



Lookout SSE Platform

**Secure Internet Access
Secure Private Access
Secure Cloud Access**

Administration Guide

22.10.150

Copyright and disclaimer

Copyright © 2021, 2022, 2023 Lookout, Inc. and/or its affiliates. All rights reserved.

LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.

Android is a trademark of Google Inc. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. UNIX is a registered trademark of The Open Group.

All other brand and product names are trademarks or registered trademarks of their respective holders.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Lookout, Inc. programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are commercial computer software pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Lookout, Inc. and its affiliates disclaim any liability for any damages caused by the use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products and services from third parties. Lookout, Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Lookout, Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Copyright and disclaimer.....	2
About Lookout Security Service Edge (SSE).....	19
Secure Internet Access (SWG)	19
Secure Private Access (ZTNA)	19
Secure Cloud Access (CASB).....	20
Getting started.....	21
Logging in for the first time	21
Viewing feature walkthroughs	21
Accessing product information, documentation, and customer support	21
Version information	21
Documentation and videos	22
Customer support	22
Managing your password and logging out.....	22
Changing your administrative password.....	22
Resetting a forgotten password	22
Logging out	23
Onboarding cloud applications and suites	24
Supported sanctioned cloud applications.....	25
Onboarding process overview	25
Enter basic information	25
For application suites, select applications	25
Select protection models	26
Select configuration settings.....	26
Enter authorization information.....	26
Save the onboarded cloud application.....	26
Application suites	27
Applications.....	27
Onboarding Microsoft 365 suite and applications	29
Configuration steps	29
Onboarding steps.....	31

Onboarding ServiceNow applications	36
Configuration steps	36
Onboarding steps.....	37
Onboarding SAP SuccessFactors applications	39
Onboarding steps.....	39
Additional onboarding steps for App Data Protection mode	40
Assigning a key for the application	42
Onboarding Slack Enterprise applications	42
Onboarding steps.....	42
Onboarding Slack (non-enterprise) applications	46
Onboarding steps.....	46
Removing collaborators in private Slack channels.....	46
Onboarding the AWS suite and applications.....	48
Automated onboarding.....	48
Manual onboarding	48
Onboarding Azure applications	62
Configuration steps	62
Onboarding steps.....	62
Onboarding Azure Blob applications	64
Configuration steps	64
Onboarding steps.....	65
Onboarding the Google Workspace suite and applications	66
Configuration steps	66
Onboarding steps in Secure Cloud Access	68
Onboarding Google Cloud Platform (GCP)	74
Configuration steps	74
Onboarding steps.....	77
Onboarding Dropbox applications	79
Onboarding the Atlassian Cloud suite and applications	81
Entering configuration settings for protection models.....	81
Generating an API token (Confluence applications only).....	83
Onboarding Egnyte applications	85
Onboarding Figma applications.....	87

App Authentication	87
App Access	89
Capturing team IDs from the Figma application	89
Dynamic DRM	90
Onboarding Box applications	91
Configuration steps in the Box Admin Console	91
Onboarding steps in the Management Console	92
Onboarding NetSuite applications	96
Assigning a key for the application	98
Onboarding Salesforce applications	99
Configuration steps	99
Onboarding steps	102
Onboarding ZenDesk applications	105
Configuring user access (all protection models)	105
Configuring proxy information (App Access protection model)	106
Assigning a key for the application	107
Accessing cloud applications through the Secure Cloud Workspace	108
Configuring platform single sign-on	108
Logging in to the Secure Cloud Workspace via IdP	110
Working with PAC files in the Secure Cloud Workspace	111
Types of PAC files	111
Selecting a PAC file	112
Post-onboarding tasks	113
Assigning, creating, and managing keys	113
Assigning a key	113
Creating a new key without assigning it	114
Deleting an unassigned key	114
Viewing key details	115
Setting a key password policy	115
Applying event filtering to onboarded cloud applications	116
Configuring tenants for user access and privacy	118
Configuring PII Anonymization in the Management Console	119
Enabling PII Anonymization for the Management Console	119

Temporarily De-Anonymizing PII	119
Managing users	121
Administrative user management	121
Adding new users	121
Setting up a user account password policy	122
Account status for system administrator and non-administrator roles	124
Disabling a non-administrator user account	124
Re-enabling a disabled non-administrator user account	124
Reassigning the Super Administrator role	124
Enterprise user management	125
Searching for user information	125
Filtering user information	125
External user management: External User Portal	125
Setting up access to the External User Portal	126
Opening and viewing decrypted files as a registered EUP user	127
Deleting users from the external user list	127
Configuring Secure Cloud Access for enterprise integration	128
Installing an on-premise connector for system services	129
Specifications	129
Downloading the connector	130
Pre-installation steps	130
Installing the connector (SIEM, EDLP, and Log Agent)	131
Restarting and uninstalling the connector	133
Additional configuration notes for SIEM	133
Additional configuration notes for log agents	134
Additional configuration notes for EDLP	134
Adding Advanced Threat Protection (ATP) services	135
Adding external services for Enterprise Data Loss Prevention (EDLP)	136
Creating a new configuration for EDLP	137
Downloading and installing an EDLP agent	138
Stopping and starting the EDLP agent service	139
Checking the EDLP agent status	140
Symantec DLP response rule configuration (Vontu service)	140

Configuring the Forcepoint Security Manager and Protector	140
Manually upgrading the SIEM, EDLP, and Log Agents	142
For CentOS and RHEL	142
For Ubuntu	143
Configuring Enterprise Mobility Management (EMM)	147
Obtaining an API key from AirWatch Workspace ONE	147
Creating the EMM configuration in Secure Cloud Access.....	148
Configuring Lookout Mobile Enterprise Security (MES) with Secure Cloud Access.....	148
Onboarding endpoint protection for Lookout Mobile Enterprise Security	149
Configuring device settings.....	149
Viewing device management settings for Lookout MES devices	151
Configuring Security Information and Event Management (SIEM)	151
Downloading, installing, and connecting a SIEM agent.....	152
Viewing the authentication token	153
Uninstalling a SIEM agent	153
Starting, stopping, and checking the status of a SIEM agent.....	153
Viewing SIEM agent logs.....	153
Creating a new SIEM configuration	153
Additional actions.....	155
Configuring Single Sign-On (SSO).....	155
SSO groups	156
Configuring an IdP proxy	156
Updating SP and IdP settings to point to the Secure Cloud Access IdP proxy.....	156
Creating cloud service and identity provider SSO providers	158
Creating the IdP proxy	159
Creating a new SSO group.....	160
Creating a cloud authentication policy (optional).....	160
Enterprise authentication – enabling SSO.....	161
Cloud-specific SSO settings	165
Configuring data classification.....	168
Integration with Azure Information Protection (AIP)	168
Integration with Titus.....	174
Creating and managing user directories	175

Manual upload user directory	176
Azure AD user directory	177
Configuring an Okta application.....	178
Enabling inline quarantine management	183
Creating decryption agents.....	183
Creating log agents and configuring log ingestion	184
Performing one-time log ingestion	184
Performing continuous log ingestion.....	185
Upgrading a continuous log agent.....	195
Starting, stopping, and checking the status of log agent services.....	195
Creating and configuring key servers.....	196
Creating a new key server on the cloud	196
Downloading and installing the HKMS RPM file.....	196
Enabling connectivity for the on-premise key server	198
Configuring an upstream proxy	199
Creating a new upstream proxy configuration in the Management Console.....	199
Viewing details for an upstream proxy configuration	199
Modifying an upstream proxy configuration	199
Installing the on-premise connector with the upstream proxy	200
Configuring the upstream proxy for on-premise deployments.....	202
Creating and managing enterprise sites.....	202
Creating a new enterprise site for traffic tunneling	202
High Availability support.....	207
Configuring known locations	207
Configuring API clients	207
Working with AnyApp™ connectors.....	209
Installing a connector.....	209
Adding a custom application as a connector.....	209
Setting up and managing environments	211
Viewing and editing environment details	212
Creating a new environment.....	213
Customizing (overriding) settings for an environment.....	216
Debugging nodes	216

Log Download	217
Debugging settings	218
Adding packages	219
HAR logging	219
Watchdog Settings	220
Duplicating or removing an environment	221
Setting up and managing nodes	222
Node metrics	224
Node configuration information	225
Creating a node	225
Modifying node information	226
Stopping or restarting services	226
Removing a node	227
Upgrading the Node Server from the Management Console (hosted)	227
Configuring and managing certificates	228
Types of certificates	228
Importing a TLS certificate	228
Generating a new certificate	229
Viewing certificate details	230
Deleting a certificate	231
Configuring data proxy settings	232
Forward and reverse proxy settings	232
Forward proxy	232
Reverse proxy	235
Intercept SAML (Security Assertion Markup Language)	235
Upstream Proxy	236
TLS Settings	237
Incoming Request Settings	237
File Extension and Size Settings	237
Configuring protocol support and DNS resolution options	239
Protocol support options	239
DNS Resolution options	240
Configuring email gateway settings	241

Management Console configurations for email	241
Incoming emails from cloud applications or user	241
Outgoing email settings	241
Configuring Office 365 email routing	242
Creating and configuring an email flow rule in Exchange	242
Configuring a connector for routing email from Office 365 to the secure email gateway	244
Allowlisting the Lookout secure email gateway to Office 365	246
Configuring forwarding of email	246
Configuring Domain Keys Identified Mail (DKIM) for the Secure Email Gateway	247
Enabling support for DKIM	247
Configuring DKIM for subdomains	247
Configuring DPaaS settings	249
Server Settings	249
API Client	249
Configuring logs	252
Importing and exporting keys and applications	253
Exporting keys and applications	253
Importing keys and applications	254
Configuring cloud discovery settings	256
Risk Factor Weight	256
Adjusting risk factor weighting percentages	257
Adjusting distribution of cloud risk scores	257
Purge Control	257
Knowledge Base	258
Contributing to the Knowledge Base	258
User Privacy	260
Enabling PII data anonymization	260
Searching for anonymized data in user lists	261
GDPR Configuration	261
Groups of interest	262
Creating and managing notifications and alerts	263
Creating notification channels	263
Creating notification templates	264

Creating notifications	266
Creating activity alerts	267
Types of alerts	268
Creating alerts for managed cloud applications	268
Creating alerts for Cloud Discovery	270
Configuring notification and alert options in System Settings	271
Selecting alert configurations.....	271
Editing an alert configuration	272
Deleting an alert configuration	273
Configuring SSE for Secure Private Access	274
Onboarding and configuring Secure Private Access for enterprise applications	274
Step 1 – Enable Secure Private Access (ZTNA) from the Management Console	275
Step 2 – (Optional) Create a category for networks	275
Step 3 – Create connectors for gateway access	276
Step 3a – Create an environment to serve as an on-premise connector	276
Step 3b – Create a node for the on-premise connector environment	277
Step 4 – Download the required packages.....	277
Step 5 – Install the on-premise connector	277
Step 6 – Onboard enterprise applications for Secure Private Access (ZTNA).....	280
Assigning an environment for the application	282
Checking the status of a Secure Private Access (ZTNA) tunnel	283
Connecting to remote machines using SSH and RDP	283
Restart or uninstall the on-premise enterprise connector as needed	286
Upgrading the Secure Private Access (ZTNA) connector manually using a Debian package	287
Debugging options for Secure Private Access	288
Enterprise Application Discovery for Secure Private Access (ZTNA)	288
Dashboard	288
Discovered Applications.....	289
Users.....	289
User Groups.....	290
Configuring traffic steering	291
Creating and managing enterprise sites.....	291
Creating a new enterprise site for traffic tunneling	291

High Availability support.....	293
Configuring known locations	294
Managing traffic steering for Lookout clients.....	294
Creating steering configurations	294
Creating traffic steering policies.....	295
Viewing and configuring device information	296
Managing endpoint security settings	296
Managing traffic steering in native clients	297
Open port requirements for native clients.....	297
Adding device configurations for native clients (optional).....	297
Downloading and installing the Windows client.....	298
Logging into the Windows client	300
Running diagnostics for the Windows client	302
Installing the Visual C++ Redistributable package	302
Importing the certificate file	302
Uninstalling the client	303
Configuring SSE for policy management	304
Policy configuration and creation workflow	304
Create content rule templates	304
New data types	305
New DLP rule templates	310
New document rule templates	310
Create Content Digital Rights templates	312
Steps for creating CDR templates	312
Configure file type, MIME type, and file size for exclusion from scanning.....	314
Exclusion from scanning by Lookout DLP engine	314
Exclusions from scanning by the Secure Cloud Access scan engine	315
Configure folder sharing for DLP scanning	316
Set number of folder sublevels for scanning	316
Configure default policy violation actions	316
Configure tenant-level default TLS intercept settings	317
Setting the default TLS action at the tenant level	317
Overriding the default TLS action for a policy	318

Enable user coaching	319
Implementation steps for user coaching	320
User coaching for activities involving multiple files	320
Set up continuous authentication	320
Workflow steps	321
Creating and managing custom categories	324
Viewing custom category lists	325
Default system category lists	325
Creating a new custom category	326
Applying a custom category to a policy	328
Viewing custom category information in Admin Audit logs and Activity Audit logs	328
Displaying custom category information in the Web Discovery dashboard	329
Displaying charts with category data	329
Creating policies for data protection and application security	331
Viewing policy lists	332
API Access policies	332
Access Control policies	333
Creating Access Control policies	334
Web & Application policies	334
TLS policies	352
Creating cloud authentication policies	354
Creating API Access policies	360
API policies with DLP Scan or None as the content inspection type	361
API policies with Malware Scan as policy type	368
Dynamic DRM policies	370
Access Control policies for email gateway, Outlook Web Access, and ActiveSync	374
Email gateway	375
Outlook Web Access	377
ActiveSync	378
Managing connected applications	381
Managing applications from the Connected Apps tab	382
Managing AWS key use	382
Filtering and syncing connected application and AWS information	383

Cloud Security Posture Management (CSPM)	384
Cloud types supported.....	384
Infrastructure Discovery.....	384
Assessment configuration	385
Assessment Results tab	386
Past Assessment Reports tab	386
Adding a new assessment.....	386
Cloud Data Discovery	390
Onboard a cloud application for which you want to apply Cloud Data Discovery	390
Create a Cloud Data Discovery policy.....	390
Create a Cloud Data Discovery scan	391
Associate a scan with a Cloud Data Discovery policy.....	392
View scan details.....	393
Overview tab	393
Basic tab	394
Policy tab	394
Past Scans tab.....	395
Generate a scan report.....	395
Generating activity reports for Box cloud applications	396
Violation management and quarantine	401
Quarantine Management.....	401
Selecting information to view	401
Taking action on a quarantined file.....	402
Viewing and searching for quarantined documents.....	403
Quarantine Copy	403
Reviewing messages in the Quarantine Copy list	404
Selecting information to display and review	404
Deleting a message from the Quarantine Copy list.....	404
CDD Violation Management.....	405
Selecting information to view	405
Taking action on a quarantined CDD item.....	405
Monitoring and managing system activity	407
Viewing user and system activity from the Home Dashboard.....	407

Data cards.....	407
Event details	409
Viewing additional details	410
Refreshing all data	410
Exporting data	410
Monitoring cloud activity from charts	411
Application Activities	411
Anomalous Activities.....	413
Office 365.....	419
AWS Monitoring	419
Secure Private Access.....	420
Web Activities	420
Customizing and refreshing a dashboard display.....	420
Exporting data for reporting	420
Printing a report or chart.....	421
Working with activity audit logs.....	422
Filtering data	423
Hiding the chart view.....	428
Exporting data	429
Monitoring user activity through Admin Audit Logs	429
Audit log information	429
Filtering and searching for Admin Audit Log information.....	429
Insights Investigate.....	430
Incident Management tab	430
Incident Insights tab	431
Entity Insights tab.....	433
Viewing and updating user risk information.....	434
Managing devices	435
Viewing lists of devices and their status.....	436
Devices listed in the Lookout DRM tab.....	436
Devices listed in the ActiveSync tab	437
Devices listed in the EMM tab	437
Devices listed in the Lookout MES tab	437

Changing the profile and actions for a device	438
In the Lookout DRM tab	438
In the ActiveSync tab	438
Configuring default device settings for profile, access, and device trust	438
Device Settings for Key Access	438
Default Device Profile Settings	439
Device Trust Settings	439
Verifying email addresses and managing email blacklists	440
Decrypting and viewing files using client devices	442
Downloading an encrypted file for the first time	442
Updating existing client applications	442
Decryption using client devices: desktop applications	443
Windows desktop	443
Installing a new Windows desktop application	443
Decrypting and viewing files with the Windows desktop application	443
Logging out of the Windows desktop application	444
Reporting issues with the Windows desktop application	444
MacOS desktop	444
Installing a new MacOS application	445
Decrypting and viewing files with the MacOS desktop application	445
Logging out of the MacOS application	446
Decryption using client devices: mobile applications	447
Android	447
Installing the Android mobile app	447
Decrypting and viewing files with the Android mobile app	447
Logging out of the Android mobile app	447
iOS	447
Installing the iOS mobile app	447
Decrypting and viewing files with the iOS mobile app	448
Logging out of the iOS mobile app	448
Application and web discovery	449
Application Discovery	449
The Enterprise App Discovery dashboard	449

Viewing additional details for activity, cloud applications, users, and groups	450
Search filters	451
Viewing discovered and Knowledge Base cloud apps	452
Exporting information and submitting unrecognized domains	452
Exporting a Discovered Cloud Risk report	453
Viewing details about a cloud application	454
Configuring cloud risk scores	455
Viewing user data	456
Viewing user group data	457
Onboarding and creating policies for discovered cloud applications	457
Creating and editing policies for discovered cloud applications	458
Web Discovery	461
Web Discovery dashboard	461
Creating and editing policies for web categories and domains	463
Viewing user data	466
Viewing user group data	467
Creating, viewing, and scheduling reports	468
Uploading a company logo	468
Setting a time zone	468
Selecting report types for web activity	469
Selecting report types for cloud applications	469
Visibility	469
Compliance	469
Threat Protection	470
Data Security	470
IaaS	470
Secure Private Access (ZTNA)	470
Custom	470
Displaying report information	470
Scheduling a new report	471
Downloading generated reports	472
Managing report types and scheduling	473
Quick reference: Home Dashboard charts	474

Application Activities	474
Policy Analytics	474
Activity Monitoring	476
Encryption Statistics	477
Privileged User Activities	478
Anomalous Activities	479
Office 365	480
Overview	480
Admin Activities	480
Exchange	481
OneDrive	481
SharePoint	482
Teams	482
Yammer	482
IaaS Monitoring Dashboard	483
Amazon Web Services	483
Microsoft Azure	483
Google Cloud Platform	485
Secure Private Access	487
Activity Monitoring	487
Policy Analytics	487
Web Activities	489
Policy Analytics	489
Activity Monitoring	489
Quick reference: RegEx examples	490
Quick reference: Supported file types	491
Quick reference: ECCN information for SSE	494
Index	496

About Lookout Security Service Edge (SSE)

Lookout Security Service Edge (SSE) is a comprehensive security solution that provides a single platform for protection, discovery, and monitoring of websites and data stored in cloud applications used by your organization.

Lookout SSE supports these important components of cloud security:

- Secure Internet Access (SWG)
- Secure Private Access (ZTNA)
- Secure Cloud Access (CASB)

Secure Internet Access (SWG)

The Secure Internet Access (SWG) solution keeps users safe from cyberthreats and unauthorized traffic from entering and spreading through their internal networks. As a cloud-based solution, Secure Internet Access monitors user web traffic and enforces policies that define conditions for access to specific websites or types of sites. It plays an important role in protecting employee and user work environments from infections coming from malicious web traffic, sites with vulnerabilities, Internet-borne viruses, malware, and other cyberthreats.

Secure Internet Access also ensures implementation of and compliance with an organization's standards to protect confidential information from exposure.

URL filtering, cloud anti-malware, ability to decrypt and inspect websites accessed via HTTPS, Data Loss Prevention (DLP), and Secure Cloud Access (CASB) are standard Secure Internet Access functions, all of which are available as part of Lookout SSE.

Secure Internet Access addresses these common use cases:

- **Monitor and control access to websites** -- Protect users from accessing applications, websites, and web content that does not comply with the organization's acceptable use policies.
- **Monitor and control access to risky applications** -- Control usage and user activities based on analytics and insights. Gain visibility into sanctioned and unsanctioned applications and their risk levels.
- **Detect and defend against threats** -- Protect users and devices from threats posed by access to malicious websites, or access to compromised websites that have unintended malicious content on both encrypted and clear-text web traffic.
- **Provide data protection and application security** -- Prevent corporate data loss from insider threats, unintentional data sharing, or data exfiltration from accessing phishing or malicious websites.

Secure Private Access (ZTNA)

Secure Private Access (ZTNA) provides secure remote access to an organization's applications, data, and services based on clearly defined access control policies. Unlike Virtual Private Networks (VPNs), which grant access to an entire network, Secure Private Access grants access only to specific services or applications. Because more and more users are accessing resources from anywhere, Secure Private Access can help eliminate gaps in other secure remote access technologies and methods.

Secure Private Access enforces granular, adaptive, and context-aware policies for providing secure and seamless access to private applications hosted across clouds and corporate data centers, from any

remote location and from any device. That context can be a combination of user identity, user or service location, time of the day, type of service, and security posture of the device.

Secure Private Access allows “least privilege” access only to specific applications within a network, reducing the attack surface and preventing lateral movement of threats from compromised accounts or devices. Secure Private Access builds upon the concept of **Zero Trust**, which asserts that to ensure data safety and integrity, organizations must not trust any entity inside or outside the security perimeters. Instead, they must verify every user or device before granting access to sensitive resources.

