log for a description of the event. You can also contact Kiteworks technical support at https://community.kiteworks.com for assistance.

Once you resolve an issue with a server and you want to use it the primary server again, first assign it the Secondary role and allow it to replicate the current primary server. You can check the audit log to get the restoration status. Then you can change role assignments, making it the new primary server and changing the other server back to a secondary server.

Once you resolve an issue with a server and you want to use it the primary server again, first assign it the Secondary role and allow it to replicate the current primary server. You can check the audit log to get the restoration status. Then you can change role assignments, making it the new primary server and changing the other server back to a secondary server.

Maintenance Mode

Turn on maintenance mode

When you need to perform work on the server, you can turn on maintenance mode. While in maintenance mode, users will not be able to access the system.

To turn on maintenance mode:

1. You can turn on maintenance mode in the following ways:
   - Go to System Setup > Maintenance Mode.
   - Go to System Setup > Locations > Maintenance Mode.
2. Turn on the Maintenance Mode Status switch.

Appendix A - Event tracking, license rules, user roles and permissions

Events tracked for reporting

The following list are some of the events that are tracked and available for reporting:

Table 59. Events tracked for reporting

Event	Event
add_folder delete_folder_permanent recover_folder change_folder_owner	delete_folder update_folder remove_user_from_folder
add_user user_type_changed suspend_user add_source_user user_login_failed	delete_user activate_user delete_source_user
add_file delete_file lock_file recover_file delete_file_version view_file move_file download_file	add_file_version delete_file_permanent unlock_file promote_file_version quarantine_file copy_file send_file
set_favorite	unset_favorite
set_notification	unset_notification
add_permission modify_permission	delete_permission
add_contact modify_contact	delete_contact

Table 59. Events tracked for reporting (continued)

Event	Event
update_settings reset_password update_profile	update_password update_username update_preferences
send_mail send_preview	send_message
add_task update_task	remove_task
add_comment edit_comment	remove_comment reply_comment
add_tag update_tag	remove_tag
download	upload
user_logged_in switched_to_ access_ecm blocked_access	user_logged_out switched_to_enduserportal access_folder
add_server add_source edit_source	update_server_role delete_source
ec_download_file ec_lock_file ec_return_file	ec_upload_file ec_unlock_file
application_settings_changed external_services_settings network_settings	system_update ssl_settings_changed location_settings

Monitor license usage

You can monitor license usage and availability from the following locations in the admin console:

- On the System Status page, license information is displayed in the Current Activities section.
- On the Users > User Management tab the number of licenses used is displayed at the top of the page. For detailed information on the license count, license expiration date, and the license recycling policy, click the information icon.

You can also export the list of deleted and demoted user accounts to a comma separated values (.csv) text file for reporting purposes.

License rules

- All verified internal user accounts consume licenses, regardless of their profile or status (inactive, deactivated, suspended).
- External user accounts assigned the Owner, Manager, or Collaborator role consume licenses since they can store content.
- Suspending or deactivating a user account (such as due to inactivity) does not release its license. To free up the license, you must delete the account. When deleting a user account, you have the option to assign the user's existing folder and file access to another user.
- Unverified user accounts do not consume licenses.

The following table defines which Kiteworks users are licensed.

Table 60. User license status

Folder role	Account type	Can download files	Can upload files	Licensed
Collaborator	Internal or External	Yes	Yes	Yes
Downloader	Internal	Yes	No	Yes
Downloader	External	Yes	No	No
Viewer	Internal	No	No	Yes
Viewer	External	No	No	No
Uploader	External	Yes, but only the files they uploaded to the folder	Yes	No
Custom*	Internal or External	Yes	No	Yes
* With Kiteworks version 8.0, a custom role is available for allowing users to only download and delete files from Kiteworks folders. Automated workflows can also use this role to move content between systems. A user assigned this role consumes a user license. To access this feature, please contact Kiteworks technical support to enable it for you.				

License recycling policy

A user license can be recycled once per license term.

Kiteworks releases a user license back to the license pool the first time the user profile or folder role is demoted to one that does not consume a license, or the user is deleted during a license term.

If the same demoted or deleted user subsequently consumes a license during the same license term, they will hold that license until the license expiration date, even if that user is demoted or deleted again by an administrator.

User roles and permissions

Permissions for working with folders

Table 61. Permissions for working with folders

Action	Owner	Manager	Collaborator	Downloader	Viewer	Uploader*
Add folders to Favorites	✓	✓	✓	✓	✓	–
Change user access to folders	✓	✓	–	–	–	–
Create folders	✓	✓	✓	–	–	–
Delete folders						
-- Nonrestricted folders	✓	✓	✓	–	–	–
-- Restricted folders	✓	✓	–	–	–	–
-- Top-level folders	✓	✓	–	–	–	–
-- Delete folders permanently	✓	✓	–	–	–	–
Download folders						
-- Nonrestricted folders	✓	✓	✓	✓	–	✓
-- Restricted folders	✓	✓	–	–	–	–
Edit folder properties	✓	✓	✓	–	–	–
Leave folders	✓	✓	✓	✓	✓	✓
Move folders	✓	✓	–	–	–	–
Rename folders	✓	✓	–	–	–	–

Table 61. Permissions for working with folders (continued)

Action	Owner	Manager	Collaborator	Downloader	Viewer	Uploader*
Recover folders	✓	✓	✓	–	–	–
Send messages to folder members	✓	✓	✓	–	–	–
Share folders	✓	✓	–	–	–	–
Subscribe to folder notifications	✓	✓	✓	✓	✓	–
Upload folders	✓	✓	✓	–	–	–
View and download folder activity (from the details pane)	✓	✓	✓	–	–	–
View folder details (from the details pane)	✓	✓	✓	✓	✓	–
View folder members	✓	✓	✓	–	–	–
View folder properties	✓	✓	✓	–	–	–
* Users assigned the Uploader role can see and work with only folders they upload to a shared folder.						

Permissions for working with files

Table 62. Permissions for working with files

Action	Owner	Manager	Collaborator	Downloader	Viewer	Uploader*
Add comments to files	✓	✓	✓	✓	–	–
Copy files						
-- Nonrestricted folders	✓	✓	✓	✓	–	–
-- Restricted folders	✓	✓	–	–	–	–

Table 62. Permissions for working with files (continued)

Action	Owner	Manager	Collaborator	Downloader	Viewer	Uploader*
Create and edit Microsoft Office files	✓	✓	✓	–	–	✓
Create and edit tasks	✓	✓	✓	–	–	–
Delete files						
-- Nonrestricted folders	✓	✓	✓	–	–	✓
-- Restricted folders	✓	✓	–	–	–	–
-- Delete files permanently	✓	✓	–	–	–	–
Download files						
-- Nonrestricted folders	✓	✓	✓	✓	–	✓
-- Restricted folders	✓	✓	–	–	–	–
Edit their own comments	✓	✓	✓	✓	–	–
Edit file expiration dates	✓	✓	✓	–	–	–
Edit files in the app editor	✓	✓	✓	–	–	–
Lock and unlock files						
-- Personal files	✓	✓	✓	–	–	–
-- Other user files	✓	✓	–	–	–	–
Manage file versions	✓	✓	✓	–	–	–
Move files						
-- Nonrestricted folders	✓	✓	If allowed by administrator	–	–	✓

Table 62. Permissions for working with files (continued)

Action	Owner	Manager	Collaborator	Downloader	Viewer	Uploader*
-- Restricted folders	✓	✓	–	–	–	–
Open files	✓	✓	✓	✓	✓	✓
Push files to folder member devices						
-- Nonrestricted folders	✓	✓	–	–	–	–
-- Restricted folders	–	–	–	–	–	–
Recover files	✓	✓	✓	–	–	–
Rename files	✓	✓	✓	–	–	✓
Request files	✓	✓	✓	–	–	–
Send files						
-- Nonrestricted folders	✓	✓	✓	✓	–	✓
-- Restricted folders	–	–	–	–	–	–
Share files						
-- Nonrestricted folders	✓	✓	–	–	–	–
-- Restricted folders	–	–	–	–	–	–
Upload files to folders	✓	✓	✓	–	–	✓
View and annotate PDFs	✓	✓	✓	–	–	–
View comments	✓	✓	✓	✓	–	–
Work with files offline	✓	✓	✓	✓	–	–
* Users assigned the Uploader role can see and work with only files they upload to a shared folder.						

Appendix B - Authorization and Authentication

Kerberos setup and usage

Perform the following steps to set up and use Kerberos.

To set up Kerebos:

1. On the domain controller, create a new user (for example, kerbuser) specifically for Kerberos authentication. DO NOT use this user account for normal logins. Leave this account untouched.
2. On the domain controller, create a keytab file for Kiteworks host name.
   - Generic command:

     ```
     ktpass -princ HTTP/[Kiteworks host name]@[DOMAIN REALM] -mapuser
     [new user created in step 1 on whose account the keytab will be
     linked]@[DOMAIN REALM] -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL
     -pass [password for the new user created in step 1] -out [keytab
     file output path]
     ```

   - So, for example:

     If your Kiteworks box hostname is test-kiteworks.yourcompany.net,

     And the domain realm is EXAMPLE.COM

     And the user created in step 1 is kerbuser,

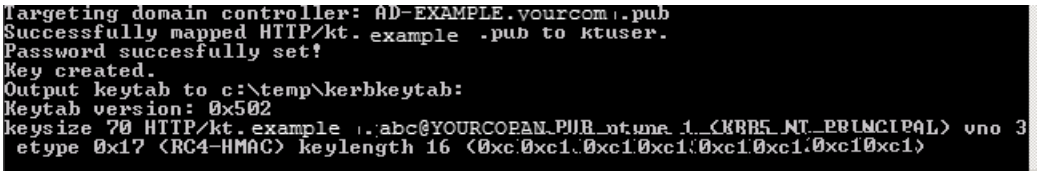
     And the keytab file output path is c:\temp\kerbkeytab

     Then the command to generate keytab is the following (generate the Keytab on your Domain Controller using the following parameter -crypto AES256-SHA1 if the account supports Kerberos AES 256 bit Encryption):

     ```
     ktpass -princ HTTP/[Kiteworks host name]@[DOMAIN REALM] -mapuser
     Your_Kerb_User@[DOMAIN REALM] -crypto AES256-SHA1 -ptype KRB5_NT_
     PRINCIPAL -pass Kerb_User_Password -out [keytab file output path]
     ```

     Ensure that the Kerberos account you have created has the following permission in active directory.
3. Enable Kerberos SSO, upload the generated keytab file from KW and complete the other Kerberos setup settings.
4. On a windows box connected to the DOMAIN REALM, open a browser and go to your login page.
5. Click Login via Kerberos link and if everything is fine, you should be auto logged in.
6. If you are creating the user on an AD box, you do not need AES 128 or 256-bit encryption checked, but for clarity purposes user accounts with these options checked have been created and Kerberos authentication still works with Kiteworks, tested in the yourcompany.pub domain.

   If you are creating the user and password, remember that the password is typed in the clear while in the command prompt, as shown in the output below.



Kiteworks setup

To set up Kiteworks to use Kerebos:

1. Enable Setup SSO with Kerberos. Kerberos Settings are based on the steps above. The other 2 tabs are the same as SAML SSO.
2. Authentication Realm is the Domain Realm for the AD box and must be in all UPPERCASE. Key Distribution Center, is the IP or FQDN of the Key Distribution Center, this is generally the AD box.
3. In order for Kerberos to work you have to log onto the domain as the user created in your AD, in order to simulate this RDP is used.
4. Log in via RDP to the domain as the user. The sign in screen displays after going to kt.yourcompany.pub
5. Click the Login using the Kerberos link. You should be in the Kiteworks Web User interface.
6. In the Kiteworks Admin Console, go to Users > User Management and verify that the user was created successfully.
7. You can see when a SSO user logged into Kiteworks and the IP they accessed from under Activity and Reports.

Kerberos checklist

1. While creating the keytab file, ensure that "DOMAIN REALM" is entered in all CAPITAL letters (for example: AD.EXAMPLE.NET).
2. ALWAYS create a new user to map the keytab file.
3. If there is any issue and you need to re-generate the keytab file for the same host name, then delete the old user which was mapped to the previous keytab for the same host name.
4. Ensure that the keytab file is not mapped to more than one user.
5. On the domain controller, you can run the command given below and check the output to confirm only one entry is returned.

   `setspn -q HTTP/{Kiteworks host name}`

   For example:

   `setspn -q HTTP/kiteworks.yourcompany.net`
6. Ensure that the browser is able to fetch the ticket for the Kiteworks host.

   Firefox browser: Add {Kiteworks host name} in network.negotiate?auth? uris section of About::config.
7. After the keytab file is uploaded, ensure that the keytab file is correct.

   SSH to the Kiteworks box and run the command below:

   `kinit -k -t /etc/krb5.keytab HTTP/{Kiteworks host name}`

   For example:

   `kinit -k -t /etc/krb5.keytab HTTP/kiteworks.yourcompany.net`

   If this command does not return any error, it means the keytab file is correct. This is the MOST important step to ensure that the keytab and Kerberos setup on the Kiteworks server is correct.
8. Ensure the new keytab file is used. Restart nginx.
9. Ensure that the user's browser is sending the latest Kerberos ticket.

   This is to ensure that after a new keytab is generated and uploaded it to the server, the user browser does not send a Kerberos ticket that uses the old keytab.

   Clear the old Kerberos ticket by running the command below on the user machine.

   `klist purge` (note that this command will clear all the Kerberos tickets on user's desktop, so please inform the user before running it).

10 Ensure that the Kerberos ticket is listed for the host name by running this command:

`klist`

If the SPN is mapped to two users, the browser will not be able to get the Kerberos ticket.

Typical errors

- `HTTP 401 error`

  This means that the server prompted the browser for the Kerberos ticket but the browser did not send back a ticket

  Possible solution:

  Check if step 6 listed above was done correctly.

  Check if SPN is not mapped to two different AD entries (step 5 above).

- `HTTP 500 server error`

  These errors are recorded in nginx error log (/log/nginx/ngsync.error.log)

  Possible cause/solution:

  Check if the keytab is correct (step 7 above).

  Check if the keytab is mapped to one user (step 5 above).

  Sample nginx error log entry:

  2016/03/15 07:34:39 [error] 582#0: *106 gss_acquire_cred() failed: : Used service principal: HTTP/kpkiteworks.yourcompany.net@AD.EXAMPLE.NET, client: 10.254.100.101, server: kpkiteworks.yourcompany.net, request: "GET /kauth HTTP/1.1", host: "kpkiteworks.yourcompany.net", referrer: "https://kpkiteworks.yourcompany.net/idp/module.php/core/loginuserpass.php?Auth State=_01212121212129a12121a121ca121212121213A%2F%2Fkpkiteworks.yourcompany.net"

- `HTTP 403 error`

  This indicates that the key tab is likely correct but the Kerberos ticket is incorrect.

  Possible solution:

  Check if the browser is sending the latest ticket (step 9 above).

  Check if the browser is able to fetch the ticket for the SPN (step 10 above).

  Check if SPN is not mapped to two different AD entries (step 5 above).

Best practices to avoid errors

Delete any old user that is mapped to SPN.

Create a new user and keytab file and map the SPN to the new user.

Configure ADFS with Kiteworks

This section details the steps required to connect Kiteworks to an ADFS Identity Provider (idP), including configuring ADFS and configuring Kiteworks.

Assumptions

ADFS is employed as an idP.

Configure ADFS

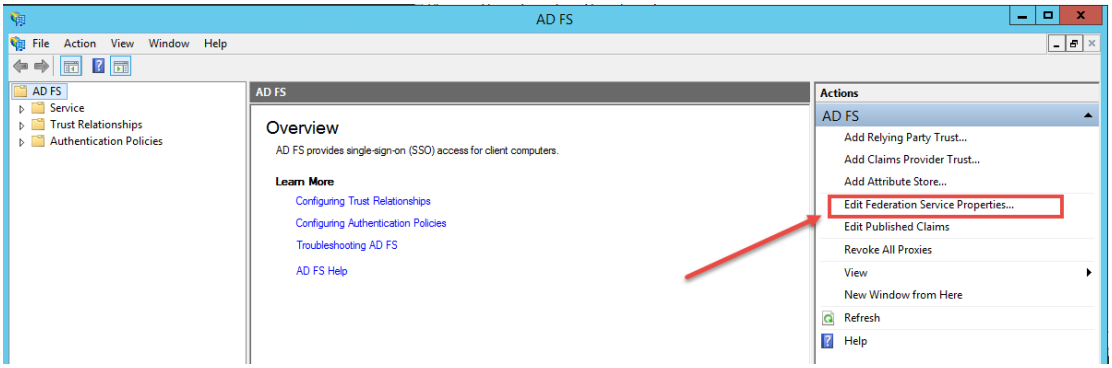
To configure ADFS:

1. Discover idP Entity ID.
2. Add Relying Party Trust.
3. Edit Claim Rules.
4. Export RSA Public Key Certificate.

Discover idP entity ID

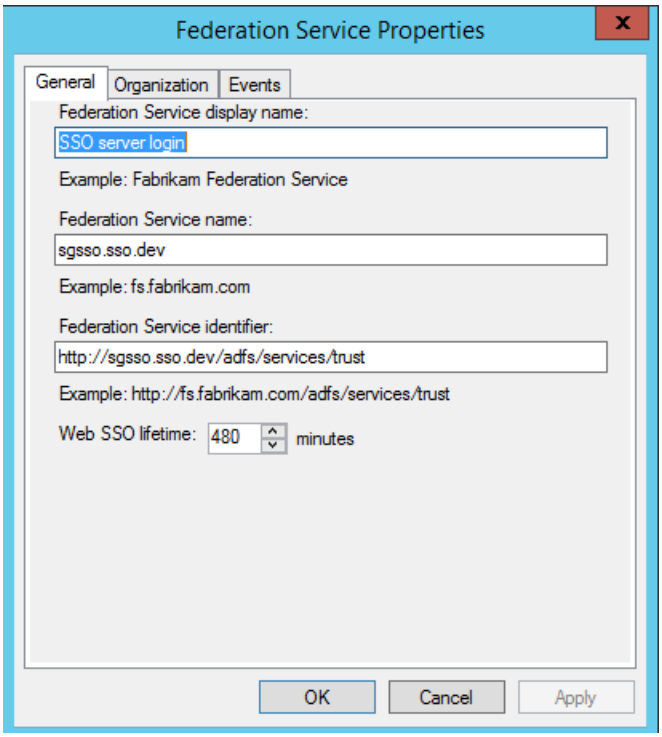
To discover the idP Entity ID:

1. Open the ADFS Management console.
2. Click Edit Federation Services Properties.



3. Copy the Federation Service Identifier value. This value will likely be:
   <the full qualified domain name of your ADFS server/adfs/services/trust>.
   Here, we're using:
   http://adfs_server.example.com/adfs/services/trust

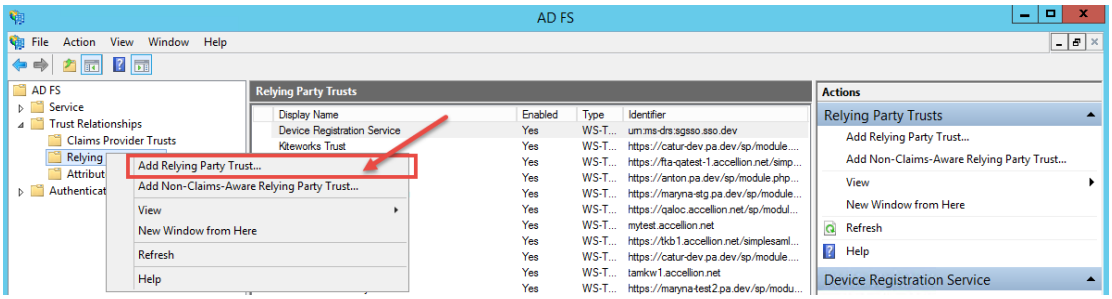
4 Click Cancel.



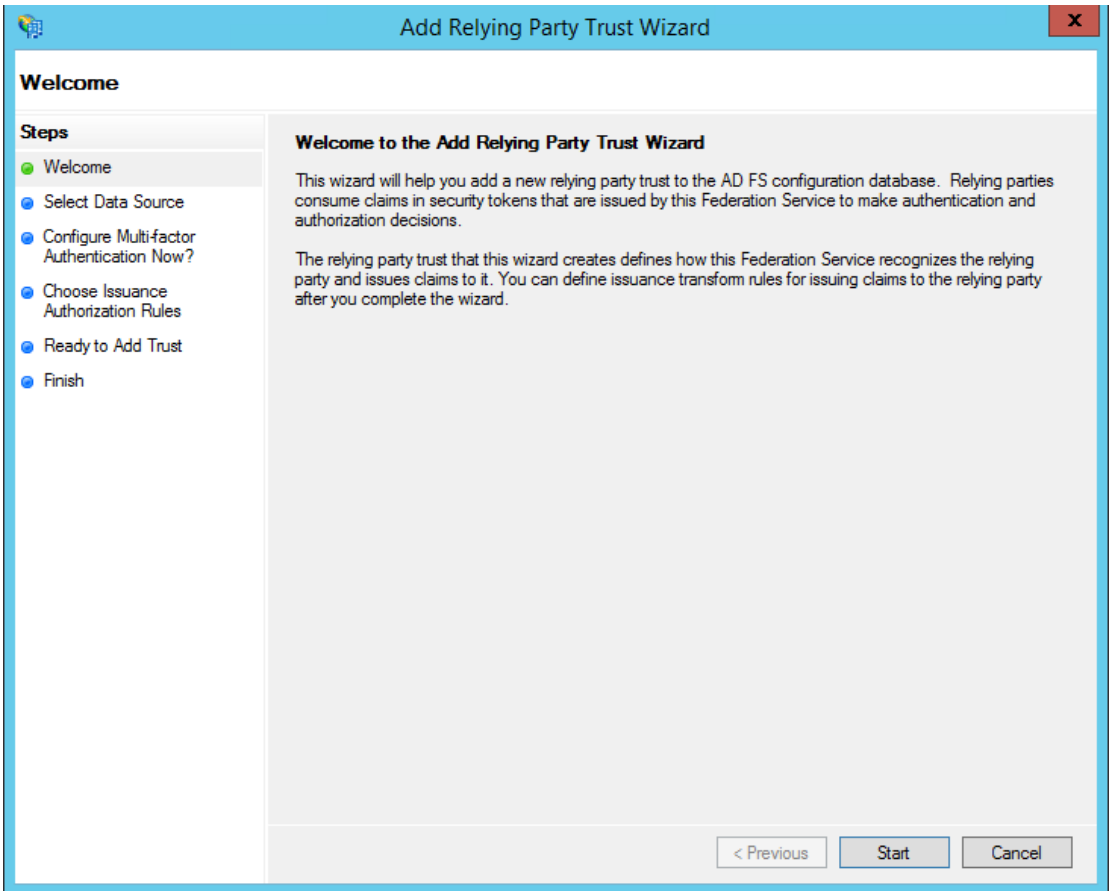
Add relying party trust

To add relying party trust:

1 From the ADFS Management console, right-click Relying Party Trusts and select Add Relying Party Trust.



2 Click Start. The steps listed on the left of the screen are the steps to add the Relying Party Trust.



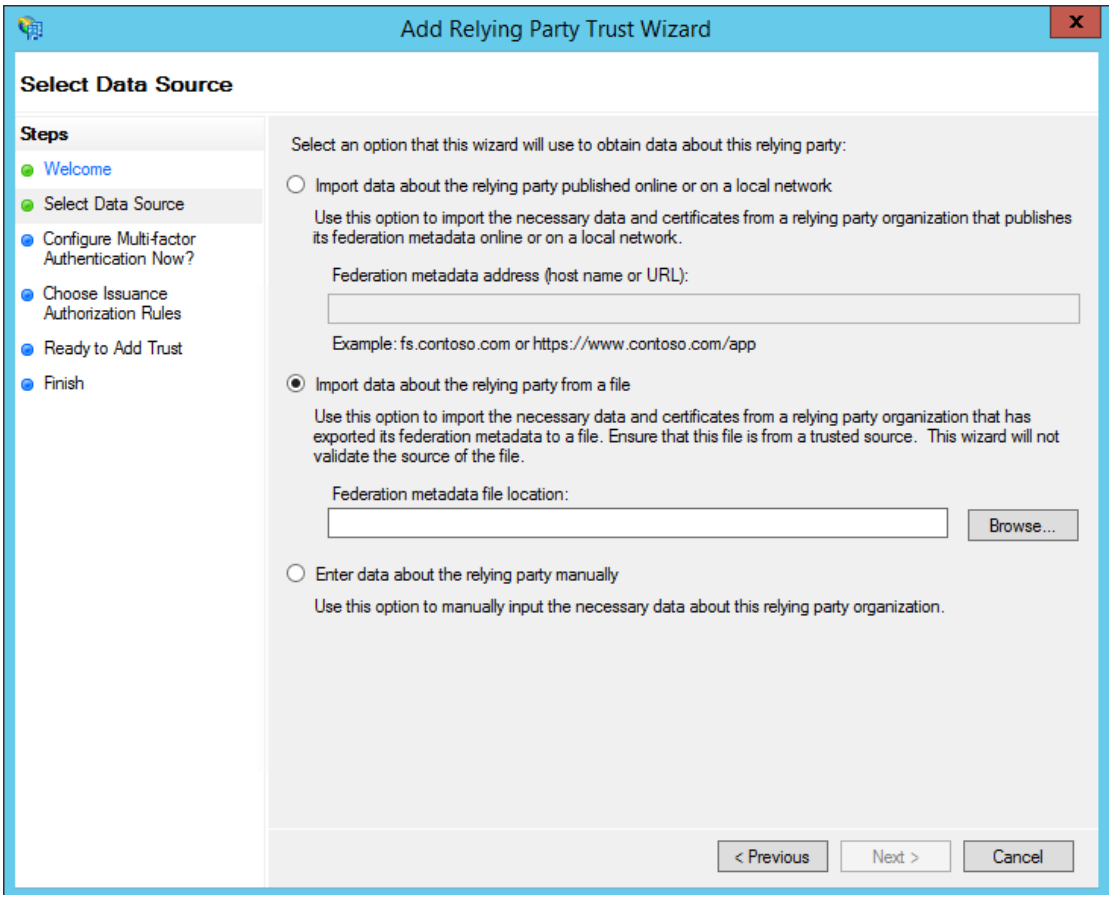
Import data about the relying party

To import data about the relying party:

