Forcepoint CASB

Service Provider API Connection Guide

Published 2021

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this document and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this document is subject to change without notice.

Last modified: **19-Dec-2021**

CONTENTS

CHAPTER 1

Overview

Forcepoint CASB Compliance, Cloud Governance and Service Provider auditing provide:

- Visibility into cloud application user accounts
- Convenient review of cloud application security settings with an easy workflow to handle any required changes
- Data Classification for sensitive data
- Application programming interface (API)-based auditing and anomaly detection

Forcepoint CASB uses 2 methods to extract data from the cloud service:

- **Web connection**: Retrieve data from the cloud service user interface (log in as a user).
- **Service API connection**: Retrieve data from the cloud service using the service-provided API.

API connection is the default mode. Forcepoint CASB uses the web connection to retrieve information not available using the API.

Forcepoint CASB requires specific administrator rights when accessing a cloud service through an API connection. While most of the rights are for read-only access, some require full read and write access:

- **Full access to user files**: Required for remediation. You cannot copy or remove sharing permissions without file permissions.
- **Full access to user contacts**: Required to identify with whom files have been shared.
- **Full control to all site collections**: Required for data classification. This overrides individual site controls for remediation.

This document contains guidelines for setting Web and API connections on each supported asset and creating user accounts and API keys in the cloud service that are required by Forcepoint CASB to extract the relevant data.

CHAPTER 2

Supported Applications

Forcepoint CASB supports API and Web connections for the following cloud services:

- Salesforce
- Microsoft Office 365 and Azure
- Microsoft Exchange Online
- Amazon Web Services (AWS)
- Google G Suite
- Dropbox
- Box
- ServiceNow
- Cisco Webex

Note: Forcepoint is constantly evaluating and adding more cloud services to Forcepoint CASB.

This chapter discusses the following:

Salesforce

Service supported licenses

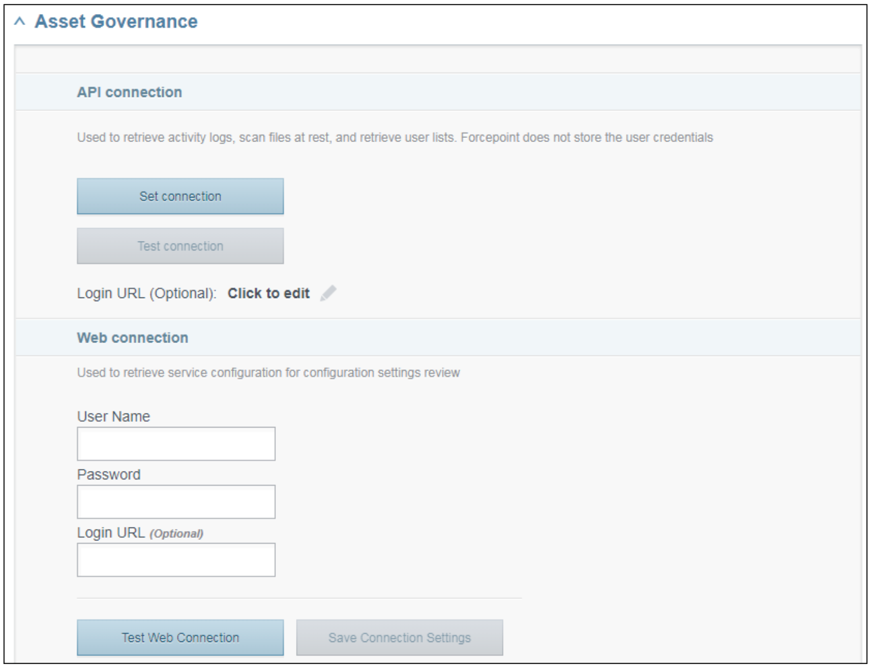
Salesforce API and web connections require one of the following licenses:

- Enterprise
- Unlimited
- Performance Edition

Supported capabilities summary

- Users and Configuration Governance scanning
- Data Classification scanning
- API-based auditing and anomaly detection

Configurations and supported capabilities in detail



Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Login URL (Optional): Click to edit

Used to retrieve service configuration for configuration settings review

User Name

Password

Login URL *(Optional)*

API connection

Configuration

Connect Forcepoint CASB to a Salesforce API using an administrator account that has access to relevant data. For more information, see "Required Salesforce setup and preparations" below.