Secure Private Access addresses these common use cases:

- **Secure remote access to private applications** -- As organizations move their business-critical applications across multiple cloud environments for easy collaboration, they are challenged to monitor each device to secure access and prevent data exfiltration. Secure Private Access enables adaptive, context-aware access to private apps from any location and device. Access is denied by default unless explicitly allowed. The context for app access may include identity, device type, user location, and device security posture.
- **Enhance or replace VPN connections** -- Securing remote user access through software and hardware-intensive VPNs can increase the capital expenditure and bandwidth costs. Secure Private Access provides fast, direct access to cloud applications, reducing networking complexity, cost, and latency while optimizing the remote workforce.
- **Limit user access** -- Perimeter-based security solutions permit full network access to any user with valid login credentials, potentially exposing sensitive data to compromised accounts and insider threats. Once they have access to the entire network, bad actors can move freely through the network, largely undetected. With Secure Private Access, user access is restricted to specific applications as well as on a need-to-know basis. All connections are verified before access is granted to specific internal resources.

Secure Cloud Access (CASB)

As part of SSE, Secure Cloud Access (CASB) provides strong policy controls to support cloud-based applications under PCI, PII, HIPAA, GDPR, and more. In addition, the Secure Cloud Access policy engine enables you to manage sharing of external content and access to public links.

To meet the compliance and regulatory requirements in an enterprise environment, Secure Cloud Access supports a comprehensive policy engine that can be configured in a variety of ways to protect content containing sensitive information. You can apply DLP policies to one, some, or all of the cloud applications in your organization, as well as to specific users, groups, sites (for example, SharePoint) and folders within those cloud applications. Secure Cloud Access provides out-of-the-box DLP templates for rules that commonly apply to data such as Social Security Number, Credit Card number, Personal Identifiable information (PII), PCI-DSS compliance, and so on.

Secure Cloud Access supports multiple SaaS, PaaS, and IaaS cloud applications, and any mix of hosted, hybrid, and on-premise deployments.

Secure Cloud Access provides client applications on multiple operating systems (desktop and mobile) that allow authorized users to download, decrypt, and view encrypted documents. The desktop applications also can be used to re-encrypt content that users have modified.

Getting started

The following sections provide instructions for the next steps after you have deployed SSE.

- Logging in for the first time
- Viewing feature walkthroughs
- Accessing product information, documentation, and customer support
- Managing your password and logging out

Once you log in, you will be provided with options for onboarding cloud applications.

Logging in for the first time

After your enterprise has purchased Secure Cloud Access or Secure Cloud Access with Secure Internet Access, you will receive an email with a link that provides a user name and a temporary password. Click the link.

The user name you see in the **Create Account** screen is prepopulated from the email.

1. Enter the temporary password.
2. In the **Password** field, enter a new password for future use. Hints are provided as a guide to the type and number of characters allowed.
3. Re-enter the new password in the **Confirm Password** field and click **Create**.

Note The email link and temporary password expire in 24 hours. If more than 24 hours have passed before you see this email, contact Support to get a new temporary link and password.

When you have completed the login steps, the initial welcome screen appears.

When you are ready to onboard unsanctioned or sanctioned cloud applications, select these areas from the Management Console:

- To initiate cloud discovery for unsanctioned cloud applications: **Choose Administration > Log Agents** to upload log files and create log agents.
- To onboard sanctioned cloud applications: Choose **Administration > App Management**. Then, follow the instructions for onboarding cloud applications.

Viewing feature walkthroughs

Click the **i** menu to view a list of how-to walkthroughs of SSE features.

Accessing product information, documentation, and customer support

Click the **question mark** icon to display the help menu.

Version information

Click the **About** link.

Documentation and videos

The following links are available:

- **Walkthrough Videos** – Opens the Walkthrough Videos page, with links to videos about product features.

You can also access links to feature videos from any Management Console page that displays a video link at the upper right.

- **Online Help** – Opens the online help for the product. The help includes a clickable Table of Contents and an index for searching.
- **Documentation** – Opens a link to a downloadable PDF of the Lookout SSE Administration Guide.
- **Release Notes** – Opens a link to a downloadable PDF of the Lookout SSE Release Notes.

Customer support

Click the email link to contact Lookout customer support.

Managing your password and logging out

Use the following procedures to change your password, reset a forgotten password, and log out.

Changing your administrative password

1. Click the **Profile** icon.
2. Click **Change Password**.
3. Enter your current password in the **Old Password** field.
4. Enter your new password in the **New Password** and **Confirm Password** fields.
5. Click **Update**.

Resetting a forgotten password

If you forgot your password, perform the following steps to reset it.

1. From the **Login** screen, click **Forgot your password?**.
2. In the **Forgot Password** screen, enter your user name and click **Reset**.
3. You will receive an email with a temporary password and a link to reset your password.

This temporary password will expire in 24 hours. If more than 24 hours have passed since you received your temporary password, you will see a **Token Expired** message when you try to enter your temporary password. If this happens, repeat the first two steps to receive a new temporary password.

4. In the email, click the link for the new temporary password.
5. The **Forgot Password** dialog box is displayed with your first name, last name, and user name filled in.
6. Enter the temporary password provided. If you copy and paste the temporary password from the email instead of typing it, be sure not to copy any extra spaces or characters.

7. Enter your new password in the **New Password** and **Confirm New Password** fields. As you type, tool tips appear at the right that provide guidance for the required format and number of characters.
8. Click **Create**.

Logging out

Click the **Profile** icon and click **Logout**.

Onboarding cloud applications and suites

The following sections provide instructions for configuring and onboarding cloud applications and application suites. Once cloud applications are onboarded, you can create and configure policies for those cloud applications.

For Secure Internet Access, you can also create and configure policies for web access.

- **Onboarding process overview**
- Onboarding steps, by cloud application and suite
 - **Office 365 suite and applications**
 - **ServiceNow**
 - **SAP SuccessFactors**
 - **Slack Enterprise**
 - **Slack (non-enterprise)**
 - **AWS suite and applications**
 - **Azure**
 - **Google Workspace suite and applications**
 - **Google Cloud Platform (GCP)**
 - **Dropbox**
 - **Atlassian Cloud Suite and applications**
 - **Egnyte**
 - **Figma**
 - **Box**
 - **NetSuite**
 - **Salesforce**
 - **ZenDesk**

Supported sanctioned cloud applications

SSE supports the following cloud types.

Adobe	HubSpot
Alfresco (Preview)	Jira
Azure (Preview)	Jive
AWS suite, including S3	NetSuite
Atlassian suite, including Bitbucket and Confluence	Office 365 suite, including OneDrive and SharePoint
Box	OWA
SAP C4C	Salesforce
CloudTrail (AWS)	ServiceNow
CMIS	ShareFile
Concur	SharePoint
Custom application	Slack
DocuSign	Sococo (Preview)
Dropbox	SAP SuccessFactors
Egnyte (Preview)	SugarSync
GCP	Workday
Google Workspace, including Google Drive and	ZenDesk
Gmail	
GitHub	
SAP Hana	

Support is available for custom applications you create to meet your specific data security needs.

For each cloud application you onboard, you will need to provide a **service account** with login credentials for the managed administrative user of that application. These application-specific login credentials enable the administrator to manage the account details for an application and monitor user activity for it.

Note SSE does *not* store cloud-specific administrator credentials.

Onboarding process overview

Some onboarding steps vary depending on the cloud you are onboarding and the types of protection you choose. The following overview summarizes the onboarding procedure.

1. From the Management Console, select **Administration > App Management**.
2. Click **New**. Then, perform the following steps.

Enter basic information

1. Choose a cloud application type.
2. **(Required)** Enter a name for the new cloud application. Use only alphabetical characters, numbers, and the underscore character (_). Do **not** use spaces or any other special characters.
3. **(Optional)** Enter a description for the new application.

For application suites, select applications

If you are onboarding a cloud type that is an **application suite**, you will be prompted to select the applications in that suite that you want to protect. Click the check marks for the applications to include.

Select protection models

Depending on the cloud type you chose, some or all of the following protection models will be available. For suites, the selected protection models apply to the entire suite.

- **App Authentication** – Provides expanded controls for access that go beyond user IDs, such as denial of logins from non-compliant or compromised devices and from users with patterns of risky behavior.
 - **App Access** – Provides context controls for cloud applications and custom applications; allows access control based on user risk factors and IP risk configurations, as well as DRM-style encryption.
 - **API Access** – Provides an out-of-band approach to data security; performs ongoing monitoring of user activities and administrative functions.
 - **Cloud Security Posture** – Used for cloud types for which you want to apply Cloud Security Posture Management functionality. For more information, see **Cloud Security Posture Management (CSPM)**.
 - **Dynamic DRM** – Allows or denies access to keys for decryption of encrypted files.
 - **Email** – Used for Office 365 cloud application types that include email as one of the cloud applications.
 - **ActiveSync Device Management** – Used for cloud types for which you want to apply device management with ActiveSync.
 - **Cloud Data Protection** -- Used for ServiceNow and SuccessFactors cloud types.
 - **Cloud Data Discovery** -- Used for cloud types for which you want to apply Cloud Data Discovery functionality. For more information, see **Cloud Data Discovery**.
4. Select one or more protection modes, depending on the type of protection you want to enable for a cloud. You can create policies for the cloud application based on the protection modes you choose.
 5. Click **Next**.

Select configuration settings

You will need to set configuration information for the cloud application you are onboarding. These configuration settings will vary, depending on the cloud type and the protection modes you choose.

For example, if you enabled the **App Access** protection mode in the previous step, you will be prompted to enter proxy information and SAML configurations. This information will enable routing of traffic through the reverse proxy (proxy chaining) for access to this cloud according to the SSO settings you set up.

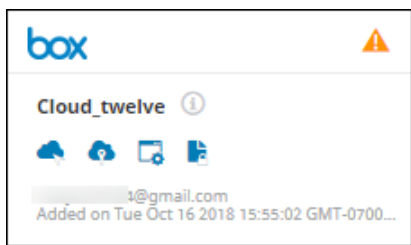
Enter authorization information

For most protection modes, you will need to go through an authorization step by logging in to the cloud application with your administrator credentials for the account.

Save the onboarded cloud application

1. Click **Next** to view a summary of information about the new cloud application. The summary shows the cloud type, name and description, the selected protection modes, and other information, depending on the cloud type and selected protection modes for the cloud application.
2. Click **Previous** to correct any information or click **Save** to confirm the information.

The new cloud application is added to the **App Management** page.



The display in the grid shows the following information:

- The **name** of the cloud application.
- A **description** (if provided). To view the description, hover over the information icon next to the cloud application name.
- The **protection modes** available for the cloud application. Each icon represents a protection mode. The protection modes you selected for this cloud appear in blue; those not selected for this cloud appear in gray. Hover over each icon to see its protection type.
- The **key assignment status**. The orange icon at the upper right indicates that the application is waiting for a key to be assigned. You can assign a key now or do so later. Once you assign a key to the cloud application, the orange icon is replaced by a green check mark.
- The **user ID** (email address) of the administrator user who onboarded the application.
- The **date** and **time** the application was onboarded.
- The next sections provide instructions for onboarding cloud applications and suites.

Application suites

- Office 365 suite and applications
- Google Workspace (Gmail and Google Drive)
- Atlassian Cloud Suite
- AWS

Applications

- ServiceNow
- Slack Enterprise
- Azure
- Google Cloud Platform (GCP)
- Dropbox
- Egnyte
- Box
- Salesforce

Onboarding Microsoft 365 suite and applications

This section outlines the procedures for onboarding a Microsoft 365 suite and applications and enabling audit logging.

Note The following user roles are required for onboarding.

- Office Apps Administrator
- SharePoint Administrator
- Teams Administrator
- Application Administrator
- Cloud Application Administrator
- Guest Inviter
- Privileged Authentication Administrator
- Privileged Role Administrator
- Global Reader
- Compliance Administrator
- Compliance Data Administrator

Configuration steps

Microsoft 365 application suite

Secure Cloud Access can provide protection options to the entire suite of Microsoft 365 applications, including Exchange, Microsoft Teams, and Yammer, in addition to OneDrive and SharePoint.

The Microsoft 365 cloud type is an application suite. You can onboard the suite, and then select the applications for which to apply protection. Some configurations, such as key management, will apply to the entire suite and cannot be specified by application. Other configurations can be customized for each application in the suite.

Secure Cloud Access provides a dedicated dashboard for monitoring activity in the Microsoft 365 suite applications. You can select the Office 365 dashboard from the **Monitor** menu.

Turning on audit log search and verifying mailbox management by default

For monitoring of applications in the Microsoft 365 suite, you must configure settings for these options:

Turn on audit log search. You must turn on audit logging in the Microsoft Security & Compliance Center before you can start searching the Microsoft 365 audit log. Turning on this option enables user and administrator activity from your organization to be recorded in the audit log. The information is retained for 90 days.

For more details and instructions about how to turn on audit log search and turn it off, see

<https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off>

Verify that management of mailboxes by default is enabled. Microsoft now turns on mailbox audit logging by default. With mailbox management enabled, certain actions performed by mailbox owners, delegates, and administrators are logged automatically. The corresponding mailbox audit records will be available when you search for them in the mailbox audit log.

To verify that management of mailboxes is enabled, you must run the following command in the Exchange Online PowerShell:

```
Get-OrganizationConfig | FL AuditDisabled
```

A value of **False** (FL) indicates that mailbox auditing by default is enabled.

For more details, see

<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

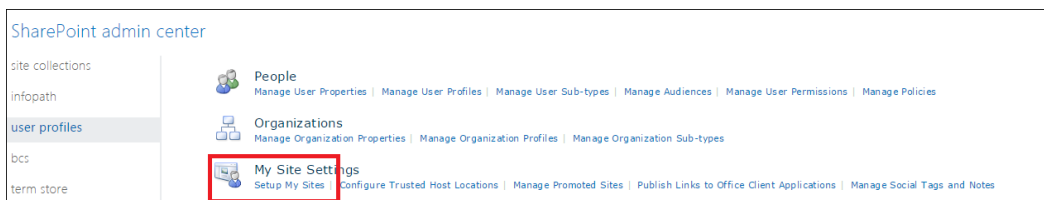
SharePoint / OneDrive

Creating sites for new SharePoint or OneDrive users

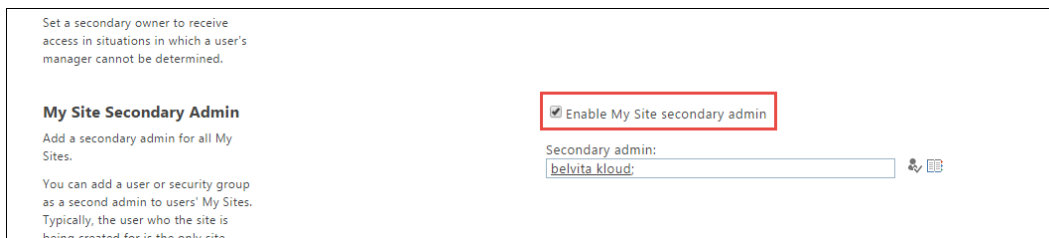
When new users are added to a SharePoint or OneDrive account, you must perform the following procedure to start monitoring and protecting data in the personal sites for these users. You should also perform a user sync.

Perform the following steps to add sites for new SharePoint or OneDrive users.

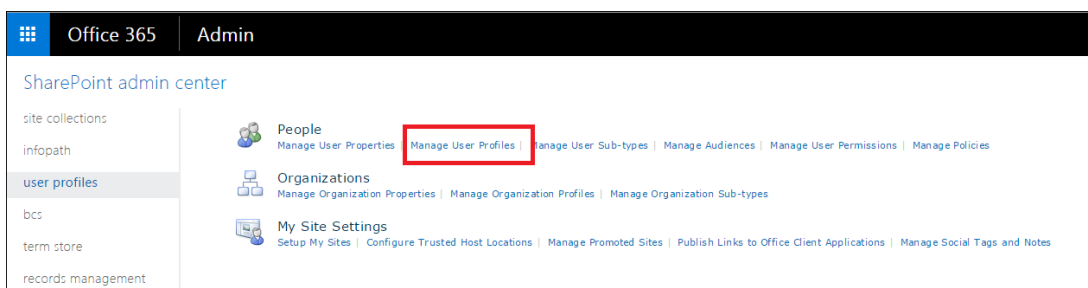
1. Log in as the administrator.
2. Go to **Admin > SharePoint admin center > user profiles > My Site Settings > Setup My Sites**.



3. Under **Setup My Sites**, check **Enable My Site secondary admin**, and select the admin as the site admin.



4. Go to **User Profiles > Manage User Profiles**.



5. Under **Manage User Profiles**, right-click the user's profile, and click **Manage site collection owners**. User profiles are not displayed by default. They appear only when you search for them.

Site Collection Administrators

Site Collection Administrators are given full control over all Web sites in the site collection. They may also receive site use confirmation mail. Enter users separated by semicolons.

belvita kloud: test2 user:

Creating a Quarantine site in SharePoint

You must create a SharePoint site called **Quarantine-Site** to enable the Quarantine action to work.

Exchange

Secure Cloud Access provides support for the ActiveSync protocol, allowing you to enforce policies and perform management actions on mobile devices.

Configuration to enable support for mobile devices using ActiveSync

To enable support for mobile devices using ActiveSync, you must update the **CNAME** record in your DNS server settings. Once the DNS changes take effect, the mobile devices must reconfigure their email profiles that use ActiveSync.

Update the **CNAME** record as follows:

Name	Target
autodiscover.<company.com>	autodiscover.<ciphercloud.io>

Configurations in the Exchange Admin Center

Update the settings in the Exchange Admin Center as follows:

1. Log in to Office 365.
2. Select **Exchange > Admin Center > mail Flow > Remote domains**.

Use rich-text format:

☐ Always

☒ Never

☐ Follow user settings

Supported Character Set

MIME character set:

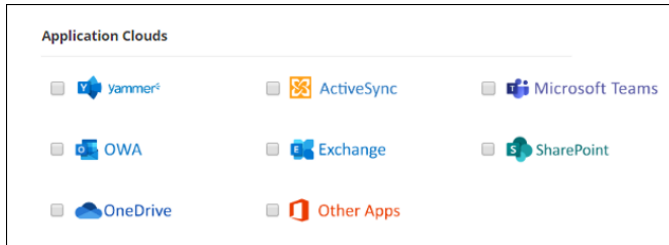
Choose to always or never send messages using rich-text format. Use Follow user settings to send email messages that use the rich-text settings specified by the Outlook user.

3. Under **Use rich-text format**, select **Never**.

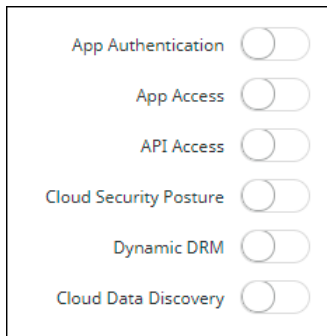
Onboarding steps

1. Go to **Administration > App Management** and click **New**.
2. Choose **Office 365**. This is the Microsoft 365 application suite.
3. Click **Next**.

4. Enter a **Name** (required) and a **Description** (optional) for the new cloud application. For the name, use only alphabetical characters, **numbers**, and the underscore character (_). Do not use spaces or any other special characters.
5. Select the applications in the suite that you want to protect. The named applications are the specific applications that are supported. The Other Apps selection includes any unsupported or partially supported applications such as Calendar, Dynamics365, Excel, Word, Planner, Sway, Stream, and Video.



6. Click **Next**.
7. Select one or more **protection models**. The protection options you see vary, depending on the applications you selected in the previous step, and will apply to those applications. You cannot select protection models for individual applications.



App Authentication	Available for all Microsoft 365 applications.
App Access	<p>Available for all Microsoft 365 applications. Because file deletion and renaming functions in Microsoft 365 CAC require API calls, you must also choose API Access as a protection mode for these functions to work properly. If you select only App Access without API Access:</p> <ul style="list-style-type: none"> • File upload blocking will upload empty (zero byte) files. • Encrypted file names will not be given the .ccsecure extension. • CAC policies that include folders and sites will not work because folders and sites are not synced. • User-based CAC policies will not work because user sync does not occur. <p>If these limitations are not critical in your organization, selection of API Access is optional.</p>
API Access	<p>Available for all Microsoft 365 applications. Must be also enabled if you enable App Access, Dynamic DRM, or Cloud Data Discovery.</p>

Cloud Security Posture	Available for all Microsoft 365 applications. Select this mode if you want to implement Cloud Security Posture Management (CSPM) functionality for this cloud. For more information about CSPM, see Cloud Security Posture Management.
Dynamic DRM	Available for all Microsoft 365 applications. Requires either API Access or App Access mode to be enabled.
Email	Available if you selected Exchange as a Microsoft 365 application.
ActiveSync Device Management	Available if you selected ActiveSync as a Microsoft 365 application. Secure Cloud Access supports the ActiveSync protocol for mobile devices, allowing enterprises to apply controls for real-time sync and send activities for Office 365 email. Select the ActiveSync Device Management option to create and configure policies for sync and send actions related to Microsoft 365 emails on mobile devices. If you choose this protection model, make sure you have configured the Exchange client on your device. For instructions, see Configuring Microsoft Exchange account on your mobile device . Once the mobile device is registered, the unique ID (UUID) of the mobile device will be displayed in the Management Console. To verify, go to Protect > Device Management > ActiveSync > User .
Cloud Data Discovery	Available for OneDrive and SharePoint applications. Select this mode if you want to implement Cloud Data Discovery functionality for this application. Also requires API Access to be enabled.

8. Click **Next**.
9. Enter the following configuration information. The fields you see depend on the protection models you selected.

- Proxy
 - The **Custom HTTP Header Name** and **Custom HTTP Header Value** fields are configured on the cloud level (as opposed to the cloud application level). If this is the **first** Microsoft 365 cloud application you are onboarding, the values you enter in these two fields will apply to all other Office 365 cloud applications you onboard. If this is **not** the first Microsoft 365 cloud application you are onboarding, these field values will be initialized from the first Microsoft 365 cloud you onboarded.
 - The remaining fields are configured for the cloud application you are onboarding. Enter values as needed.