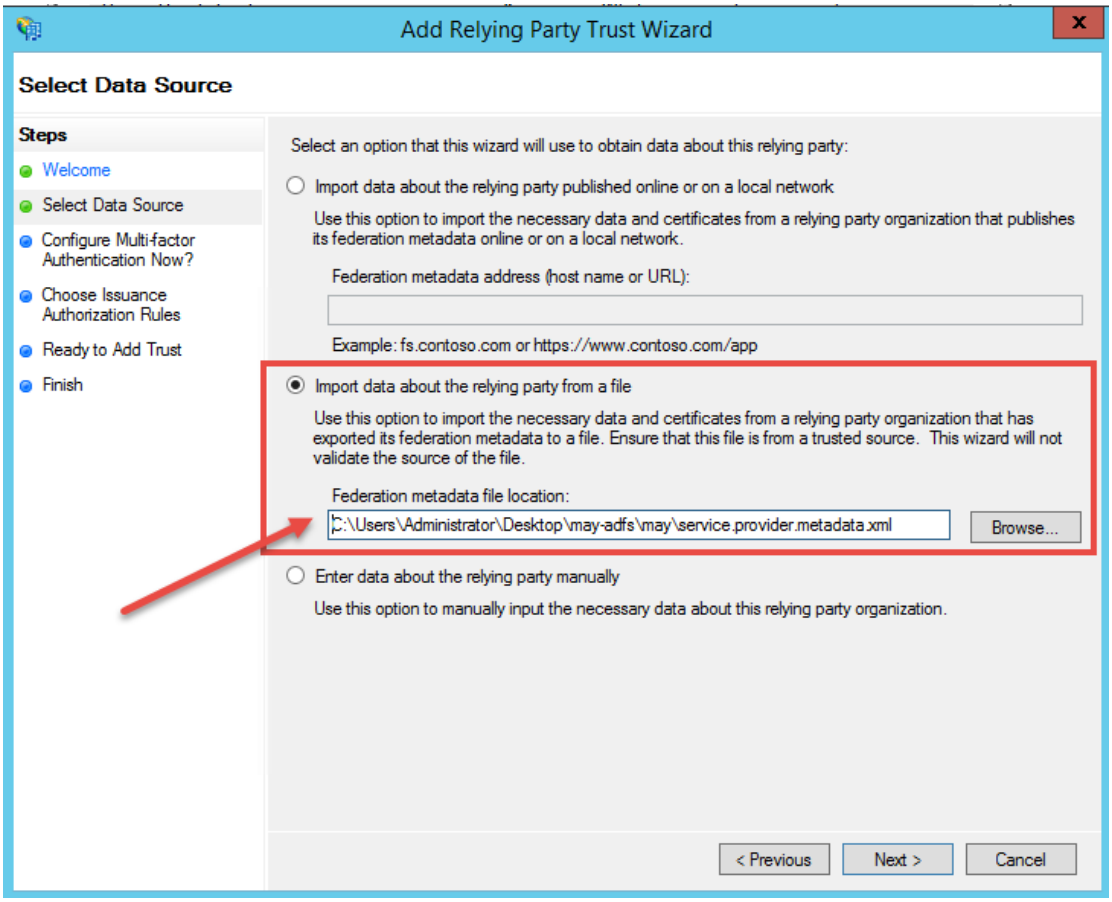
1 From the ADFS Management console, right-click Relying Party Trusts and select Add Relying Party Trust.

2 Click Start. The steps listed on the left of the screen are the steps to add the Relying Party Trust.

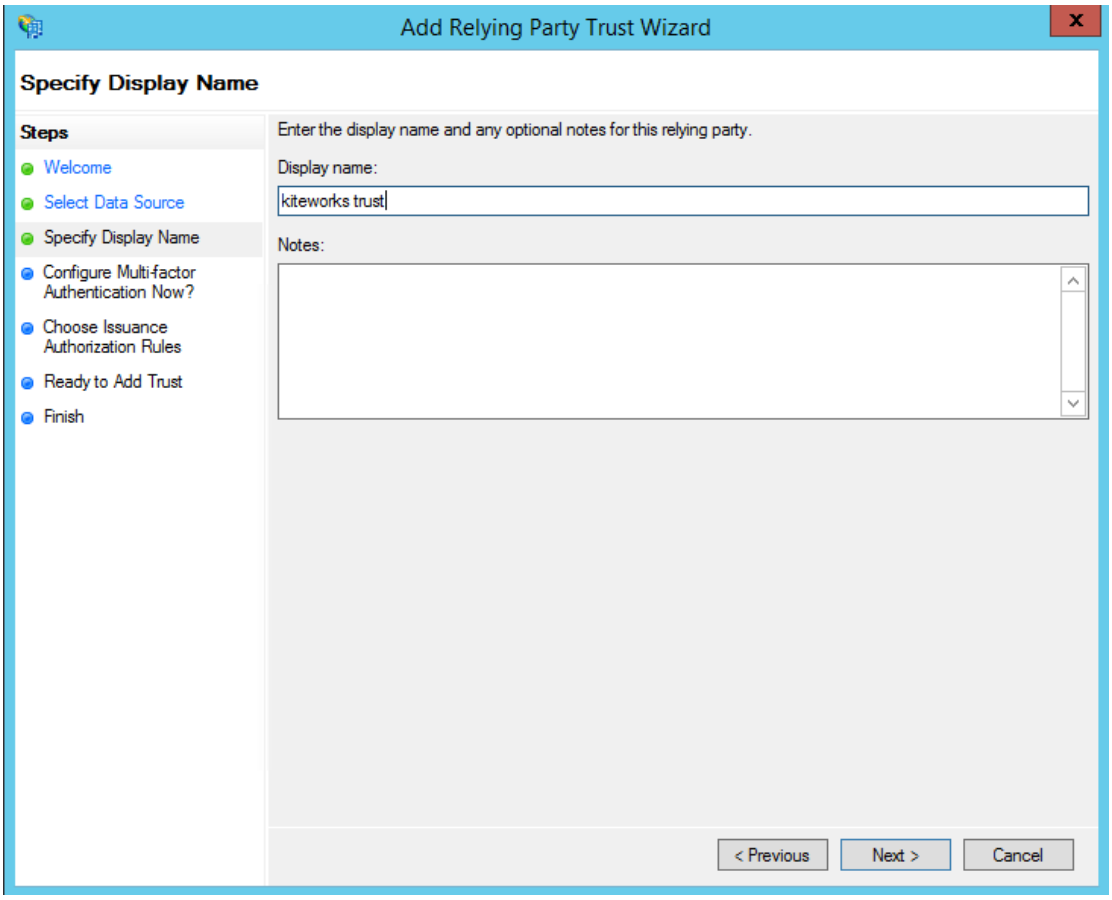
3 Select Import data about the relying party from a file. Click Next.



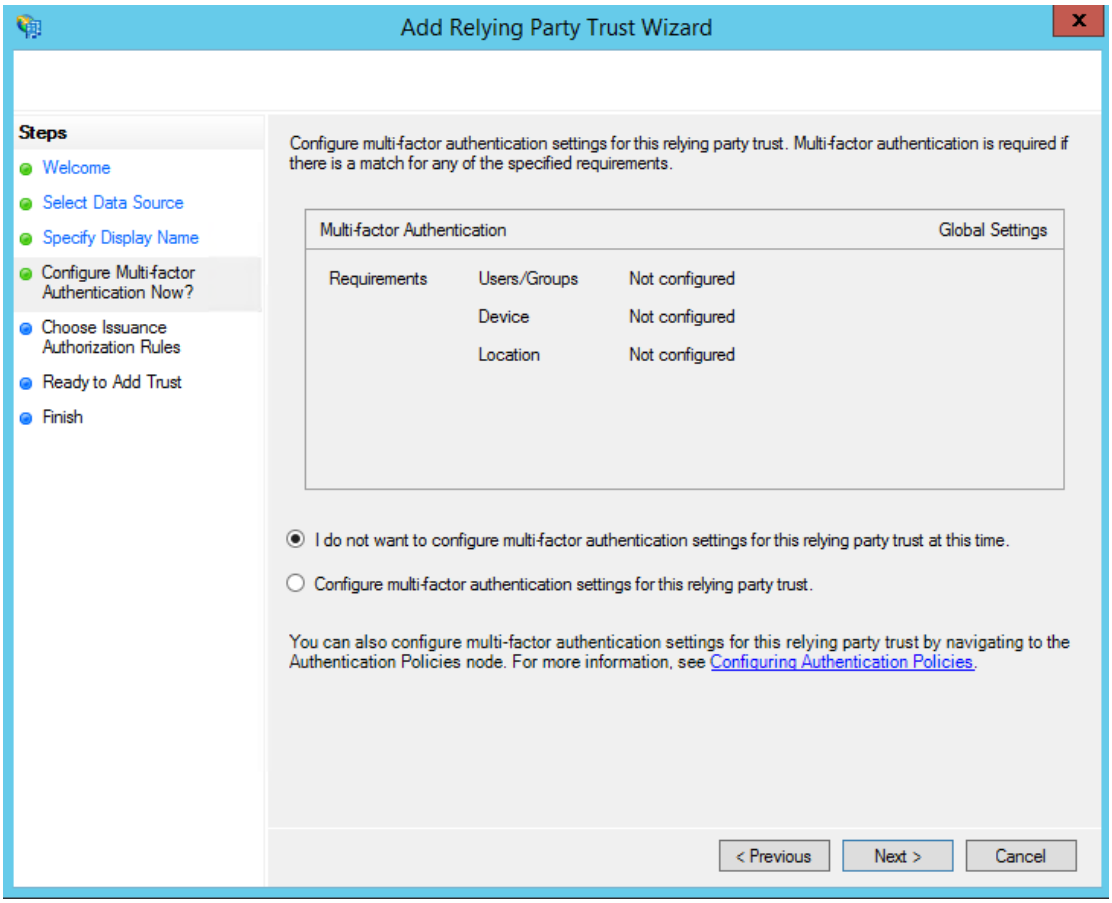
4. This file is generated from the Kiteworks Admin Console. Click the Application icon in the Kiteworks Admin Console. Click Authentication and Authorization > SSO Setup and select SSO Setup with SAML 2.0.
5. Select Initiate Auth Request.
6. The idP Entity ID is the Federation Service Identifier value explained in Discover idP entity ID. The example that was used was: http://adfs_server.example.com/adfs/services/trust
7. Enter the Service Provider Entity ID and the Single Sign-On Service URL. The Service Provider Entity ID for Kiteworks can be your Kiteworks host name.
8. Populate the form fields with information from the external idP Source (see the SSO Setup Fields table below).
9. Click Save, and then click Download Service Provider Metadata and save the file.
10. Click Browse and upload the service.provider.metadata.xml file. Click Next.



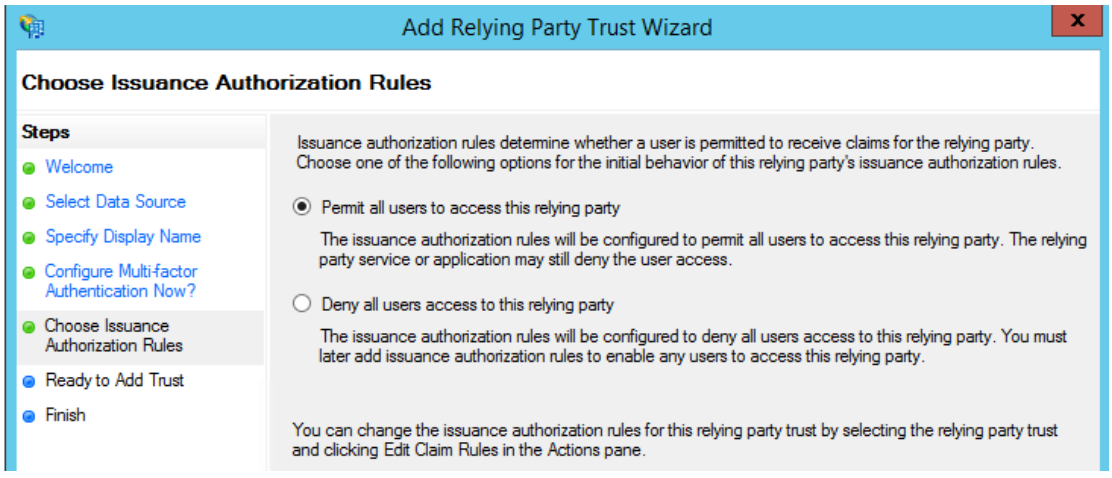
11 Specify a Display Name. Click Next.



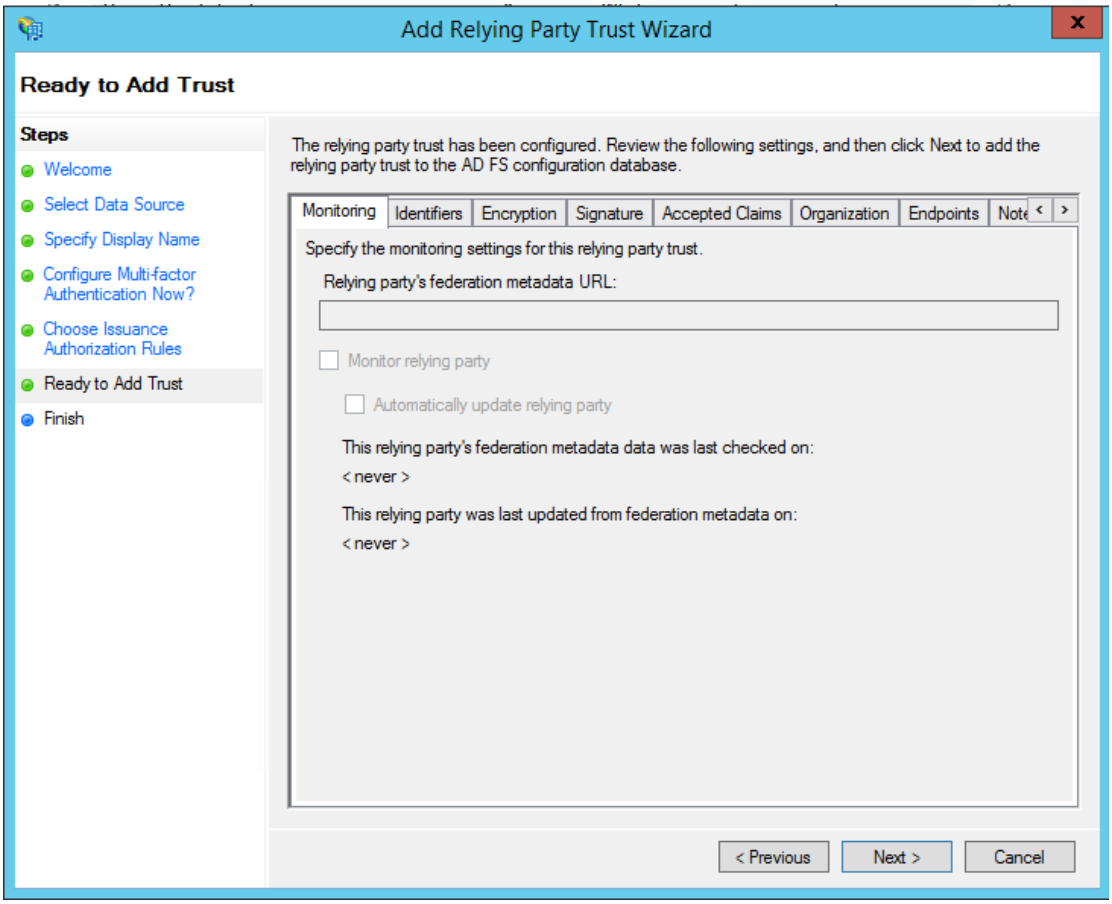
12 Configure multi-factor authentication. In this case I do not want to configure multi-factor authentication settings for this relying party trust at this time is selected. Click Next.



13 Choose issuance authorization rules. In this case Permit all users to access this relying party is selected. Click Next.



14 The relying trust party is now configured. Click Next.



15 Click Close to add the relying party trust.

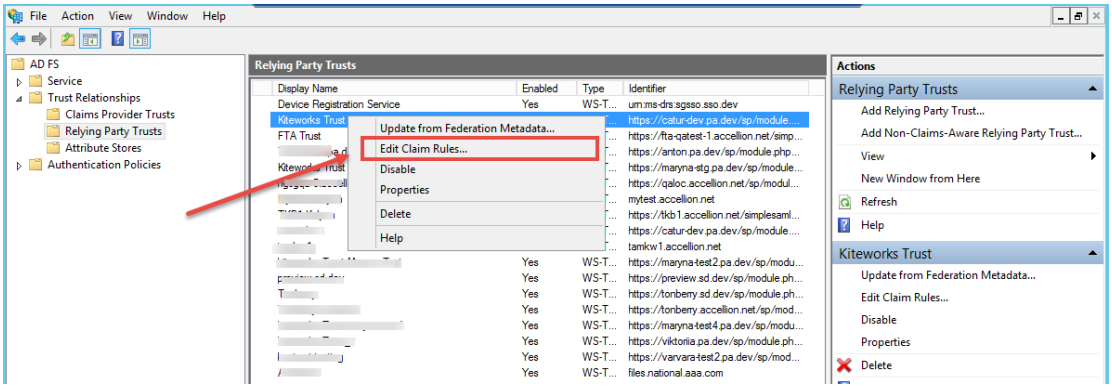
Edit claim rules

To edit claim rules:

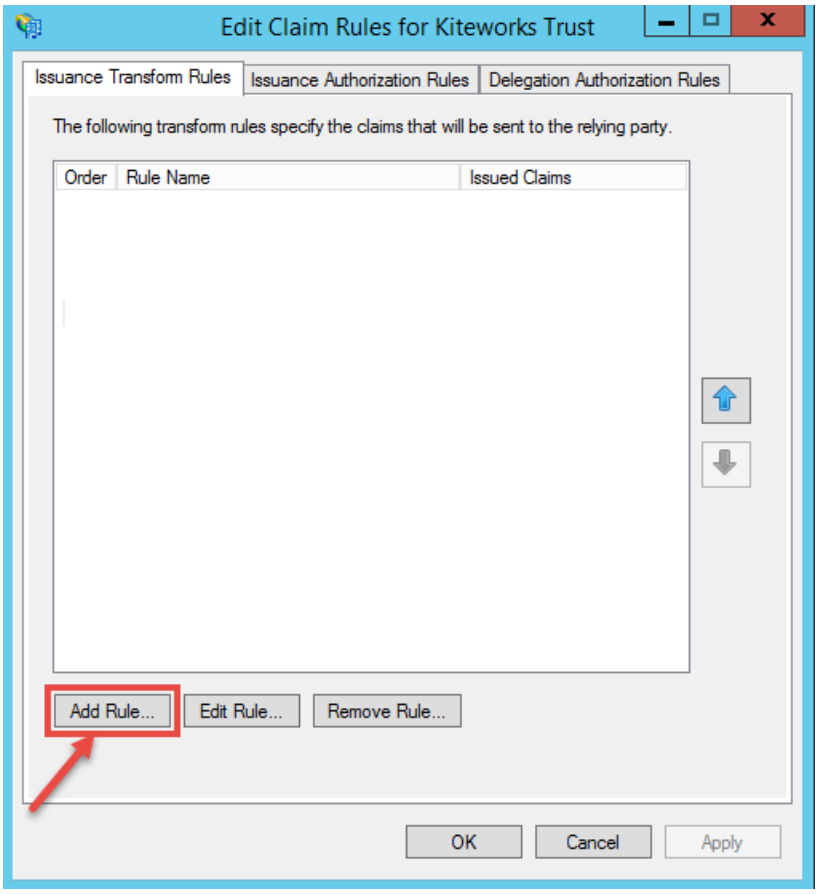
1 From the ADFS Management console, under Trust Relationships, click Relying Party Trusts.

2 From the list shown, select and right-click Kiteworks Trust.

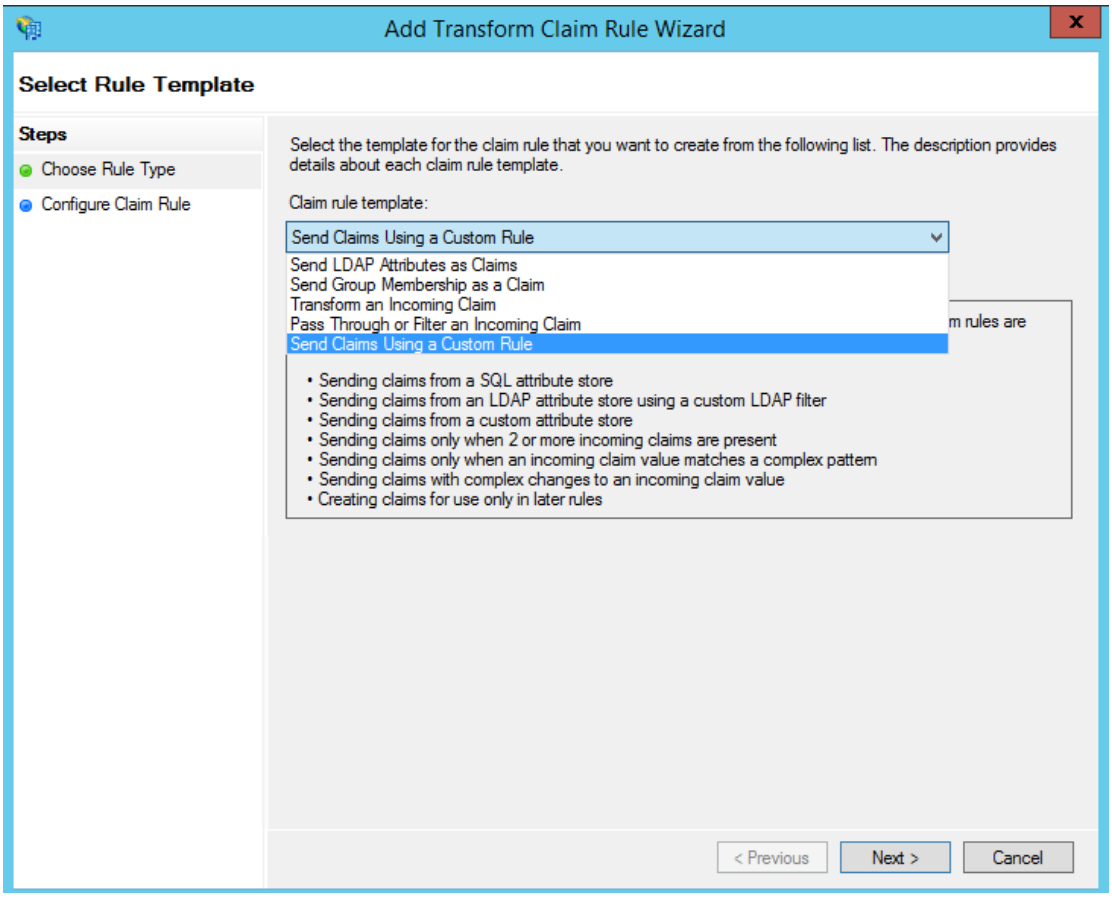
3 From the right-click menu, select Edit Claim Rules.



4 In the dialog box, click Add Rule.



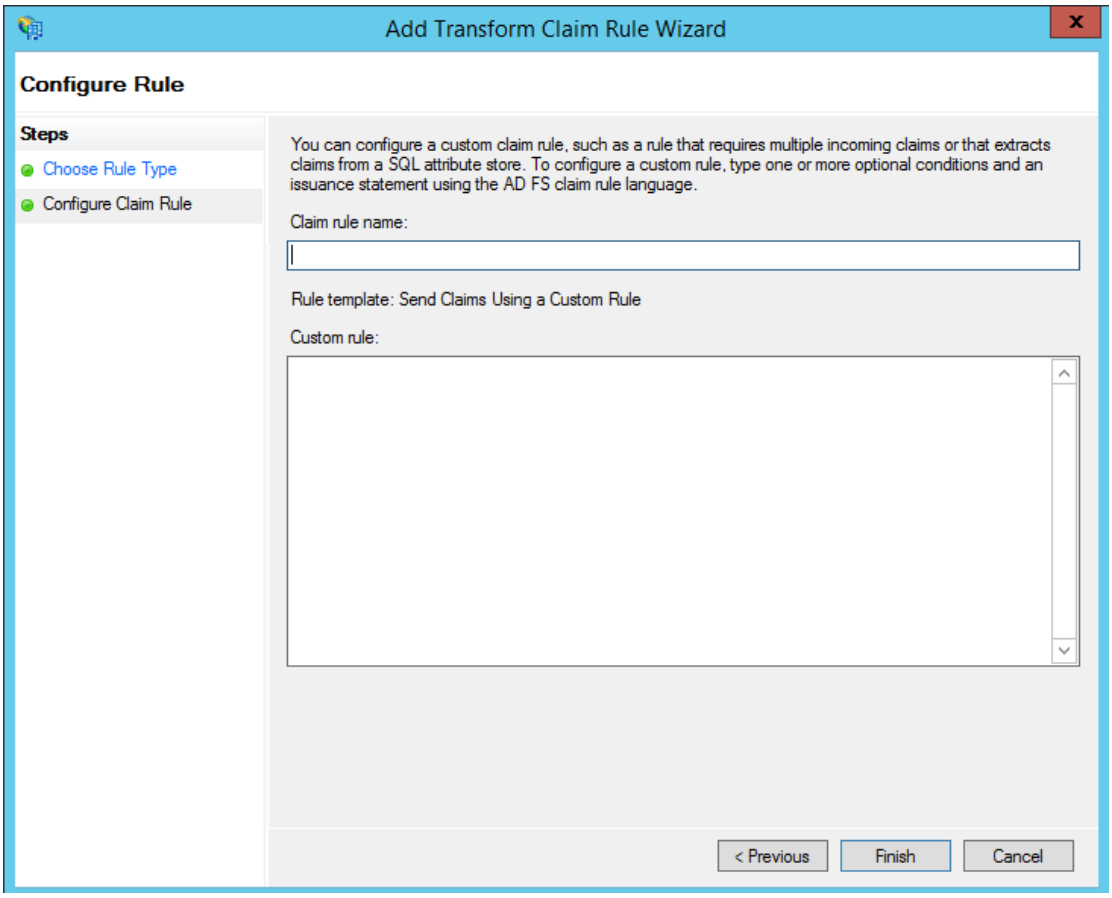
5 From the drop-down menu under Claim rule template, select Send Claims Using a Custom Rule. Click Next.