Supported capabilities

Forcepoint CASB uses an API connection to import:

- User and administrator data for the Forcepoint CASB Users and Configuration Governance report.
- The following logs for Forcepoint CASB API-based auditing and anomaly detection:
  - login/logout log
  - Audit Trail: Contains logs of administrative actions.
  - Extended Event Monitoring log: Contains logs of API calls, report export, and URI requests among other logs (requires extra cost in Salesforce).
- Files, documents, and attachments for Forcepoint CASB Data Classification for data-at-rest and near real time data-in-motion. Forcepoint CASB applies corrective (mitigation) actions if needed.

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required Salesforce setup and preparations" below.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the Salesforce service is not the default Salesforce URL (login.salesforce.com).

Supported capabilities

Forcepoint CASB uses a web connection to import service configurations and settings, such as Password and Authentication settings, for the Forcepoint CASB Users and Configuration Governance report.

Required Salesforce setup and preparations

Allowing Forcepoint CASB to import data from Salesforce.com (SFDC) through an API connection and/or web connection requires authorization by a Salesforce administrator and the addition of Forcepoint CASB IP addresses to the Salesforce Trusted IP Ranges list.

Creating the user and profile in Salesforce

This section explains how to create the Salesforce administrator to be used by Forcepoint CASB for the API connection and/or web connection.

Salesforce has a very flexible permissions model and it supports Role Based Access Control. This functionality is delivered through User Profiles. Forcepoint recommends creating a dedicated user for the Forcepoint CASB connections. The new user should have one of the following profiles:

- **Forcepoint CASB Minimal Permissions Administrator**: A custom profile with the minimal set of permissions required for Forcepoint CASB functionality.
- **System Administrator**: A default Salesforce administrator profile.

To create a new admin:

1. Log in to your SFDC account with a System Administrator profile.
2. In the top pane, click the **Setup** link.
3. In the left pane, go to **Manage Users > Users**.
4. Click the **New User** button.
5. Fill in the required user details.

To create a new profile:
(If the System Administrator profile is used, this procedure can be skipped.)

1. Log in to SFDC with a System Administrator profile.
2. In the top pane, click **Setup**.
3. In the left pane, under **Administer**, go to **Manage Users > Profiles**.
4. Create a new profile by cloning the “Standard User” profile and:
   a. For a web connection, configure all permissions to match precisely the images displayed in Appendix A, Images 6 through 10 ("Salesforce Reference Images" on page 45).

      Note: The Forcepoint CASB Minimal Permissions Administrator profile does not require any view or modify permissions to the actual CRM data.

   b. For an API connection, also grant the profile the following permissions:

      i. API Enabled

      ii. View Event Log Files

      iii. Manage Users

    iv. View Setup and Configuration
    v. View All Data
5. Save the profile and go to **Manage Users > Users**.
6. Edit the user created above.
7. Under **Profile**, select the custom profile created above.
8. Save the user settings.