- **Login Domain Prefix** -- For example, **companyname.com** (as in `<username>@companyname.com`)
- **Specific Domains** – Office 365-specific domain names that need to be redirected. Enter or select domains for this cloud application.
- **Tenant Identifier Domain Prefix** -- For example, **Secure Cloud Access protect** (as in **Secure Cloud Access protect.onmicrosoft.com**)
- **API Settings** (required only for API Access protection) --
 - **Content Collaboration Scan** – Toggle is enabled by default. This setting enables events for File CheckIn/CheckOut to be processed. If this toggle is disabled, these events are not processed.
 - **Internal Domains** -- Enter one or more internal domains.
 - **Archive Settings** – Enables archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files (including those for SharePoint and Teams) are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

Notes

- If you onboard Microsoft Teams as an application, be sure that an Active Sync directory is created, because the Azure AD is the source of user information. To create a directory, go to **Administration > Enterprise Integration > User Directory**.
- When the authorized administrator for a cloud account is changed, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

The **Archive Settings** option is available for onboarded cloud applications with **API Access** protection mode selected.

Two options are available:

- **Remove from Trash**
- **Archive**

For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Note For OneDrive cloud applications, files for non-administrator user accounts are **not** removed from the Trash when the **Remove from Trash** flag is enabled.

Click the toggles to enable or disable the settings. If you select the **Archive** action, you must also select the **Remove from Trash** option for archiving to be enabled.

Enter the number of days for which to retain archived files. The default value is 30 days.

- **Authorization** -- Authorize the components. You will need to provide your Microsoft 365 login credentials when prompted. Click the buttons as follows:
 - **OneDrive and SharePoint** -- Click *each* **Authorize** button. If you did not select either of these applications earlier, these buttons do not appear.
 - **Office 365** -- Clicking **Authorize** authorizes the Office 365 suite components you selected, *except* for OneDrive and SharePoint, which must be authorized separately. This authorization is for monitoring only.

10. Click **Next**.

11. View the summary page to verify that all information is correct. If it is, click **Next**.

The onboarding is complete. The cloud application is added to the list on the **App Management** page.

Enabling audit logging and managing mailbox auditing

Once you have onboarded an Office 365 suite with applications, you must turn on audit logging in your Microsoft 365 account before you can search the audit log. Event polling will start 24 hours after audit logging is enabled.

For information and instructions regarding about audit logging for Microsoft 365, see the following Microsoft documentation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide>

Also, verify that management of mailboxes by default is enabled. Microsoft now turns on mailbox audit logging by default. For information and instructions about managing mailbox auditing, see the following Microsoft documentation.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide>

Onboarding ServiceNow applications

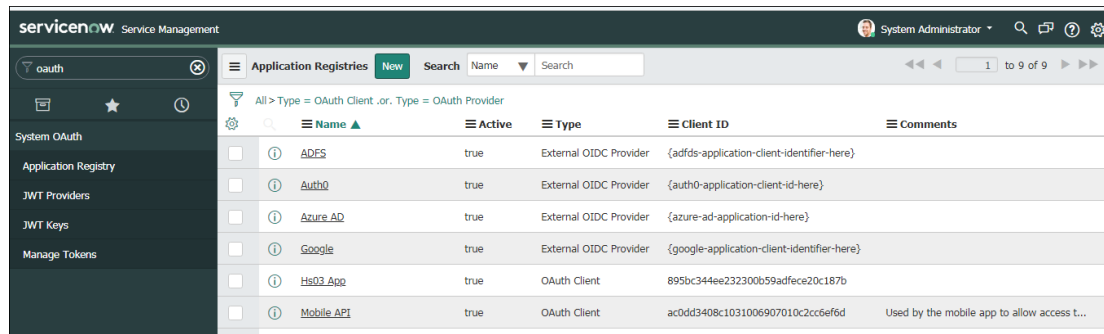
The following section provides instructions for onboarding ServiceNow applications.

Configuration steps

Before onboarding the ServiceNow application, create an OAuth application.

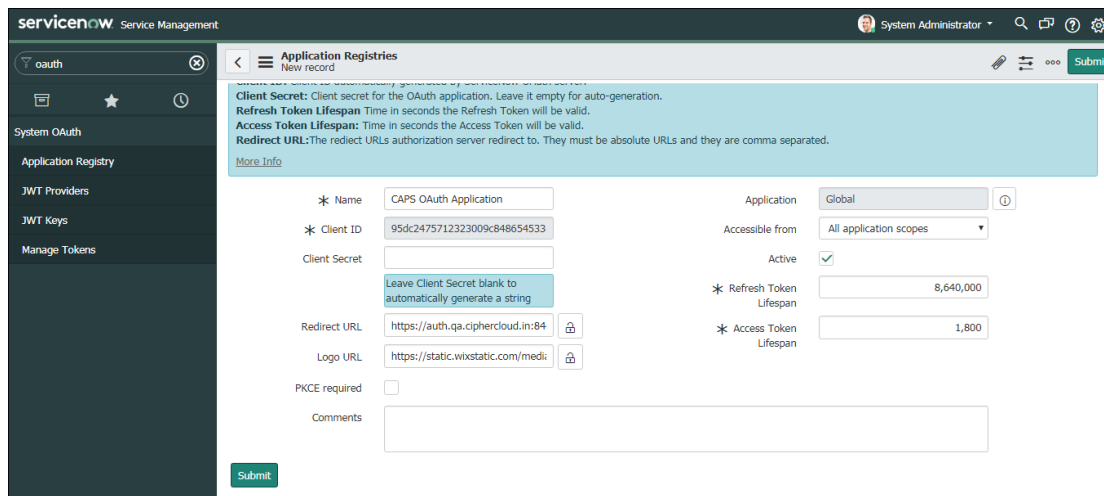
1. Log in to ServiceNow as an administrator.
2. To create an OAuth application, go to

System OAuth > Application Registry > New > Create an OAuth API endpoint for external clients.



Name	Active	Type	Client ID	Comments
ADFS	true	External OIDC Provider	{adfs-application-client-identifier-here}	
Auth0	true	External OIDC Provider	{auth0-application-client-id-here}	
Azure AD	true	External OIDC Provider	{azure-ad-application-id-here}	
Google	true	External OIDC Provider	{google-application-client-identifier-here}	
HS03 App	true	OAuth Client	895bc344ee232300b59adfec20c187b	
Mobile API	true	OAuth Client	ac0dd3408c1031006907010c2cc6ef6d	Used by the mobile app to allow access t...

3. Enter the following information:
 - **Name** – Enter a name for this OAuth app.
 - **Redirect URL** – Enter the appropriate URL.
 - **Logo URL** – Enter the appropriate URL for the logo.
 - **PKCE Required** -- Leave unchecked.



Client Secret: Client secret for the OAuth application. Leave it empty for auto-generation.
Refresh Token Lifespan: Time in seconds the Refresh Token will be valid.
Access Token Lifespan: Time in seconds the Access Token will be valid.
Redirect URL: The redirect URLs authorization server redirect to. They must be absolute URLs and they are comma separated.

Name: CAPS OAuth Application
Client ID: 95dc2475712323009c848654533
Client Secret: [Leave Client Secret blank to automatically generate a string]
Redirect URL: https://auth.qa.ciphercloud.in:84
Logo URL: https://static.wixstatic.com/medi
PKCE required: ☐
Comments: [Empty text area]

Application: Global
Accessible from: All application scopes
Active: ☒
Refresh Token Lifespan: 8,640,000
Access Token Lifespan: 1,800

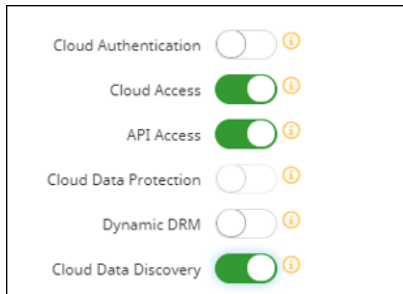
Submit

4. Click **Submit**.
5. Open the newly created app and note the **Client ID** and **Client Secret** values.

Onboarding steps

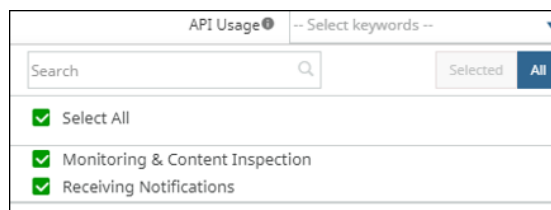
1. From the Management Console, go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **ServiceNow** and click **Next**.
4. Enter a **Name** (required) and a **Description** (optional). Then click **Next**.
5. Select one or more protection modes and click **Next**.

Note Cloud Data Protection is not available.



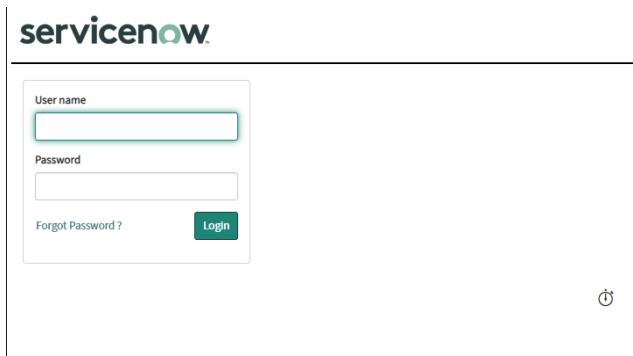
6. On the **Configuration** page, enter the information for the protection modes you selected in the previous step.
 - For **App Authentication**, no additional information is required. Click **Next** to display the summary information.
 - For **App Access**, enter the domains for this account.
 - For **API Access**, enter:
 - The **API Usage type**, which defines how this application will be used with API protection. Check **Monitoring & Content Inspection**, **Receiving Notifications**, or **Select All**.

If you select only **Receiving Notifications**, this cloud application is not protected; it is used only to receive notifications.



- The OAuth App Client ID
- The OAuth App Client Secret
- The ServiceNow Instance ID
- For **Dynamic DRM**, you must also select either **App Access** or **API Access** as protection modes. No additional information is needed for Dynamic DRM itself.

- For **Cloud Data Discovery**, enter
 - The OAuth App Client ID
 - The OAuth App Client Secret
 - The ServiceNow Instance ID
7. Click **Authorize**.
 8. When prompted, log in to the ServiceNow application.

The image shows the ServiceNow login interface. At the top left is the 'servicenow' logo. Below it is a login form with two input fields: 'User name' and 'Password'. Below the 'Password' field is a link that says 'Forgot Password?'. To the right of this link is a green 'Login' button. In the bottom right corner of the form area, there is a small circular icon with a power symbol inside.

9. When prompted, click **Allow**.

If authorization is successful, you should see a **Re-Authorize** button when you return to the Management Console. Click **Next** and **Save** to complete onboarding.

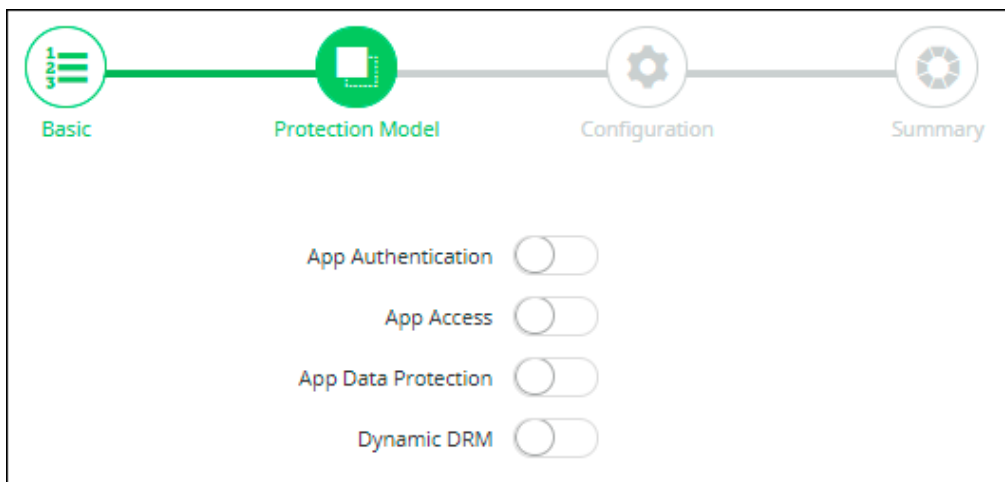
Onboarding SAP SuccessFactors applications

To complete these configurations, you must have valid login credentials for access to SAP SuccessFactors and the Lookout Management Console.

SAP SuccessFactors can be onboarded in inline mode only.

Onboarding steps

1. Go to **Administration > App Management** and click **New**.
2. Select **SuccessFactors** from the dropdown list.
3. Click **Next**.
4. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
5. Select one more protection models.



- **App Authentication**
 - **App Access**
 - **App Data Protection** (A subscription is needed for this option. See **Additional onboarding steps for App Data Protection model** for information about the additional fields included with this option.)
 - **Dynamic DRM**
6. Click **Next** to enter configuration details.

The screenshot shows a configuration window with a progress bar at the top indicating four steps: Basic, Protection Model, Configuration (current), and Summary. Below the progress bar, the 'Proxy' section is visible, containing the following fields:

- Company ID
- Home Page Url
- Specific Domains (with a dropdown menu showing "-- Enter Domain values --")
- Tenant ID for SAP Analytics Cloud

The fields you see depend on the protection mode or modes you selected. The following fields are displayed for all protection modes except **App Data Protection**.

- **Company ID** -- Enter the company ID used when logging into your SAP SuccessFactors instance.
- **Home Page URL** -- Enter the URL of the SAP SuccessFactors instance being onboarded.
- **Specific Domains** -- Enter the list of SAP SuccessFactors domains relevant to the Company ID. Separate each domain by a comma. You must prepare a list of the domain names of SAP SuccessFactors modules, such as **Employee Central**, **Learning Management System**, **API**, and **others**. You must ensure that no domain name is missed.
- For details and examples about specific domains, see the section **Cloud Onboarding Steps** in the *SAP SuccessFactors Administration Guide*.
- **Tenant ID for SAP Analytics Cloud** – To access the external SAP analytics cloud, enter the SAP analytics URL.

7. Click **Next**, then click **Save**.

Additional onboarding steps for App Data Protection mode

If you have opted for a subscription that enables the **App Data Protection** mode, you will need to provide additional information if you select this protection mode.

Enter this information as follows:

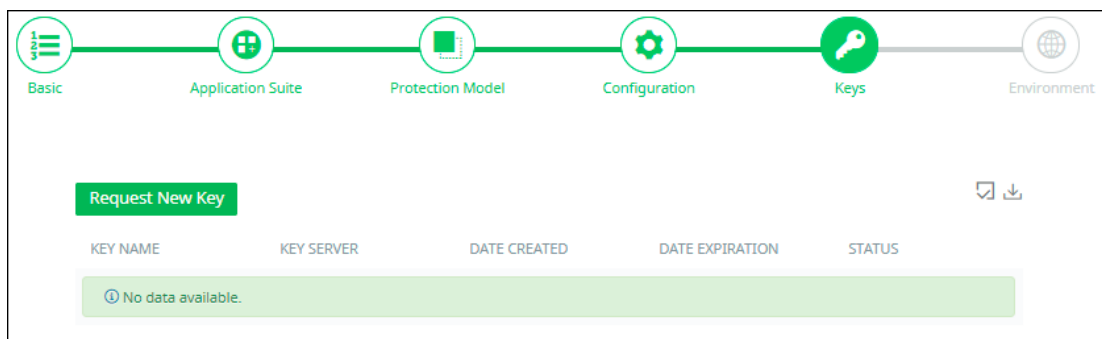
- **Version** – You can select a version of the connector **only** if more than one SAP SuccessFactors connectors are installed. Otherwise, only the version of the currently installed connector is displayed in the dropdown list. For example, if you have installed the SAP SuccessFactors Connectors of two versions (for instance, V2.0.0.103 and V2.1.0.199), both versions are listed.
- **Exclude Domains** – Enter any domain names that should be excluded (separating each name with a comma) and click **Save** to close the text box.
- **PII PickList IDs** – Enter the IDs for all picklists that contain PII data (separating each item with a comma) and click **Save** to close the text box.
- To obtain picklist IDs, you must download the data model files from your SAP SuccessFactors instance. For information regarding downloading the data model files, see the section *Enable conditional encryption* in the *SAP SuccessFactors Administration Guide*.
- **Custom PII Field Reference Mappings** -- Enter the following configuration:
 - `<country-code>=GlobalInfo/<Custom-Stringn>,GlobalInfo/<Custom-Stringn>;`
 - **Example:** `GBR=GlobalInfo/Custom-String13,GlobalInfo/Custom-String5;`
 - For additional details about this configuration, see the section **Protecting text fields in Global Information portlet for Great Britain (GBR), Oman (OMN), and Qatar (QTR)** in the *SAP SuccessFactors Administration Guide*.

- **Web Resource Caching** – Click the **Web Resource Caching** toggle to enable the cache, which will provide improved performance. Without enabling this option, you might notice degradation of performance when generating PDF reports.
- **XLS Parser** – Enter the following value:
`com.ciphercloud.csg.connector.impl.parsers`
- **PDF Parser** – Enter the following value:
`com.ciphercloud.csg.connector.impl.parsers.XlsParserV2`

Assigning a key for the application

To assign a key to the onboarded application, modify the application settings as follows.

1. Go to **Administration > App Management** and open the onboarded application by clicking the pencil icon.
2. Go to the **Keys** page.



3. Click **Request New Key**. A request is generated to assign a new key from the available keys. A message appears at the lower right portion of the screen confirming the key request.

You can also create a new key and assign it to the application. To create a new key, go to **Administration > Key Management** and create the key. For more information, see **Assigning, creating, and managing keys**.

4. Click **Save**.

Onboarding Slack Enterprise applications

This section outlines the procedure for onboarding a Slack enterprise cloud application. For these applications, you can choose several protection modes including **API Access**, which provides expanded access controls that go beyond user IDs, such as denial of logins from non-compliant or compromised devices and from users with patterns of risky behavior.

A non-enterprise Slack application is also available with a smaller number of protection models. For information, see **Onboarding Slack (non-enterprise) applications**.

Onboarding steps

1. Go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **Slack Enterprise** and click **Next**.

4. Enter a **Name** (required) and a **Description** (optional). Then click **Next**.
5. Select one or more **protection models**.
 - **App Authentication**
 - **App Access**
 - **API Access**
 - **Dynamic DRM**
 - **Cloud Data Discovery**
6. Enter the information for the selected protection modes.
 - For **App Authentication** – No further information is required. Click **Next** to confirm the policy.
 - For **App Access** – Enter all applicable Custom HTTP Header Values, the Slack Specific Domains, and the Slack Tenant Identifier Domain Prefix.

The screenshot shows a form titled "Proxy" with the following fields:

- Custom HTTP Header Name1: X-Slack-Allowed-Workspaces-Reques
- Custom HTTP Header Name2: X-Slack-Allowed-Workspaces
- Custom HTTP Header Value1: (empty)
- Custom HTTP Header Value2: (empty)
- Slack Specific Domains: (empty)
- Slack Tenant Identifier Domain Prefix: (empty)

- For **API Settings** – Enter or select the following information:
 - **API Usage** -- Defines how this application will be used with API protection. **Check Monitoring & Content Inspection, Receiving Notifications, or Select All.**

The screenshot shows a dialog box for "API Usage" with a search bar and a list of options:

- ☐ Select All
- ☐ Monitoring & Content Inspection
- ☐ Receiving Notifications

Buttons at the bottom: Save, Cancel.

If you select *only* **Receiving Notifications**, this cloud application is not protected. It will be used only to *receive* notifications.

- **Enable Review of Quarantine Files** -- Click this toggle to enable reviewing of tombstoned files through the Slack channel.
- **Slack Enterprise Domain** (Full Login Domain) -- Enter the full domain for your organization. Example: `https://<name>.enterprise.slack.com`

API Settings

API Usage ⓘ -- Select keywords -- ▾

Enable Review of Quarantine files ☐

Internal Domains

Slack Enterprise Domain (Full Login Domain) ⓘ

7. Click **Authorize**. Enter Slack credentials when prompted.
8. Slack displays a prompt requesting that you confirm permissions to access your organization's messages, modify messages, and view elements from workspaces, channels, and users in your organization.

Click **Allow** to confirm these permissions.

⚠ Access all of your organization's messages
(including all private channels and direct messages), as well as your organization's files ▶

⚠ Make changes to your organization's messages
(including all messages in private channels and direct messages), as well as your organization's files ▶

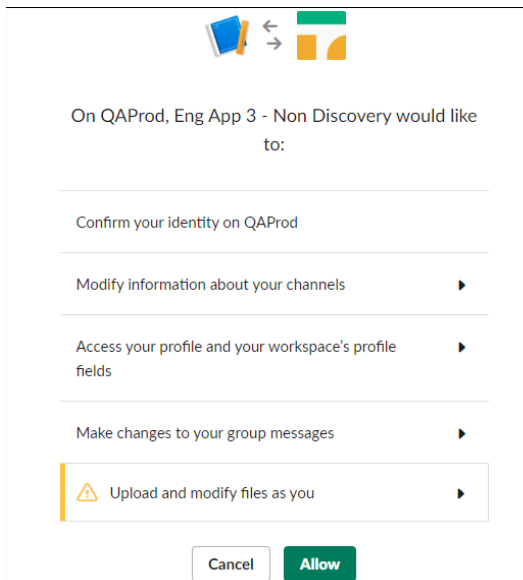
⚠ View events from all workspaces, channels and users (Enterprise Grid only) ▶

9. Authorize one or more workspaces. Click **Authorize** next to the workspace name to authorize it. At least one workspace must be authorized.
10. When prompted to install the app in the workspace, click **Allow**.