6 Under Claim rule name, type: Step 1

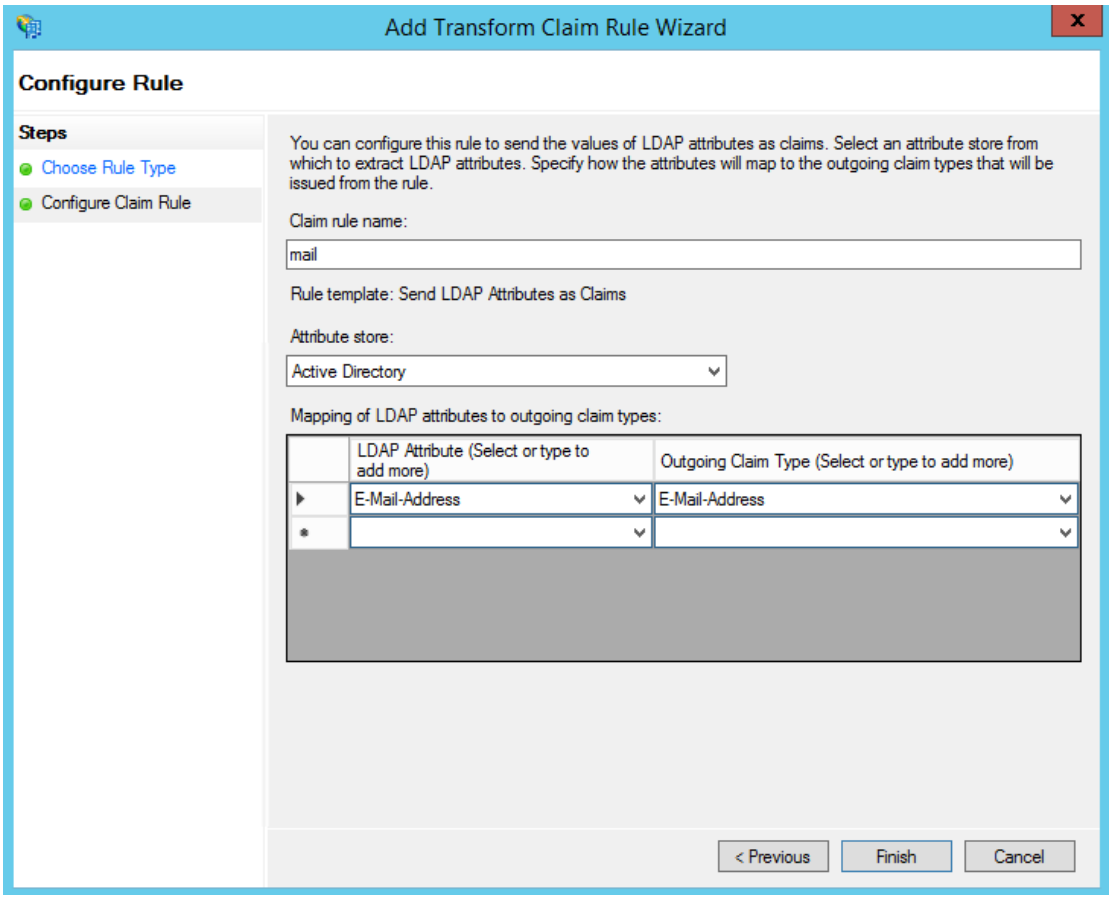
7 Under Custom rule, type:
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"), query = ";mail;{0}", param = c.Value);

8 Click Finish.



9 From the ADFS Management console, under Trust Relationships, click Relying Party Trusts.
10 From the list shown, select and right-click Kiteworks Trust.
11 From the right-click menu, select Edit Claim Rule.
12 Click Add Rule.
13 From the drop-down menu under Claim rule template, select Send Claims Using a Custom Rule. Click Next.
14 Under Claim rule name, type: Step 2
15 Under Custom rule, type:
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer,
Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/
ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:
nameid-format:emailAddress");
16 Click Finish.
17 From the ADFS Management console, under Trust Relationships, click Relying Party Trusts.
18 From the list shown, select and right-click Kiteworks Trust.
19 From the right-click menu, select Edit Claim Rules.
20 From the dialog box, click Add Rule.

21 From Claim rule template drop down menu, select Send LDAP Attributes as Claims. Click Next.
22 Under Claim rule name, type: mail
23 From the Attribute store drop-down list, select Active Directory.
24 On the list of Mapping of LDAP attributes to outgoing claim types, select E-Mail Addresses.
25 Under Outgoing Claim Type, select mail.
26 Click Finish.

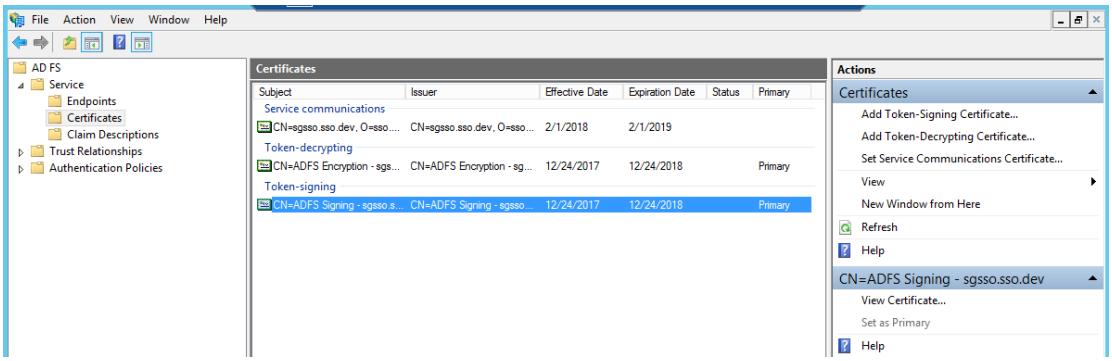


27 Click OK.

Export RSA public key certificates

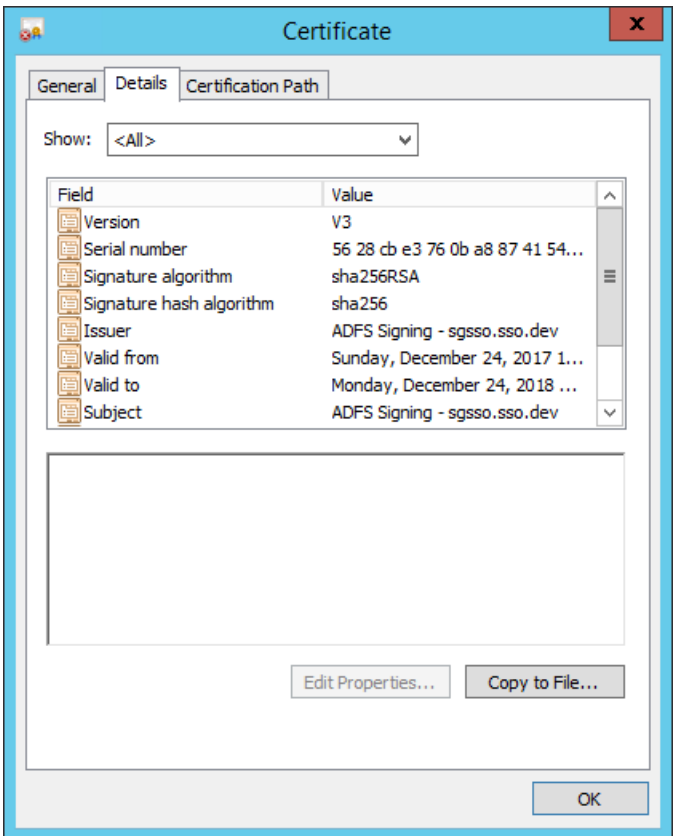
To export RSA public key certificates:

1 On the ADFS Management console, navigate to: AD FS > Service> Certificates
2 Double-click the Token-signing certificate. The Certificate window appears.



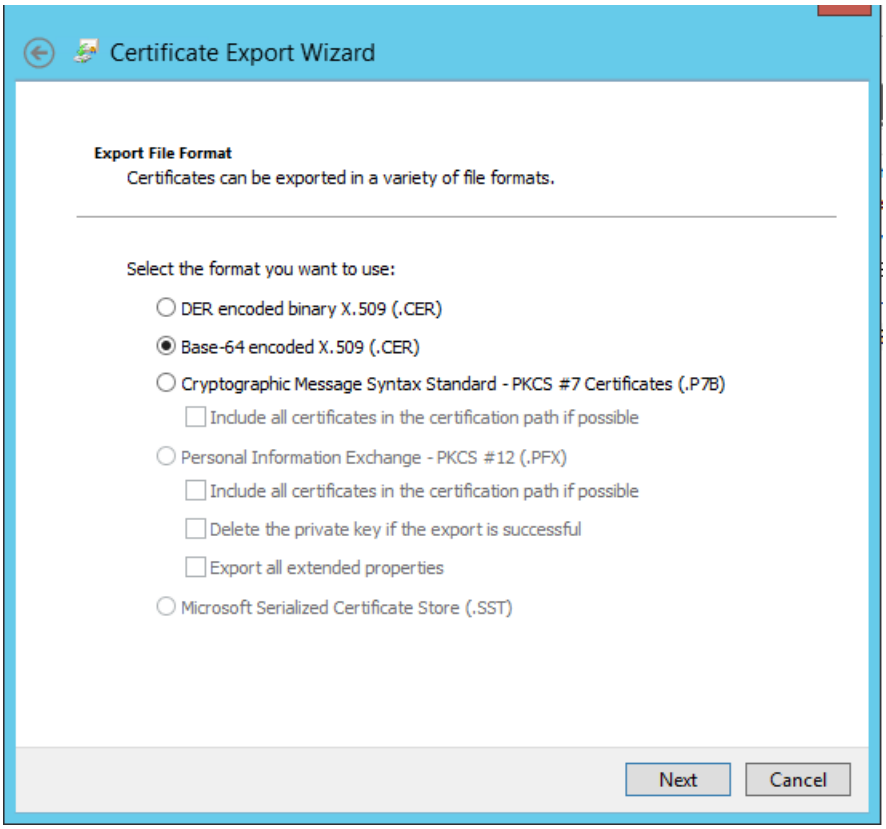
3 On the Certificate window, click the Details tab.

4 Click Copy to File. The Certificate Export Wizard begins.



5 Click Next.

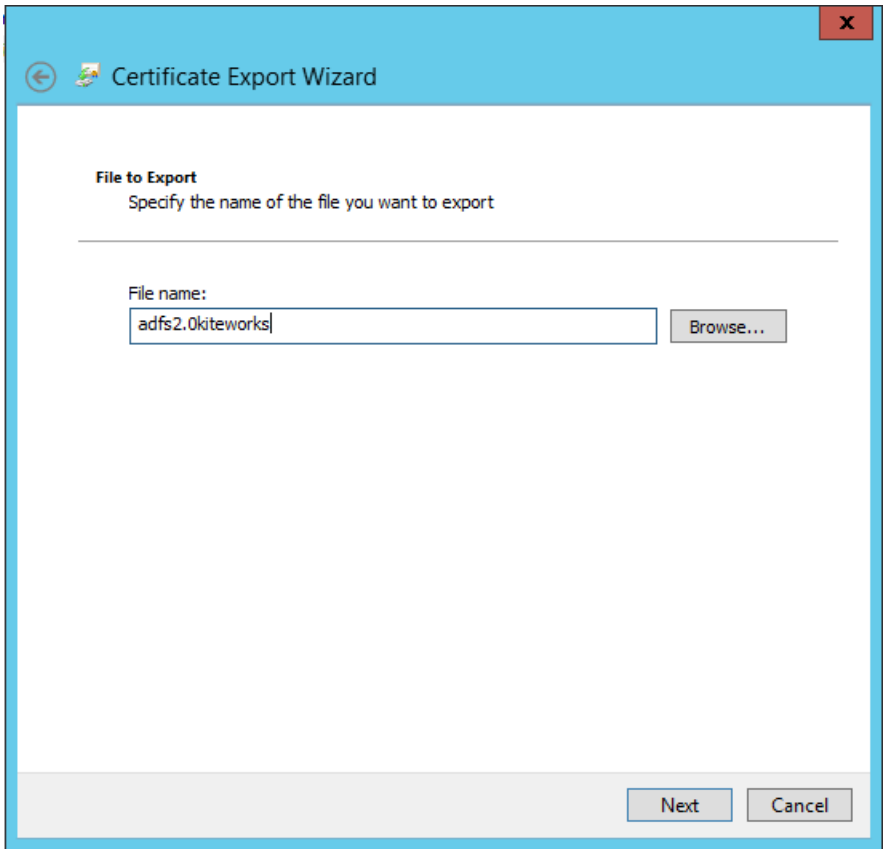
6 Select the Base-64 encoded X.509 (.CER) radio button, and then click Next.



7 Type the file name of the certificate to be exported and if desired, browse to the location where you would like the file to be saved.

Important: Note the location of the destination of the certificate; it is needed to configure Kiteworks external SSO.

8 Click Next.



9 Click Finish.

Table 63. SSO setup fields

Field	Value	Description
idP Entity ID	http://[adfs2.0FQDN]/adfs/services/trust	This is the value discovered in the step "Discover idP entity ID"
Service Provider Entity ID	The address of your Kiteworks server.	The Entity ID used by the Service Provider to refer to themselves during communications and to look up the metadata for other entities.

Table 63. SSO setup fields (continued)

Field	Value	Description
Single Sign-On Service URL	https://[adfs2.0FQDN]/adfs/ls/idpinitiatedsignon.aspx?loginToRp=	The FQDN for the ADFS idP. If authenticating via AuthNRequest, ensure the AuthNRequest checkbox is checked and use: https://[adfs2.0FQDN]/adfs/ls
Single Logout Service URL	The address of your Kiteworks server.	
RSA Public Key Certificate		Open the certificate saved above in "Export RSA public key certificates". Copy and paste the contents of the certificate into the field.

SAML

In Kiteworks the use of SAML consists of three parts, see following list. The three parts together allow a user to access and utilize the capabilities of Kiteworks from various devices: web, mobile, thick client, plugin, 3rd party product or automation client. All communications within the control of Kiteworks operates over SSL.

- Identity Provider (idP)
- Service Provider (SP)
- SAML Message
- Identity Provider

An Identity Provider establishes the identity of the user and is responsible for authenticating the user with the authentication mechanisms that the idP is configured for. In Kiteworks, Kiteworks is an Identity provider for Kiteworks users and users sourced from a configured LDAP store. Kiteworks can also be configured to use an external idP. The Identity Provider provides a SAML Message to the Service Provider that contains assertions about the user that was authenticated. The assertions that Kiteworks supports are discussed within the SAML Message section. The Identity provider and the Service Provider are configured to trust and accept communications from each other. This trust allows for Service Provider initiated requests and Identity Provider initiated requests and responses.

Kiteworks identity provider

The Kiteworks system is an idP. Currently Kiteworks is also the only Service Provider that the Kiteworks idP has an established trust with. Users that self-register or are invited to the system but are not found in an LDAP configured source are considered Kiteworks users that the Kiteworks idP can authenticate. The credentials are stored within Kiteworks. If a user is found within a configured LDAP source then the user

is authenticated against LDAP with the credentials provided. If the user is found within LDAP but unable to provide the correct password, the user will not be able to gain access to the system. When the Kiteworks idP is able to authenticate the user, the idP fashions a SAML Message that contains assertions about the user that was authenticated. The message is signed to prevent tampering of the message content. The message is then sent to the Kiteworks service provider typically by the end user's web browser. For SAML communication to be trusted, certificates are required. On setup of a Kiteworks system or tenant, the system generates a new certificate with public and private keys that are utilized by the Kiteworks idP and Kiteworks service provider to securely communicate SAML Message. The certificates generated are 2048 bit.

External identity provider

Kiteworks can be configured to allow users to authenticate with an external Identity Provider. Any Identity Provider that supports SAML 2.0 can be utilized. Examples of such Identity providers are Azure AD, ADFS, Okta, OneLogin, OpenIdP. Configuration must occur on both the idP and Kiteworks service provider to successfully communicate between the external idP and Kiteworks service provider. This configuration is dependent on the idP. Kiteworks requires to know the Issuer ID of the SAML Message, the public key of the Identity Provider, The login endpoint for the idP and the service provider ID that the idP is expecting. While the SSO Logout URL can be provided, it is not currently used. The External idP can enforce Authorization to Kiteworks via its processing engine for Authentication requests; how and what steps are in place by the external idP are out of scope.

Service provider

Kiteworks is a Service Provider via the APIs that it exposes. The consumers of the APIs are the various devices mentioned in the introduction. The Service Provider is partially responsible for the Authorization of the user. The service provider consumes the SAML assertions provided in the SAML Message. Using the information in the SAML assertions, the identity of the user that was authenticated is obtained. The service provider then processes the SAML Request based on rules to determine Authorization of the user into Kiteworks. Authorization may be restricted due to licensing. The other assertions provided are used to update the user within the Kiteworks system. Details of the assertions are provided in the SAML Message section. The Kiteworks service provider will provide a web cookie that is then consumed by the RelayState value of the request. The web cookie identifies the user within the Kiteworks system. The cookie is then either used by the RelayState as needed. For the web application this means that the user is able to utilize Kiteworks via a common web browser. For devices that require an OAuth token, the RelayState will be the OAuth endpoint to which the end point consumes the cookie and provides the caller with an OAuth code to redeem for an access token.

SAML messages

SAML 2.0 Messages are supported by Kiteworks. Go to http://en.wikipedia.org/wiki/SAML_2.0 for more information. The focus of this section is on the assertions supported by Kiteworks. The basics of SAML 2.0 messages is outside the scope. Kiteworks supports various assertions as each idP can designate how they issue assertions. Kiteworks supports the following assertions.

Table 64. Supported assertions

Field	Value	Description	Precedence	Description
N/A	UID	String:email	4	Required (unless alias). Email of the user that was authenticated.
UID	mail	String:email	1	Support for idPs that cannot specify UID Assertion.
UID	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	String:email	2	Support for Azure AD.
UID	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	String:email	3	Support for Azure AD where Email is not available.
UID	usertype	Number		The value provided assigns the user to the associated user profile ID from the Kiteworks Admin Console user profile list. If the assertion is not provided, Kiteworks will map by LDAP (if available) or by email domain.

SAML requests

SAML requests initiated by Kiteworks can be done in one of three ways and can depend on the external idP utilized. All SAML requests involve the query string and are done via HTTP-Redirect communication to the idP.

Table 65. SAML requests

Request type	Description	Sample
AuthnRequest	AuthnRequest is a protocol by which a request is made via a SAML AuthnRequest formatted message to the idP. The message specifies the target application. For this to be initiated, the user is redirected to an endpoint on the Kiteworks service provider which generates the AuthnRequest http://en.wikipedia.org/wiki/SAML_2.0#Authentication_Request_Protocol. The receiver may or may not support the RelayState argument back to the Kiteworks service provider. Kiteworks will use state from the AuthnRequest to redirect the consumer back to the RelayState to finish the request flow.	https://kiteworks.local/saml/login.php?sp=sp-sso&RelayState=https%3A%2F%2Fkiteworks.local Redirects to: (returns added for formatting purposes) https://idp.local?SAMLRequest=fVLBUsIwFPyVTu5p0za0NAPMoBxkBpUR9ODFCekDMrZJ7EtB%2F95SdMQL1327%2B97uvBHKunJi2vq9eYKPFtAHn3VlUPSDMWkbI6xEjcLIGlB4JVbT%2B4VIQiZcY71VtiIXkusKiQiN19aQYD4bkzeZsaQolAQFRZYkbDPIhopDFm8lBYg5DGPYDlk%2BYCR4gQY75Zh0Rp0csYW5QS%2BN7yAWc8oKytJ1kooBFyl%2FJcGsS6ON9L1q771DEUWV3WkTHrUp7RFDAz7KsmQo43xL4xQSyvNBRguel3TDFJcqL3ks0%2BiULSHB9DfArTXY1tCsoDloBc9Pi78V0Oj30O9t7dCa0MmwhEOELqpt2VYQur3r7U5Qb0ulwjPqKKIlwfKn2JvuSm121zvdnEko7tbrJV0%2BrtZkMjr5ir6jZnLtrFF0yRydv%2BGh2zGfLW2l1Vc0OVP%2B%2F8jkGw%3D%3D&RelayState=https%3A%2F%2Fkiteworks.local

OAuth with SAML

Where Kiteworks uses SAML to communicate the identity of a user from a trusted identity provider, OAuth in Kiteworks is used for obtaining an access token to access the APIs that Kiteworks exposes to consumers with a valid access token. The OAuth end points supported are documented within Authentication and Authorization of Kiteworks APIs. This section aims to describe how an OAuth token is obtained when SAML is involved. In the following steps the actors are as follows:

- User - user of the device
- Device - the browser, mobile application, thick client, plugin,
- Browser - web browser that User uses to authenticate
- Kiteworks service provider
- Kiteworks idP
- External idP

To obtain an OAuth token:

1. Device requests authorization for an access token /oauth/authorize from Kiteworks service provider.
2. Kiteworks service provider determines if user is already authenticated.
   - No: proceed to step 3
   - Yes: proceed to step 10
3. Kiteworks service provider redirects requester to Kiteworks idP with RelayState of /oauth/authorize.
4. Kiteworks idP provides web login form.
5. User of Device decides on Kiteworks idP or external idP.
   - Kiteworks idP: proceed to step 6
   - External idP: proceed to step 10
6. User enters credentials into form and submits
7. Kiteworks idP validates credentials:
   - User authenticates correctly: proceed to step 8
   - User fails to authenticate: proceed to step 4
8. Kiteworks idP generates SAML Message and redirects browser to Kiteworks service provider via HTTP-POST with SAMLResponse and RelayState if provided.
   - Proceed to step 11
9. Browser is redirected to external idP with authnRequest on query string.
10. External idP processes request, authenticates user.
11. External idP generates SAML Message and redirects Browser to Kiteworks service provider via HTTP-POST with SAMLResponse.
12. Kiteworks service provider processes SAMLResponse, issues web cookie, and redirects Browser to /oauth/authorize.
13. /oauth/authorize issues code to device.
14. Device retrieves code from /oauth/authorize response.
15. Device submits code to /oauth/token for redemption.
16. Device retrieves access token from response.
17. Device executes API requests using access token obtained.

For information on connecting your Kiteworks system to Azure SSO, refer to the *Kiteworks Deployment Guide*.

Appendix C - Supported file types

File types supported when previewing files

Table 66. File types supported for viewing files

Extension	File format	Online Viewer	Android mobile app	iOS mobile app
.bmp	Device Independent Bitmap	✓	✓	✓
.csv	CSV (Comma delimited)	✓	–	–
.doc	Word 97-2003 Document	✓	✓	✓
.docm	Word Macro-Enabled Document	✓	–	–
.docx	Word Document	✓	✓	✓
.dot	Word 97-2003 Template	✓	–	–
.dotm	Word Macro-Enabled Template	✓	–	–
.dotx	Word Template	✓	–	–
.gif	GIF Graphics Interchange Format	✓	✓	✓
H.264	High definition video	✓	–	–
.html	Web page	✓	–	–
.jpg	JPEG File Interchange Format	✓	✓	✓
.mov	Apple video	✓	–	✓
.mp3	MPEG-3 video	✓	✓	✓
.mp4	MPEG-4 video	✓	✓	✓
.odf	OpenDocument formula and mathematical equations	✓	–	–
.odg	OpenDocument graphics document	✓	–	–
.odp	OpenDocument presentation document	✓	–	–
.ods	OpenDocument spreadsheet document	✓	–	–
.odt	OpenDocument text document	✓	–	–

Table 66. File types supported for viewing files (continued)

Extension	File format	Online Viewer	Android mobile app	iOS mobile app
.odtt	OpenDocument text document	✓	–	–
.ogm	Ogg media file	✓	–	–
.ogv	Ogg video file	✓	–	–
.pdf	PDF	✓	✓	✓
.png	PNG Portable Network Graphics Format	✓	✓	✓
.pot	PowerPoint 97-2003 Template	✓	–	–
.potm	PowerPoint Macro-Enabled Template	✓	–	–
.potx	PowerPoint Template	✓	–	–
.pps	PowerPoint 97-2003 show	✓	–	–
.ppt	PowerPoint 97-2003 Presentation	✓	✓	✓
.pptm	PowerPoint Macro-Enabled Presentation	✓	–	–
.pptx	Strict Open XML Presentation	✓	✓	✓
.rtf	Outline/RTF	✓	–	–
.svg	Scalable Vector Graphics	✓	–	–
.tga	Truevision Graphics Adapter raster graphic	✓	–	–
.tif	TIFF Tag Image File Format	✓	–	–
.txt	Text (Tab delimited)	✓	✓	✓
.vsd	Microsoft Visio drawing file	✓	–	–
.webm	Audiovisual media file	✓	–	–
.wpd	WordPerfect document	✓	–	–
.xlsb	Excel Binary Workbook	✓	–	–
.xls	Excel 97-Excel 2003 Workbook	✓	✓	✓
.xlsx	Strict Open XML Spreadsheet	✓	✓	✓
.xml	XML data	✓	✓	✓

Appendix D - Supported technology

Supported technology

Browsers

Table 67. Supported technology - Browsers

Browser	Supported versions
Chrome	73 or later
Firefox	84 or later
Microsoft Edge	73 or later
Safari	13.1.2 or later **Note:** Safari allows you to configure plugin behavior in the browser on a website basis. Note that Apple has removed NPAPI plugin support in Safari version 12, therefore the Java plugin cannot be enabled in the Safari browser version 12 or later.