Trusting Forcepoint CASB IP addresses

To establish both web and API connections successfully, the Forcepoint CASB Management server IP needs to be listed in the Salesforce Trusted IP Ranges. To configure:

1. Log in to your SFDC account with a System Administrator profile.
2. In the left pane, go to **Security Controls > Network Access**.
3. Above the table, click **New**.
4. Enter the Forcepoint CASB Management external IP addresses in both the **Start IP Address** and **End IP Address** fields:
    a. For Forcepoint CASB customers under the Forcepoint CASB EU cluster:
        - 52.58.180.78
        - 52.59.6.31
        - 35.157.195.161
        - 52.59.33.95
        - 52.59.10.175
        - 52.59.19.4
        - 18.184.10.148
        - 18.197.37.30
        - 35.157.61.151
        - 35.158.30.123
        - 18.197.132.141
        - 18.197.110.58

    b. For Forcepoint CASB customers under the Forcepoint CASB US cluster:

- 52.8.46.99
- 52.8.177.6
- 52.52.213.124
- 13.56.88.15
- 52.53.41.167
- 52.8.82.168
- 52.8.108.130
- 52.8.38.124
- 52.9.86.40

5. Click **Save**.

For more information about device activation, refer to Appendix A, Images 4 and 5 ("Salesforce Reference Images" on page 45).

Microsoft Office 365 and Azure

Service supported licenses

Microsoft Office 365 API and web connections require one of the following licenses:

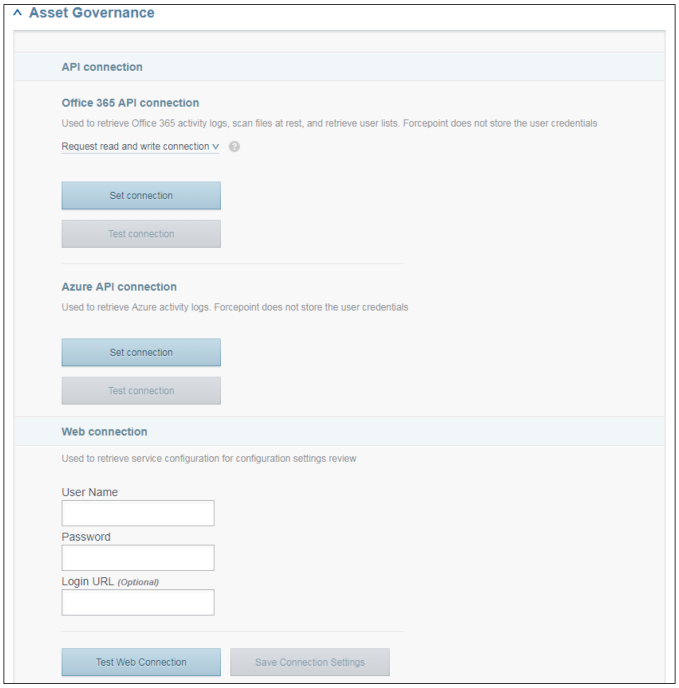
- Office 365 for Business
- Office 365 for Enterprise (E1-E5)

Microsoft Azure API connections require the **Pay-As-You-Go** subscription.

Supported capabilities summary

- Users and Configuration Governance scanning for Office 365
- Data Classification scanning on Office 365 OneDrive and SharePoint Online
- API-based auditing and anomaly detection for both Office 365 and Azure

Configurations and supported capabilities in detail



Asset Governance

API connection

Office 365 API connection

Used to retrieve Office 365 activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Request read and write connection

Azure API connection

Used to retrieve Azure activity logs. Forcepoint does not store the user credentials

Web connection

Used to retrieve service configuration for configuration settings review

User Name

Password

Login URL *(Optional)*

Office 365 API connection

Configuration

- Read-Only / Read and Write connection: Configure the API connection to allow either read-only access or read-write access to Office 365 data. Read-only access allows only the Forcepoint CASB Audit Only mitigation action.
- Connect Forcepoint CASB to the Office 365 API using an administrator account that has access to relevant data. For more information, see "Required Office 365 setup and preparations" on page 13.

Supported capabilities

Forcepoint CASB uses the Office 365 API connection to import:

- User and administrator data for the Forcepoint CASB Users and Configuration Governance report.