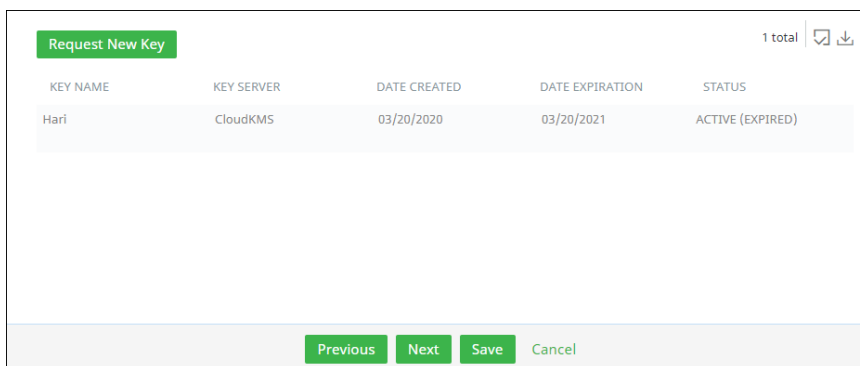
Note If you want to enable additional functionality, you need to onboard and authorize each workspace separately. If the workspaces are not authorized separately, the following actions will not be supported:

- **Encrypt**
- **Watermark**
- **Removed external shared link**

11. In response to the prompt for non-discovery access, click **Allow**.



12. Click **Next**. The **Key Management** page is displayed.



13. To request a new key now, click **Request New Key**. The administrator will be notified, and a key will be assigned. Then, click **Save**.

To request a new key later, click **Save**.

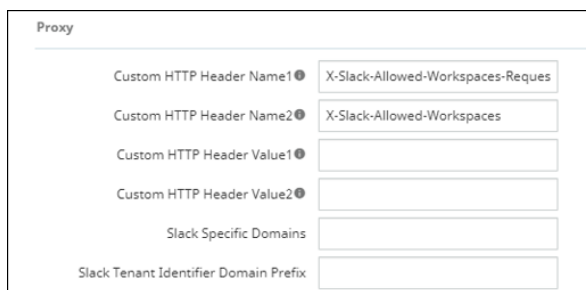
Onboarding Slack (non-enterprise) applications

The following section outlines the procedure for configuring non-enterprise Slack applications. These applications offer a more limited number of protection modes.

Onboarding steps

1. Go to **Administration > App Management**.
2. From the **Managed Apps** tab, click **New**.
3. Select **Slack** and click **Next**.
4. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
5. Select one or more protection models:
 - **App Authentication**
 - **App Access**
 - **Dynamic DRM**

If you select **Dynamic DRM**, you must also select **App Access**.
6. On the **Configuration** page, enter the information for the selected protection modes.
 - For **App Authentication**, no additional information is required. Click **Next** to display the summary and confirm the policy.
 - For **App Access** and **Dynamic DRM**, enter the Custom HTTP Header Values, Slack Domains, and Tenant Identifier Domain Prefix for this Slack account.



The screenshot shows a 'Proxy' configuration window with the following fields:

- Custom HTTP Header Name1: X-Slack-Allowed-Workspaces-Reques
- Custom HTTP Header Name2: X-Slack-Allowed-Workspaces
- Custom HTTP Header Value1: (empty)
- Custom HTTP Header Value2: (empty)
- Slack Specific Domains: (empty)
- Slack Tenant Identifier Domain Prefix: (empty)

7. Click **Authorize**.
8. Enter login credentials to authorize access to the account.
9. Confirm the information and save the policy.

Removing collaborators in private Slack channels

Once you have onboarded a Slack application, you can configure Slack to remove collaborators in private channels. Perform the following steps to configure these settings.

1. In Slack **Workspace** settings, click the **Permissions** tab.
2. Click **Expand** to expand the **Channel Management** options. (The button label changes to **Close** when the options are expanded.)

Settings | **Permissions** | **Attachments** | **Access Logs**

Messaging Expand
Set who can use @everyone, @channel, and @here.

Invitations Expand
By default, any member can invite new people to your workspace. If you'd like, you can change this so invitations require [admin approval](#).

Channel Management Close
Choose who can create, archive, remove members, and manage posting permissions in channels.

People who can create private channels:
Everyone, plus Multi-Channel Guests (default)

People who can create public channels:
Everyone, except guests (default)

People who can archive channels:
Everyone, except guests (default)

People who can remove members from private channels:
Everyone, except guests (default)

- Under **People who can remove members from private channels**, make sure that **Everyone, except guests** (the default option) is selected.

Everyone, except guests (default)

People who can remove members from private channels:

Everyone, except guests (default)

People who can remove members from public channels:
Workspace Owners and Admins only (default)

People who can manage posting permissions in channels:

You can override this setting by creating an organization-level policy in Slack. To do so:

- Go to the **Manage Organization** page and select **Organization Policies** under **Settings** in the left menu.

ELPS Ciphercloud 3

Settings | **Permissions** | **Apps**

Messaging Add Policy
Set who can use @everyone, @channel, and @here.

Channel Management Add Policy
Choose who can create, archive, remove members, and manage posting permissions in channels.

Guest Management Add Policy
Set who can invite and manage guests.

User Groups Add Policy
Set who can create and manage user groups.

Message Editing & Deletion Add Policy
Choose when to allow message editing and deletion.

Workspace Analytics Add Policy
Choose who can view the workspace Analytics page.

Custom Emoji Add Policy
Choose who can manage custom emoji.

Slackbot Responses Add Policy
Choose who can manage [Slackbot responses](#).

- Click the **Permissions** tab.
- For **Channel Management**, click **Add Policy**.
- Under **People who can remove members from private channels**, make sure that **Everyone, except guests** (the default option) is selected.

Onboarding the AWS suite and applications

This section outlines instructions for onboarding the AWS suite in Secure Cloud Access. You can choose to perform an automated or manual onboarding depending on your needs.

Secure Cloud Access supports most AWS S3 storage types for file upload.

Lookout supports these storage types:

- Standard
- Intelligent-Tiering
- Standard-IA
- One Zone-IA
- Reduced redundancy
- Glacier Instant Retrieval

Lookout does not support these storage types:

- Glacier Flexible Retrieval (formerly Glacier)
- Glacier Deep Archive

Automated onboarding

You can onboard the AWS suite automatically using the provided Terraform module.

Onboarding with Terraform

1. In the Management Console, select **Administration > System Settings > Downloads**.
2. Locate the file **aws-onboarding-terraform-module-*<version>*.zip** and download it.
3. Extract the contents of the zip file.
4. Locate and open the file **README-Deployment steps.pdf**.
5. Follow the instructions provided in the README file to complete the automated onboarding.

Manual onboarding

This section outlines instructions for configuring the AWS suite for manual onboarding in Secure Cloud Access, followed by the manual onboarding instructions.

Configuration steps

Before you onboard the AWS application manually, you must perform a set of configuration steps.

Note These configuration steps are required only if you plan to onboard AWS in **API mode**. If you plan to onboard AWS in **inline** mode, skip to **Onboarding steps**.

To get started, log in to the AWS console (<http://aws.amazon.com>).

Then, perform these configuration steps.

- Step 1 – Create an IAM role for Lookout Secure Cloud Access

- Step 2 – Create a Cloud Trail
- Step 3 – Create Simple Queue Service (SQS)
- Step 4 – Configure Event Notifications for the Cloud Trail Bucket
- Step 5 – Create an Identity Access Management (IAM) Monitor policy
- Step 6 – Create an IAM DLP policy
- Step 7 – Create an IAM CSPM policy
- Step 8 – Create an IAM KMS policy
- Step 9 – Attach the policies to the IAM role

Step 1 – Create an IAM role for Lookout Secure Cloud Access

1. In the AWS console, click **Roles** and select **Create role**.
2. Select **Role Type: Another AWS Account**.
3. **For Account ID**, obtain this ID from the Lookout DevOps team. This is the account ID for the AWS account in which the tenant Management Server is onboarded.
4. Under **Options**, check **Require External ID**.
5. Enter the following information:
 - **External ID** – Enter a unique attribute to be used while onboarding AWS S3 in Secure Cloud Access (for example, **aws-security-monitor**).
 - **Require MFA** – Do not check.
6. Click **Next: Permissions**. Do not attach any policies at this point.
7. Click **Next: Tags** and (optional) enter any tags you want to include to the **Add Tags** page.
8. Click **Next: Review**.
9. Enter a **Role Name** (for example, **AWS-Security-Monitor**) and click **Create Role**.
10. Search for the role name you created and click it.
11. Copy the role ARN.
12. Select **Roles > Trust relationships tab > AWS-Security-Monitor summary view**. Locate the Condition section and copy the **ExternalID** value.

Step 2 – Create a Cloud Trail

To create a new cloud trail, follow these steps.

1. From **Services**, go to **Cloud Trail**.
2. Select **Trails** from the left panel.
3. Click **New Trail** and enter the following information.
 - **Trail name** – **ccawstrail** (for example)
 - **Storage location** – Select **Create new S3 bucket** to create a new bucket or **Use existing S3 bucket** to pick up existing buckets in which to store logs. Enter or select the desired bucket name.

4. Click **Next**. The **Choose log events** screen is displayed.
 - **Events** – Select **Management events** and (optionally) **Data events**.
 - **Management Events** – Select **Read** and **Write**.
 - **Data Events** (optional) – Configure data events if you want to see activity audit logs and AWS monitoring screens.
5. Click **Next**.
6. Click **CreateTrail**.
7. Copy the Cloud Trail ARN and S3 Bucket ARN.

Step 3 – Create Simple Queue Service (SQS)

1. Under **Services**, go to **Simple Queue Service (SQS)**.
2. Click **Create New Queue**.
3. Enter a **Queue Name** and select **Standard Queue** as the queue type.
4. Click **Create Queue**.
5. Copy the new queue's ARN.
6. Go to the **Access Policy** section.
7. Click the **Edit** button and paste the following policy information.

```
{
  "Version": "2012-10-17",

  "Id": " default_policy_ID",
  "Statement": [
    {
      "Sid": "__receiver_statement",
      "Effect": "Deny",
      "Principal": {
        "AWS": "<<Role_ARN>>"
      },
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage"
      ]
    }
  ]
}
```

```

],
"Resource": "<<Queue_ARN>>"
"Condition": {
  "ArnNotEquals": {
    "aws:PrincipalArn": "<<Role_ARN>>"
  }
},
{
  "Sid": "__sender_statement",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": "sqs:SendMessage",
  "Resource": "<<Queue_ARN>>",
  "Condition": {
    "ArnEquals": {
      "aws:SourceArn": "<<S3_Bucket_ARN>>"
    }
  }
}
]
}

```

In the above code, make sure to replace all of the strings in double brackets (<< >>) with the appropriate values:

- Replace <<Role_ARN>> with the role ARN that you copied at the end of [Step 1 – Create an IAM role for Lookout Secure Cloud Access](#).
- Replace <<Queue_ARN>> with the queue ARN that you copied in step 5 of this section.
- Replace <<S3_Bucket_ARN>> with the bucket ARN that you copied at the end of [Step 2 – Create a Cloud Trail](#).

8. Click **Create Queue**.

Step 4 – Configure Event Notifications for the Cloud Trail Bucket

1. Under **Buckets**, go to the bucket that stores the CloudTrail logs (for example, **awstrailevnts**).
2. Click the **Properties** tab for the bucket.
3. Go to the **Event Notifications** section and click **Create event notification**.
4. Enter the following information for the notification.
 - **Name** – any naming (for example, SQS Notification)
 - **Event Types** – Select **All object create events**.
 - **Filters** - Enter any filters to apply to the notification.
 - **Destination** – Select **SQS Queue**.
 - **Specify SQS Queue** – Select **LookoutAWSQueue** (select the SQS queue created in [Step 3 – Create Simple Queue Service \(SQS\)](#).)

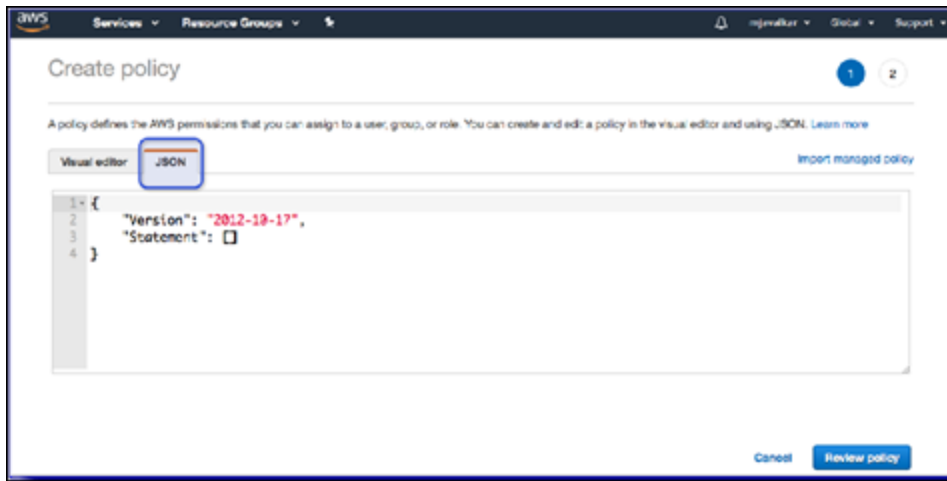
Note: Make sure that your S3 Bucket and SQS queue are in the same region.

5. Click **Save Changes**.

The event is created.

Step 5 – Create an Identity Access Management (IAM) Monitor policy

1. Click **Services** and select **IAM**.
2. Select **Policies** and click **Create Policy**.
3. Click the **JSON** tab.



4. Copy and paste the following policy information.

```
{
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sqs:ChangeMessageVisibility",
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource": [
        "<<Lookout Monitoring Queue ARN>>"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",

```

```

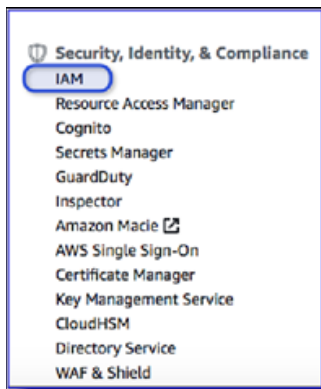
        "s3:ListBucket",
        "s3:PutBucketAcl"
    ],
    "Resource": [
        "<< List of s3 bucket arns to monitor or arn:aws:s3:::* >>"
    ]
},
{
    "Sid": "VisualEditor3",
    "Effect": "Allow",
    "Action": [
        "iam:ListGroupsForUser",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:GetUser",
        "iam:GetGroup"
    ],
    "Resource": "*"
}
]
"Version": "2012-10-17"
}

```

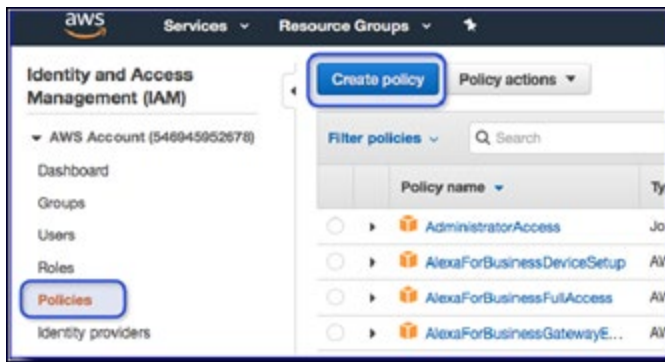
5. Click **Review Policy** at the lower right portion of the screen.
6. Give the policy the name **lookout-aws-monitor** and click **Create Policy**.

Step 6 – Create an IAM DLP policy

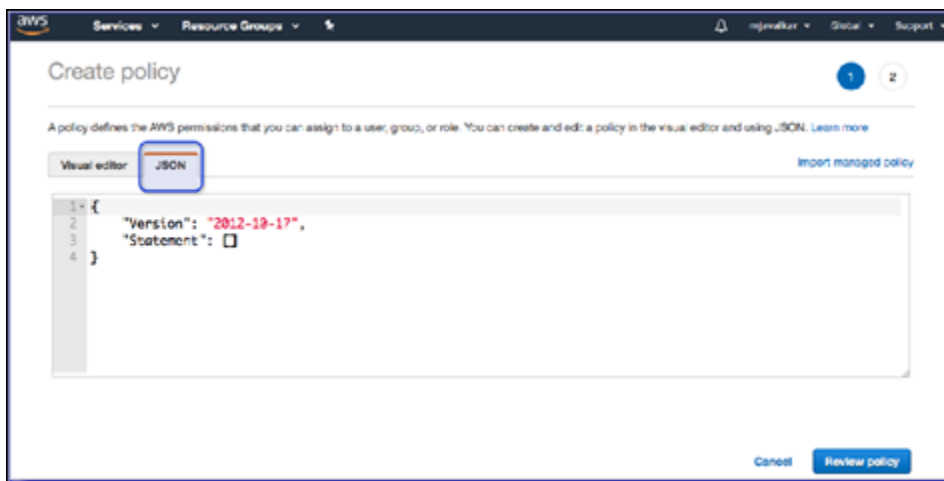
1. Click **Services** and select **IAM**.



2. Select **Policies** and click **Create Policy**.



3. Click the **JSON** tab.



4. Copy and paste the following policy information.

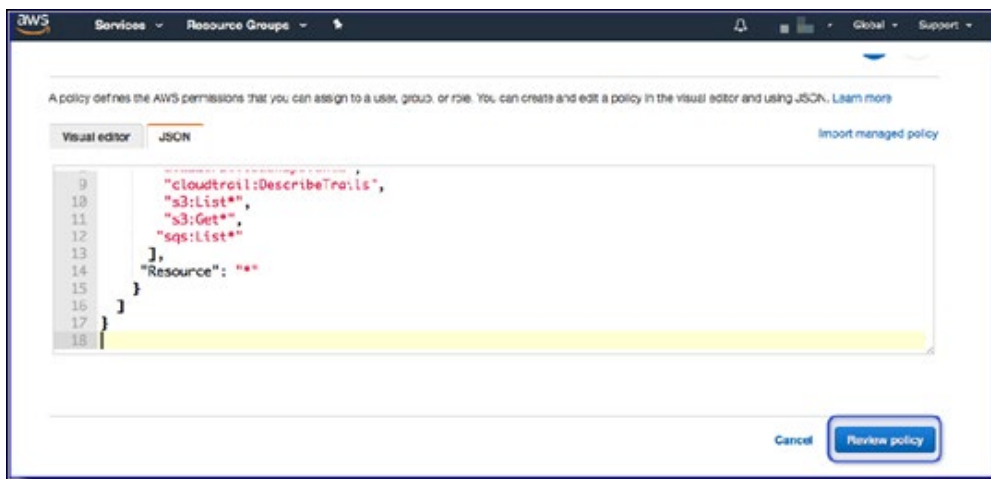
```
{
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:GetGroup",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "s3:ListAllMyBuckets",
        "s3:GetBucketNotification",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutBucketNotification",
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetBucketAcl",
        "s3:PutBucketAcl",
```

```

        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:AddPermission",
        "sns:ListSubscriptionsByTopic",
        "sqs:CreateQueue",
        "sqs:GetQueueUrl",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage"
        "cloudtrail:DescribeTrails"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Sid": "LookoutCASBAwsDlpPolicy"
  }
],
"Version": "2012-10-17"
}

```

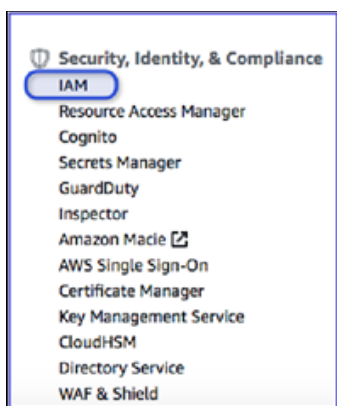
5. Click **Review Policy** at the lower right portion of the screen.



6. Name the policy **lookout-api-policy** and click **Create Policy**.

Step 7 – Create an IAM CSPM policy

1. Click **Services** and select **IAM**.



2. Select **Policies** and click **Create Policy**.



3. Click the **JSON** tab.



4. Copy and paste the following policy information:

```
{
  "Statement": [
```



```

{
  "Action": [
    "account:*",
    "cloudhsm:AddTagsToResource",
    "cloudhsm:DescribeClusters",
    "cloudhsm:DescribeHsm",
    "cloudhsm:ListHsms",
    "cloudhsm:ListTags",
    "cloudhsm:ListTagsForResource",
    "cloudhsm:TagResource",
    "cloudtrail:AddTags",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetEventSelectors",
    "cloudtrail:GetTrailStatus",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:TagResource",
    "config:Describe*",
    "dynamodb:ListStreams",
    "dynamodb:TagResource",
    "ec2:CreateTags",
    "ec2:Describe*",
    "ecs:DescribeClusters",
    "ecs:ListClusters",
    "ecs:TagResource",
    "elasticbeanstalk:AddTags",
    "elasticfilesystem:CreateTags",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "glacier:AddTagsToVault",
    "glacier:ListVaults",
    "iam:GenerateCredentialReport",
    "iam:Get*",
    "iam:List*",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "lambda:TagResource",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "rds:AddTagsToResource",
    "rds:DescribeDBInstances",
    "redshift:CreateTags",
    "redshift:DescribeClusters",
  ]
}

```

```

        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:PutBucketTagging",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "sns:GetTopicAttributes",
        "sns:List*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Sid": "LookoutCASBAwsCspmPolicy"
}
],
"Version": "2012-10-17"
}

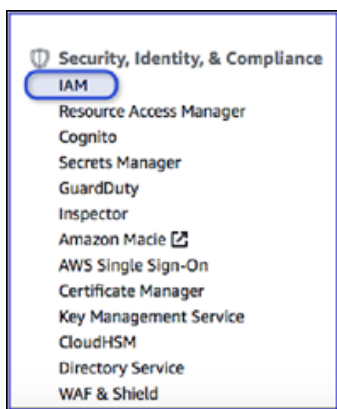
```

5. Click **Review Policy**.
6. Give the policy the name **lookout-cspm-policy** and click **Create Policy**.

Step 8 – Create an IAM KMS policy

Perform the following steps if the S3 bucket has KMS enabled.