Repositories Gateway sources

Table 68. Supported technology - Repositories Gateway sources

Name	Supported versions	Authentication compatability
Box	Business and Enterprise plans	• AD/LDAP • Box oAuth
Dropbox	Personal and business	• Dropbox oAuth
File Share	CIFS, SMB, V1, V2 Distributed File System (DFS)	• AD/LDAP
Google Drive	Google Drive for Business	• AD/LDAP • Google oAuth
Home Share	Windows, Unix	• AD/LDAP
Manage Legal Content (iManage)	iManage Work 2.0.2004.1501	• AD/LDAP

Table 68. Supported technology - Repositories Gateway sources (continued)

Name	Supported versions	Authentication compatability
Microsoft Office Online Server	2019, 2016, 2013	• AD/LDAP
OneDrive for Business	OneDrive for Business	• AD Sync • Microsoft ID • oAuth
SFTP Share		
SharePoint	2016, 2013, 2010, 2007	2016, 2013, 2010 • Windows claim-based with NTLM (no identity provider) • Windows claim-based authentication Basic (no identity provider) • Classic Mode Authentication With NTLM • Classic Mode Authentication with Basic (clear text) 2007 • Classic Mode Authentication With NTLM • Classic Mode Authentication with Basic (clear text)
SharePoint Online	Office 365	• AD Sync • Microsoft ID • oAuth

Hardware security modules

Table 69. Supported technology - Hardware security modules

Name	Supported versions
Thales Luna HSM Client	10.6.0

Microsoft Office Web Application (OWA)

Table 70. Supported technology - Microsoft Office Web Application (OWA)

Name	Supported versions
MS Office Online Server	219, 2016, 2013

Mobile operating systems

Table 71. Supported technology - Mobile operating systems

Software	Supported versions
Android	9 or later
iOS	15 or later

Kiteworks plugins

Kiteworks Desktop Client (Also called Kiteworks for Desktop)

Table 72. Supported technology - Kiteworks Desktop Client

Software	Supported versions
Operating system	Mac 10.10 or later Windows 11, Windows 10, Windows 8.1
.NET	.NET Framework 4.6.2
Note: SDC Requirements: The Secure Desktop Container on Windows requires Bitlocker functionality. The following versions of Windows are supported: • Windows 8 Pro or Enterprise • Windows 10 Pro, Enterprise, Education	

Kiteworks for iManage Work

Table 73. Supported technology - Kiteworks for iManage Work

Software	Supported versions
Kiteworks	7.0 or later
Kiteworks for iManage Work	2.0.2004.1501
Kiteworks for Outlook Plugin	2.0.2004.3804 or later
Operating system	Windows 10, Windows 8.1
Outlook	2019, 2016, 2013, 2010
.NET	.NET Framework 4.6.2

Kiteworks for Office

Table 74. Supported technology - Kiteworks for Office

Software	Supported versions
Operating system	Windows 11, Windows 10, Windows 8.1
MS Office	2019, 2016, 2013, 2010
.NET	.NET Framework 4.6.2

Kiteworks for Outlook Desktop

Table 75. Supported technology - Kiteworks for Outlook Desktop

Software	Supported versions
Kiteworks for Outlook Plugin	2.0.2004.3804 or above
Operating system	Windows 11, Windows 10, Windows 8.1
Outlook	2019, 2016, 2013, 2010
.NET	.NET Framework 4.6.2
Microsoft Edge WebView 2	Bundled with the installer

Kiteworks for Salesforce Lightning

Table 76. Supported technology - Kiteworks for Salesforce Lightning

Software	Supported versions
Kiteworks	8.3 or later
Salesforce Lightning	Support Cloud, Sales Cloud, and Customer Experience Cloud platforms

Kiteworks for SharePoint

Table 77. Supported technology - Kiteworks for SharePoint

Software	Supported versions
SharePoint	2013, 2010

Kiteworks for Secure MFT Client

Table 78. Supported technology - Kiteworks for Secure MFT Client

Software	Supported versions
Computer and processor	2 GHz or faster (32-bit or 64-bit)
Memory	4 GB RAM (32-bit or 64-bit)
Hard disk	16 GB (32-bit) or 20 GB (64-bit) of available disk space
Operating system	Windows 10, Windows 8.1, Windows 8, Windows 7 Windows Server 2019, Windows Server 2016 (2.5 GHz 64-bit processor, 4 GB RAM, 40 GB available disk space) On any Linux - via Docker Engine v20.10.24 or later
Browsers	The following browsers are supported to run Secure MFT Client as a Windows service: • Chrome 73 or later • Firefox 84 or later • Microsoft Edge 73 or later
Note: The Secure MFT Client can be installed as a desktop app or to run as a Windows service. It can be run as a Docker container on Linux.	

Virtualization platforms

Table 79. Supported technology - Virtualization platforms

Software	Supported versions
VMware	ESXi 8.0, 7.0, 6.7, 6.5, 6.0, 5.5
Hyper-V	2016, 2012

Appendix E - Kiteworks disaster recovery capabilities

Kiteworks disaster recovery

This section is intended for hardware and virtual Kiteworks systems and describes the processes that an administrator can perform before Kiteworks technical support intervenes to backup and restore a Kiteworks system. If you have an Kiteworks hosted solution, please contact Kiteworks technical support.

Note: Restoring data from a backup requires support intervention. Please contact Kiteworks technical support if data needs to be restored from a backup.

Disaster recovery (DR) capabilities

Kiteworks can be deployed and configured to withstand a disaster or major outage and be fully online and recoverable back to its original state. The modular architecture of Kiteworks provides data redundancy and high-availability.

Data redundancy

Kiteworks offers data redundancy, in which data is stored in multiple locations. Data can be stored on two or more servers. If one server goes down the data is still available on the other server.

High-availability

Kiteworks offers high-availability in which the system operates continuously without failure for a long period of time.

Kiteworks provides the following three options for recovery and DR when a server is deleted or becomes unusable:

Single-server recovery with snapshots

Three-server, high-availability cluster with DR

Central replication of locations around the globe

Single-server recovery with snapshots

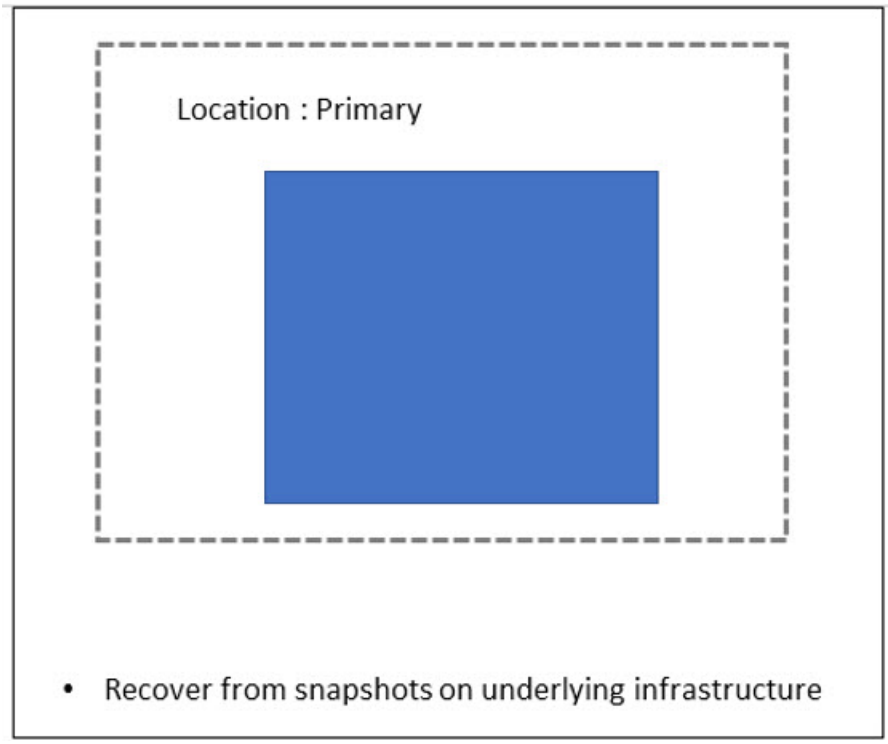
In single server deployments, snapshots of the entire system are taken every 3rd day and in case of a disaster can be rebuilt using the last snapshot.

Amazon-based snapshots can be taken every three days for Kiteworks hosted instances on AWS (Amazon Web Services).

In Microsoft Azure, snapshots are taken every Monday, Wednesday and Saturday for Kiteworks hosted virtual machines.

Snapshots can be taken manually or automated based on the virtualization environment, i.e., VMware, Hyper-V, ESX, etc. Server snapshots can be configured on your VMware or ESX servers to take server snapshots. These snapshots are taken to restore the system, so if the server has a problem, you can go back to a previous working state and restore the system.

Example: Single server recovery from snapshots



What is a snapshot?

A snapshot preserves the state and data of a virtual machine at a specific point in time. The state includes the virtual machine's power state.

The data includes all of the files that make up the virtual machine. This includes disks, memory, and other devices, such as virtual network interface cards.

A virtual machine provides several operations for creating and managing snapshots and snapshot chains. These operations let you create snapshots, revert to any snapshot in the chain, and remove snapshots.

Note: Any new data after the snapshot will be lost if you are recovering using the last snapshot.

Basic recovery procedure from a snapshot

1 Take an "offline" snapshot of all nodes in the cluster.

Recommendations:

- Power down all the servers one at a time in a "reverse order" (turn off the DBMM, aka, the Primary Application Server last).
- If an "offline" snapshot cannot be taken, try to take a simultaneous snapshot of all the servers at the same time. This is especially important for the Application Server since otherwise, there will be loss of data in the database. This is also important for the Storage servers to mitigate new files getting lost.
- At the very minimum it is recommended to switch the cluster in maintenance mode prior to taking the snapshot.
- When restoring the cluster, be sure to restore the servers "powered off" and then power on the nodes. Do not restore when "powered on" because this can put the system in a state where it is not functional until Kiteworks technical support can get into the system to run specialized recovery scripts.

2. Power on the Primary (aka DBMM) first.
3. After the primary server is powered on, begin powering on the remaining Application servers one by one. Let each Application server fully power on before powering on the next Application server. This gives the servers the best chance possible to sync with each other and avoid "disagreements" between the database servers, which would prevent the Application role from establishing a quorum.
4. After all of the Application servers are online, power on the Storage servers.
5. Power on other servers such as Repositories Gateway, Search, SFTP, Antivirus, etc.
6. Power on the Web servers last since they depend on the Application and Storage servers and once the Web servers are running users will start interacting with your site again
7. Once all of the servers are powered on and the system is green in the Admin interface, turn off maintenance mode.

   Note: The Admin can perform some checks to ensure the cluster is functional. If any failures are observed, please contact Kiteworks technical support.

Examples of alerts that might display while a cluster is powering back on:

- The Galera monitor (internally: galera_cluster_alert.py) which sends out emails until the Application servers are back up.
- Storage monitors (internally: data_storage_alert.py, storage_alert.py, and system_storage_alert.py) which sends out emails about storage not being available.

Three-server, high-availability cluster with DR

Kiteworks can be fully replicated and distributed to mitigate losing a major portion of the infrastructure. In a three-server, high-availability cluster you can configure database redundancy and file replication. If one server goes down you can still access the system from the other 2 servers depending on what roles are on the servers.

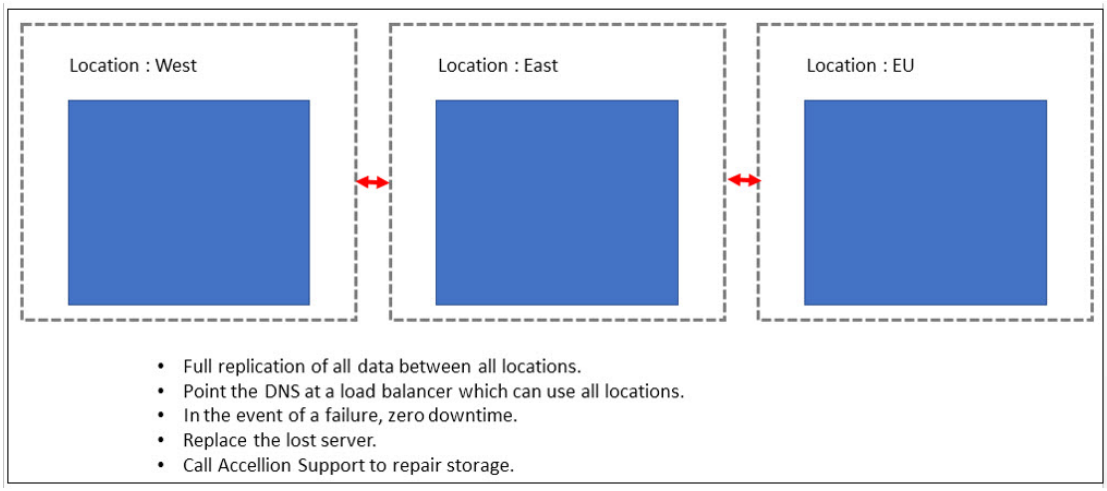
Important: If the primary DBMM server goes down you will need to reassign another server as the DBMM primary server in order to maintain basic functionality. For example:

1. Configure two servers with Application and Storage roles in Location 1 and the third server with an Application role and Storage role in Location 2. Or you can have all the three servers in different locations but for DR you need a minimum of two locations. One is the production location and the other is the DR location.
2. Setup file replication.
3. Setup database redundancy.

   If any of the two locations fail the other location will have the complete database and all the files to recover fully from a disaster. Enable the Search role and to rebuild the entire Search Index.

   In a cluster, there are different strategies for each server, namely the Application, Storage and Search servers.

Example: Three-Server, High-Availability Cluster with Disaster Recovery



See the *Kiteworks Deployment Guide* which provides sizing requirement for the different roles.

Replace dead servers with new servers

Once a server goes down, service is not interrupted but the server will have to be removed from the cluster and replaced with a new server. The new server will need to join the cluster with the same roles enabled as the dead server for it to take over the dead server's place.

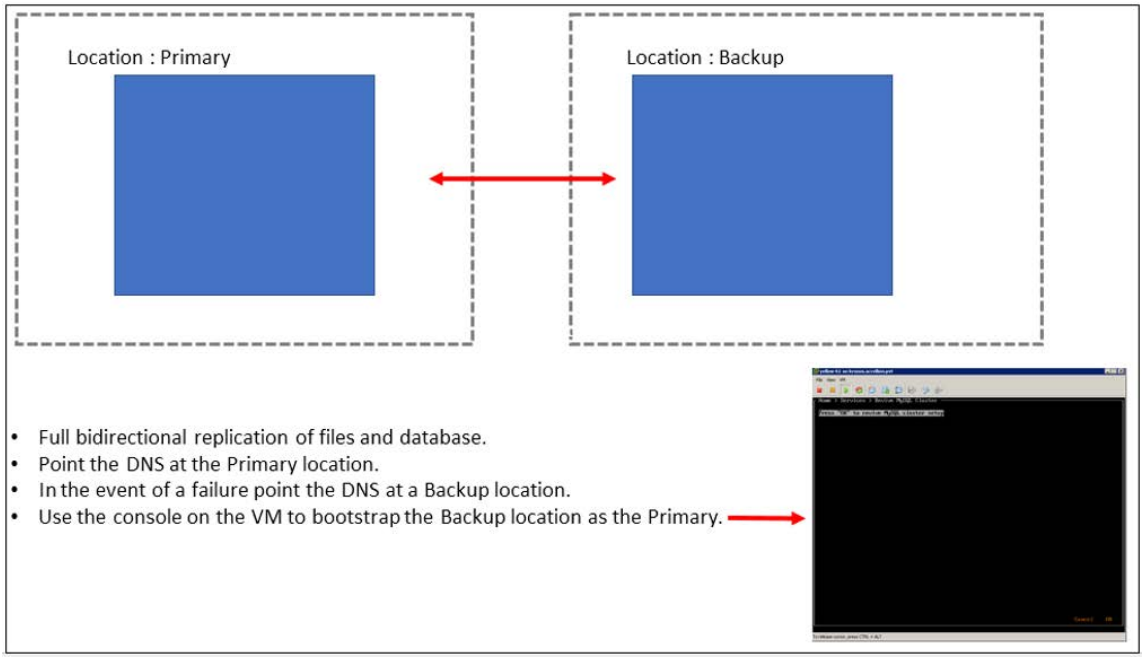
In most cases a new server can be easily deployed and joined to the cluster. For example, if the cluster configuration is h1, h2 and h3 and h2 went down and could not be revived. Replace h2 by deploying a new server h4 and add it to the same place as h2 enabling the same roles that were enabled in h2.

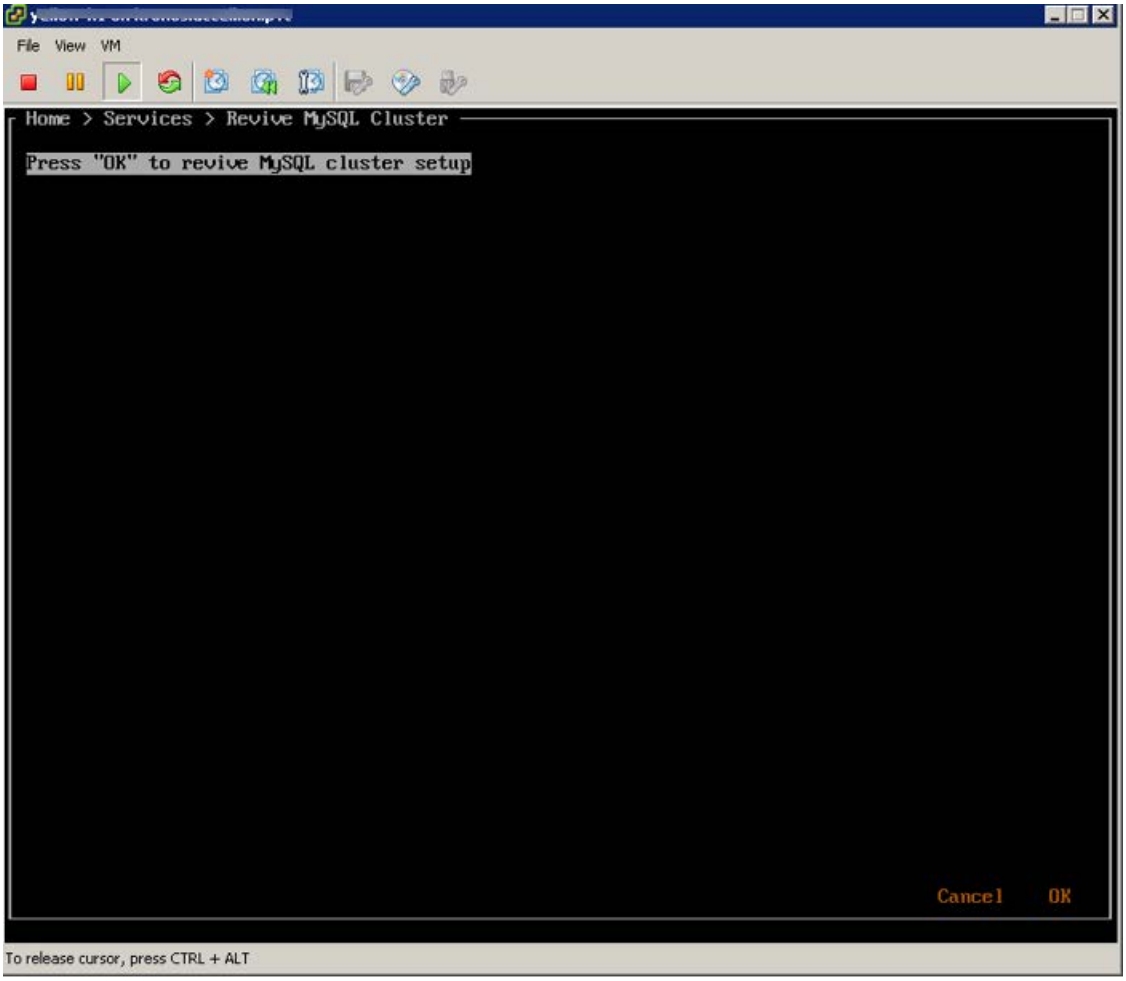
Note: If Storage was configured on the dead server, Kiteworks technical support will need to be contacted to rebuild and re-replicate Storage.

Convert standby server to active primary servers

If there is a disaster and the Standby server needs to be made the Primary server, use the VMware console to bootstrap the Standby server to lock it down and ensure that DNS is pointing to it. You can now use it as the active Primary server.

Example: Two-Server, Hot-Standby Cluster Setup.

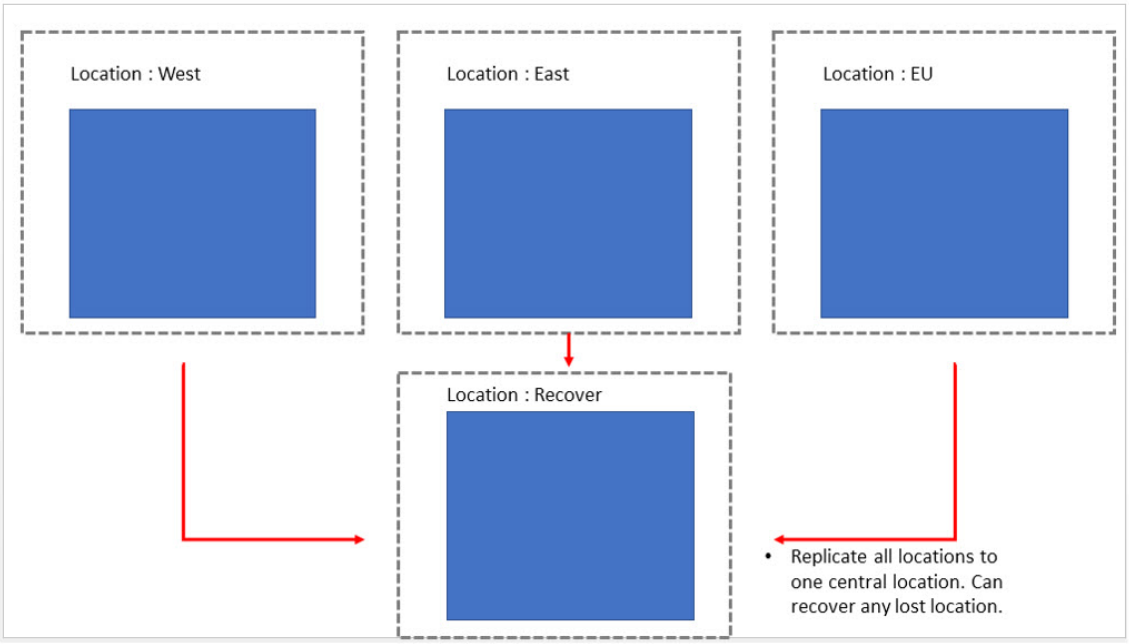

Location : Primary
Location : Backup
• Full bidirectional replication of files and database.
• Point the DNS at the Primary location.
• In the event of a failure point the DNS at a Backup location.
• Use the console on the VM to bootstrap the Backup location as the Primary.


File View VM
Home > Services > Revive MySQL Cluster
Press "OK" to revive MySQL cluster setup
Cancel OK
To release cursor, press CTRL + ALT

Central replication of locations around the globe

A central "Recovery" location is configured where everything is replicated in the center while lots of locations are configured around the globe. Ensure that the Central Replication Location has Application, Storage and Search Roles and all the Application and Storage roles in all the other locations will be replicated and backed up in the middle Central Location.

Example: Central Replication of Locations Around the Globe.



Promote the DBMM server

If the DBMM or the Primary Application server is unavailable, the Kiteworks system will continue to operate as long as a quorum of Application servers are available. However, as the Primary Application server is responsible for sending emails, the Kiteworks system will not be able to send emails until another server is promoted to the Primary Application role.

Important: In the case of promoting the DBMM server, the Admin needs to configure the Application servers to use the mail relay (firewall and correct routing information). Kiteworks recommends that the mail relay be configured for all Application servers to save time in a disaster situation. We strongly recommend that you contact Kiteworks technical support in a disaster situation. However, you will want to bring back the failed Application server as soon as possible. If there are not enough Application servers to form a quorum, users will no longer be able to access Kiteworks content until a majority of the Application servers become available again.