1. Click **Services** and select **IAM**.



2. Select **Policies** and click **Create Policy**.



3. Click the **JSON** tab.



4. From an S3 bucket, obtain the KMS key for the KMS policy information.
 - a. Click an S3 bucket.
 - b. Click **Bucket Properties**.
 - c. Scroll to the default encryption section and copy the AWS KMS key ARN.

If different keys are assigned to buckets, you will need to add them under **Resource** in the policy information (step 5).

5. Copy and paste the following policy information:

```
{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:ReEncryptTo",
```

```

        "kms:DescribeKey",
        "kms:ReEncryptFrom"
    ],
    "Resource": [ "<AWS_KMS_key_ARN>"
    ]
}

```

6. Click **Review Policy**.
7. Give the policy the name **lookout-kms-policy** and click **Create Policy**.

Step 9 – Attach the policies to the IAM role

1. In the AWS console, go to **Services** and select IAM.
2. Select **Roles** and search for the role that you created in [Step 1 – Create an IAM role for Lookout Secure Cloud Access](#).
3. Click on that role and go to the **Permissions** tab.
4. Under **Add permissions**, select **Attach policies**.
5. Select the policies that you created in steps 5, 6, 7, and 8 earlier.
6. Save the role.

Onboarding steps

1. In the Lookout Management Console, go to **Administration > App Management** and click **New**.
2. Select **AWS** from the dropdown list.
3. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
4. For the application, check **Amazon Web Services** and click **Next**.
5. Select one or more of the following protection models by clicking the toggle for each protection model to include.
 - **Cloud Authentication**
 - **App Access**
 - **API Access**
 - **Cloud Security Posture**
 - **Dynamic DRM**
6. Click **Next**.

Notes

- To onboard AWS in **inline** mode, you must choose both **App Authentication** and **App Access**. To onboard AWS in **API** mode, choose **API Access**.
- If you choose **Dynamic DRM**, you must also choose **API Access**.
- **Cloud Security Posture Management (CSPM)** provides tools to monitor resources used in your organization and assess security risk factors against security best practices for AWS cloud

applications. To enable use of CSPM, you must choose **Cloud Security Posture** as a protection mode.

7. If you selected **API Access**:

- a. Click the **AWS Monitoring** toggle and enter the following information in the **API** section of the **Configuration** page. This is the information you had generated in Step 2 of the configuration steps (**Create an Identity Access Management (IAM) role for Secure Cloud Access**).
 - **External ID**
 - **Role ARN**
 - **SQS Queue Name and SQS Region (see Step 6 – Create Simple Queue Service [SQS])**
- b. In the **Authentication** section, click the **Authorize** button and click **Next**.

A popup message appears prompting you to confirm that the required policies (according to the selected protection modes) are assigned to the role.

Note Be sure your browser is configured to allow pop-ups to be displayed.
- c. Click **Continue** to confirm that the required policies are displayed.

When the authorization is complete, a green checkmark appears next to the **Authorize** button, and the button label now reads **Re-Authorize**.
- d. Click **Next** to display a summary of the onboarding settings.
- e. Click **Save** to complete onboarding.

The new cloud application is displayed as a tile on the **App Management** page.

8. If you selected **App Authentication** and **App Access**:

- a. In the **Tenant Identifier Domain Prefix** field on the **Configuration** tab, enter your AWS account ID(s). You can enter more than one, separated by commas.

To locate your AWS account ID, log on to AWS and click your username in the top right corner. If you have multiple accounts, you can also find their account ID numbers on the login page where you select which one you want to log in to.
- b. Click **Next**.
- c. For User Access, you can click **All Users** or use the controls to select specific users to allow access to this application.
- d. Click **Next** to display a summary of the onboarding settings.
- e. Click **Save** to complete onboarding. The new cloud application is displayed as a tile on the **App Management** page.

Onboarding Azure applications

This section outlines the procedures for onboarding Azure cloud applications. For Azure Blob Storage onboarding instructions, see the next section.

Configuration steps

To use the CSPM feature for an Azure account, you need a Service Principal that has access to the corresponding subscription.

The Service Principal should have the **Reader** or **Monitoring Reader** role with access to **Azure AD user, group, or service principal** and associated **Client Secret**.

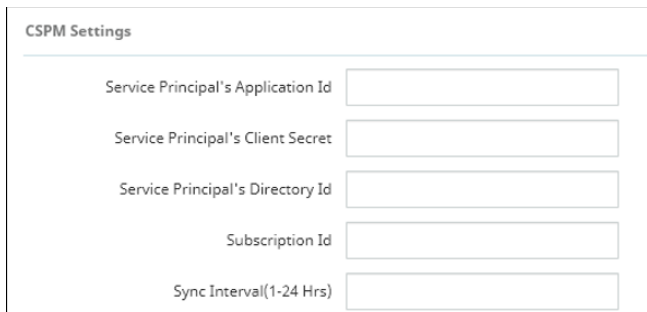
Before onboarding, you should have the **Subscription ID** of the account, and the following information from the Service Principal:

- **Application (Client) ID**
- **Client Secret**
- **Directory (Tenant) ID**

Onboarding steps

1. From the Management Console, select **Administration > App Management**, and click **Add New**.
2. Select **Azure**. Then, enter the details for the application.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select one or more of the following protection models for the application and click **Next**.
 - **Cloud Authentication**
 - **API Access**
 - **Cloud Security Posture**

Note The **Cloud Security Posture** protection model is required if you want to implement Cloud Security Posture Management (CSPM) functionality.
5. Depending on the protection models you selected, enter the required configuration details.



The screenshot shows a form titled "CSPM Settings" with five input fields:

- Service Principal's Application Id
- Service Principal's Client Secret
- Service Principal's Directory Id
- Subscription Id
- Sync Interval(1-24 Hrs)

- If you selected **App Authorization**, no additional configuration is required. Click **Next** to view the summary information.
 - If you selected **App Access** or **API Access**, no additional configuration is needed other than authorization. Go to the **Authorization** step.
 - If you selected **Cloud Security Posture**, enter the following information from the Azure configuration steps you performed earlier.
 - **Service Principal's Application Id**
 - **Service Principal's Client Secret**
 - **Service Principal's Directory Id**
 - **Subscription Id**
 - **Sync Interval** (1-24 Hrs) is how often (in hours) that CSPM will retrieve information from the cloud and refresh the inventory. Enter a number.
6. Click **Authorize** and enter your Azure login credentials.
 7. Review the summary information to verify that it is correct. If it is, click **Save** to complete onboarding.

Onboarding Azure Blob applications

This section outlines the procedures for onboarding Azure Blob Storage cloud applications.

Notes

- Lookout does not support Azure Data Lake Storage generation 2 storage accounts. Lookout is unable to log activity or take actions on blobs using this storage type.
- Lookout does not support content-related actions on immutable containers, due to retention and legal hold policies enforced by Azure.

Configuration steps

In preparation for onboarding Azure Blob, do the following:

- Ensure that you have an active Azure account and that you have the Subscription ID of the account.
- Ensure that your Azure subscription has at least one storage account with the storageV2 type.
- Ensure that you have a storage account to use for quarantine actions. You will be prompted to select the storage account during onboarding. You can use an existing storage account, or, if you prefer, create a new dedicated storage account for quarantine.
- Create a new custom role at the subscription level, and assign it to an admin account. This will be used for authorization on the Lookout Management Console. See details for this step below.
- Ensure that your Azure account has the EventGrid resource registered. See details for this step below.

Creating a custom role

1. Copy the following code into a new text document.

```
{
  "properties": {
    "roleName": "lookoutCASBrole",
    "description": "Lookout CASBrole",
    "assignableScopes": ["/subscriptions/<Subscription-ID>"],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/encryptionScopes/read",
          "Microsoft.Storage/storageAccounts/blobServices/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/write",
          "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/read",
          "Microsoft.Storage/storageAccounts/queueServices/read",
          "Microsoft.Storage/storageAccounts/queueServices/queues/write",
          "Microsoft.EventGrid/eventSubscriptions/delete",
          "Microsoft.EventGrid/eventSubscriptions/read",
          "Microsoft.EventGrid/eventSubscriptions/write",
          "Microsoft.Storage/storageAccounts/write",
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.EventGrid/systemTopics/read",
          "Microsoft.EventGrid/systemTopics/write",
          "Microsoft.Insights/eventtypes/values/Read",
          "Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticSettings/read"
        ],
        "notActions": [],
        "dataActions": [
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/permanentDelete/action",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteBl"
        ]
      }
    ]
  }
}
```



```
obVersion/action", "Microsoft.Storage/storageAccounts/queueServices/queues/
messages/read", "Microsoft.Storage/storageAccounts/queueServices/queues/mes
sages/delete"], "notDataActions": []]]}]}
```

2. Replace the text "<Subscription-ID>" with the subscription ID for your Azure account. If desired, you can also replace the `roleName` and `description` values.
3. Save the text file with a .json extension.
4. In the Azure console, **navigate to Azure Subscription > Access Control (IAM)**.
5. Click **Add** and select **Add custom role**.
6. For **Baseline Permissions**, select **Start from JSON**.
7. Use the file browser to select and upload the .json file that you saved in step 2 above.
8. If needed, enter or update the name and (optional) description of your new role.
9. Select **Review + Create** to see all settings for your new role.
10. Click **Create** to finish creating the new role.
11. Assign the new role to a user with admin permissions on your Azure account.

Registering the EventGrid resource

1. In the Azure console, navigate to **Azure Subscription > Resource Providers**.
2. Use the filter field to search for Microsoft.EventGrid. Select it and click **Register**.

Onboarding steps

1. From the Management Console, select **Administration > App Management** and click **+New**.
2. Select **Azure**. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Click **Next**.
3. Select **Microsoft Azure Blob Storage** and click **Next**.
4. Select **API Access** (required). If needed, you can also select **Cloud Security Posture** (optional). Click **Next**.
5. For both Azure and Azure Blob Storage, click the **Authorize** button and enter the credentials for the account that you assigned your new role to in the previous section. If prompted, click **Accept** to give Lookout permissions on your Azure account.
6. After you have authorized both accounts, the **Subscription Id** field appears. Select your Azure subscription.
7. The **Destination Storage Account** field appears. Select the storage account that you want to use as a quarantine container.
8. Click **Next**.
9. Ensure that the details shown on the summary page are correct. If they are, click **Next** to finish onboarding.

Onboarding the Google Workspace suite and applications

This section outlines the procedures for onboarding Google Workspace (formerly G Suite) along with Gmail and Google Drive applications.

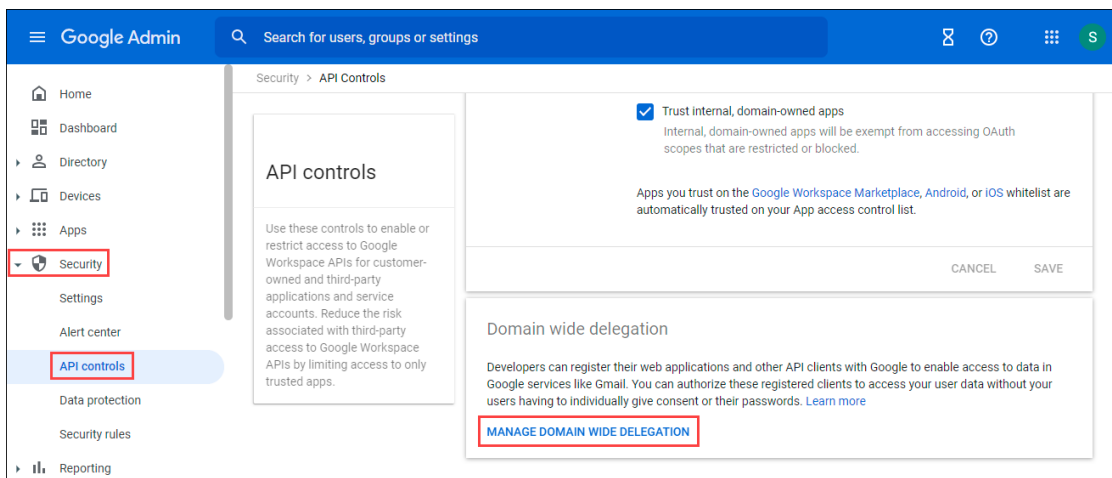
Configuration steps

The enterprise account used for Google Drive must be part of the Google Workspace business plan.

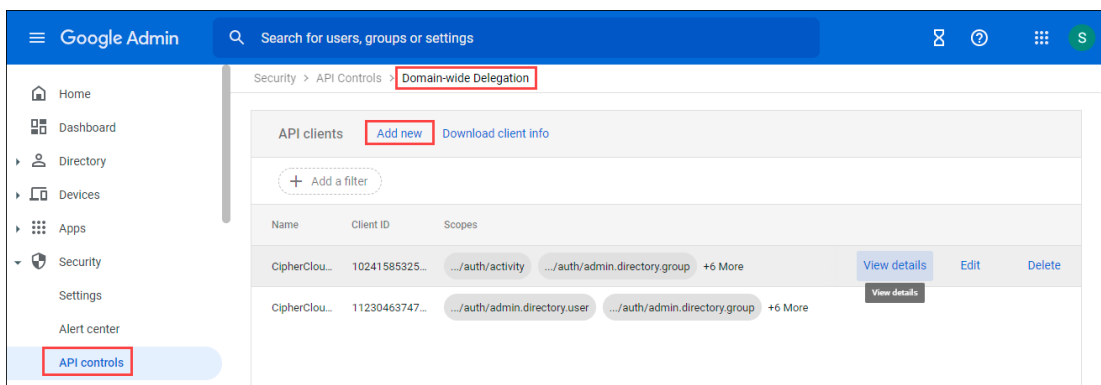
The authenticated user must be an administrator with super admin privileges.

Updating API access settings

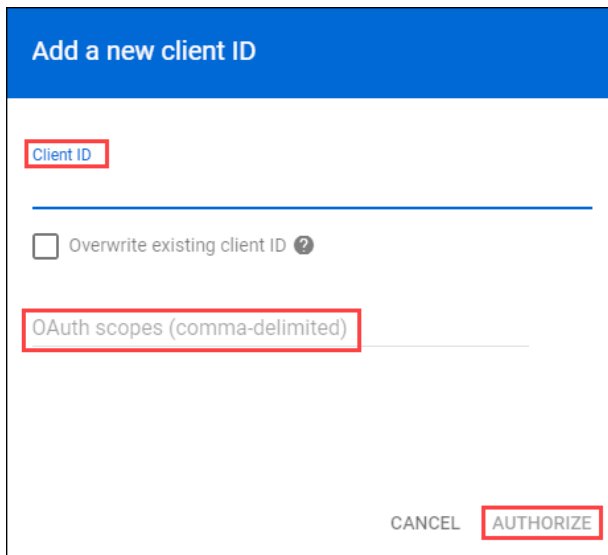
1. Log in to the Google Workspace application and click **Security** from the left panel.



2. Under Security, click **API controls**.
3. Scroll down and click Manage **Domain-wide Delegation**.



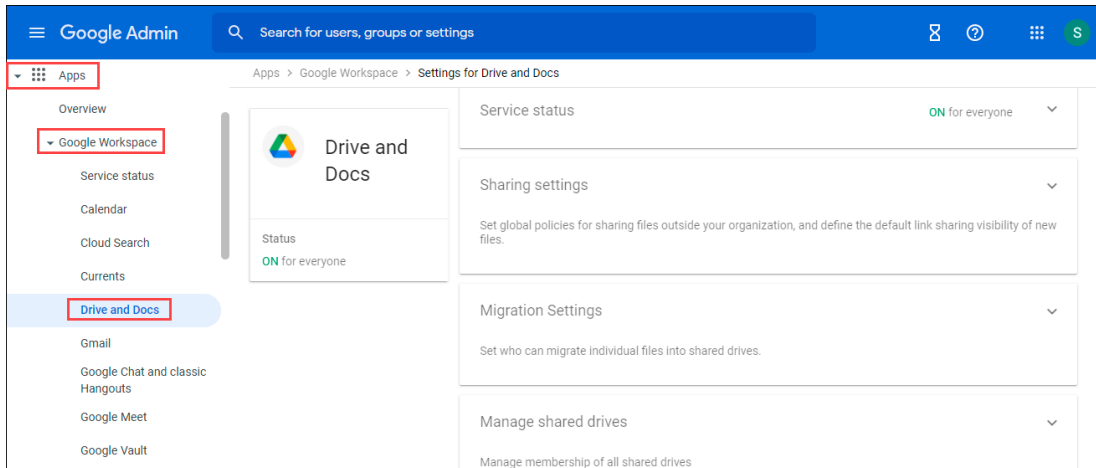
4. Click **Add New**.



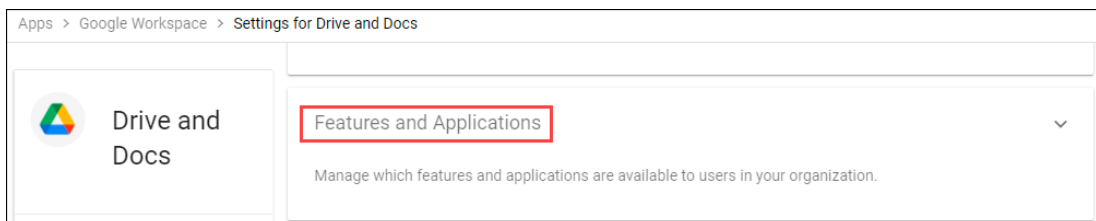
5. Enter the **Client ID**:
`102415853258596349066`
6. Enter the following **OAuth scopes**:
`https://www.googleapis.com/auth/activity,`
`https://www.googleapis.com/auth/admin.directory.group,`
`https://www.googleapis.com/auth/admin.directory.user,`
`https://www.googleapis.com/auth/admin.reports.audit.readonly,`
`https://www.googleapis.com/auth/drive,`
`https://www.googleapis.com/auth/drive.activity.readonly,`
`https://www.googleapis.com/auth/admin.directory.user.security,`
`https://www.googleapis.com/auth/userinfo.email`
7. Click **Authorize**.

Updating folder access information

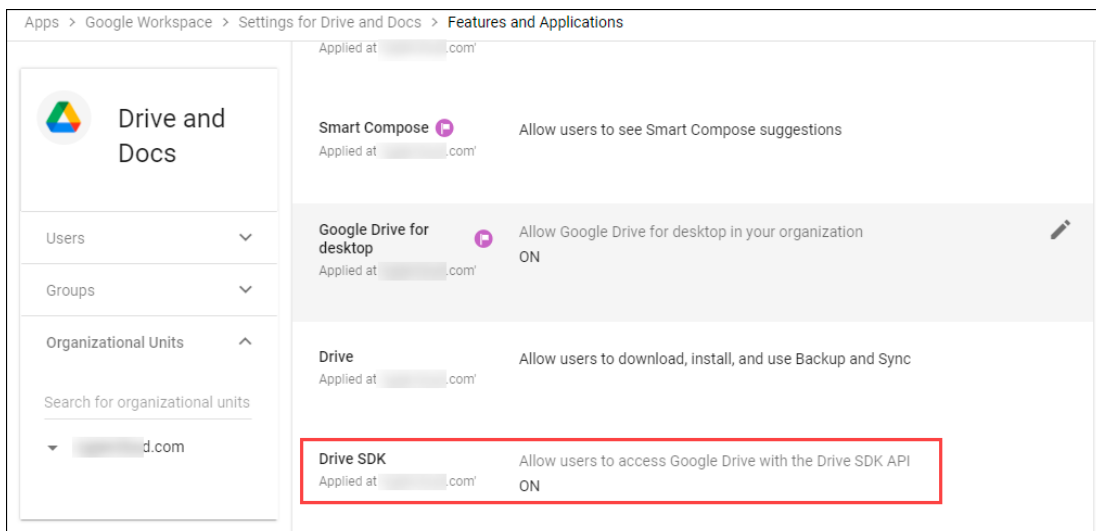
1. From the left panel, click **Apps > Google Workspace > Drive and Docs**.



2. Scroll down and click **Features and Applications**.



3. Make sure that **Drive SDK** is on.



Onboarding steps in Secure Cloud Access

1. From the Management Console, select **Administration > App Management** and click **New**.
2. Select **Google Workspace** from the list.

3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select any or all of the following Google Workspace applications:
 - **Gmail (Web App)** – For standard Gmail traffic
 - **Gmail (SMTP)** – For Gmail traffic processed through the Lookout gateway
 - **Other Apps** (Other Google applications)
 - **Google Drive**
5. Click **Next** and select one or more **protection models**.

The available protection models depend on the applications you selected in the previous step. The following table lists the protection modes available for each Google Workspace application.

Google Workspace application	Protection models available
Gmail (Web App)	App Authentication App Access Dynamic DRM
Gmail (SMTP) (Available based on customer license)	Email
Other Apps	App Authentication App Access Dynamic DRM
Google Drive	App Authentication App Access API Access Dynamic DRM Cloud Data Discovery

Note Some protection models require one or other models to be enabled or must be selected for specific functions.

- **App Authentication** requires either **API Access** or **App Access** protection modes to be enabled.
 - **Dynamic DRM** requires either **API Access** or **App Access** protection modes to be enabled.
 - **Cloud Data Discovery** must be selected if you want to implement Cloud Data Discovery (CDD) for this cloud application. You must also select **API Access** protection mode as well.
6. Click **Next**.
 7. Enter the following configuration information. The fields you see depend on the protection models you selected.
 - **Proxy** settings (required mainly for **App Access** protection mode)

The screenshot shows a configuration window with two main sections: 'Proxy' and 'API Settings'.