For example: if the DBMM or the Primary Application server goes down in a three-Application server cluster, you can detect that the DBMM or the Primary Application server has gone down, and then reassign the DBMM server to one of the remaining two Application servers (service restart may be necessary). When the old DBMM server is powered on, it will rejoin the cluster. Once the old DBMM server comes back up, the database will be updated from the other Application servers and it will know it is no longer the DBMM server.

Note: The DBMM role can now be moved successfully back to the same server after an outage.

Best practices for backup and recovery of Kiteworks deployments

File backup and recovery is integrated into Kiteworks and facilitated by the following:

File versions

There is a limitation of 10 file versions (or based on the Admin configuration) unless the file is permanently deleted, in which case the file versions before that will be lost. This is a form of partial backup or limited backup.

Expiration reminders

The user will receive a reminder before a file expires. Make a backup of the file or download it to another location. This is just a reminder and not backup and recovery.

Folder and file recovery

Unless folders or files are permanently deleted you can recover them.

Disable file purging

If a file has been deleted the user can use the DLI (Data Leak Investigator) to recover the file. This action would need an eDiscovery license. Once eDiscovery archiving is configured, even if the user deletes the file Kiteworks will not delete it. eDiscovery archiving consumes a lot of storage.

Location-based replication

Files can be replicated based on location. If a file is deleted from one location the same file will not be deleted in the other location as well. This will help if one of the location's crashes. This is data redundancy and not backup.

Note: Any recovery outside of these tools will require assistance from Kiteworks technical support.

Appendix F - AppConfig settings and MDM capabilities

Version 1.1 MDM AppConfig capabilities

Kiteworks supports app configuration and management for developers and customers.

Kiteworks supports three custom fields in AppConfig.

Table 80. Supported custom fields in AppConfig

Server URL	String	Provide the hostname or a fully qualified URL to your company's server (which would be the URL for the installation from Kiteworks).
serverUrlForced	Checkbox	Only allows the use of the provided Server URL (which is a checkbox to prevent the user from using the mobile app to access a different Kiteworks-based instance). If marked, users will not be allowed to connect to any other server except the one provided above. Supported from app version 8.1.

In addition to the AppConfig settings, the following MDM functionalities are natively supported from the Kiteworks Admin Console:

- Force authentication every time the app is launched
- Whitelist apps for Open In
- Control tokens (revoke session tokens)
- Remote Wipe
- Disable clipboard copy/paste action

Appendix G - JSON and single line syslog examples

JSON and single line syslog examples

Listed below are the activities, keywords and examples of the JSON and Single Line syslog.

JSON syslog message format

The format in the Examples column in the table below follows this structure:


```
Jan 31 19:40:36 sgqa-h123 rest_server.py: {"user_id": 3245,
"description": "activities_test_folder_add_folder_top_1580499603:
Created folder activities_test_folder_add_folder_nested_1580499604",
"successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User",
"flag": 1, "user_type": "internal", "data": {"is_folder_upload": 0,
"parent_folder": {"path": "activities_test_folder_add_folder_top_
1580499603", "id": 39309, "name": "activities_test_folder_add_folder_
top_1580499603"}, "session":
"56c304986d7d84257d882bb7b6f317f40d9180f6", "folder": {"name":
"activities_test_folder_add_folder_nested_1580499604", "path":
"activities_test_folder_add_folder_top_1580499603/activities_test_
folder_add_folder_nested_1580499604", "id": 39310}}, "user_ip":
"xxx.xxx.xx.xxx", "application": "kiteworks", "app_host":
"sgqa-.accc.gur", "client_device": "None", "url_host":
"sgqa-.accc.gur", "user_agent": "python-requests/2.14.1", "client_id":
"kw_user", "user_name": "user@email.com", "event": "add_folder"}
```


Where:

- Jan 31 19:40:36 is the Date.
- sgqa-h123 is the Server name.
- rest_server.py: is the Process used.
- "user_id": 3245 is the User name.
- "description": "activities_test_folder_add_folder_top_1580499603: Created folder activities_test_folder_add_folder_nested_1580499604" is the Description of the activity.
- "successful": 1 is the variable whether the activity was successful or unsuccessful.
- "tenant_id": 0 is the ID of the tenant.
- "client_name": "kiteworks Web User" is the Client name.
- "flag": 1 is the value of the Flag (true or false).
- "user_type": "internal" is the User type (internal or external).
- "data": {"is_folder_upload": 0 is the data type.
- "parent_folder": {"path": "activities_test_folder_add_folder_top_1580499603", "id": 39309 is the Parent folder path and ID of the folder.
- "name": "activities_test_folder_add_folder_top_1580499603"} is the folder name.
- "session": "56c304986d7d84257d882bb7b6f317f40d9180f6" is the Session ID.
- "folder": {"name": "activities_test_folder_add_folder_nested_1580499604" is the folder name.

- "path": "activities_test_folder_add_folder_top_1580499603/activities_test_folder_add_folder_nested_1580499604" is the path of the folder.
- "id": 39310 is the ID of the folder.
- "user_ip": "xxx.xxx.xxx.xxx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "python-requests/2.14.1", "client_id": "kw_user", "user_name": "user@email.com", "event": "add_folder" is the JSON string.

Note: These fields can change depending on the event that is logged. Some fields will be common for all events while others will not.

Table 81. JSON syslog message examples

Activity (event name)	Keywords	Examples
Repositories Gateway Cloud role enabled	Repositories Gateway Cloud role disabled	Feb 4 12:59:27 sgqa-h123 rest_server.py: {"user_id": 1, "description": "'Repositories Gateway Cloud' role was enabled for host sgqa-h123", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {"session": "51b73d00d7025a298b4d57da036a62bb31774147", "role_name": "Repositories Gateway Cloud", "enable": true, "hostname": "sgqa-h123"}, "user_ip": "192.168.200.16", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 OPR/66.0.3515.44", "client_id": "kw_admin", "user_name": "user@email.com", "event": "update_server_role"}
Logging in	Logged in	Feb 4 05:09:21 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged into Admin Interface", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_admin", "user_name": "user@email.com", "event": "admin_logged_in"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 4 03:25:25 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Software update check	Software update check	Feb 4 03:33:21 sgqa-h123 sw_update_check.py: {"user_id": null, "description": "Software update check done.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {"notified": true, "sw_version": "6.3.0-ng18", "email": "user@email.com"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-h123", "user_agent": "software_update_check_cron", "client_id": "", "user_name": "System", "event": "sw_update_check"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 4 03:48:05 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 4 03:54:29 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
Logging in	Logged in	Feb 4 04:04:51 sgqa-h123 rest_server.py: {"user_id": 242, "description": "Logged in", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "user_logged_in"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Copy file	Copied file	Feb 4 04:05:08 sgqa-h123 gunicorn: {"user_id": 242, "description": "Test1: Copied file \"Kiteworks_for_iManage_Web_User_Guide.pdf\" from email Testing Copy_to_Folder", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {"dest_ folder": {"name": "Test1", "path": "Test1", "id": 24480}, "file": {"hash": "e7c0f2ed5e...df5961467", "name": "Kiteworks_for_iManage_Web_User_ Guide.pdf", "hash_algo": "sha3-256", "mime": "application/pdf", "file_id": 23815, "path": "Test1/Kiteworks_for_iManage_Web_User_Guide.pdf", "id": 36448, "size": 506184}, "session": "0d18ab19aef4c35c29b775f74ff8b0bec33ca6b1", "source_file": {"path": null, "file_id": null, "id": 44067, "name": "Kiteworks_for_iManage_Web_User_ Guide.pdf"}, "version_added": null, "source_folder": {"name": "", "path": "", "id": 10}, "mail": {"sender": null, "secure_body": 0, "self_copy": 0, "email_ package_id": 2041, "id": 9906, "subject": "Testing Copy_to_Folder"}}, "user_ ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_ name": "user@email.com", "event": "copy_file"}
Copy file	Copied file	Feb 4 04:05:08 sgqa-h123 gunicorn: {"user_id": 242, "description": "Test1: Copied file \"K8Nn46\" from email Testing Copy_to_Folder", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {"dest_folder": {"name": "Test1", "path": "Test1", "id": 24480}, "file": {"hash": "29642b6bf60e3...1ce730bb", "name": "K8Nn46", "hash_algo": "sha3-256", "mime": "application/octet-stream", "file_id": 23816, "path": "Test1/K8Nn46", "id": 36449, "size": 51200}, "session": "0d18ab19aef4c35c29b775f74ff8b0bec33ca6b1", "source_file": {"path": null, "file_id": null, "id": 44068, "name": "K8Nn46"}, "version_added": null, "source_ folder": {"name": "", "path": "", "id": 10}, "mail": {"sender": null, "secure_ body": 0, "self_copy": 0, "email_package_id": 2041, "id": 9906, "subject": "Testing Copy_to_Folder"}}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "copy_file"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Copy file	Copied file	Feb 4 04:05:08 sgqa-h123 gunicorn: {"user_id": 242, "description": "Test1: Copied file \"Kiteworks_Automation_Agent_User_Guide.pdf\" from email Testing Copy_to_Folder", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {"dest_folder": {"name": "Test1", "path": "Test1", "id": 24480}, "file": {"hash": "78294a63e1ea...07102c13a2", "name": "Kiteworks_Automation_Agent_User_Guide.pdf", "hash_algo": "sha3-256", "mime": "application/pdf", "file_id": 23817, "path": "Test1/Kiteworks_Automation_Agent_User_Guide.pdf", "id": 36450, "size": 529635}, "session": "0d18ab19aef4c35c29b775f74ff8b0bec33ca6b1", "source_file": {"path": null, "file_id": null, "id": 44069, "name": "Kiteworks_Automation_Agent_User_Guide.pdf"}, "version_added": null, "source_folder": {"name": "", "path": "", "id": 10}, "mail": {"sender": null, "secure_body": 0, "self_copy": 0, "email_package_id": 2041, "id": 9906, "subject": "Testing Copy_to_Folder"}}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "copy_file"}
Copy file	Copied file	Feb 4 04:05:08 sgqa-h123 gunicorn: {"user_id": 242, "description": "Test1: Copied file \"Kiteworks_for_Desktop_Silent_Installation_Guide.pdf\" from email Testing Copy_to_Folder", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {"dest_folder": {"name": "Test1", "path": "Test1", "id": 24480}, "file": {"hash": "d3600f9466....a39b9226349", "name": "Kiteworks_for_Desktop_Silent_Installation_Guide.pdf", "hash_algo": "sha3-256", "mime": "application/pdf", "file_id": 23818, "path": "Test1/Kiteworks_for_Desktop_Silent_Installation_Guide.pdf", "id": 36451, "size": 1318178}, "session": "0d18ab19aef4c35c29b775f74ff8b0bec33ca6b1", "source_file": {"path": null, "file_id": null, "id": 44070, "name": "Kiteworks_for_Desktop_Silent_Installation_Guide.pdf"}, "version_added": null, "source_folder": {"name": "", "path": "", "id": 10}, "mail": {"sender": null, "secure_body": 0, "self_copy": 0, "email_package_id": 2041, "id": 9906, "subject": "Testing Copy_to_Folder"}}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "copy_file"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Logging in	Logged in	Feb 4 04:05:28 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged into Admin Interface", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_admin", "user_name": "user@email.com", "event": "admin_logged_in"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 4 04:20:30 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
Software update check	Software update check	Feb 4 05:09:29 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Software update check done.", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {"notified": false, "sw_version": "6.3.0-ng18", "session": "6419e614360de793c9857e1a279963d894e9b1b5", "email": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-h123", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_admin", "user_name": "user@email.com", "event": "sw_update_check"}
Logging in	Logged in	Feb 4 06:02:30 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged in", "successful": 1, "tenant_id": 0, "client_name": "testapp", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "5d286ee0-9de0-5d94-b210-c1739a7e761a", "user_name": "user@email.com", "event": "user_logged_in"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Access token	Access token granted	Feb 4 06:02:31 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Access token granted for account \"user@email.com\" to the application \"testapp\"", "successful": 1, "tenant_id": 0, "client_name": "testapp", "flag": 1, "user_type": "internal", "data": {"token_type": "access"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "5d286ee0-9de0-5d94-b210-c1739a7e761a", "user_name": "user@email.com", "event": "oauth_set_token"}
Refresh token	Refresh toke granted	Feb 4 06:02:31 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Refresh token granted for account \"user@email.com\" to the application \"testapp\"", "successful": 1, "tenant_id": 0, "client_name": "testapp", "flag": 1, "user_type": "internal", "data": {"token_type": "refresh"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "5d286ee0-9de0-5d94-b210-c1739a7e761a", "user_name": "user@email.com", "event": "oauth_set_token"}
Create secure mail	Created secure mail	Feb 4 06:14:38 sgqa-h123 gunicorn: {"user_id": 1, "description": "Created secure draft Subject: \"string\"", "successful": 1, "tenant_id": 0, "client_name": "testapp", "flag": 1, "user_type": "internal", "data": {"mail": {"secure_body": 1, "self_copy": 1, "email_package_id": 2088, "id": 10010, "subject": "string"}, "session": "be637510d36e52d97b2de95302ef53a52e6e3681", "attachments": []}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "5d286ee0-9de0-5d94-b210-c1739a7e761a", "user_name": "user@email.com", "event": "created_draft"}
Create secure mail	Created secure mail	Feb 4 06:18:48 sgqa-h123 gunicorn: {"user_id": 1, "description": "Created secure draft Subject: \"string\"", "successful": 1, "tenant_id": 0, "client_name": "testapp", "flag": 1, "user_type": "internal", "data": {"mail": {"secure_body": 1, "self_copy": 0, "email_package_id": 2089, "id": 10011, "subject": "string"}, "session": "be637510d36e52d97b2de95302ef53a52e6e3681", "attachments": []}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "5d286ee0-9de0-5d94-b210-c1739a7e761a", "user_name": "user@email.com", "event": "created_draft"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Failed upload	Failed upload	Feb 4 10:02:23 sgqa-h123 rest_server.py: {"user_id": 3144, "description": "Failed upload attempt of file OnkmVZJ8", "successful": 0, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "external", "data": {"mime": null, "error_msg": null, "name": "OnkmVZJ8", "node_ip": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "acfsmon_cron", "client_id": "", "user_name": "user@email.com", "event": "upload"}
File add	File added	Feb 4 11:07:51 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/application.log-20200204.gz' was added.\nSymbolic path: '/log/application.log-20200204.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-04T11:07:51.566+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"gid_after": "500", "symbolic_path": "/log/application.log-20200204.gz", "uid_after": "500", "perm_after": "100644", "uname_after": "prometheus", "path": "/var/log/kwlog/application.log-20200204.gz", "gname_after": "prom-wheel", "event": "added"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 1, "description": "File added to the system.", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck", "syscheck"], "mail": false, "id": "554"}, "decoder": {"name": "syscheck_new_entry"}, "id": "1580814471.480", "location": "syscheck"}
File add	File added	Feb 4 11:07:55 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/eapi_node2.log-20200204.gz' was added.\nSymbolic path: '/log/eapi_node2.log-20200204.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-04T11:07:55.574+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"gid_after": "500", "symbolic_path": "/log/eapi_node2.log-20200204.gz", "uid_after": "500", "perm_after": "100644", "uname_after": "prometheus", "path": "/var/log/kwlog/eapi_node2.log-20200204.gz", "gname_after": "prom-wheel", "event": "added"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 2, "description": "File added to the system.", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck", "syscheck"], "mail": false, "id": "554"}, "decoder": {"name": "syscheck_new_entry"}, "id": "1580814475.858", "location": "syscheck"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
File add	File added	Feb 4 11:07:55 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/rsyslog-stats-20200204.gz' was added.\nSymbolic path: '/log/rsyslog-stats-20200204.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-04T11:07:55.581+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"gid_after": "0", "symbolic_path": "/log/rsyslog-stats-20200204.gz", "uid_after": "0", "perm_after": "100600", "uname_after": "root", "path": "/var/log/kwlog/rsyslog-stats-20200204.gz", "gname_after": "root", "event": "added"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 3, "description": "File added to the system.", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck", "syscheck"], "mail": false, "id": "554"}, "decoder": {"name": "syscheck_new_entry"}, "id": "1580814475.1234", "location": "syscheck"}
File delete	File deleted	Feb 4 11:07:55 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/application.log-20200129.gz' was deleted.\n", "application": "kiteworks", "timestamp": "2020-02-04T11:07:55.575+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"path": "/var/log/kwlog/application.log-20200129.gz", "event": "deleted"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 1, "description": "Lower the log level for File deleted", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck"], "mail": false, "id": "100070"}, "decoder": {"name": "syscheck_integrity_changed"}, "id": "1580814475.1593", "location": "syscheck"}
File delete	File deleted	Feb 4 11:21:22 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/rsyslog-stats-20200128.gz' was deleted.\nSymbolic path: '/log/rsyslog-stats-20200128.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-04T11:21:22.913+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"path": "/var/log/kwlog/rsyslog-stats-20200128.gz", "symbolic_path": "/log/rsyslog-stats-20200128.gz", "event": "deleted"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 2, "description": "Lower the log level for File deleted", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck"], "mail": false, "id": "100070"}, "decoder": {"name": "syscheck_integrity_changed"}, "id": "1580815282.1840", "location": "syscheck"}
Logging in	Logged in	Feb 4 12:58:40 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged into Admin Interface", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "192.168.200.16", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 OPR/66.0.3515.44", "client_id": "kw_admin", "user_name": "user@email.com", "event": "admin_logged_in"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
Access token	Access token granted	Feb 4 12:59:26 sgqa-h123 rest_server.py: {"user_id": null, "description": "Access token granted for account \"System\" to the application \"TWS Connector\"", "successful": 1, "tenant_id": 0, "client_name": "TWS Connector", "flag": 1, "user_type": "", "data": {"token_type": "access"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "python-requests/2.20.0", "client_id": "02", "user_name": "System", "event": "oauth_set_token"}
Repositories Gateway Cloud role disabled	Repositories Gateway Cloud role enabled	Feb 4 12:59:33 sgqa-h123 rest_server.py: {"user_id": 1, "description": "'Repositories Gateway Cloud' role was disabled for host sgqa-h123", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {"session": "51b73d00d7025a298b4d57da036a62bb31774147", "role_name": "Repositories Gateway Cloud", "enable": false, "hostname": "sgqa-h123"}, "user_ip": "192.168.200.16", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 OPR/66.0.3515.44", "client_id": "kw_admin", "user_name": "user@email.com", "event": "update_server_role"}
Software update check	Software update check	Feb 5 03:16:16 sgqa-h123 sw_update_check.py: {"user_id": null, "description": "Software update check done.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {"notified": true, "sw_version": "6.3.0-ng19", "email": "user@email.com"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-h123", "user_agent": "software_update_check_cron", "client_id": "", "user_name": "System", "event": "sw_update_check"}
Logging in	Logged in	Feb 5 03:19:50 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged into Admin Interface", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web Admin", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "10.254.12.78", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0", "client_id": "kw_admin", "user_name": "user@email.com", "event": "admin_logged_in"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
LDAP/AD address book sync	LDAP/AD address book sync	Feb 5 03:28:50 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
Failed login	Failed login	Feb 5 03:36:37 sgqa-h123 rest_server.py: {"user_id": 0, "description": "User: user@email.com login failed", "successful": 0, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "internal", "data": {"user": {"name": "user@email.com"}, "error_msg": "Login Failed"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "user_login_failed"}
Logging in	Logged in	Feb 5 03:36:43 sgqa-h123 rest_server.py: {"user_id": 1, "description": "Logged in", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "internal", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "user_logged_in"}
Create folder	Created folder	Feb 5 03:36:57 sgqa-h123 rest_server.py: {"user_id": 1, "description": "/: Created folder \u45cb\uac2f\u61b4\u1e7f\u4595\ud6a5\ub0c0\u3ec3\ue8d1\u31cc\uc628\u1e9a\u4041\u15ac\u693b", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "internal", "data": {"is_folder_upload": 0, "parent_folder": {"path": "", "id": 3, "name": ""}, "session": "bd38ea5531262abe719ad6ab120d1915c0bec369", "folder": {"name": "\u45cb\uac2f\u61b4\u1e7f\u4595\ud6a5\ub0c0\u3ec3\ue8d1\u31cc\uc628\u1e9a\u4041\u15ac\u693b", "path": "\u45cb\uac2f\u61b4\u1e7f\u4595\ud6a5\ub0c0\u3ec3\ue8d1\u31cc\uc628\u1e9a\u4041\u15ac\u693b", "id": 45486}}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "add_folder"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
LDAP/AD address book sync	LDAP/AD address book sync	Feb 5 03:48:28 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "10.254.90.36", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 5 03:50:49 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 5 04:02:24 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
Logging in	Logged in	Feb 5 09:24:11 sgqa-h123 rest_server.py: {"user_id": 242, "description": "Logged in", "successful": 1, "tenant_id": 0, "client_name": "kiteworks Web User", "flag": 1, "user_type": "external", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36", "client_id": "kw_user", "user_name": "user@email.com", "event": "user_logged_in"}
File add	File added	Feb 5 09:50:03 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/tws/cloud_handler.log' was added.\nSymbolic path: '/log/tws/cloud_handler.log'.\n", "application": "kiteworks", "timestamp": "2020-02-05T09:50:03.467+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"gid_after": "501", "symbolic_path": "/log/tws/cloud_handler.log", "uid_after": "500", "perm_after": "100644", "uname_after": "prometheus", "path": "/var/log/kwlog/tws/cloud_handler.log", "gname_after": "prometheus", "event": "added"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 1, "description": "File added to the system.", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck", "syscheck"], "mail": false, "id": "554"}, "decoder": {"name": "syscheck_new_entry"}, "id": "1580896203.959", "location": "syscheck"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
File add	File added	Feb 5 09:50:09 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/rsyslog-stats-20200205.gz' was added.\nSymbolic path: '/log/rsyslog-stats-20200205.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-05T09:50:09.479+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"gid_after": "0", "symbolic_path": "/log/rsyslog-stats-20200205.gz", "uid_after": "0", "perm_after": "100600", "uname_after": "root", "path": "/var/log/kwlog/rsyslog-stats-20200205.gz", "gname_after": "root", "event": "added"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 2, "description": "File added to the system.", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck", "syscheck"], "mail": false, "id": "554"}, "decoder": {"name": "syscheck_new_entry"}, "id": "1580896209.1325", "location": "syscheck"}
File delete	File deleted	Feb 5 10:03:39 sgqa-h123 hids_notifyd.py: {"full_log": "File '/var/log/kwlog/rsyslog-stats-20200129.gz' was deleted.\nSymbolic path: '/log/rsyslog-stats-20200129.gz'.\n", "application": "kiteworks", "timestamp": "2020-02-05T10:03:39.530+0000", "agent": {"id": "000", "name": "sgqa-h123"}, "syscheck": {"path": "/var/log/kwlog/rsyslog-stats-20200129.gz", "symbolic_path": "/log/rsyslog-stats-20200129.gz", "event": "deleted"}, "manager": {"name": "sgqa-h123"}, "rule": {"firedtimes": 1, "description": "Lower the log level for File deleted", "level": 5, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck"], "mail": false, "id": "100070"}, "decoder": {"name": "syscheck_integrity_changed"}, "id": "1580897019.1684", "location": "syscheck"}
Software update check	Software update check	Feb 6 03:16:18 sgqa-h123 sw_update_check.py: {"user_id": null, "description": "Software update check done.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {"notified": true, "sw_version": "6.3.0-ng19", "email": "user@email.com"}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-h123", "user_agent": "software_update_check_cron", "client_id": "", "user_name": "System", "event": "sw_update_check"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 6 03:22:01 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}

Table 81. JSON syslog message examples (continued)

Activity (event name)	Keywords	Examples
LDAP/AD address book sync	LDAP/AD address book sync	Feb 6 03:28:52 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 6 03:42:26 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}
LDAP/AD address book sync	LDAP/AD address book sync	Feb 6 03:56:21 sgqa-h123 rest_server.py: {"user_id": null, "description": "LDAP/AD address book was synced.", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "sgqa-.accc.gur", "client_device": "None", "url_host": "sgqa-.accc.gur", "user_agent": "sync_ldap_cron", "client_id": "", "user_name": "System", "event": "ldap_sync"}

JSON syslog samples of AV and DLP scans

AV scan example

Jun 30 02:35:36 sule-h123 rest_server.py: {"user_id": null, "description": "'sulley.jpg' passed scanning by Anti Virus", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 0, "user_type": "", "data": {"file_owner": {"id": 1, "name": "user@example,com"}, "scanning_type": "AV", "skipped": null, "service_name": "Anti Virus", "malicious": false, "ec_source": {"id": null, "name": null}, "quarantined": null, "kp_xfer_transaction_id": null, "file": {"hash": "eb6dsdsdsdsab8e71ddsdsdsds0c9b8f", "name": "sule.jpg", "hash_algo": "sha3-256", "mime": "image/jpeg", "file_id": 1320, "path": "My Folder/sulley.jpg", "id": 1490, "size": 21745}, "status_reason": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "user@company.com", "client_device": "None", "url_host": "sulley-h1", "user_agent": "add_file", "client_id": "", "user_name": "System", "event": "malware_scanning"}