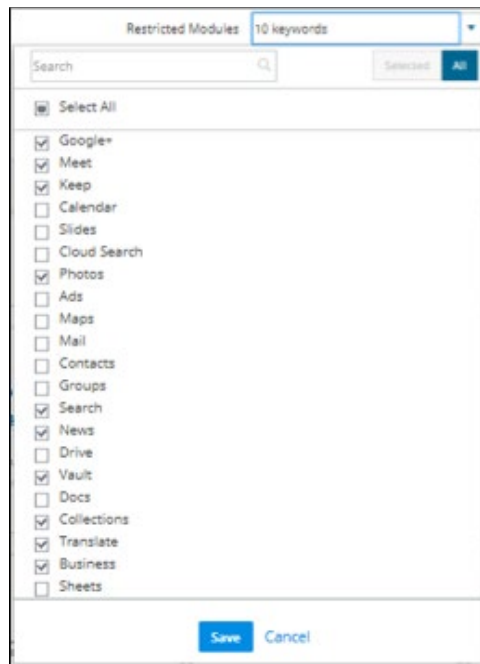
Proxy Section:

- Custom HTTP Header Name:** A text field containing 'X-GooGApps-Allowed-Domains'.
- Custom HTTP Header Value:** An empty text field.
- Login Domain:** A dropdown menu showing '-- Select keywords --' with a blue edit icon to its right.
- Restricted Modules:** A dropdown menu showing '10 keywords' with a downward arrow.
- Restriction Behavior:** A dropdown menu showing 'Block' with a downward arrow.
- Specific Domains:** A dropdown menu showing '-- Select keywords --' with a blue edit icon to its right.

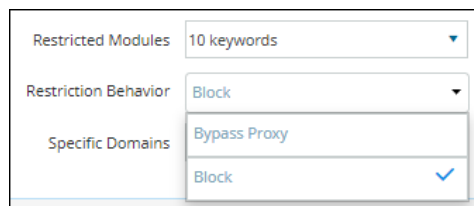
API Settings Section:

- Internal Domains:** An empty text field.

- The **Custom HTTP Header Name** and **Custom HTTP Header Value** fields are configured on the cloud type level (as opposed to the cloud application level). If this is the **first** Google Workspace cloud application you are onboarding, the values you enter in these two fields will apply to all other Google Workspace cloud applications you onboard.
- If this is **not** the first Google Workspace cloud application you are onboarding, these field values will be initialized from the first onboarded Google Workspace cloud application. If all of your onboarded Google Workspace cloud applications must be independent of one another, make sure that the **Custom HTTP Header Value** field is empty for all of your Google Workspace cloud applications.
- **Login Domain** -- Enter your enterprise business domain name.
- The **Restricted Modules** and **Restriction Value** fields are configured on the cloud type level (as opposed to the cloud application level). If you are onboarding multiple Google Workspace applications, make sure that the module configurations are the same for all of the applications.
- **Restricted Modules** – Whether a module will be able to bypass the proxy or be blocked.
 - **Unchecked** – Unchecked modules/applications will go through the proxy.
 - **Checked** – Check modules/applications will behave according to the Restriction Behavior selections.



- **Restriction Behavior** – How Google Workspace will restrict the selected modules.



- **Bypass Proxy** – The restricted modules will bypass the proxy.
 - **Block** – The restricted modules will be blocked.
- **Specific Domains** – Leave this field blank.

- **API Settings** (required for **API Access** protection mode)

The screenshot shows a configuration interface with the following sections:

- API Settings**: Contains an 'Internal Domains' text input field.
- Archive Settings**:
 - Permanent Delete**: 'Remove from Trash' and 'Archive' are disabled (greyed out).
 - Content Digital Rights**: 'Remove from Trash' and 'Archive' are enabled (green).
 - Time to retain archived files**: A text input field containing '30' followed by 'Days'.
- Authorization**: At the bottom, there is a Google Drive logo and a green 'Authorize' button.

- **Internal domains** – Enter necessary internal domains, along with enterprise business domain.
- **Archive Settings** (for Google Drive) -- Enables archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

Note When the authorized administrator for a cloud account is changed in Secure Cloud Access, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

Two options are available:

- **Remove from Trash**
- **Archive**

Archive Settings

Permanent Delete

Remove from Trash ☐

Archive ☐

Content Digital Rights

Remove from Trash ☒

Archive ☒

Time to retain archived files Days

For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Click the toggles to enable or disable the settings.

Enter the number of days for which to retain archived files. The default value is 30 days.

- **Authorization** -- If you selected Google Drive as one of your Google Workspace applications, authorize Google Drive and click **Next**.

Grant access to G Suite domain user data.

1. If you have just provisioned a new G Suite domain with no activity in Drive, please upload a file to your Google Drive account to ensure at least one event is present.
2. Go to your G Suite domain's [Admin console](#).
3. Click **Security**.
4. Click on **API Reference** and ensure *Enable API access* is checked.
5. While still on the Security page, click **Advanced Settings** (you may need to click **Show More** at the bottom of the page first).
6. Click **Manage API Client Access**.
7. Under **Client Name**, enter `112304637475516022006`
8. Under **One or More API Scopes**, enter
<https://www.googleapis.com/auth/admin.directory.user>,
<https://www.googleapis.com/auth/admin.directory.group>,
<https://www.googleapis.com/auth/admin.reports.audit.readonly>,
<https://www.googleapis.com/auth/drive>,
<https://www.googleapis.com/auth/drive.activity.readonly>.

Review the instructions in the screen that appears and click **Continue** to authorize access to your Google Drive account. Enter your account credentials.

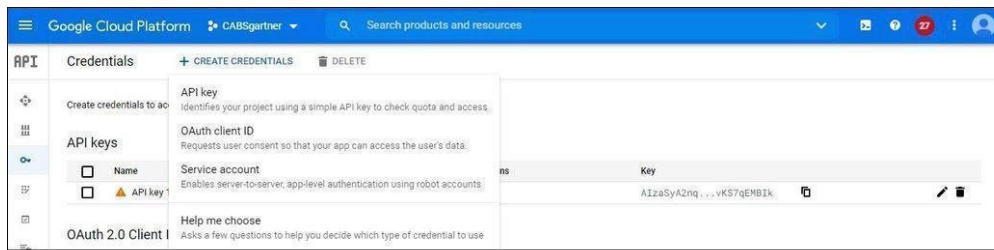
In the **Summary** page, review the summary information to verify that all information is correct. If it is, click **Save** to complete onboarding.

Onboarding Google Cloud Platform (GCP)

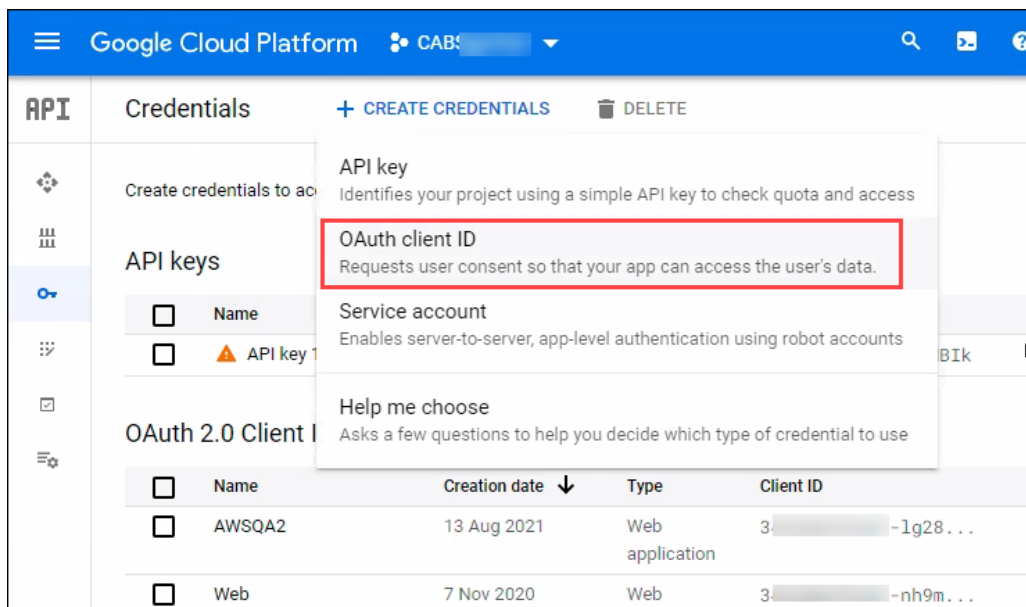
This section outlines procedures for configuration and onboarding of Google Cloud Platform applications.

Configuration steps

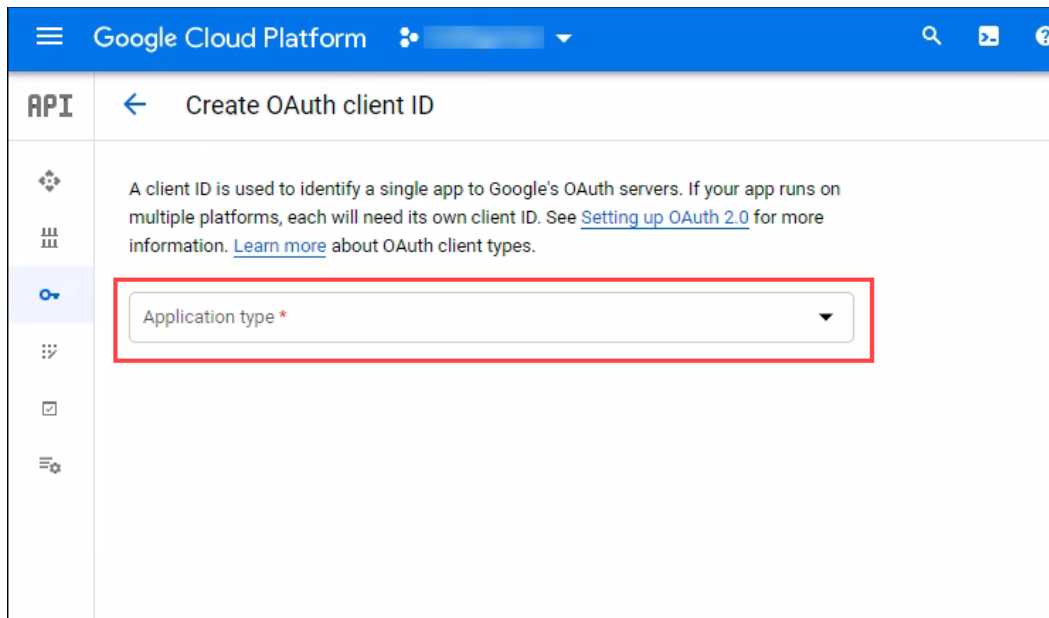
1. Create a service account in GCP Org. For more information, go to <https://cloud.google.com/docs/authentication/getting-started>
2. Create an OAuth client ID.
 - a. In the Google Cloud Platform, go to the **Credentials** page.



- b. From the **Projects** list, select the project containing your API.
 - c. From the **Create Credentials** dropdown list, select **OAuth client ID**.



- d. From the dropdown list, select **Web application** as the application type.



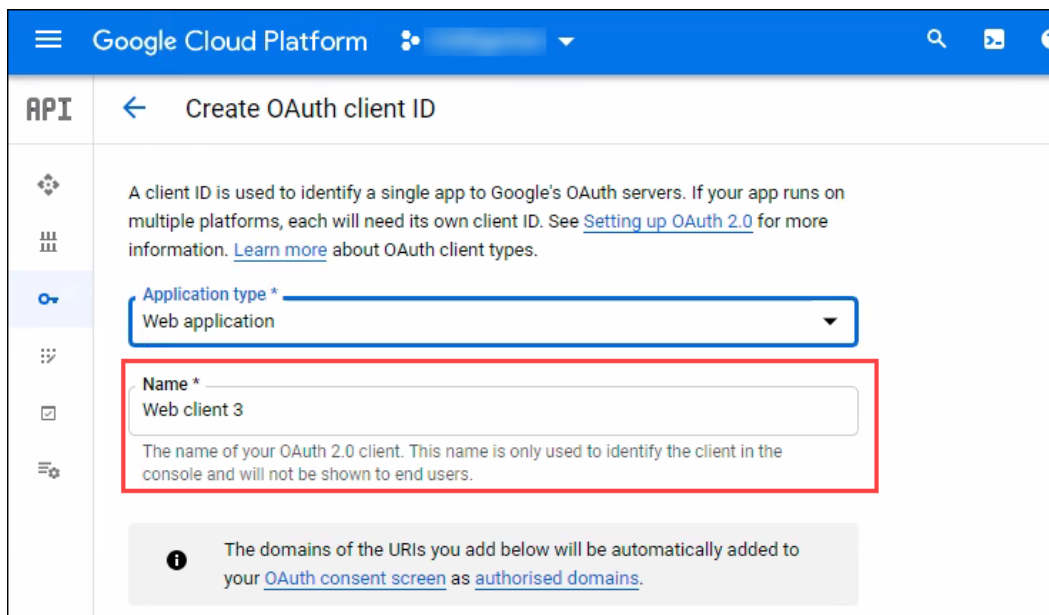
Google Cloud Platform

API < Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *

- e. In the **Application** field, enter a **Name**.



Google Cloud Platform

API < Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
Web client 3

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorised domains](#).

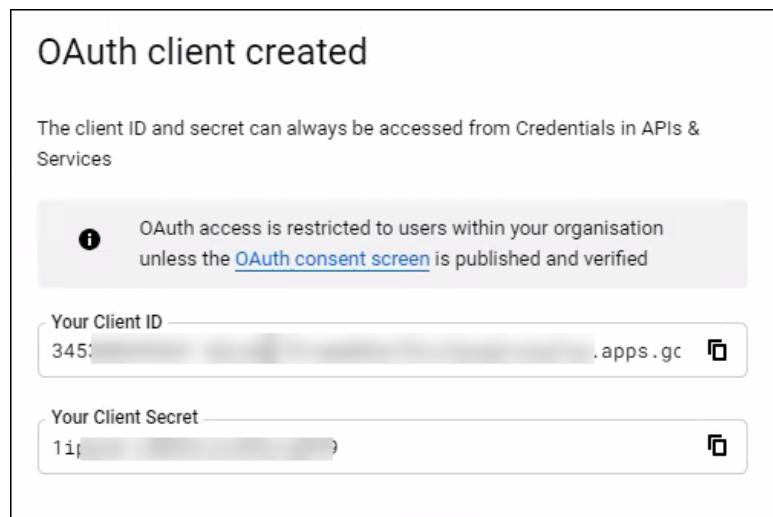
- f. Fill in the remaining fields as needed.
- g. To add a redirect URL, click **Add URI**.

The screenshot shows the 'Create OAuth client ID' page in the Google Cloud Platform console. The left sidebar contains a menu with icons for API, Authorized JavaScript origins, Authorized redirect URIs, and a key icon. The main content area has two sections: 'Authorized JavaScript origins' (For use with requests from a browser) and 'Authorized redirect URIs' (For use with requests from a web server). The 'Authorized redirect URIs' section is highlighted with a red box. Below this section are 'CREATE' and 'CANCEL' buttons.

- h. Enter the redirect URL and click **Create**.

The screenshot shows the 'Create OAuth client ID' page in the Google Cloud Platform console. The left sidebar contains a menu with icons for API, Authorized JavaScript origins, Authorized redirect URIs, and a key icon. The main content area has two sections: 'Authorized JavaScript origins' (For use with requests from a browser) and 'Authorized redirect URIs' (For use with requests from a web server). The 'Authorized redirect URIs' section is highlighted with a red box. Below this section is a text input field labeled 'URIs *' containing the URL 'https://cloudauth.ciphercloud.io'. Below the input field are '+ ADD URI' and 'CREATE' buttons.

A message appears with the client ID and the client secret. You will need this information when you onboard the Google Cloud Platform application.



Onboarding steps

1. From the Management Console, select **Administration > App Management**, and click **New**.
2. Select **GCP from the dropdown list**.

Tip To find an app, enter the first few characters of the app name, then select the app from the search results.

3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select one or more **protection models** and click **Next**.

The options are

- **API Access**
 - **Cloud Security Posture**
5. Enter the following configuration information. The fields you see depend on the protection models you selected in the previous step.
 - If you selected **API Access**, enter:
 - **Client Id**
 - **Client Secret**

This is the information created during the GCP pre-onboarding configuration steps. To review those steps, go back to **Configuration steps**.

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth access is restricted to users within your organisation unless the [OAuth consent screen](#) is published and verified

Your Client ID
345: [masked] .apps.g

Your Client Secret
1i [masked]

Be sure to enter exactly the same information in the **Client ID** and **Client Secret** fields here.

API Settings

Client Id

Client Secret

- If you selected **Cloud Security Posture**, enter:
 - **Service Account Credentials (JSON)** --The service account credentials for the JSON file you downloaded in the configuration steps.
 - **Sync Interval (1-24 Hrs)** – How often CSPM will retrieve information from the cloud and refresh the inventory. Enter a number.

CSPM Settings

Service Account Credentials (JSON)

Sync Interval(1-24 Hrs)

6. Click **Authorize**.

Authorization

Authorize

Previous **Next** **Cancel**

- If you selected only **Cloud Security Posture**, the **Summary** page appears. Review it and save the new GCP application to complete onboarding.
- If you selected **API Access** or both **API Access** and **Cloud Security Posture**, enter your GCP account login credentials when prompted.

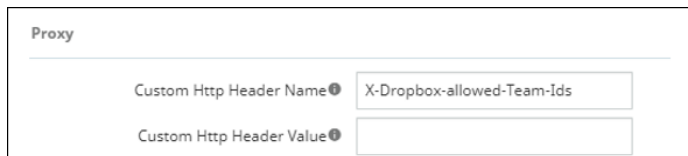
Note If you entered an invalid client secret or client ID on the **Configuration** page, an error message will appear after you click **Authorize**. Review your client secret and client ID entries, make any corrections, and click **Authorize** again. Once the system recognizes the entries as valid, enter your GCP login credentials when prompted.

After your GCP login credentials have been accepted, save the new GCP cloud application to complete onboarding.

Onboarding Dropbox applications

This section outlines procedures for onboarding Dropbox cloud applications.

1. From the Management Console, select **Administration > App Management**, and click **New**.
2. From the **Choose an app** list, select **Dropbox**.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. From the **Configuration** page, select one or more protection models:
 - **App Authentication**
 - **App Access**
 - **API Access**
 - **Dynamic DRM**
 - **Cloud Data Discovery (CDD)**
5. Enter the following configuration information. The fields you see depend on the protection modes you selected in the previous step.
 - If you selected *only* **App Authentication**, no other configuration is required. Click **Next**.
 - If you selected **App Access**, enter the following information.



Proxy

Custom Http Header Name ⓘ	X-Dropbox-allowed-Team-Ids
Custom Http Header Value ⓘ	

The **Custom HTTP Header Name** and **Custom HTTP Header Value** fields are configured on the cloud type level (as opposed to the cloud application level). If this is the **first** Dropbox cloud application you are onboarding, the values you enter in these two fields will apply to all other Dropbox cloud applications you onboard.

If this is **not** the first Dropbox cloud application you are onboarding, these field values will be initialized from the first onboarded Dropbox cloud application. If all of your onboarded Dropbox cloud applications must be independent of one another, make sure that the **Custom HTTP Header Value** field is empty for all of your Dropbox cloud applications.

- If you selected **API Access**, enter one or more internal domains.

You can also configure **Archive Settings**. These settings enable archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

Note When the authorized administrator for a cloud account is changed, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

The **Archive Settings** option is available for onboarded cloud applications with **API Access** and **Cloud Data Discovery** protection modes selected.

Two options are available:

- **Remove from Trash**
- **Archive**

For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Click the toggles to enable or disable the settings. If you select the **Archive** action, also select the **Remove from Trash** option.

Enter the number of days for which to retain archived files. The default value is 30 days.

Then, click **Authorize**, and enter your Dropbox administrator login credentials.

- If you selected **Dynamic DRM**, you must also select either **API Access** or **App Access**. Then, enter the configuration information needed for either of those protection modes.
6. Click **Next** and review a summary to verify that all information is correct. If it is, click **Save**. The new cloud application is added to the **App Management** page.

Onboarding the Atlassian Cloud suite and applications

This section outlines procedures for onboarding the Atlassian cloud suite and applications.

1. From the Management Console, select **Administration > App Management** and click **New**.
2. select **Atlassian** from the app list.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select the applications in the suite to include and click **Next**.

Application Clouds

<input type="checkbox"/> Jira Service Desk	<input checked="" type="checkbox"/> Confluence	<input type="checkbox"/> Other Apps
<input type="checkbox"/> Bitbucket	<input checked="" type="checkbox"/> Jira Software	

5. Select one or more **protection models**.

- **App Authentication**
- **App Access**
- **API Access**
- **Dynamic DRM**

Entering configuration settings for protection models

Enter required configuration information for the protection models you selected.

App Authentication

If you selected only **App Authentication**, no configuration information is required. Click **Next** to view the summary and save the cloud application.

App Access and Dynamic DRM

If you selected **Dynamic DRM**, you must select **App Access** as well.

1. Enter the following proxy-related information for **App Access** and **Dynamic DRM** protection.
 - **Enterprise Subdomain** – Enter a subdomain associated with this cloud application. For example, if the Atlassian URL is **mycompany.atlassian.net**, **mycompany** is the enterprise subdomain.
 - **Login Domain Prefix** – Enter the appropriate login prefix for the domain.
 - **Restricted Modules** – From the list, check the modules for which you want to block or bypass the proxy.
 - **Restriction Behavior** – Select either option:
 - **Bypass Proxy** – The modules selected for restriction will bypass the proxy.

- **Block** – The modules selected for restriction will be blocked.
2. Click **Next** to enter authorized user information for users or user groups.
 - a. Click **New**.
 - b. Select **User** or **User Group**.
 - c. For **User** –
 - Click in the **User** box; then select **All** or **Selected**.
 - For **All**, click **Save**.
 - For **Selected**, enter the valid usernames of the users to include and click **Save**.
 - d. Click **Add**.
 - e. For **User Group** –
 - Click in the **User Group** box. Drill down from the appropriate Directories list, select the user group, and click the right-arrow symbol to move it to the **Selected** list.
 - Click **Save**.
 - Click **Add**.

The users and user groups you added appear in the **Authorized Users** list.

3. Click **Next**. If you want to request a new key, click **Request New Key**. A key request will be sent to the administrator.
4. Click **Save** to save the settings.