AV scan (flagged) example

Jun 30 02:38:57 sule-h123 rest_server.py: {"user_id": null, "description": "'eicar.txt' was flagged and quarantined by Anti Virus", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {"file_owner": {"id": 1, "name": "user@example,com"}, "scanning_type": "AV", "skipped": null, "service_name": "Anti Virus", "malicious": true, "ec_source": {"id": null, "name": null}, "quarantined": true, "kp_xfer_transaction_id": null, "file": {"hash": "44d88dsdsdsds8f36dedsdsdsdsbb02f", "name": "eicar.txt", "hash_algo": "sha3-256", "mime": "text/plain", "file_id": 1321, "path": "My Folder/eicar.txt", "id": 1592, "size": 68}, "status_reason": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "user@company.com", "client_device": "None", "url_host": "sulley-h1", "user_agent": "add_file", "client_id": "", "user_name": "System", "event": "malware_scanning"}

DLP scan example

Jun 30 02:35:36 sule-h123 rest_server.py: {"user_id": null, "description": "'sulley.jpg' passed scanning by DLP", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 0, "user_type": "", "data": {"file_owner": {"id": 1, "name": "user@example,com"}, "scanning_type": "DLP", "skipped": null, "service_name": "DLP", "ec_source": {"id": null, "name": null}, "dlp_locked": null, "prohibited": false, "file": {"hash": "eb6a3dsdsdsds8e7dsdsdse160c9b8f", "name": "sule.jpg", "hash_algo": "sha3-256", "mime": "image/jpeg", "file_id": 1320, "path": "My Folder/sulley.jpg", "id": 1490, "size": 21745}, "kp_xfer_ transaction_id": null, "status_reason": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_ host": "user@company.com", "client_device": "None", "url_host": "sulley-h1", "user_agent": "add_file", "client_id": "", "user_name": "System", "event": "dlp_scanning"}

DLP scan (flagged) example

Jun 30 02:46:19 sule-h123 rest_server.py: {"user_id": null, "description": "'dlp.txt' was flagged and dlp-locked by DLP", "successful": 1, "tenant_id": 0, "client_name": "", "flag": 1, "user_type": "", "data": {"file_ owner": {"id": 1, "name": "user@example,com"}, "scanning_type": "DLP", "skipped": null, "service_ name": "DLP", "ec_source": {"id": null, "name": null}, "dlp_locked": true, "prohibited": true, "file": {"hash": "5d8dsdsdsdb55f51adsdsdsds830086", "name": "dlp.txt", "hash_algo": "sha3-256", "mime": "text/plain", "file_id": 1323, "path": "My Folder/dlp.txt", "id": 1594, "size": 18}, "kp_xfer_transaction_ id": null, "status_reason": null}, "user_ip": "xx.xxx.xx.xx", "application": "kiteworks", "app_host": "user@company.com", "client_device": "None", "url_host": "sulley-h1", "user_agent": "add_file", "client_id": "", "user_name": "System", "event": "dlp_scanning"}

Single line syslog message format

The format in the Examples column in the table below follows this structure:

```
Aug 21 09:15:40 ngsgqa-46-h1 gunicorn: user@email.com id=2 (external), xx.xxx.xx.xxx, add_file, file_changes, My Folder: Uploaded file fresh_ roses.jpg, File: id=56 size=51636
```

Where:

- Aug 21 09:15:40 is the Date
- sgqa-h123 gunicorn: is the Server name.
- gunicorn is the Process used.
- user@email id=2 (external): is the User name.
- xx.xxx.xx.xx is the IP Address of the server.
- add_file: is the Activity Type
- file_changes is the Activity Group
- My Folder: Uploaded file fresh_roses.jpg, File: id=56 size=51636 is the Activity performed

Table 82. Single line syslog message examples

Revoked Web Token	Revoked Web Token	Mar 23 19:16:45 KWSRVxxxx-h1 rest_server.py: kwsrvxxxx@kiteworks.com id=2 (internal), xxx.xxx.xxx.xx, Activity Type: oauth_revoke_token, Activity Group: admin, Activity: Revoked access token for KWSRVxxxx@kiteworks.com from client Kiteworks Web Admin
Create Folder	Created folder	Feb 26 08:28:19 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Created folder 26-02-2019
Delete Folder	Deleted folder	Feb 26 08:29:41 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Deleted 26-Feb-19.
Delete Folder Permanently	Permanently deleted folder	Feb 26 08:30:47 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Permanently deleted 26-Feb-19.
Update Folder		
	Renamed folder	Rename Folder Feb 26 08:31:41 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Updated settings of 26-February-2019: Renamed folder from "26-02-2019" to "26-February-2019".
	Changed description	Changed Description Feb 26 08:32:21 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Updated settings of 26-February-2019: Changed description from "New Folder" to "Image file only".
	Changed expiration	Changed Expiration Feb 26 08:32:55 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Updated settings of 26-February-2019: Changed expiration from "Never expires" to 22 Mar 2019.
Recover Folder	Recovered	Feb 26 08:34:00 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Recovered "26-February-2019" from to 22 Mar 2018.

Table 82. Single line syslog message examples (continued)

Change Owner	Changed owner	Mar 13 08:56:10 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: /: Updated settings of (folder_name) [belonged to user@email.com]: Renamed folder from "(folder_ name)" to "(folder_name) [belonged to user@email.com]".
Add File	Uploaded file	Feb 26 08:35:22 sgqa-h123 rest_server.py: None, Activity: 26-February-2019: Generated fingerprint for file DC1.jpg. File: id=17 size=5266467.
Add File Version	Versions_Add	Feb 26 08:37:39 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Version was updated for DC2.jpg. File: id=17 size=2101546.
Delete File	Deleted file	Feb 26 08:40:55 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Deleted DC2.jpg. File: id=17 size=2101546.
Delete File Permanent	Permanently deleted file	Feb 26 10:15:39 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Permanently deleted DC1.jpg. File: id=22 size=5266467.
Lock/Unlock File	Locked file	Lock File Feb 26 08:43:29 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Locked file DC1.jpg. File: id=22 size=5266467. Unlock File Feb 26 08:41:38 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Unlocked file DC1.jpg. File: id=22 size=5266467.
Recover File	Recovered file	Feb 26 10:16:31 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Recovered file DC2.jpg. File: id=17 size=2101546.

Table 82. Single line syslog message examples (continued)

Promote File Version	Promoted a new file version	Feb 26 10:18:33 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity: My Folder: Promoted a new file version age-of-empires-3-2005030907024766].jpg. File: id=53 size=312753.
Delete File Version	Deleted a file version	Feb 26 10:19:42 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity: My Folder: Deleted a file version age-of-empires-3-20050309070237826.jpg. File: id=53 size=330048.
Add	Added to favorites	Add to Favorites Feb 26 08:45:54 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: "26-February-2019" added to favorites.
Remove favorite	Removed from favorites	Removed from Favorites Feb 26 08:48:13 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: "26-February-2019" removed from favorites.
Subscription of Notification	Subscribed for notifications	Subscribe for Notification Feb 26 08:51:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Subscribed for notifications: ['comment added', 'file added'].
	Unsubscribed for notifications	Unsubscribe Notification Feb 26 08:51:41 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Unsubscribed for notifications: ['comment added', 'file added'].
Add/Remove/Modify Permission	Added new permission Manager	Feb 26 08:53:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Added new permission Manager for user@email.com user.
Download File	Downloaded file	Feb 26 08:56:24 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Downloaded file DWfile.jpg. File: id=21 size=2101546.

Table 82. Single line syslog message examples (continued)

Send File	Sent message + files	Feb 26 08:57:37 sgqa-h123 jobqueued.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Sent e-mail Subject: "Send Mail" To: user@email.com with files [DWfile.jpg].
Move File	Moved file	Move a File Feb 26 09:02:46 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-02-19: Moved file "DWfile.jpg" from folder 26-February-2019. File: id=25 size=2101546.
Copy File	Copied files	Copy file Feb 26 09:03:49 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Copied file "DWfile.jpg" from folder 26-02-19. File: id=26 size=2101546.
Withdrawn File	File withdraw	Feb 26 09:11:18 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: File withdraw Subject: "Test file withdraw" To: user@email.com with files [Test File.doc].
Quarantine File	Quarantined by	Feb 26 10:22:27 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity: My Folder: Uploaded file eicar.com.txt. File: id=54 size=68. Feb 26 10:22:27 sgqa-h123 rest_server.py: None, Activity: My Folder: Generated fingerprint for file eicar.com.txt. File: id=54 size=68. Feb 26 10:22:31 sgqa-h123 rest_server.py: xx.xxx.xx.xx, Activity: 'eicar.com.txt' was flagged and quarantined by Anti-Virus.
Unquarantine File	Released from quarantine	Feb 26 10:23:46 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity: My Folder: eicar.com.txt released from quarantine by user@email.com. File: id=54 size=68.
Add Contact	Added a contact	Feb 26 09:14:41 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Contact added: user@email.com.
Delete Contact	Deleted a contact	Feb 26 09:15:54 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Contact deleted: user@email.com.

Table 82. Single line syslog message examples (continued)

Modify Contact	Updated a contact	Feb 26 09:15:25 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Contact updated: Set "name" from "user@email.com" to "santheep".
Add Comment	Added a comment	Feb 26 09:16:44 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Added a comment to file DWfile.jpg. File: id=26 size=2101546.
Update Comment	Edited a comment	Feb 26 09:17:11 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Edited a comment on file DWfile.jpg. File: id=26 size=2101546.
Delete Client	Client was deleted	Feb 26 10:27:10 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity: Client my-client was removed.
Add Task	Created a task	Feb 26 09:20:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Created a task on file "DWfile.jpg" assigned to user@email.com due 27 Feb 2019. File: id=26 size=2101546.
Update Task	Update a task	Feb 26 09:20:35 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Updated a task assigned to user@email.com on DWfile.jpg. File: id=26 size=2101546.
Delete Task	Delete a task	Feb 26 09:21:01 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: 26-February-2019: Deleted a task from file "DWfile.jpg" assigned to user@email.com due 27 Feb 2019. File: id=26 size=2101546.
Add User	Added new user	Feb 26 09:27:52 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Added new standard User user@email.com.

Table 82. Single line syslog message examples (continued)

Delete User	Deleted user	Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Deleted. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Permanently deleted. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Deleted. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Permanently deleted. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Deleted My Folder. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Permanently deleted My Folder. Feb 26 09:31:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: User deleted: user@email.com.
Modify User	Changed user profile	Feb 26 09:29:36 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: User profile for user@email.com is changed from Restricted to Standard.
Update Username	Updated their username	No example.
Update / Reset Password	Reset password	Feb 26 09:37:26 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Set password for user@email.com.
Login Information	Logged in	Feb 26 09:38:40 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Logged in.
Logout Information	Logged out	Feb 26 09:38:12 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Logged out.

Table 82. Single line syslog message examples (continued)

Access Folder / Repositories Gateway content	Viewed file	Mar 13 09:49:05 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: qa11/: Viewed file 1test4.doc. File: id=900000010000000000007339 size=None.
Add Admin User	Added rights	Example 1: Feb 26 09:40:23 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Added new standard User user@email.com. Feb 26 09:40:23 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Changed user@email.com role to Helpdesk Admin. Example 2: Feb 26 09:41:45 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Added new standard User user@email.com. Feb 26 09:41:45 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Changed user@email.com role to System Admin.
Activate User	Activated user	Feb 26 09:43:38 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: User activated: user@email.com.
Deactivate User /Suspend User	Suspended users	Feb 26 09:43:16 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: User suspended: user@email.com.
Change Usertype	Removed rights Changed Role	Feb 26 09:44:18 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Changed user@email.com role to User.
Update Username	Updated their username	Feb 26 10:30:57 sgqa-h123 rest_ server.py: user@email.com id=2 (internal), xx.xxx.xx.xx, Activity: Updated username from "user@email.com" to "santheep"
Add Server	Added server	Feb 27 07:53:25 sgqa-five-h1 rest_ server.py: user@email.com id=2 (internal), xx.xxx.xx.xx, Activity: Cluster config token was generated. Feb 27 07:53:44 sgqa-five-h1 rest_server.py: 10.254.90.56, Activity: Cluster config token was validated. Feb 27 07:55:02 sgqa-five-h1 rest_server.py: None, Activity: Added server sgqa-five-h2.

Table 82. Single line syslog message examples (continued)

Decommission Server	Removed server	Feb 27 08:01:26 sgqa-five-h1 rest_server.py: xx.xxx.xx.xx, Activity: Removed server sgqa-five-h2.
Add Role	Enabled role	Feb 27 07:59:46 sgqa-five-h1 rest_ server.py: user@email.com id=2 (internal), xx.xxx.xx.xx, Activity: 'Anti-virus/DLP' role was enabled for host sgqa-five-h1.
Remove Role	Disabled role	Feb 27 08:00:08 sgqa-five-h1 rest_ server.py: user@email.com id=2 (internal), xx.xxx.xx.xx, Activity: 'Anti-virus/DLP' role was disabled for host sgqa-five-h1.
Network Settings Change	Settings Change	Mar 13 09:01:35 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: IPv4 network settings was updated for kwcluster-h123: Set "search_base" from "[u'kiteworks.pvt', u'search.local']" to "[u'kiteworks.pvt', u'search.local', u'acc.dev']".
Mail Relay Change	Updated external services send mail	Mar 13 09:04:25 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Updated external services. Set "Apply these "Mail Settings" to all hosts" from "False" to "True". Set "Mail Relay Server" from "mail.sd.dev" to "mail1.sd.dev".
Mail Gateway Change	Updated external services	Mar 13 09:06:00 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Gateway IPv4 was configured for kwcluster-h123: set 'gateway_ip' from 10.254.1.2 to 10.254.1.1.
DNS Settings Change	Updated settings DNS	Mar 13 09:05:59 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: DNS was configured for kwcluster-h123: set 'dns_ servers' from [[u'10.254.1.1']] to [[u'10.254.1.2']].
Software Update Check	Software update check	Feb 26 09:45:52 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Software update check done.
Repositories Gateway Lock	Locked file	Cannot lock.
Repositories Gateway Unlock	Unlocked file	Cannot lock.

Table 82. Single line syslog message examples (continued)

Repositories Gateway Return File	Returned file	Mar 13 09:45:44 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: user@email.com returned 1test4.doc to Enterprise Source qa11. File: id=900000010000000000000009 size=None.
Repositories Gateway Add Source	Added Repositories Gateway source	Mar 13 09:47:49 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: user@email.com added an Enterprise Source qa2.
Repositories Gateway Delete Source	Removed Repositories Gateway source	Mar 13 09:48:28 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: user@email.com deleted an Enterprise Source qa2.
Repositories Gateway Add Source Credential Error	Invalid credentials	Mar 13 09:14:52 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Admin failed to add Repositories Gateway source sftp://canary.sd.dev/.
Repositories Gateway Tray Copy	Copied file	Mar 13 09:17:52 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: Move Tray: Uploaded file "extension.DOCX". File: id=441 size=None.
Repositories Gateway Tray Move (uses Copy in back-end)	Copied file	Mar 13 09:24:14 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: My Folder: Uploaded file extension.DOCX. File: id=442 size=4. Mar 13 09:24:14 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: Repositories Gateway: internal//: Copied file "extension.DOCX" to folder My Folder. File: id=442 size=4.
Repositories Gateway Add Source Admin	Add source	Mar 13 09:14:03 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Admin added Repositories Gateway source (name).
Repositories Gateway Deleted Source Admin	Delete source	Mar 13 09:13:12 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Admin deleted Repositories Gateway source (name).

Table 82. Single line syslog message examples (continued)

Repositories Gateway Edit Source Admin	Edited content source	Mar 13 09:22:27 kwcluster-h123 rest_ server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity: Admin edited content source "qa11": Name changed from qa1 to qa11. Description changed from qa1 ec source to qa1 ec source2.
Send Mail	Sent e-mail	Feb 26 09:51:38 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Created draft Subject: "Test -Send Email". Feb 26 09:51:41 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: /: Uploaded file send-view-preview-fixed.mp4. File: id=46 size=5100324. Feb 26 09:51:41 sgqa-h123 rest_server.py: None, Activity: /: Generated fingerprint for file send-view-preview-fixed.mp4. File: id=46 size=5100324. Feb 26 09:51:42 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Changed draft Subject: "Test -Send Email". Feb 26 09:51:54 sgqa-h123 jobqueued.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Sent e-mail Subject: "Test -Send Email" To: user@email.com with files [DWfile.jpg, send-view-preview-fixed.mp4].
Receive Mail	Received e-mail and View Email	Feb 26 09:55:27 sgqa-h123 rest_ server.py: user@email.com id=5 (internal), xx.xxx.xx.xxx, Activity: Viewed an e-mail Subject: "Test send Email" To: user@email.com.
Create Mail Draft	Created draft	Feb 26 09:56:13 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Created draft Subject: "draft test" with files [DWfile.jpg].
Change Mail Draft	Changed draft	Feb 26 09:56:52 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Changed draft Subject: "draft test test" with files [DWfile.jpg].
Delete Mail Draft	Delete draft	Feb 26 09:57:30 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Deleted draft Subject: "draft test test".

Table 82. Single line syslog message examples (continued)

Request File Send Request	Received file request	Feb 26 09:58:47 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Requested a file. Subject: "File request: Req_file" To: user@email.com.
Request File Receive Request	Received file request	No Activity Shown.
Request File Withdrew Request	Withdrew file request	Feb 26 10:01:25 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Withdrew file request Subject: "File request: Req_ file" To: user@email.com.
Preview Send	Sent file preview	Feb 26 10:03:47 sgqa-h123 jobqueued.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Sent file preview Subject: "Test - send view-only" To: user@email.com with files [DWfile.jpg].
Preview Receive	Received preview	Feb 26 10:04:23 sgqa-h123 rest_ server.py: user@email.com id=5 (internal), xx.xxx.xx.xxx, Activity: Viewed an e-mail Subject: "Test -send view-only" To: user@email.com.
DLP Flagged File or DLP Locked File	DLP locked	Feb 27 06:47:20 sgqa-h123 rest_server.py: xx.xxx.xx.xx, Activity: 'Password.docx' failed scanning by DLP (icap_ host) and was dlp-locked.
DLP Unlocked by Admin	Unlocked DLP file	Feb 27 06:49:31 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: Admin unlocked dlp file. File: id=55 size=11844.
Two-Factor Login Accept	Apply Two-Factor Authentication	Mar 13 09:40:13 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: 2FA login accept.
Two-Factor Challenge	2FA login challenge	Mar 13 09:39:25 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: Logged in. Mar 13 09:39:27 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: 2FA login challenge.

Table 82. Single line syslog message examples (continued)

Two-Factor Error	2FA login failed	Mar 13 09:41:11 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: Logged in. Mar 13 09:41:12 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: 2FA login challenge. Mar 13 09:41:16 kwcluster-h123 rest_ server.py: user@email.com id=36 (external), xx.xxx.xx.xx, Activity: 2FA login failed.
Branding Create	A template branding has been created	Feb 26 10:06:04 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: The template branding Test1 has been created.
Branding Delete	A template branding has been deleted	Feb 26 10:08:22 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: The template branding Test has been deleted.
Branding Activate	A template branding has been activated	Feb 26 10:07:19 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: The template branding Test has been activated.
Branding Disable	A template branding has been activated	Feb 26 10:07:59 sgqa-h123 rest_ server.py: user@email.com id=1 (internal), xx.xxx.xx.xxx, Activity: The template branding Test has been deactivated.
Update Email Templates	Email template modified	No example.

Activity group and activity type syslog message format

The format in the Activity column in the table below follows this structure:

```
Sep 2 01:22:06 sgqa-h123 rest_server.py: user@email.com id=3
(internal), xxx.xxx.xx.x, Activity Type: admin_logged_in, Activity
Group: admin, Activity: Logged into Admin Interface
```

Where:

- Aug 21 09:15:40 is the Date
- sgqa-h123 is the Server name
- rest_server.py is the Process used.
- user@email.com id=3 (internal) is the User name
- xxx.xxx.xx.x is the IP Address of the server
- admin_logged_in is the Activity Type
- admin is the Activity Group
- Logged into Admin Interface is the Activity performed

Table 83. Activity group and activity type examples

admin	admin_logged_in	Sep 2 01:22:06 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.x, Activity Type: admin_logged_in, Activity Group: admin, Activity: Logged into Admin Interface
admin	sw_update_check	Sep 2 01:22:20 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: sw_update_check, Activity Group: admin, Activity: Software update check done.
admin	system_update	Sep 2 01:22:29 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.x, Activity Type: system_update, Activity Group: admin, Activity: Updated software
admin	reboot_host	Sep 2 01:33:10 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.x, Activity Type: reboot_host, Activity Group: admin, Activity: The host sgqa-h123 was rebooted
admin	update_server_role	Sep 2 03:22:30 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: update_server_role, Activity Group: admin, Activity: 'Anti-virus/DLP' role was enabled for host sgqa-h123
admin	user_logged_out	Sep 2 06:33:05 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: user_logged_out, Activity Group: admin, Activity: Logged out.
admin	user_logged_in	Sep 2 06:33:33 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: user_logged_in, Activity Group: admin, Activity: Logged in.
admin	license_uploaded	Sep 2 06:45:38 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: license_uploaded, Activity Group: admin, Activity: New license was successfully uploaded.
admin	tos	Sep 2 07:14:48 kwcluster-h123 rest_server.py: user@email.com id=36 (external), xx.xxx.xx.xxx, Activity Type: tos, Activity Group: admin, Activity: Terms of Service accepted.
admin	external_services_settings	Sep 2 07:41:54 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: external_services_settings, Activity Group: admin, Activity: Updated external services. Set "" from "" to "sgqa-h123". Set "HSM Provider" from "" to "luna".
file_changes	add_file	Sep 2 07:46:33 kwcluster-h123 gunicorn: user@email.com id=36 (external), xx.xxx.xx.xxx, Activity Type: add_file, Activity Group: file_changes, Activity: /: Uploaded file Screen Shot 2019-07-02 at 16.27.25.png. File: id=1041 size=106689

Table 83. Activity group and activity type examples (continued)

admin	upload_to_tray	Sep 2 07:46:35 kwcluster-h123 rest_server.py: user@email.com id=36 (external), xx.xxx.xx.xxx, Activity Type: upload_to_tray, Activity Group: admin, Activity: Move Tray: Uploaded file "Screen Shot 2019-07-02 at 16.27.25.png". File: id=1041 size=106689
folder_ changes	add_permission	Sep 2 08:54:23 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: add_permission, Activity Group: folder_changes, Activity: 2fabypass: Added new permission Collaborator for user@email.com user.
user_ preferences	set_notification	Sep 2 08:54:30 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: set_notification, Activity Group: user_preferences, Activity: 2fabypass: Subscribed for notifications: ['file added'].
user_ preferences	unset_ notification	Sep 2 08:54:30 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: unset_notification, Activity Group: user_preferences, Activity: 2fabypass: Unsubscribed for notifications: ['comment added'].
file_changes	view_file	Sep 2 08:54:37 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: view_file, Activity Group: file_changes, Activity: 2fabypass: Viewed file Share folders - draft 1.docx. File: id=79 size=30719
admin	update_csi _settings	Sep 3 02:45:11 latest1-h122 rest_server.py: user@email.com id=14 (external), xx.xxx.xx.xx, Activity Type: update_csi_settings, Activity Group: admin, Activity: Updated ATP fireeye settings: Set "Policy for Files that#012Could Not be Scanned" from "lock" to "report_only". Set "Analysis Image Profile" from "win7x64-sp1m" to "winxp-sp3m,osx-10.11.3". Set "API Username" from "user1" to "api_ analyst_of_latest". Set "API Password" from "*********" to "*********".
admin	activate_csi _service	Sep 3 02:46:34 latest1-h122 rest_server.py: user@email.com id=14 (external), xx.xxx.xx.xx, Activity Type: activate_csi_service, Activity Group: admin, Activity: Content security integration FireEye AX has been activated.
mail	created_draft	Sep 3 02:47:28 latest1-h122 gunicorn: user@email.com id=14 (external), xx.xxx.xx.xx, Activity Type: created_draft, Activity Group: mail, Activity: Created draft Subject: "test 1" with files [AWS_Dev_ Instances_2019-09-03.csv]

Table 83. Activity group and activity type examples (continued)

mail	send_mail	Sep 3 02:48:03 latest1-h122 jobqueued.py: user@email.com id=14 (external), xx.xxx.xx.xx, Activity Type: send_mail, Activity Group: mail, Activity: Sent e-mail Subject: "test 1" To: user@email.com with files [AWS_Dev_Instances_2019-09-03.csv]
folder_ changes	add_folder	Sep 3 02:51:20 latest1-h122 rest_server.py: user@email.com id=14 (external), xx.xxx.xx.xx, Activity Type: add_folder, Activity Group: folder_changes, Activity: /: Created folder test
admin	tfa_login _challenge	Sep 3 03:09:36 latest1-h122 rest_server.py: user@kiteworks.com id=4 (internal), 10.254.1.1, Activity Type: tfa_login_challenge, Activity Group: admin, Activity: 2FA login challenge.
mail	expiration _notification	Sep 3 03:13:34 kwcluster-h123 cleanup_expire.py: 10.254.90.68, Activity Type: expiration_notification, Activity Group: mail, Activity: Sent file/folder expiration notification to users: user@email.com.
admin	add_client	Sep 3 04:46:42 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_client, Activity Group: admin, Activity: Client tokengen was added
admin	system_setting_ switched	Sep 3 04:46:49 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: system_setting_switched, Activity Group: admin, Activity: System setting switched. Set SSH to enabled
admin	add_ldap_ source	Sep 3 04:46:50 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_ldap_source, Activity Group: admin, Activity: Updated Application Settings. ldap1: LDAP source was added
admin	application _settings_ changed	Sep 3 04:46:52 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: application_settings_changed, Activity Group: admin, Activity: Updated application settings. Set "check_users_against_ldap" from "True" to "False".
admin	add_user	Sep 3 04:46:55 kw-sgqa-h123 rest_server.py: user@email.com id=7 (external), None, Activity Type: add_user, Activity Group: admin, Activity: Registered as a new standard User
admin	user_login_ failed	Sep 3 04:47:24 kw-sgqa-h123 rest_server.py: user@email.com id=11 (external), xx.xxx.xx.xx, Activity Type: user_login_failed, Activity Group: admin, Activity: User: user@email.com login failed

Table 83. Activity group and activity type examples (continued)

admin	edit_client	Sep 3 07:14:15 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: edit_client, Activity Group: admin, Activity: Client tokengen was edited: Set "scope" from "[u'*/*/*', u'sources/*', u'account/*', u'folders/*', u'files/*', u'members/*', u'comments/*', u'tasks/*', u'mail/*', u'favorite/*', u'tray/*', u'kp/*', u'admin/*']" to "['*/*/*', '*/sources/*', '*/folders/*', '*/files/*', 'GET/folders/*', '*/comments/*', 'GET/files/*', '*/tasks/*', '*/mail/*', '*/tray/*', '*/admin/*']". Set "description" from "A tokengen testing app" to "This is a test Client for test automation". Set "refresh_token" from "True" to "False".
admin	update_user_ profile_mapping	Sep 3 07:14:22 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: update_user_profile_mapping, Activity Group: admin, Activity: User profile mapping (standard) was updated.
admin	add_admin_ user	Sep 3 07:14:29 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_admin_user, Activity Group: admin, Activity: Changed appadmin@kiteworks.com role to Application Admin.
admin	add_ldap_group	Sep 3 07:14:35 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_ldap_group, Activity Group: admin, Activity: LDAP group sub-kiteworkers has been added.
admin	change_ldap _source	Sep 3 07:14:41 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: change_ldap_source, Activity Group: admin, Activity: Updated Application Settings. 10.254.12.144: LDAP source was changed: Set "paging_info" from "" to "None".
admin	add_dl	Sep 3 07:14:41 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_dl, Activity Group: admin, Activity: Updated Application Settings. Enabled distribution list for LDAP source: 10.254.12.144
admin	add_csi_service	Sep 3 09:43:51 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: add_csi_service, Activity Group: admin, Activity: Added new ATP fireeye content security integration: fireeye
admin	tfa_login_accept	Sep 3 14:53:35 latest1-h122 rest_server.py: user@email.com id=23 (external), xx.xxx.xxx.xx Activity Type: tfa_login_accept, Activity Group: admin, Activity: 2FA login accept.