API Access

1. Enter the following API access information.


API Settings

API Token

Polling Timezone

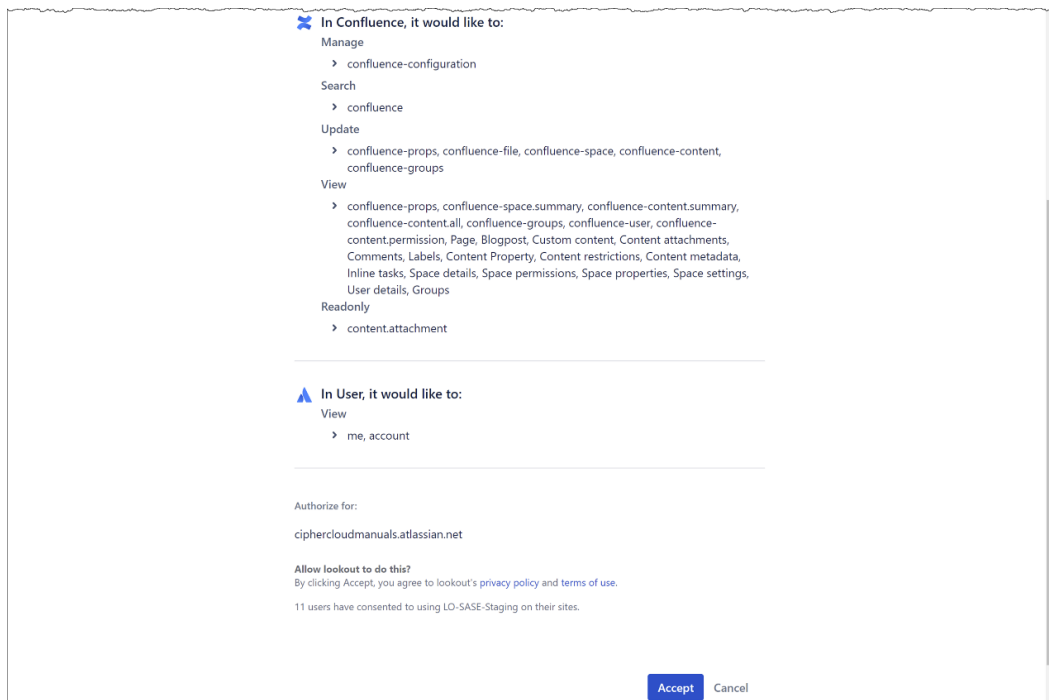
--Select--

Authorization

 Confluence

Authorize

- **API Token (Confluence applications only)** – Enter an API token. To create an API token from your Atlassian account, see the following section, **Generating an API Token**.
- **Polling Timezone (Confluence applications only)** – Select a timezone for polling from the dropdown list. The selected timezone must be the same as that of the cloud application instance, not the timezone of the user.
- **Authorization** – Click the **Authorize** button next to *each* app included in the suite.
- When prompted, click **Accept** to authorize domain access for each of the selected apps.



The **Authorize** button labels will now say **Re-Authorize**.

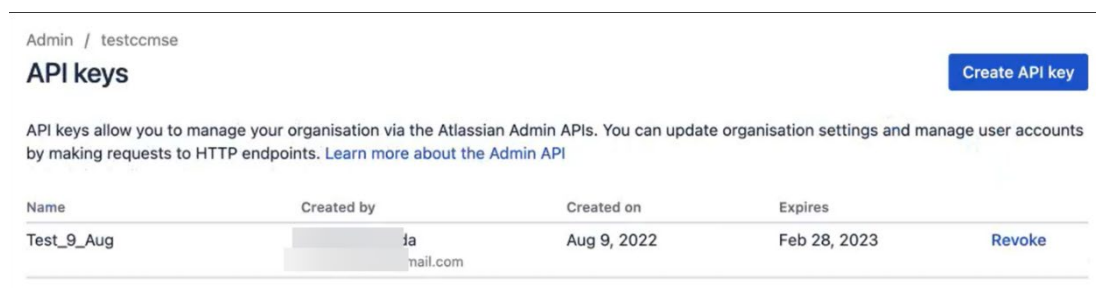
- **Domains** – For each app included in the suite, select the applicable domain or accept the domain shown. Select *only* domains that are included in the access authorization in the previous step.
2. Click **Next**.
 3. Review the information on the **Summary** page. Click **Save** to save and onboard the application.

Generating an API token (Confluence applications only)

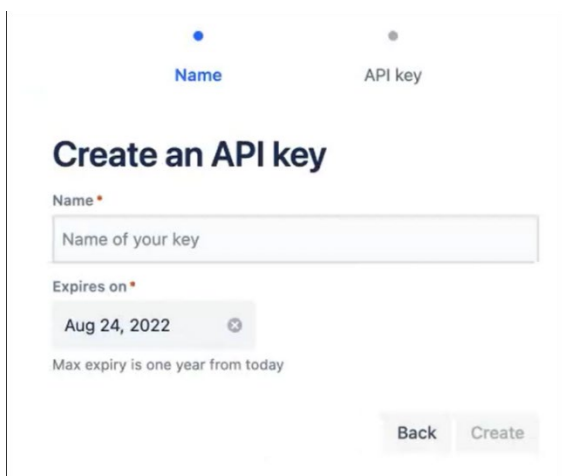
You can generate an API token for Confluence applications from your Atlassian account.

1. Log into your Atlassian account.
2. Select **Administration** from the left menu.
3. From the **Administration** page, select **API Keys** from the left menu.

Any API keys you created previously are listed.



4. Click **Create API Key** to generate a new key.



The screenshot shows a web form titled "Create an API key". At the top, there are two tabs: "Name" (selected, indicated by a blue dot) and "API key" (indicated by a grey dot). The form contains two main sections. The first section, under the "Name" tab, has a label "Name" with a red asterisk, followed by a text input field containing the placeholder text "Name of your key". The second section, under the "Expires on" label with a red asterisk, features a date picker showing "Aug 24, 2022" with a clear icon (an 'x' in a circle). Below the date picker, a note states "Max expiry is one year from today". At the bottom right of the form, there are two buttons: "Back" and "Create".

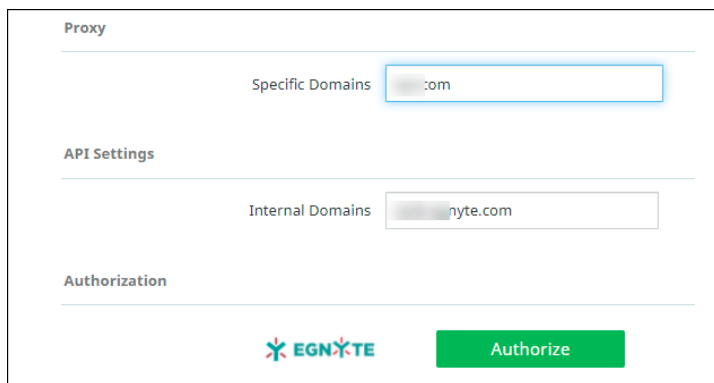
5. Give the new key a **name** and select an **expiration date**. Then, click **Create**.

The new API key is created and is added to the list of keys on the **Administration** page. For each key, the system generates an alphanumeric string that serves as the API token. Enter this string in the **API Token** field in the Secure Cloud Access Management Console.

Onboarding Egnyte applications

This section outlines the procedure for onboarding an Egnyte cloud application.

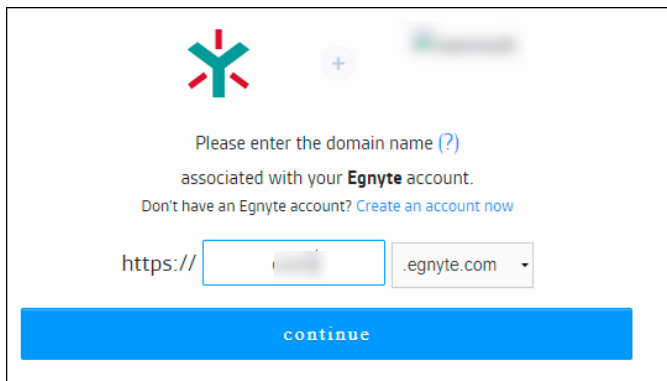
1. Go to **Administration > App Management** and click **New**.
2. Choose **Egnyte** from the dropdown list and click **Next**.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select one or more available **protection models**:
 - **App Authentication**
 - **App Access**
 - **API Access**
 - **Dynamic DRM**
5. Click **Next** and enter the following configuration information, depending on the protection modes you selected:
 - If you selected only **App Authentication**, no configuration settings are required. Click **Next** to view the summary and save the cloud application.
 - If you selected **App Access**, enter one or more domain names, separating each name with a comma.
 - If you selected **API Access**, click **Authorize Egnyte**, and enter your Egnyte login credentials.
 - If you selected *both* **API Access** and **App Access**, enter one or more domain names, then click **Authorize Egnyte**.



The screenshot shows a configuration form for Egnyte. It is divided into three sections: **Proxy**, **API Settings**, and **Authorization**. In the **Proxy** section, there is a label 'Specific Domains' followed by a text input field containing '.com'. In the **API Settings** section, there is a label 'Internal Domains' followed by a text input field containing 'nyte.com'. At the bottom of the form, there is the Egnyte logo (a stylized 'X' with 'EGNYTE' text) and a green button labeled 'Authorize'.

- If you selected *only* **Dynamic DRM**, you must also select either **API Access** or **App Access**.

6. Enter a domain name associated with your Egnyte account and click **Continue**.



The screenshot shows a web interface for configuring a domain. At the top, there is a logo consisting of a stylized 'Y' shape with red and green segments, followed by a plus sign in a circle and a blurred text element. Below the logo, the text reads: "Please enter the domain name (?) associated with your **Egnyte** account." followed by a link: "Don't have an Egnyte account? [Create an account now](#)". Below this is a text input field with "https://" on the left, a blurred domain name in the center, and a dropdown menu showing ".egnyte.com" on the right. At the bottom is a large blue button labeled "continue".

7. Once your authorization is successful, save the new cloud application.

Onboarding Figma applications

1. Go to **Administration > App Management** and select **New**.
2. Select **Figma** from the list.
3. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
4. Select one or more **protection models** and click **Next**.

The screenshot shows a four-step onboarding process: Basic, Protection Model, Configuration, and Summary. The 'Protection Model' step is currently active. Below the progress bar, there are three toggle switches: 'App Authentication', 'App Access', and 'Dynamic DRM', all of which are currently turned off.

5. Configure the settings for the protection models you selected.

App Authentication

1. Enter user access information.
2. Enter authorized user information for users or user groups and click **New**.

The screenshot shows the 'Authorized Users' interface. At the top, there is a '+ New' button, a search bar, and icons for checkmark, download, and help. Below this is a table with columns: USERS/GROUPS, TYPE, PERMISSIONS, and ACTIONS. The table is currently empty, displaying a message 'No data available.' At the bottom of the table, there are pagination controls: 'First', '<', '>', and 'Last'. At the very bottom of the interface, there are three buttons: 'Previous', 'Next', and 'Cancel'.

3. Select **User** or **User Group**.
For **User** –
 - a. Click in the **User** box; then select **All** or **Selected**.
 - b. For **All**, click **Save**.
 - c. For **Selected**, enter the valid email addresses of the users to include, and click **Save**.

Search

☐ All ☒ Selected

j[redacted]e@lookout.com, jan[redacted]:@lookout.com

Save Cancel

d. Click **Add**.

For **User Group** –

- a. Click in the **User Group** box. Drill down from the appropriate Directories list, select the user group, and click the right-arrow symbol to move it to the **Selected** list.

< File Services

Selected User Groups

NAME	Name
Bob_Group	
Feller_Group	
Mohit_Group	
Tessa_Group	File Services / Tessa_Group

Save Cancel

b. Click **Save**.

c. Click **Add**.

The users and user groups you added appear in the **Authorized Users** list.

Authorized Users			
+ New		Search	3 total
USERS/GROUPS	TYPE	PERMISSIONS	ACTIONS
[redacted]te@lookout.com	User	Allow	
[redacted]doe@lookout.com	User	Allow	
[redacted]it_Group	User Group	Allow	

4. Click **Next**.
5. Review the information on the **Summary** page. Click **Save** to save and onboard the application.
The Figma application is added to the **Managed Apps** list.


App Access

1. Enter proxy information.

Proxy

Figma Tenant Identifier Domain Prefix

Home Page Url

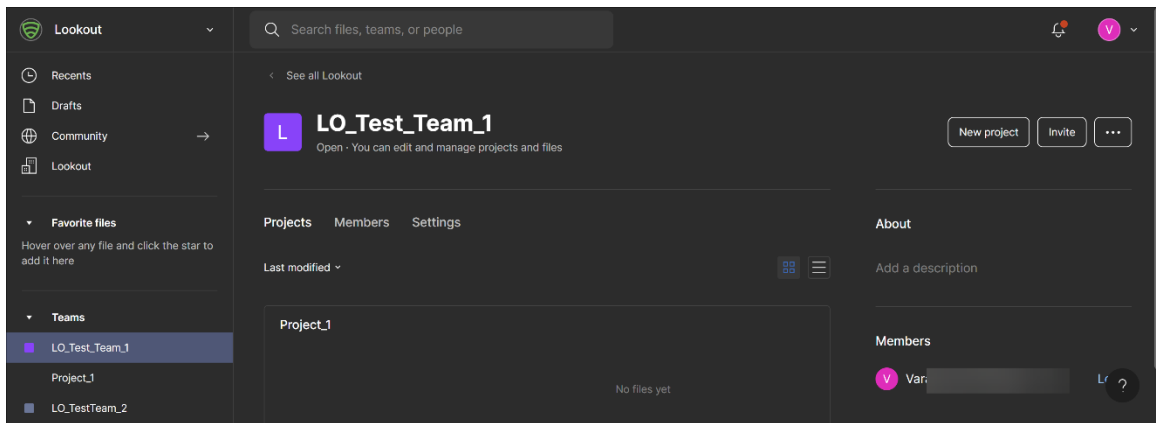
Specific Domains 

- **Figma Tenant Identifier Domain Prefix** – Enter the name of the domain and the team IDs specified in Figma (see the following section for information about Team IDs). Separate each team ID with a comma.
 - **Home Page URL** – The URL for the application home page appears.
 - **Specific Domains** – Enter any specific domains used with the application. Click **Next**.
2. Enter user access information. Perform the steps for adding authorized users and groups as outlined in the **App Authentication** section.
 3. Review the information in the **Summary** page. Click **Save** if the information is correct, or **Previous** to make any corrections.

The Figma application is added to the **Managed Apps** list.

Capturing team IDs from the Figma application

To obtain Figma team information, log in to Figma and select **Teams** from the left menu. The teams are listed with the project information for each team.



Dynamic DRM

If you choose DRM, you must also choose either **App Access** or **App Authentication**. The configuration values for those protection modes will apply.

Onboarding Box applications

This section outlines prerequisite configuration and onboarding steps for Box applications.

Configuration steps in the Box Admin Console

For connectivity to Box cloud applications, several user account settings are required to enable proper policy creation and visibility into Box user activities.

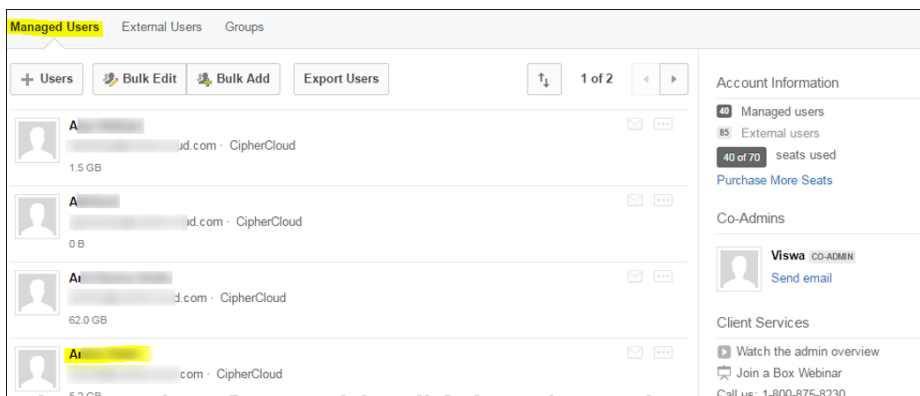
Perform the following steps to configure the ADMIN account for a Box cloud application.

Note The ADMIN account is required for authorization of a Box cloud application. Authorization or re-authorization cannot be completed with CO-ADMIN (co-administrator) account credentials.

1. Log in to Box using the ADMIN credentials for the Box account.
2. Click the **Admin Console** tab.



3. Click the **Users** icon.
4. From the **Managed Users** window, select the admin account you want to validate and use to connect to your Box cloud application.

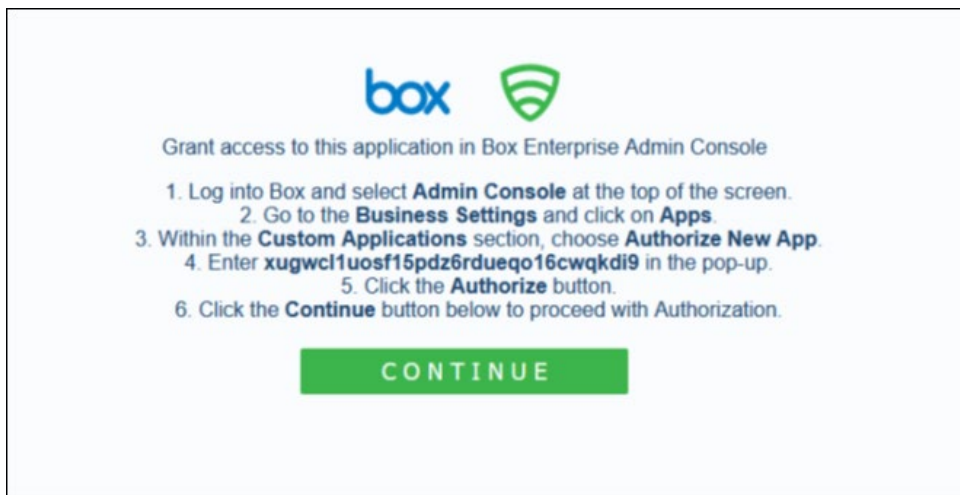


5. Expand the **User Account** information.
6. In the Edit User Access Permissions window, be sure that Shared contacts / Allow this user to see all managed users is checked.

Note Do **not** allow co-administrators to monitor other co-admin activities. Only an administrator should monitor other co-admin activities.

7. Go to **Apps > Custom Apps**.

8. Choose **Authorize New App**.
9. In the pop-up window that appears, enter the following string:
xugwcl1uosf15pdz6rdueqo16cwqkdi9
10. Click **Authorize**.
11. Click **Continue** to confirm access to your Box enterprise account.



Onboarding steps in the Management Console

1. Go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **Box** from the list.
4. Enter a **Name** (required) and a **Description** (optional).
5. Click **Next** and select one or more available **protection models**:
 - **App Authentication**
 - **App Access**
 - **API Access**
 - **Dynamic DRM**
 - **Cloud Data Discovery**
6. Click **Next** and enter the configuration information. The fields you see on the **Configuration** screen depend on the deployment and the protection modes you chose in the previous step.
7. Enter the information needed for each protection model you select.
 - For **App Authentication** (Login CAC) -- No configuration details are needed. Click **Next** to display the summary information.
 - For **App Access** -- In the **Proxy** section, enter:
 - The **Enterprise Subdomain** for your organization (for example, **mycompanyinc**)

- One or more **Specific Domains** used in your organization (for example, **mycompanyinc.app.box**). Click **Save** to save the list.

- For **Dynamic DRM** – You must also choose either **App Access** or **App Authentication** protection modes.
- For **Cloud Data Discovery** -- You must also choose the **API Access** protection mode.
- For **API Access** – In the **API Settings** section, enter a valid **Admin Email** address for the Box account. *This address must be for the Admin account and not for a co-admin account.* Then, enter names of **Internal Domains**.

- **For API Access – Archive Settings** enable archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

Note When the authorized administrator for a cloud account is changed, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

The **Archive Settings** option is available for onboarded cloud applications with **API Access** protection mode selected.

Two options are available:

- **Remove from Trash**
- **Archive**

Archive Settings

Permanent Delete

Remove from Trash ☐

Archive ☐

Content Digital Rights

Remove from Trash ☒

Archive ☒

Time to retain archived files Days

For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Click both toggles to enable or disable the settings.

Enter the number of days for which to retain archived files. The default value is 30 days.


Note For Box applications, the original files are **not** removed from the Trash.

For **API Access**, enter the **Enterprise ID** used to authorize access to Box.

Identity

Enterprise Id

8. When you have entered the required configurations, click **Next** to authorize access to Box.
9. In the **Grant Access to Box** screen, enter the Enterprise ID for this Box account, and click **Continue**.

box 

Grant access to this application in Box Enterprise Admin Console

1. Log into Box and select **Admin Console** at the top of the screen.
2. Go to the **Business Settings** and click on **Apps**.
3. Within the **Custom Applications** section, choose **Authorize New App**.
4. Enter **xugwcl1uosf15pdz6rduqo16cwqkd9** in the pop-up.
5. Click the **Authorize** button.
6. Click the **Continue** button below to proceed with Authorization.