Table 83. Activity group and activity type examples (continued)

admin	cluster_config_ token_ generated	Sep 4 02:46:02 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: cluster_config_token_ generated, Activity Group: admin, Activity: Cluster config token was generated
file_changes	delete_file	Sep 4 03:43:22 kwcluster-h123 rest_server.py: 10.254.90.68, Activity Type: delete_file, Activity Group: file_changes, Activity: /: Deleted Screen Shot 2019-07-02 at 16.27.25.png. File: id=1041 size=106689
admin	update_ branding_ template	Sep 4 04:45:37 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity Type: update_branding_ template, Activity Group: admin, Activity: The template branding test has been updated..
admin	activate_ branding _template	Sep 4 04:46:32 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xx, Activity Type: activate_branding_ template, Activity Group: admin, Activity: The template branding test has been deactivated..
admin	oauth_set_ token	Sep 4 08:03:28 latest1-h122 rest_server.py: user@email.com id=14 (external), xx.xxx.xx.xxx, Activity Type: oauth_set_token, Activity Group: admin, Activity: Access token granted for account "user@email.com" to the application "SFTP client"
admin	admin_set _password	Sep 4 09:20:01 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: admin_set_password, Activity Group: admin, Activity: Set password for user@email.com
folder _changes	delete_folder	Sep 4 09:20:27 kw-sgqa-h123 rest_server.py: user@email.com id=13 (internal), xx.xxx.xx.xx, Activity Type: delete_folder, Activity Group: folder_changes, Activity: /: Deleted activities_test_folder_ add_folder_top_1567588826
folder _changes	recover_folder	Sep 4 09:20:48 kw-sgqa-h123 rest_server.py: user@email.com id=13 (internal), xx.xxx.xx.xx, Activity Type: recover_folder, Activity Group: folder_changes, Activity: /: Recovered "activities_test_ folder_add_folder_top_1567588827" from /
folder _changes	update_folder	Sep 4 09:20:48 kw-sgqa-h123 rest_server.py: user@email.com id=13 (internal), xx.xxx.xx.xx, Activity Type: update_folder, Activity Group: folder_changes, Activity: /: Updated settings of activities_ test_folder_add_folder_top_1567588848_updated: Renamed folder from "activities_test_folder_add_folder_top_1567588848" to "activities_test_folder_add_folder_top_1567588848_updated".

Table 83. Activity group and activity type examples (continued)

folder_ changes	delete_folder_ permanent	Sep 4 09:20:49 kw-sgqa-h123 rest_server.py: user@email.com id=13 (internal), xx.xxx.xx.xx, Activity Type: delete_folder_ permanent, Activity Group: folder_changes, Activity: /: Permanently deleted activities_test_folder_add_folder_top_1567588849
folder _changes	change_folder _owner	Sep 4 09:20:50 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: change_folder_owner, Activity Group: folder_changes, Activity: activities_test_folder_add_folder_ top_1567588849: Changed owner from user@email.com to user@email.com
admin	delete_user	Sep 4 09:20:50 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: delete_user, Activity Group: admin, Activity: Users deleted: user@email.com, user@email.com.
admin	client_manage	Sep 5 03:37:08 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: client_manage, Activity Group: admin, Activity: Client Kiteworks for Outlook Desktop was enabled.
file_changes	lock_file	Sep 5 04:56:53 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: lock_file, Activity Group: file_ changes, Activity: files: Locked file Chapter 2 ws 3 A - Copy.pdf, File: id=21 size=363534
file_changes	add_file_version	Sep 5 10:00:01 kw-sgqa-h123 rest_server.py: user@email.com id=43 (internal), xx.xxx.xx.xx, Activity Type: add_file_version, Activity Group: file_changes, Activity: activities_test_folder_add_ folder_top_1567677586: Version was updated for t00KXD0z, File: id=259 size=8
file_changes	delete_file	Sep 5 10:00:21 kw-sgqa-h123 rest_server.py: user@email.com id=43 (internal), xx.xxx.xx.xx, Activity Type: delete_file, Activity Group: file_changes, Activity: activities_test_folder_add_folder_ top_1567677602: Deleted FsFFbP2K 1567677606, File: id=261 size=8
user_ preferences	set_favorite	Sep 5 17:15:33 latest1-h122 rest_server.py: user@email.com id=23 (external), xx.xxx.xxx.xx Activity Type: set_favorite, Activity Group: user_preferences, Activity: "Sandstone Project" added to favorites
admin	tfa_login_failed	Sep 5 23:13:32 latest1-h122 rest_server.py: user@email.com id=20 (external), xxx.xx.xxx.xx, Activity Type: tfa_login_failed, Activity Group: admin, Activity: 2FA login failed.
admin	session_started	Sep 6 04:08:49 kwcluster-h123 rest_server.py: user@company.com id=40 (external), xxx.xxx.xx.x, Activity Type: session_started, Activity Group: admin, Activity: Session started.

Table 83. Activity group and activity type examples (continued)

folder_ changes	copy_file	Sep 6 04:41:36 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: copy_file, Activity Group: folder_changes, Activity: f1: Copied file "Amazing-Tree-Landscape-Wallpaper.jpg" from folder files, File: id=42 size=680659
folder_ changes	move_folder	Sep 6 04:42:42 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: move_folder, Activity Group: folder_changes, Activity: My Folder: Moved folder "f2" from f1
file_changes	update_file	Sep 6 06:13:33 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: update_file, Activity Group: file_changes, Activity: f1/malware.txt: Updated File: Renamed file from "malware" to "malware.txt", File: id=47 size=249
mail	view_mail	Sep 9 03:20:25 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: view_mail, Activity Group: mail, Activity: Viewed an e-mail Subject: "asd" To: user@email.com
mail	changed_draft	Sep 9 19:25:14 latest1-h122 gunicorn: user@email.com id=23 (external), xxx.xxx.xxx.xxx, Activity Type: changed_draft, Activity Group: mail, Activity: Changed draft Subject: "Test" with files [Geological Interview.wav]
folder _changes	modify_ permission	Sep 10 04:24:20 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: modify_permission, Activity Group: folder_changes, Activity: 2fabypass: Updated permission for user@email.com user, changed from Collaborator to Viewer.
admin	application_ flush _memcached	Sep 10 09:22:57 latest1-h122 rest_server.py: user@email.com id=14 (external), 10.254.12.117, Activity Type: application_flush_ memcached, Activity Group: admin, Activity: Memcached data was flushed
mail	download_email	Sep 11 04:52:24 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: download_email, Activity Group: mail, Activity: Downloaded attachment malware.doc. Subject: "asd" To: user@email.com, File: id=afb557b6a76d4d86ad2e3e023fc084be size=249
user	download_ external	Sep 13 00:43:28 latest1-h122 rest_server.py: user@email.com id=20 (external), xxx.xx.xxx.xx, Activity Type: download_external, Activity Group: user, Activity: Downloaded plugin_outlook_1.3.1909.2201_ win.exe

Table 83. Activity group and activity type examples (continued)

file_changes	download	Sep 13 07:38:42 sgqa-h123 gunicorn: user@email.com id=4 (internal), xx.xxx.xx.xx, Activity Type: download, Activity Group: file_changes, Activity: f1: Downloaded file Class 3 Monthly July 2019.docx, File: id=108 size=351239
file_changes	upload	Sep 15 16:39:17 latest1-h122 rest_server.py: user@email.com id=23 (external), xx.xxx.xxx.xx, Activity Type: upload, Activity Group: file_changes, Activity: Failed upload attempt of file Annual Report.docx
folder _changes	delete_ permission	Sep 16 13:32:51 latest1-h122 rest_server.py: user@email.com id=23 (external), xxx.xxx.xxx.xxx, Activity Type: delete_permission, Activity Group: folder_changes, Activity: Sandstone Project: Removed permission Collaborator for user@email.com user
mail	send_preview	Sep 18 01:53:42 sgqa-h123 jobqueued.py: user@email.com id=3 (internal), xx.xxx.xx.xx, Activity Type: send_preview, Activity Group: mail, Activity: Sent file preview Subject: "prevew" To: user@email.com with files [Kiteworks_Migration_Administrators_Guide.pdf]
folder _changes	move_file	Sep 20 09:15:23 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: move_file, Activity Group: folder_changes, Activity: TestFolder-1/Folder2/MoveFolder: Moved file "pdf_sample_150kB.pdf" from folder Folder1, File: id=1271 size=142786
file_changes	recover_file	Sep 20 09:43:31 kw-sgqa-h123 rest_server.py: ebwoxolq@kiteworks.com id=315 (internal), xx.xxx.xx.xx, Activity Type: recover_file, Activity Group: file_changes, Activity: activities_test_folder_add_folder_top_1568972609: Recovered file YN7ryng5 1568972609, File: id=1290 size=8
admin	delete_user _profile	Sep 22 12:21:35 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: delete_user_profile, Activity Group: admin, Activity: User profile standard_copy_b2hLd was deleted.
admin	user_type _changed	Sep 22 12:21:35 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: user_type_changed, Activity Group: admin, Activity: User profile for qocpnbz8@kiteworks.com is changed from standard_copy_b2hLd to standard
admin	add_user_ profile	Sep 22 12:21:35 kw-sgqa-h123 rest_server.py: user@email.com id=1 (internal), xx.xxx.xx.xx, Activity Type: add_user_profile, Activity Group: admin, Activity: User profile standard_copy_A9mgT was added.

Table 83. Activity group and activity type examples (continued)

user_ preferences	unset_favorite	Sep 23 16:59:51 latest1-h122 rest_server.py: user@email.com id=6 (external), xx.xx.xx.xxx, Activity Type: unset_favorite, Activity Group: user_preferences, Activity: "MKV files" removed from favorites
mail	delete_draft	Sep 24 08:58:24 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: delete_draft, Activity Group: mail, Activity: Deleted draft Subject: "Sanity send mail subject x3equJYa 1569315502"
file_changes	promote_file_ version	Sep 24 08:59:51 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: promote_file_version, Activity Group: file_changes, Activity: sanity ySmTTPMn 1569315490: Promoted a new file version sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
file_changes	delete_file_ version	Sep 24 09:00:25 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: delete_file_version, Activity Group: file_changes, Activity: sanity ySmTTPMn 1569315490: Deleted a file version automation_file_ipzhRxTo_1569315563, File: id=8779 size=1000
comments	add_comment	Sep 24 09:00:28 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: add_comment, Activity Group: comments, Activity: sanity ySmTTPMn 1569315490: Added a comment to file sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
comments	edit_comment	Sep 24 09:00:31 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: edit_comment, Activity Group: comments, Activity: sanity ySmTTPMn 1569315490: Edited a comment on file sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
comments	remove_ comment	Sep 24 09:00:33 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: remove_comment, Activity Group: comments, Activity: sanity ySmTTPMn 1569315490: Deleted a comment from file sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
mail	send_message	Sep 24 09:00:54 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: send_message, Activity Group: mail, Activity: Sent message Subject: "Sanity send folder message subject ieQb5ggv 1569315653" To: qa000009qa@kiteworks.com

Table 83. Activity group and activity type examples (continued)

tasks	add_task	Sep 24 09:00:57 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: add_task, Activity Group: tasks, Activity: sanity ySmTTPMn 1569315490: Created a task on file "sanity lMiqeXpr 1569315494.docx" assigned to qa000009qa@kiteworks.com due 27 Sep 2019, File: id=8779 size=236147
tasks	update_task	Sep 24 09:01:13 sgqa-h123 rest_server.py: qa000009qa@kiteworks.com id=18 (external), xxx.xxx.xxx.xx, Activity Type: update_task, Activity Group: tasks, Activity: sanity ySmTTPMn 1569315490: Updated a task assigned to user@email.com on sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
tasks	remove_task	Sep 24 09:01:18 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: remove_task, Activity Group: tasks, Activity: sanity ySmTTPMn 1569315490: Deleted a task from file "sanity lMiqeXpr 1569315494.docx" assigned to user@email.com due 26 Sep 2019, File: id=8779 size=236147
user_ preferences	add_contact	Sep 24 09:01:47 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: add_contact, Activity Group: user_preferences, Activity: Contact added: qa000009qa@kiteworks.com
user_ preferences	modify_contact	Sep 24 09:01:55 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: modify_contact, Activity Group: user_preferences, Activity: Contact updated: Set "email" from "" to "tstauto2@kiteworks.com".
user_ preferences	delete_contact	Sep 24 09:01:57 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: delete_contact, Activity Group: user_preferences, Activity: Contact deleted: updated contact dQjWhI3R 1569315714
file_changes	delete_file _permanent	Sep 24 09:03:55 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xxx.xx, Activity Type: delete_file_permanent, Activity Group: file_changes, Activity: updated sanity folder Y9cb4gSi 1569315738: Permanently deleted sanity lMiqeXpr 1569315494.docx, File: id=8779 size=236147
user_ preferences	update_settings	Sep 24 09:24:02 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: update_settings, Activity Group: user_preferences, Activity: Updated settings

Table 83. Activity group and activity type examples (continued)

admin	remote_wipe	Sep 24 09:24:19 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: remote_wipe, Activity Group: admin, Activity: Initiated remote wipe for tstauto2@kiteworks.com device UuNCGUzI
admin	add_source_ admin	Sep 24 09:25:14 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: add_source_admin, Activity Group: admin, Activity: Admin added Repositories Gateway source en4G3OfA
admin	edit_source_ admin	Sep 24 09:25:19 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: edit_source_admin, Activity Group: admin, Activity: Admin edited content source "XdKXfgHr": Name changed from Sharepoint SGQA - 2010 to XdKXfgHr. Description changed from SharePoint 2010 Repositories Gateway source to oK7rrGlA.
admin	generate _e_discovery	Sep 24 09:35:12 sgqa-h123 rest_server.py: automation.dliadmin@kiteworks.com id=7 (external), xxx.xxx.xx.xxx, Activity Type: generate_e_discovery, Activity Group: admin, Activity: Created an activities report for automation.dliadmin@kiteworks.com from 25 Aug 2019 to 24 Sep 2019
admin	delete_e_ discovery	Sep 24 09:37:20 sgqa-h123 rest_server.py: automation.dliadmin@kiteworks.com id=7 (external), xxx.xxx.xx.xxx, Activity Type: delete_e_discovery, Activity Group: admin, Activity: Deleted an activities report for qa000020qa@kiteworks.com from 14 Sep 2019 to 24 Sep 2019
admin	create_alias_ hostname	Sep 24 09:40:34 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: create_alias_hostname, Activity Group: admin, Activity: Hostname txlf3vz3acc.blue has been created.
admin	disable_alias_ hostname	Sep 24 09:40:44 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: disable_alias_ hostname, Activity Group: admin, Activity: Hostname ojqocyrvacc.blue has been disabled.
admin	enable_alias_ hostname	Sep 24 09:40:44 sgqa-h12323 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: enable_alias_hostname, Activity Group: admin, Activity: Hostname ojqocyrvacc.blue has been enabled.

Table 83. Activity group and activity type examples (continued)

admin	delete_alias_ hostname	Sep 24 09:40:49 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: delete_alias_hostname, Activity Group: admin, Activity: Hostname bnvlfjzpacc.blue has been deleted.
file_changes	quarantine_file	Sep 24 09:51:03 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: quarantine_file, Activity Group: file_changes, Activity: test_eapi_quarantine_file_parent_ 1569318659/test_eapi_quarantine_file_nested_1569318660: wQ9sIBRp 1569318660 quarantined by tstauto2@kiteworks.com, File: id=8886 size=8
file_changes	unquarantine_ file	Sep 24 09:51:13 sgqa-h123 rest_server.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: unquarantine_file, Activity Group: file_changes, Activity: test_eapi_quarantine_file_ parent_1569318659/test_eapi_quarantine_file_nested_ 1569318660: wQ9sIBRp 1569318660 released from quarantine by tstauto2@kiteworks.com, File: id=8886 size=8
mail	send_file_ request	Sep 24 09:52:28 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: send_file_request, Activity Group: mail, Activity: Requested a file. Subject: "File request: " To: qa000020qa@kiteworks.com
file_changes	push_file	Sep 24 09:52:31 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: push_file, Activity Group: file_changes, Activity: shortlinks_test_UIiZKhQG/ErigRsxR 1569318733 has been pushed to all members of the shortlinks_ test_UIiZKhQG folder, File: id=8889 size=8
kitepoint	ec_upload_file	Sep 24 10:09:17 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: ec_upload_file, Activity Group: kitepoint, Activity: Uploaded file automation_file_ 83aKbE9X_1569319749 to Enterprise Source Sharepoint SGQA - 2010, File: id=900000010000000000004196 size=5
file_changes	unlock_file	Sep 24 10:19:51 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: unlock_file, Activity Group: file_changes, Activity: files_test_sVFdkRnm: Unlocked file 7BIuRHkg 1569320381, File: id=8944 size=8
file_changes	download_zip	Sep 24 10:33:13 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: download_zip, Activity Group: file_changes, Activity: Downloaded archive "Archive_ nlXoD16c.zip" from "files_test_GU5WWjuF" with File: ESLvymDg

Table 83. Activity group and activity type examples (continued)

comments	reply_comment	Sep 24 12:13:50 sgqa-h123 rest_server.py: qa000020qa@kiteworks.com id=10 (external), xxx.xxx.xx.xxx, Activity Type: reply_comment, Activity Group: comments, Activity: filtering_1569327219: Replied to a comment on file automation_ file_64dekucy_1569327227, File: id=9270 size=5
mail	file_withdrawn	Sep 24 13:00:29 sgqa-h123 gunicorn: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: file_withdrawn, Activity Group: mail, Activity: File withdraw Subject: "test" To: qa000020qa@kiteworks.com with files [jofG7kQH 1569329927]
mail	download_email _zip	Sep 24 13:01:03 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: download_email_zip, Activity Group: mail, Activity: Downloaded archive with attachments. Subject: "this is a test msg" To: qa000020qa@kiteworks.com with File: dTEJYnTA 1569330049
admin	modify_ permission_by_ user_profile	Sep 24 13:27:18 sgqa-h123 jobqueued.py: tstauto2@kiteworks.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: modify_permission_by_ user_profile, Activity Group: admin, Activity: Role: Manager is removed and no users are affected due to the change of User Profile settings.
mail	withdraw_file _request	Sep 24 13:49:54 sgqa-h123 rest_server.py: qa000010qa@kiteworks.com id=893 (external), xxx.xxx.xx.xxx, Activity Type: withdraw_file_request, Activity Group: mail, Activity: Withdrew file request Subject: "File request: ow7oLXFO 1569332985" To: qa000012qa@kiteworks.com
user_ preferences	reset_password	Sep 24 15:09:47 sgqa-h123 rest_server.py: user@email.com id=5 (external), xxx.xxx.xx.xxx, Activity Type: reset_password, Activity Group: user_preferences, Activity: Reset password
admin	delete_dl	Sep 24 15:22:52 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: delete_dl, Activity Group: admin, Activity: Updated Application Settings. Disabled distribution list for LDAP source: 192.168.129.68
	delete_recent	Sep 9 18:45:30 latest1-h122 gunicorn: user@email.com id=23 (external), xxx.xxx.xxx.xxx, Activity Type: delete_recent, Activity Group: , Activity: Deleted Expense Spreadsheet.xlsx from recents
	activation_code _create	Sep 10 23:05:33 latest1-h122 rest_server.py: user@email.com id=51 (internal), xx.xx.xx.xxx, Activity Type: activation_code_create, Activity Group: , Activity: Activation code has been sent to user@email.com

Table 83. Activity group and activity type examples (continued)

	activation_code _verify	Sep 10 23:09:53 latest1-h122 rest_server.py: user@email.comuser@email.com id=51 (internal), xx.xx.xx.xxx, Activity Type: activation_code_verify, Activity Group: , Activity: Activation code verification
	add_tfa_source	Sep 24 02:43:34 kwcluster-h123 rest_server.py: user@email.com id=1 (external), xx.xxx.xx.xxx, Activity Type: add_tfa_source, Activity Group: , Activity: Created Radius TFA source: yubi
	converter_ config _changed	Sep 24 11:06:46 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: converter_config_changed, Activity Group: , Activity: Converter config changed from "enabled" to "disabled".
	delete_tfa_ source	Sep 24 15:11:04 sgqa-h123 rest_server.py: user@email.com id=3 (internal), xxx.xxx.xx.xxx, Activity Type: delete_tfa_source, Activity Group: , Activity: Deleted TFA source: emailotp1

Single line syslog samples of AV and DLP scans

AV scan example

Jun 30 03:14:20 sgqa-h1234 rest_server.py: xx.xxx.xx.xx,, Activity Type: malware_scanning, Activity Group: system, Activity: 'sulley.jpg' passed scanning by Anti Virus, File: id=1490 size=21745

AV scan (flagged) example

Jun 30 03:21:24 sgqq-h1234 rest_server.py: xx.xxx.xx.xx, Activity Type: malware_scanning, Activity Group: system, Activity: 'eicar.txt' was flagged and quarantined by Anti Virus, File: id=1595 size=68

DLP scan example

Jun 30 03:14:20 sgqa-h1234rest_server.py: xx.xxx.xx.xx,, Activity Type: dlp_scanning, Activity Group: system, Activity: 'sulley.jpg' passed scanning by DLP, File: id=1490 size=21745

DLP scan (flagged) example

Jun 30 03:22:23 sgqa-h1234 rest_server.py: xx.xxx.xx.xx,, Activity Type: dlp_scanning, Activity Group: system, Activity: 'dlp.txt' was flagged and dlp-locked by DLP, File: id=1596 size=18

Detection and alerting

Table 84. Alert types and examples

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Authentication failed by existing user	Failed login attempt on prometheus via SSH.	5	User: prometheus login failed	No	Feb 5 05:33:48 example-h1 /hids_notifyd.py: {"timestamp": "2021-02-05T05:33:48.574+0000", "rule": {"level": 5, "description": "PAM: User login failed.", "id": "5503", "firedtimes": 1, "mail": false, "groups": ["pam", "syslog", "authentication_failed"], "pci_dss": ["10.2.4", "10.2.5"], "gpg13": ["7.8"], "gdpr": ["IV_35.7.d", "IV_32.2"], "hipaa": ["164.312.b"], "nist_800_53": ["AU.14", "AC.7"]}, "agent": {"id": "000", "name": "example-h1"}, "manager": {"name": "example-h1"}, "id": "1612503228.0", "full_log": "Feb 5 05:33:47 example-h1 sshd[1842]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.24 user=prometheus", "predecoder": {"program_name": "sshd", "timestamp": "Feb 5 05:33:47", "hostname": "example-h1"}, "decoder": {"name": "pam"}, "data": {"srcip": "192.168.10.24", "dstuser": "prometheus", "uid": "0", "euid": "0", "tty": "ssh"}, "location": "/var/log/secure", "application": "kiteworks"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Authentication failed by non-existing user	Failed login attempt by a non-existing user via SSH.	7	User: <user name> login failed		Feb 26 07:24:12 example-h1 /hids_notifyd.py: {"timestamp": "2021-02-26T07:24:12.661+0000", "rule": {"level": 7, "description": "Possible DDoS attempt (high number of non-existent identification strings).", "id": "100050", "frequency": 2, "firedtimes": 1, "mail": true, "groups": ["local", "syslog", "ossec", "syscheck", "rootcheck"]}, "agent": {"id": "000", "name": "example-h1"}, "manager": {"name": "example-h1"}, "id": "1614324252.4073", "full_log": "Feb 26 07:24:11 example-h1 sshd[11500]: Failed password for invalid user exampleuser from 192.168.10.40 port 51223 ssh2", "predecoder": {"program_name": "sshd", "timestamp": "Feb 26 07:24:11", "hostname": "example-h1"}, "decoder": {"parent": "sshd", "name": "sshd"}, "data": {"srcip": "192.168.10.40", "srcuser": "exampleuser"}, "location": "/var/log/secure", "application": "kiteworks"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Authentication success	Prometheus login via SSH into the system. Kiteworks technical support logged in to the system to troubleshoot or fix an issue.	5	HIDS event for user prometheus: sshd: authentication success via password. Host=example-h1, User=prometheus, Source IP=192.168.10.40	No	Feb 26 06:57:55 example-h1 /hids_notifyd.py: {"hids_alert_user": "prometheus", "hids_alert": "sshd: authentication success via password. Host=example-h1, User=prometheus, Source IP=192.168.10.40"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
File added	File was added to the system.	4	HIDS event full log: File Added : <file_name> host=<host_name>, rule=100090, level=4: syscheck event type: added size: 10104 perm: rw-r--r-- uid: 0 gid: 0 sha256: cd079d… uname: root gname: root mtime: 2020-09-14T10:41:31 inode: 1441802	No	{"timestamp":"2021-05-11T11:49:49.516+0800","rule":{"level":4,"description":"File Added","id":"100090","firedtimes":216,"mail":true,"groups":["local","syslog","ossec","syscheck","rootcheck"]},"agent":{"id":"000","name":"demo-h1"},"manager":{"name":"demo-h1"},"id":"1620704989.142978","full_log":"File '/opt/lib/python3.8/site-packages/tws/tests/test_https_api.pyo' added\nMode: realtime\n","syscheck":{"path":"/opt/lib/python3.8/site-packages/tws/tests/test_https_api.pyo","mode":"realtime","size_after":"9171","perm_after":"rw-r--r--","uid_after":"0","gid_after":"0","sha3-256_after":"607d99ed42d801e160cf8dbf50b92f2d","sha1_after":"cab57c52a3346672110599d04db4bb298f4b71cf","sha256_after":"9483abd2a30c23a3cc525a2e7c1d33d7c01383b64b16965ae477a5ef1e1ea13c","uname_after":"root","gname_after":"root","mtime_after":"2021-03-22T11:17:55","inode_after":1441803,"event":"added"},"decoder":{"name":"syscheck_new_entry"},"location":"syscheck"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
File deleted	File was deleted from the system.	6	HIDS event full log: File Deleted : /opt/lib/python3.8/site-packages/tws_rpm/xml_to_obj.pyo host=demo-h1, rule=100070, level=6: syscheck event type: deleted	No	{"timestamp":"2021-05-11T11:49:51.605+0800","rule": {"level":6,"description":"File Deleted","id":"100070","firedtimes":219,"mail":true,"groups": ["local","syslog","ossec","syscheck","rootcheck"]},"agent": {"id":"000","name":"demo-h1"},"manager":{"name":"demo-h1"},"id":"1620704991.264944","full_log":"File '/opt/lib/python3.8/site-packages/tws_rpm/xml_to_obj.pyo' deleted\nMode: realtime\n","syscheck": {"path":"/opt/lib/python3.8/site-packages/tws_rpm/xml_to_obj.pyo","mode":"realtime","size_after":"5702","perm_after":"rw-r--r--","uid_after":"0","gid_after":"0","sha3-256_after":"2f995043950948886123a6266cdff55d","sha1_after":"ad24f0ca219ece88d0830144ebad4eda7fa8646c","sha256_after":"8da4a84a9a2fd23239124dfd4a2ac4377a73e9eba8beb3e711dbf58c100d920a","uname_after":"root","gname_after":"root","mtime_after":"2021-03-22T11:17:55","inode_after":792609,"event":"deleted"},"decoder": {"name":"syscheck_deleted"},"location":"syscheck"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
File modification (integrity check failure)	System file was modified.	4	HIDS event full log: File Integrity check failed. : /home/prometheus/git-setup/ngcollab/config/volume_ mappings.cfg host=demo-h2, rule=100053, level=4: syscheck event type: modified mtime: Before=2021-05-11T14:46:58, After=2021-05-11T14:47:58	*Email subject:* 'File Integrity Failure' *Email body:* Integrity check failure and Rootkit check alerts for host server.company.com: 1. File Integrity check failed. : /home/prometheus/git-setup/ngcollab/config/volume_ mappings.cfg host=demo-h2, rule=100053, level=4: syscheck event type: modified mtime: Before=2021-05-11T14:46:58, After=2021-05-11T14:47:58	{"timestamp":"2021-05-11T14:47:20.197+0800","rule": {"level":4,"description":"File Integrity check failed.","id":"100053","firedtimes":19,"mail":true,"groups": ["local","syslog","ossec","syscheck","rootcheck"]},"agent": {"id":"000","name":"demo-h1"},"manager":{"name":"demo-h1"},"id":"1620715640.422844","full_log":"File '/home/prometheus/git-setup/ngcollab/config/volume_mappings.cfg' modified\nMode: realtime\nChanged attributes: mtime\nOld modification time was: '1620715579', now it is '1620715640'\n","syscheck": {"path":"/home/prometheus/git-setup/ngcollab/config/volume_ mappings.cfg","mode":"realtime","size_after":"141","perm_after":"rw-rw-r--","uid_after":"500","gid_after":"500","sha3-256_ after":"d2368b54b3ec87ca5c7cf45220df4b4c","sha1_ after":"f44c25ecfda1162dad9e1f5f842a14305b7c32a2","sha256_ after":"095eb23e26c65bf10d43fab981d80fd73099a4ae05b6eb67a7ec38b7cb3baf0e","uname_after":"prometheus","gname_after":"prom-wheel","mtime_before":"2021-05-11T14:46:19","mtime_after":"2021-05-11T14:47:20","inode_after":2760773,"changed_attributes": ["mtime"],"event":"modified"},"decoder":{"name":"syscheck_integrity_ changed"},"location":"syscheck"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Rootkit check alert	A potential rootkit signature was detected.	7	HIDS event full log: Rootkit check alert: Rootkit 'Suspicious' detected by the presence of file '/var/log/kwlog/.log'.	*Email subject:* 'File Integrity Failure' *Email body:* 1. Rootkit check alert: Trojaned version of file '/etc/hosts' detected. Signature used: '^[^#]*f-secure.com' (Anti-virus site on the hosts file).	Mar 27 18:25:39 example-h1 /hids_notifyd.py: {"timestamp": "2021-03-27T18:25:39.095+0000", "rule": {"level": 7, "description": "Host-based anomaly detection event (rootcheck).", "id": "510", "firedtimes": 1, "mail": true, "groups": ["ossec", "rootcheck"], "gdpr": ["IV_35.7.d"]}, "agent": {"id": "000", "name": "example-h1"}, "manager": {"name": "example-h1"}, "id": "1616869539.3911", "full_log": "Rootkit 'Suspicious' detected by the presence of file '/var/log/kwlog/.log'.", "decoder": {"name": "rootcheck"}, "data": {"title": "Rootkit 'Suspicious' detected by the presence of file '/var/log/kwlog/.log'."}, "location": "rootcheck", "application": "kiteworks"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Start of service "tcpdump"	User executed "tcpdump" command line utility to potentially capture and analyze network traffic going through the system.	10	No		{"timestamp":"2021-05-31T12:45:39.179+0800","rule": {"level":10,"description":"Auditd: device enables promiscuous mode","id":"80710","firedtimes":1,"mail":true,"groups":["audit","audit_anom"],"pci_dss":["11.4","10.6.1"],"gpg13":["4.14"],"gdpr":["IV_35.7.d","IV_30.1.g"],"hipaa":["164.312.b"],"nist_800_53":["SI.4","AU.6"],"tsc": ["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"demo-h1"},"manager":{"name":"demo-h1"},"id":"1622436339.51343","full_log":"type=ANOM_PROMISCUOUS msg=audit(1622436339.154:228224): dev=lo prom=256 old_prom=0 auid=500 uid=0 gid=0 ses=11757 type=SYSCALL msg=audit(1622436339.154:228224): arch=c000003e syscall=54 success=yes exit=0 a0=3 a1=107 a2=1 a3=7ffec2aa6b70 items=0 ppid=29949 pid=18457 auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=11757 comm=\"tcpdump\" exe=\"/usr/sbin/tcpdump\" key=(null) type=PROCTITLE msg=audit (1622436339.154:228224): proctitle=74637064756D70002D55002D69006C6F002D770064756D702E706 3617000706F7274203830","decoder": {"parent":"auditd","name":"auditd"},"data":{"audit":{"type":"ANOM_PROMISCUOUS","id":"228224","dev":"lo","prom":"256","old_prom":"0","auid":"500","uid":"0","gid":"0","session":"11757"}},"location":"/var/log/audit/audit.log"}

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
Unknown service start/stop event	An alert email and event log entry to the syslog database. The service check polling time is 30 secs.	7	HIDS event full log: Service Started: host=demo-h1, rule=100052, level=7: service name=nc, port=['1234'], ip=['0.0.0.0'], process id=31767 HIDS event full log: Service Stopped: host=demo-h1, rule=100052, level=7: service name=nc, port=['1234'], ip=['0.0.0.0'], process id=22616	*Email subject:* 'File Integrity Failure' *Email body:* Integrity check failure and Rootkit check alerts for host <host_name>: 1. Service Stopped: host=<host_name>, rule=100052, level=7: service name=nc, port=['1234'], ip=['0.0.0.0'], process id=20736 2. Service Started: host=<host_name>, rule=100052, level=7: service name=nc, port=['1234'], ip=['0.0.0.0'], process id=20736	{"timestamp":"2021-05-11T14:28:56.200+0800","rule":{"level":7,"description":"Services started/stopped","id":"100052","firedtimes":9,"mail":true,"groups":["local","syslog","ossec","syscheck","rootcheck"]},"agent":{"id":"000","name":"demo-h1"},"manager":{"name":"demo-h1"},"id":"1620714536.408347","previous_output":"Previous output:\nossec: output: 'netstat listening ports':\ntcp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\ntcp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:1001 0.0.0.0:* 852/rpcbind\nudp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\nudp6 :::1001 :::* 852/rpcbind\nudp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:123 0.0.0.0:* 853/ntpd\nudp 10.254.102.130:123 0.0.0.0:* 853/ntpd\nudp 127.0.0.1:123 0.0.0.0:* 853/ntpd\nudp6 ::1:123 :::* 853/ntpd\nudp6 :::123 :::* 853/ntpd\nudp6 fe80::20c:29ff:feb3:123 :::* 853/ntpd\ntcp 0.0.0.0:22 0.0.0.0:* 1249/sshd\ntcp6 :::22 :::* 1249/sshd\ntcp 0.0.0.0:4369 0.0.0.0:* 8144/epmd\ntcp6 :::4369 :::* 8144/epmd\ntcp 0.0.0.0:9089 0.0.0.0:* 13439/splunkd\ntcp 127.0.0.1:5002 0.0.0.0:* 18844/python3\ntcp 127.0.0.1:5000 0.0.0.0:* 18850/python3\ntcp 127.0.0.1:11211 0.0.0.0:* 18852/memcached\ntcp 0.0.0.0:443 0.0.0.0:* 18854/nginx\ntcp 0.0.0.0:80 0.0.0.0:* 18854/nginx\ntcp6 127.0.0.1:7983 :::* 18875/java\ntcp6 :::8983 :::* 18875/java\ntcp 0.0.0.0:4567 0.0.0.0:* 19695/mysqld\ntcp6 :::3306 :::* 19695/mysqld\ntcp 127.0.0.1:27017 0.0.0.0:* 21001/mongod","full_log":"ossec: output: 'netstat listening ports':\ntcp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\ntcp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:1001 0.0.0.0:* 852/rpcbind\nudp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\nudp6 :::1001 :::* 852/rpcbind\nudp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:123 0.0.0.0:* 853/ntpd\nudp 10.254.102.130:123 0.0.0.0:* 853/ntpd\nudp 127.0.0.1:123 0.0.0.0:* 853/ntpd\nudp6 ::1:123 :::* 853/ntpd\nudp6 :::123 :::* 853/ntpd\nudp6 fe80::20c:29ff:feb3:123 :::* 853/ntpd\ntcp 0.0.0.0:22

Table 84. Alert types and examples (continued)

Alert type	Alert cause	Alert Level	Entry logged in the Activities list	Email notification sent to administrator	Sample JSON exported to the syslog
					0.0.0.0:* 1249/sshd\ntcp6 :::22 :::* 1249/sshd\ntcp 127.0.0.1:25 0.0.0.0:* 1263/sendmail\ntcp 0.0.0.0:4369 0.0.0.0:* 8144/epmd\ntcp6 :::4369 :::* 8144/epmd\ntcp 0.0.0.0:9089 0.0.0.0:* 13439/splunkd\ntcp 127.0.0.1:5002 0.0.0.0:* 18844/python3\ntcp 127.0.0.1:5000 0.0.0.0:* 18850/python3\ntcp 127.0.0.1:11211 0.0.0.0:* 18852/memcached\ntcp 0.0.0.0:443 0.0.0.0:* 18854/nginx\ntcp 0.0.0.0:80 0.0.0.0:* 18854/nginx\ntcp6 127.0.0.1:7983 :::* 18875/java\ntcp6 :::8983 :::* 18875/java\ntcp 0.0.0.0:4567 0.0.0.0:* 19695/mysqld\ntcp6 :::3306 :::* 19695/mysqld\ntcp 127.0.0.1:27017 0.0.0.0:* 21001/mongod","decoder":{"name":"ossec"},"previous_log":"ossec: output: 'netstat listening ports':\ntcp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\ntcp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:1001 0.0.0.0:* 852/rpcbind\nudp 0.0.0.0:111 0.0.0.0:* 852/rpcbind\nudp6 :::1001 :::* 852/rpcbind\nudp6 :::111 :::* 852/rpcbind\nudp 0.0.0.0:123 0.0.0.0:* 853/ntpd\nudp 10.254.102.130:123 0.0.0.0:* 853/ntpd\nudp 127.0.0.1:123 0.0.0.0:* 853/ntpd\nudp6 ::1:123 :::* 853/ntpd\nudp6 :::123 :::* 853/ntpd\nudp6 fe80::20c:29ff:feb3:123 :::* 853/ntpd\ntcp 0.0.0.0:22 0.0.0.0:* 1249/sshd\ntcp6 :::22 :::* 1249/sshd\ntcp 0.0.0.0:4369 0.0.0.0:* 8144/epmd\ntcp6 :::4369 :::* 8144/epmd\ntcp 0.0.0.0:9089 0.0.0.0:* 13439/splunkd\ntcp 127.0.0.1:5002 0.0.0.0:* 18844/python3\ntcp 127.0.0.1:5000 0.0.0.0:* 18850/python3\ntcp 127.0.0.1:11211 0.0.0.0:* 18852/memcached\ntcp 0.0.0.0:443 0.0.0.0:* 18854/nginx\ntcp 0.0.0.0:80 0.0.0.0:* 18854/nginx\ntcp6 127.0.0.1:7983 :::* 18875/java\ntcp6 :::8983 :::* 18875/java\ntcp 0.0.0.0:4567 0.0.0.0:* 19695/mysqld\ntcp6 :::3306 :::* 19695/mysqld\ntcp 127.0.0.1:27017 0.0.0.0:* 21001/mongod","location":"netstat listening ports"}

Appendix I - Alerts and notifications

Alerts and notifications

A partial list of alerts and notifications that may display in the admin console.

Alerts

Note: Yellow alerts are displayed if any service is down but still running on at least one other server. Red alerts are displayed if any service is down on all servers.

Service is down

A yellow alert displays when the service is down. Click the alert to see which server's service is down. A service can be down for various reasons, but the first thing to try is to re-enable the service again. Go to System Setup > Cluster Configuration > System Services to turn services on and off.

Storage is low

A yellow alert displays if less than 50% storage is left and a red alert displays if less than 10% storage is left. You can change thresholds for storage alerts. Go to System Setup > Cluster Configuration > System Configuration.

You can also add more storage if needed. Go to System Setup > Locations, and then click to expand the server you want to configure. On the Storage tab, click Manage Storage.

For improved performance, it is recommended that you use additional disks for data storage. A system without dedicated data storage degrades performance.

License is low

When the number of licenses is less than 10% a yellow alert displays. To upload additional licenses, go to Application Setup > Licenses > Kiteworks License. You can also change thresholds for license alerts. Go to Application Setup > Configuration > Kiteworks.

License is expired

A yellow alert displays when 5 days are left and a red alert displays when 3 days are left for your license to expire. To upload additional licenses, go to Application Setup > Licenses > Kiteworks License. You can also change thresholds for license alerts. Go to Application Setup > Configuration > Kiteworks.

Server needs to reboot after a software update

A red alert displays if the server needs to be rebooted after a software update. If more than one server needs to be rebooted, reboot them one at a time.

New server needs a software update

A yellow alert displays if software needs to be updated to a newly added server. Clicking it displays the Software Update page with the servers that need to be rebooted.

New software update is available

A yellow alert displays if a new software update is available without a security update. A red alert displays if the software update includes a security update. Clicking it displays the Software Update page from where you can run software update.

SSL certificate alerts

The administrator is alerted when the following issues occur:

The application URL does not match the SSL Certificate. This enforces SSL certificate checks for calls within the Kiteworks cluster. This security measure is switched on only if the system has a wild card SSL certificate.

When an SSL certificate is set to expire or has expired. Warnings are generated throughout a 60-day time period, with the final alert being displayed when the certificate expires. When a certificate expires, the appliance runs in a non-secure mode. Click the alert to upload a new certificate.

When an SSL certificate is set to expire within 7 days, a daily email notification is sent to the administrator to remind them to upload a new certificate.

NTP is not configured properly

A yellow alert displays if NTP is not configured properly. Clicking it displays the External Services tab for the server. Click NTP Settings to view the NTP server details. The server that has NTP configuration problem is displayed

Search license exists but the Search role is not active

A yellow alert displays if the Search license exists but the Search role is not active. Clicking it displays the Locations page. If an existing Search role is down, it will display in red. Click the server name to expand it, and then turn on the Search role.

AV update failure

If AV updates fail for any reason, you can troubleshoot the issue and get the AV updated to the latest definitions.

File integrity monitoring alerts

File integrity monitoring (FIM) scans the system and when scanning is complete, real time monitoring alerts and warnings are sent out to the administrator if the scan detects a failure.

Error reporting for SMS messages

When the SMS Service fails to send an SMS message, an alert is displayed indicating the number of failed messages. The audit log displays the SMS service error and once the SMS service setting is fixed, the log shows that the SMS message was sent.

Remote syslog server is unreachable

Similar to NTP alerts an email notification is sent out alerting the administrator when the Kiteworks server cannot communicate with a configured syslog server.

Administrator alerts for locations without storage roles

The administrator is alerted when a Location exists without a Storage role. The alert is displayed in red to caution the administrator that there might be users from a location where the location is unassigned to a role with ACFS.

Alert when data storage goes low or the NFS volume is unreachable

The administrator is alerted (in yellow) when Data Storage goes below the threshold. You can change thresholds for storage alerts. Go to System Setup > Cluster Configuration > System Configuration. Another alert is displayed (in red) if the NFS connection fails.

Alert when the intrusion detection for SSH/SFTP is not enabled

The administrator is alerted when Intrusion Detection for SSH/SFTP and Web is not running for a server.

Alert when file modification is detected

The administrator is alerted when any file modification is detected. The administrator is requested to contact Kiteworks technical support.

Alert when file integrity monitoring is not active

The administrator is alerted when file integrity monitoring is not active on any server.

Folder quota alert

After a folder quota is calculated, some users may exceed their quota. It is recommended you increase their user profile quota limit to allow them uninterrupted use of the folder. You can also reassign folder ownership to a user with a higher quota. Go to Users > Profiles > click the profile you want to configure > Collaboration.

File encryption alerts

In Kiteworks version 7.4.1 and later, user-generated files are automatically encrypted when uploaded to the system. If you upgrade to version 7.4.1, an encryption migration script runs in the background to encrypt existing user-generated files on the system. The script encrypts files in batches and continues to run in the background for each batch until the process completes. The alert shows the status of the encryption process. It disappears once the process completes. If there is a problem encrypting one or more files, the files are queued to be retried. If the files can't be encrypted, an alert is displayed on the dashboard indicating the number of files that were not encrypted.

If a file fails to be encrypted, you have the option to retry encrypting the file or deleting the file. Otherwise it remains unencrypted on the system. The alert remains so that you can click it to view the details of the failure.

Notifications

Notifications appear via the alert (bell) icon at the top right corner of the Admin Console.

People need to verify their accounts

Clicking it will display the User Management page displaying only users that need to verify their accounts.

People need to reset their passwords

Clicking it will display the User Management page displaying only the users that need to reset their password.

Monitoring and notifications

The following table describes what is currently being monitored in Kiteworks and how the notifications reach the administrator.

Table 85. Monitoring and notifications

Category	What is being monitored	Frequency of monitoring	Notification method
System	Node Health-check: The node with the primary application role checks if all the nodes in the Kiteworks cluster are healthy.	10 minutes	Notification email is sent once every 24 hours. Alert is also displayed when the administrator is logged in the administrator UI.
System	Memory/CPU/Disk Monitors: All boxes rely on sysstat to record the data.	1 minute	Data is available at System Status > Cluster Health. You can also configure SNMP and use SNMP clients to gather information.
System	SSL certificate expiry	Daily	Notification email is sent if the SSL certificate expiry is within 7 days. Alert is also displayed when the administrator is logged in the Kiteworks Admin Console.
System	Software update: Checks the update servers to see if any new update is available.	Daily	Notification email is sent once for every new update. Alert is also displayed when the administrator is logged in the Kiteworks Admin Console.
System	Reboot Notification: If a server is required to reboot (due to a kernel update).	N/A	User needs to be logged into the Kiteworks Admin Console to get this alert. Triggered immediately after a software update.
System	Process Monitoring: Processes can be monitored based on the roles configured on the system via SNMP.	N/A	SNMP clients can be configured to monitor the processes for different hosts based on the OIDs mentioned in the monitoring guide.
Storage	Storage Alert: Checks if the system storage fills up more than 85 % of the available space.	10 minutes	Notification email is sent once every 24 hours. Alert is also displayed when the administrator is logged in the Kiteworks Admin Console.
License	License expiry: Checks if Kiteworks license is about to get expired. For multi-tenants, the check is done for every tenant.	10 minutes	Notification email is sent once every 24 hours. Alert is also displayed when the administrator is logged in the Kiteworks Admin Console.

Table 85. Monitoring and notifications (continued)

Category	What is being monitored	Frequency of monitoring	Notification method
License	Low License Count: Checks if the usage is more than 90% of the actual licenses purchased.	Daily	Notification email is sent once every 24 hours. Alert is also displayed when the administrator is logged in the Kiteworks Admin Console.
Database	Galera Health-check: The node with primary application role checks if all the application roles are healthy.	10 minutes	To account for transient errors, email will be sent out if the health checks fail 3 times in succession.
Reporting	Multi-tenants: Calculates the storage used by tenants.	Weekly	Notification email sent out whenever the usage exceeds the allotted storage.

There are activities recorded available in the Kiteworks Admin Console and syslog for any action a user takes in Kiteworks. The following set of events are currently available in the product.

Table 86. Recorded activities

Type	Event
Folder	Add Folder, Delete Folder, Delete Folder permanently, Update Folder, Recover Folder, Change Owner
File	Add File, Add File Version, Delete File, Delete File Permanent, Lock/Unlock File, Recover File, Promote File Version, Delete File Version, Set/Unset Favorite, Add/Remove notification, Add/Remove/Modify Permission, Download File, Send File, Move/Copy File, Withdrawn File, Unquarantine File
Contact	Add/Delete/Modify Contact
Comment	Add/Update/Delete
Clients	Add/Edit/Enable/Disable/Delete
Task	Add/Update/Delete/Reply
User	Add/Delete/Modify User, Update username, Update/Reset password, Login/Logout information, Access Folder/Repositories Gateway, Add Admin User, Activate/Deactivate/Suspend User, Change UserType, Update Username
Server	Add/Decommission Server, Add/Remove role, Location/Network/SSL/Application Settings/Domain Name Change, Mail Relay/Gateway/DNS Settings Change, Software update check

Table 86. Recorded activities (continued)

Type	Event
Repositories Gateway	Lock/Unlock/Return File Add/Delete Source, Tray Copy/Move, Add/Delete/Edit Source Admin
Mail	Send/Receive Mail, Created/Changed/Deleted Draft
Request File	Send/Receive
Preview	Send/Receive
DLP	DLP Flagged/Locked File, Admin Unlocked DLP, Failed Processing
Two-Factor	Login Accept/Challenge/Error
Branding	Create/Delete/Activate/Disable Branding UI. Update Email Templates

Additional resources

Additional resources

Resources

Get support

Need assistance with your Kiteworks product? Contact us with requests for assistance or to submit product enhancements.

Contact Kiteworks technical support at https://community.kiteworks.com.

Learn more about Kiteworks products

Visit the Kiteworks Support Portal to read technical articles, view training videos, search the knowledge base, and download additional user documentation.