CONTINUE

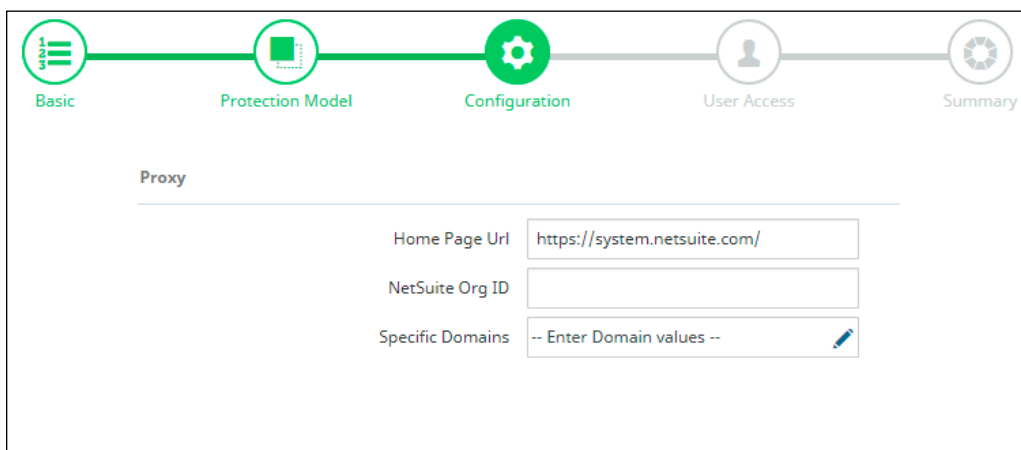
10. In the **Log in to Grant Access to Box** screen, enter the admin login credentials for the Box account, and click **Authorize**.

If the administrator has configured an SSO setup, click the **Use Single Sign On (SSO)** link and enter the credentials to authenticate. Any multi-factor authentication information is submitted.

The Box cloud application is onboarded and added to the list of managed applications in the **App Management** page.

Onboarding NetSuite applications

1. Go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **NetSuite** from the dropdown list and click **Next**.
4. Enter a **Name** (required) and a **Description** (optional). Then click **Next**.
5. Select one or more **protection models**.
 - **App Authentication**
 - **App Access**
 - **Dynamic DRM**
6. Click **Next** to enter configuration details.



Basic Protection Model Configuration User Access Summary

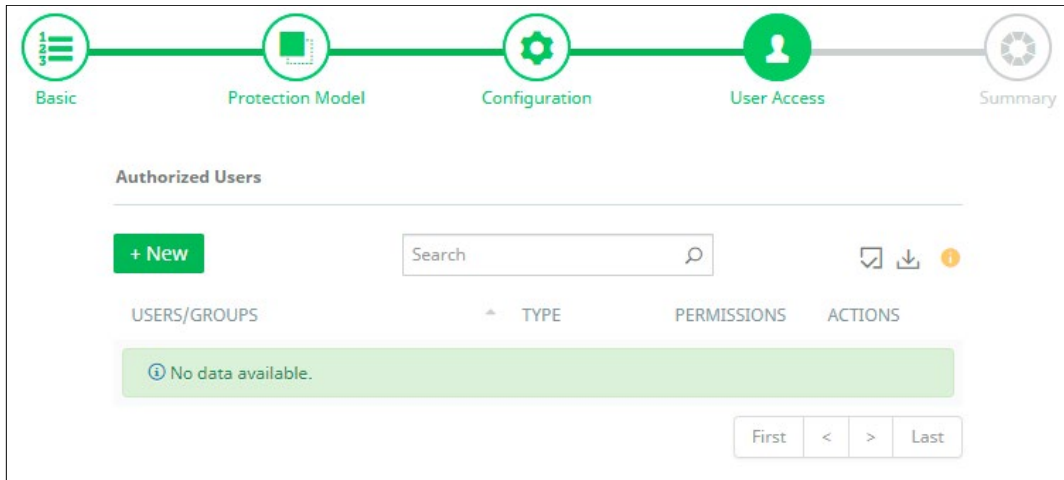
Proxy

Home Page Url

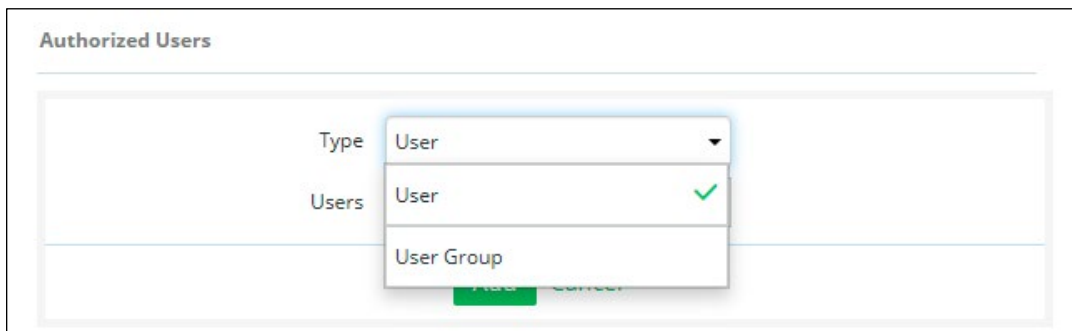
NetSuite Org ID

Specific Domains

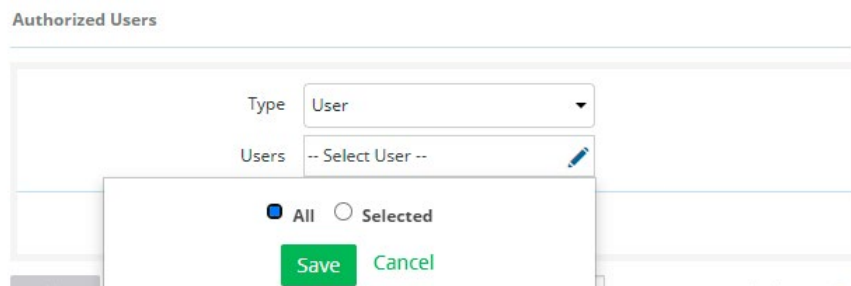
- **Home Page URL** -- The Home Page URL is prepopulated as shown.
 - **NetSuite Org ID** -- Enter the NetSuite Org ID. This is a prefix of the NetSuite domain, which is identifiable with the licensing company.
 - **Specific Domains** (optional) -- Enter the NetSuite domains relevant to the Org ID. Separate each domain name with a comma.
7. Click **Next**.
 8. Under **User Access**, click **New**.



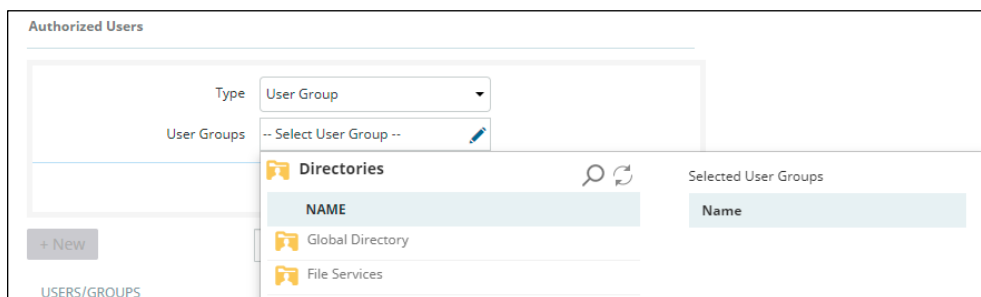
9. From the **Type** dropdown list, select **User** or **User Group** to specify the users or user groups allowed to access this application.



- If you selected **User**, select either **All** (allows access by all users) or **Selected** (allows access by users you specify by their valid email addresses).



- If you selected **User Group**, select the user groups from the directories.



10. Click **Add**.

11. Click **Next** and click **Save**.

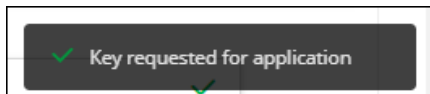
Assigning a key for the application

To assign a key to the onboarded application, modify the application settings as follows.

1. Go to **Administration > App Management** and open the onboarded application by clicking the pencil icon.
2. Go to the **Keys** page.



3. Click **Request New Key**. A request is generated to assign a new key from the available keys. A message appears at the lower right portion of the screen confirming the key request.



You can also create a new key and assign it to the application. To create a new key, go to **Administration > Key Management** and create the key. For more information, see [Assigning, creating, and managing keys](#).

4. Click **Save**.

Note For policy configuration, the current release supports the **All Activities**, **Upload**, **Download**, **Import**, and **Export** options for the NetSuite application.

Onboarding Salesforce applications

Configuration steps

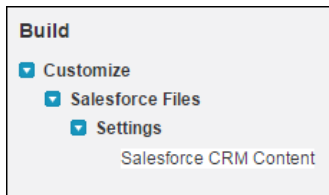
Secure Cloud Access for Salesforce scans standard objects such as Accounts, Contacts, Campaigns, and Opportunities, as well as custom objects. Configure Salesforce as described in the following sections.

- **Enable CRM content**
- **Enable scanning for structured data**
- **Enable permissions for DLP scanning**
- **Enable permissions for viewing event log files**
- **Enable permissions for Audit Trail events**
- **Enable permissions for Login History events**

Enable CRM content

For DLP scanning to work with Salesforce, the **Enable CRM** setting must be enabled in Salesforce for all users. To enable Salesforce CRM content, log in to your Salesforce account and perform the following steps:

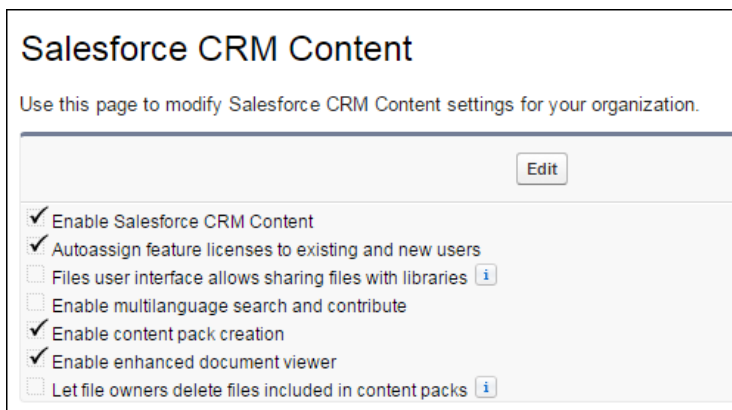
1. Using the **Quick Find** box at the top left, search for **Salesforce CRM Content**.



2. From the search results, click the **Salesforce CRM Content** link.

The **Salesforce CRM Content** settings box appears.

3. If the Enable Salesforce CRM Content and Autoassign feature licenses to existing and new users options are not checked, check them.



Enable scanning for structured data

If you are working with structured data, be sure that the **Structured Data** option is enabled.

Enable permissions for DLP scanning

System administrators have global access to Salesforce standard and custom objects. For non-administrators, the **Push Topics** and **API Enabled** permissions must be enabled for DLP to work, as follows.

To set the Push Topics option:

1. From the **Manage Users** menu, select **Users**.
2. From the **All Users** page, select a user.
3. In the **User Detail** page for that user, click the **Standard Platform User** link.

	Basic Access				Data Administration			Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Feedback Templates	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Coaching	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Goals	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Contacts	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Goal Links	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
D&B Companies	✓						Ideas	✓	✓				
Documents	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Metrics	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Metric Data Links	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Questions	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Performance Cycles	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Question Sets	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Push Topics	✓	✓	✓	✓		
Feedback Requests	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Streaming Channels	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>

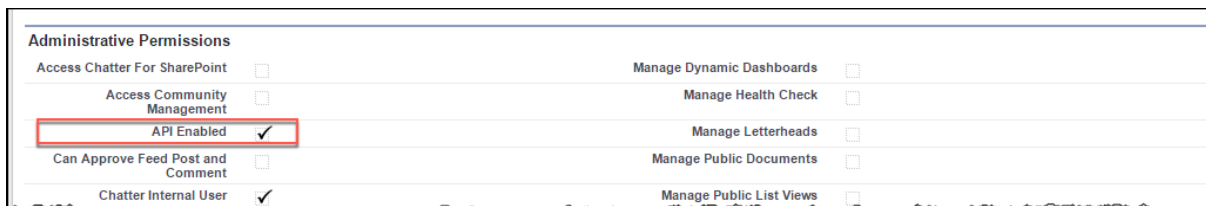
4. Scroll to the Standard Object Permissions section.

	Basic Access				Data Administration			Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Feedback Templates	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Coaching	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Goals	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Contacts	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Goal Links	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
D&B Companies	✓						Ideas	✓	✓				
Documents	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Metrics	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Metric Data Links	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Questions	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Performance Cycles	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Question Sets	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Push Topics	✓	✓	✓	✓		
Feedback Requests	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	Streaming Channels	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>

5. Under **Basic Access/Push Topics**, be sure that **Read**, **Create**, **Edit**, and **Delete** are checked.

To set the API Enabled option:

1. On the **Standard Platform User** page, scroll to the **Administrative Permissions** section.



Administrative Permissions	
Access Chatter For SharePoint	<input type="checkbox"/>
Access Community Management	<input type="checkbox"/>
API Enabled	<input checked="" type="checkbox"/>
Can Approve Feed Post and Comment	<input type="checkbox"/>
Chatter Internal User	<input checked="" type="checkbox"/>
Manage Dynamic Dashboards	<input type="checkbox"/>
Manage Health Check	<input type="checkbox"/>
Manage Letterheads	<input type="checkbox"/>
Manage Public Documents	<input type="checkbox"/>
Manage Public List Views	<input type="checkbox"/>

2. Be sure that **API Enabled** is checked.

Enable permissions for viewing event log files

To view event monitoring data, user permissions must be enabled for the **View Event Log Files** and **API Enabled** settings.

Users with **View All Data** permissions also can view event monitoring data. For more information, refer to the following link:

https://developer.salesforce.com/docs/atlas.en-us.api_rest.meta/api_rest/using_resources_event_log_files.htm

Enable permissions for Audit Trail events

To process **Audit Trail** events, permissions must be enabled for **View Setup and Configuration**.



View Setup and Configuration	<input checked="" type="checkbox"/>
------------------------------	-------------------------------------

Enable permissions for Login History events

To process **Login History** events, permissions must be enabled for **Manage Users**, which also enables permissions for the following settings:

- **Requires Reset User Passwords and Unlock Users**
- **View All Users**
- **Manage Profiles and Permission Sets**
- **Assign Permission Sets**
- **Manage Roles**
- **Manage IP Addresses**
- **Manage Sharing**
- **View Setup and Configuration**
- **Manage Internal Users**
- **Manage Password Policies**
- **Manage Login Access Policies**
- **Manage Two-Factor Authentication in User Interface**

Enable permissions for querying files

In order to enable Secure Cloud Access to access all file events, you must enable certain permissions for the admin user that you will use to onboard Salesforce.

1. In your Salesforce account, go to **Setup** and use the search box to search for **Permission Sets**.
2. Create a new permission set, giving it any name of your choosing.
3. Select **App Permissions**.
4. In the **Content** section, check the box for **Query All Files**.
5. Save the permission set.
6. Use the **Setup** search box to search for Users.
7. Click the name of the admin user that you will use to onboard Salesforce.
8. In the **Permission Set Assignments** section, click **Edit Assignments**.
9. Select the permission set that you created in step 2 above.
10. Save the user account.

Enable permissions for viewing and modifying data

In order to enable Secure Cloud Access to access all data, you must enable permissions for the admin user that you will use to onboard Salesforce.

1. In your Salesforce account, go to **Setup** and use the search box to search for **Users**.
2. Click the name of the admin user that you will use to onboard Salesforce, and click the Edit button.
3. In the Administrative Permissions section, make sure that the **View All Data** and **Modify All Data** checkboxes are selected.
4. Save the user account.

Onboarding steps

1. Go to **Administration > App Management** and click **New**.
2. Select **Salesforce** from the list.
3. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
4. Select one or more **protection models**:
 - **App Authentication**
 - **App Access**
 - **API Access**
 - **Cloud Security Posture**
 - **Dynamic DRM**

- **Cloud Data Discovery**

5. Click **Next** and enter configuration settings. The fields you see depend on the deployment and the protection modes you chose in the previous step.

- For **App Authentication** -- No configuration details are needed. Click **Next** to display the summary information.
- For **App Access** – In the **Proxy** section, enter a valid **Home Page URL**, the **Salesforce Org ID**, and one or more **Specific Domains** (for multiple domains, separate each domain with a comma).

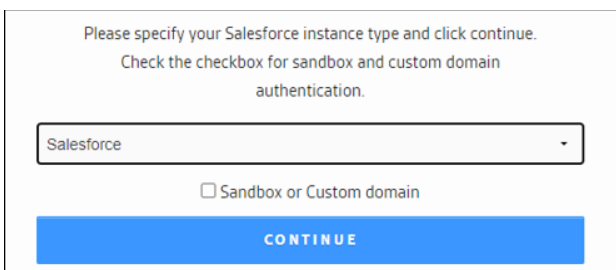
The screenshot shows the 'Proxy' configuration section. It contains three input fields: 'Home Page Url' with the value 'https://login.salesforce.com/home/h', 'Salesforce Org ID' which is empty, and 'Specific Domains' with the placeholder text '-- Enter Domain values --' and a small edit icon. At the bottom of the section are three buttons: 'Previous' (green), 'Next' (green), and 'Cancel' (light green).

- For **API Access** – Enter a **Salesforce Subdomain**.

The screenshot shows the 'Identity' and 'Authorization' configuration sections. The 'Identity' section has a 'Salesforce Subdomain' input field with the value 'login'. The 'Authorization' section features the Salesforce logo and a green 'Authorize' button. At the bottom of the section are three buttons: 'Previous' (green), 'Next' (green), and 'Cancel' (light green).

- For **Cloud Security Posture** – No other details are needed.
- For **Dynamic DRM** – You must *also* choose either **App Access** or **API Access** protection modes.
 - If you include **App Access**, enter the information in the **Proxy** section.
 - If you include **API Access**, enter a **Salesforce Subdomain** in the Identity section.
- For **Cloud Data Discovery** -- No other details are needed.

6. Click **Authorize**.



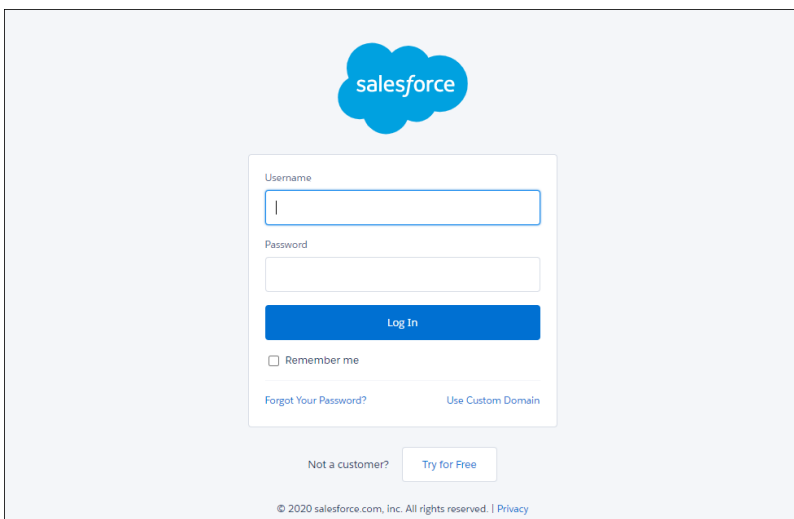
Please specify your Salesforce instance type and click continue.
Check the checkbox for sandbox and custom domain authentication.

Salesforce

☐ Sandbox or Custom domain

CONTINUE

7. Select the **Salesforce** instance from the dropdown list.
8. If this authorization is for a custom or a sandbox domain, click the box. Then, click **Continue**.



salesforce

Username

Password

Log In

☐ Remember me

[Forgot Your Password?](#) [Use Custom Domain](#)

Not a customer? [Try for Free](#)

© 2020 salesforce.com, Inc. All rights reserved. | [Privacy](#)

9. Enter the administrator login credentials for this Salesforce account. Make sure to use the same administrator account that you assigned permissions to in the **Enable permissions for querying files** section above. Then, click **Log In**.

Onboarding ZenDesk applications

1. Go to **Administration > App Management** and click **New**.
2. Select **ZenDesk** from the list.
3. Enter a **Name** (required) and a **Description** (optional). The name cannot have any spaces or special characters. Click **Next**.
4. Select one or more **protection models**.
5. If you select **Dynamic DRM**, you must also select either **App Access** or **App Authentication**.
6. Click **Next** and enter the configuration information for the protection models you selected.

Configuring user access (all protection models)

1. Under **User Access**, click **New**.

2. From the **Type** dropdown list, select **User** or **User Group** to specify the users or user groups allowed to access this application.

- If you selected **User**, select either **All** (allows access by all users) or **Selected** (allows access by users you specify by their valid email addresses).

- If you selected **User Group**, select the user groups from the directories.

3. Click **Add**.
4. Click **Next** and click **Save**.

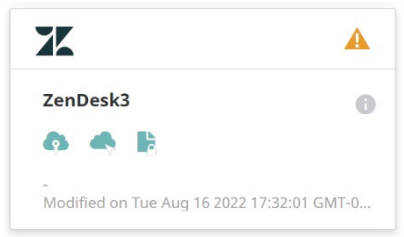
Configuring proxy information (App Access protection model)

Enter the following proxy information.

1. Enter an **Enterprise Subdomain** name.
2. (Optional) Enter any **Specific Domains**.

- a. Click the pencil icon.
 - b. In the text box, enter one or more specific domains, separating each name with a comma.
 - c. Click **Save**.
3. Click **Next**.
4. Review the information in the **Summary** page. Click **Previous** to make any updates or corrections or click **Save** to save the application.

The new application is onboarded and added to the **App Management** page.



An orange triangle in the upper right corner of the application tile indicates that a key is pending. Perform the following steps to request a key and have it assigned to the application.

Once a key is assigned, the triangle is replaced by a green check mark.

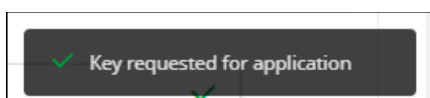
Assigning a key for the application

To assign a key to the onboarded application, modify the application settings as follows.

1. Go to **Administration > App Management** and open the onboarded application by clicking the pencil icon.
2. Go to the **Keys** page.



3. Click **Request New Key**. A request is generated to assign a new key from the available keys. A message appears at the lower right portion of the screen confirming the key request.



You can also create a new key and assign it to the application. To create a new key, go to **Administration > Key Management** and create the key. For more information, see Assigning, creating, and managing keys.

4. Click **Save**.