- The following logs for Forcepoint CASB API-based auditing and anomaly detection:
  - Partial login actions to Office 365 portal. For all login actions, see "Azure API connection" below.
  - SharePoint, OneDrive, and Exchange users and admins actions.
- OneDrive and SharePoint files for Forcepoint CASB Data Classification for data-at-rest and near real time data-in-motion. Forcepoint CASB applies corrective (mitigation) actions if needed.

Azure API connection

✎ **Note:** While an existing Office 365 asset is required for the Azure API connection to work, an Office 365 API connection is not required. The asset is required because the Azure API connection credentials must be set and tested in the Office 365 asset's Asset Governance settings section.

Configuration

Connect Forcepoint CASB to the Azure API using an administrator account that has access to relevant data. For more information, see "Required Azure setup and preparations" on page 15.

Supported capabilities

Forcepoint CASB uses an Azure API connection to import the following logs for Forcepoint CASB API-based auditing and anomaly detection:

- All Office 365 login actions: To import login activities from Azure, a special license must be purchased for Azure Active Directory. Either of the following two special licenses is sufficient:
  - Enterprise Mobility + Security E5
  - Azure Active Directory Premium P2 (included as part of Enterprise Mobility + Security E5)

  Note: The upgraded license is only needed if you want to import login activities. The license is not required to import user activities.
- Azure users activities: For user and administrator activities within the Azure portal.

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required Office 365 setup and preparations" below.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the Office 365 service is not the default Office 365 URL (login.microsoftonline.com).

Supported capabilities

Forcepoint CASB uses a web connection to import service configurations and settings, such as Password, Authentication and Collaboration settings, for the Forcepoint CASB Users and Configuration Governance report.

Required Office 365 setup and preparations

Allowing Forcepoint CASB to import data from Office 365 through an API connection and/or web connection requires authorization by an Office 365 administrator.

Creating the user and profile in Office 365

This section explains how to create the Office 365 administrator. The Office 365 permission model is delivered through User Roles. Forcepoint recommends creating a new dedicated user, connecting it to one of the profiles below:

- **Administrator profile for web connection support only:**
  - **Forcepoint CASB Minimal Permissions Administrator**: Billing admin, Password admin, SharePoint admin, Service support admin, or User admin can be used. Refer to this **article** for more information.
- **Administrator profile for API and/or web connection support:**
  - **Global Administrator**: When configuring an API connection, you must use an account with a Global Administrator profile. By default, this profile has full administrative permissions on the Office 365 platform. When an administrator sets an API connection, Forcepoint uses a custom Forcepoint-created application to set the connection. As a result, an Office 365 Global Administrator needs to give their consent to connect our application to their Office 365 account. While Office 365 requires consent from a Global Administrator to approve the application, the application only uses the minimum set of permissions listed below.

If you want the account to only have read-only permissions, select the read-only option on the asset's settings page in the Forcepoint CASB management portal. The CASB service then requests a token with the reduced, read-only permissions. The resulting user is a Global Administrator with a token that only includes the read permission.

When you configure the API connection for an Office 365 asset on the Forcepoint CASB management portal, you must enter the credentials of the Global Administrator user. After you enter the credentials, Office 365 displays the list of permissions that Forcepoint CASB requires:

- **Read and write items in all site collections (preview)**: If you selected the read and write option, this permission allows Forcepoint CASB to collect and manipulate Office 365 files.

  If you selected the read-only option, this permission is **Read items in all site collections (preview)**, which allows Forcepoint CASB to collect the Office 365 files, but not manipulate them.
- **Sign in and read user profile**: This permission allows Forcepoint CASB to log in to the Office 365 account.
- **Read directory data**: This permission allows Forcepoint CASB to extract the users, groups, and sites from Active Directory.
- **Read activity data for your organization**: This permission allows Forcepoint CASB to import the activity logs from Office 365.

In both cases, the administrator account must be managed by Cloud Azure Active Directory and have a **@onmicrosoft.com** or **@<TenantName>.com** suffix. The Tenant Name is provided by Microsoft and is based on your organization name.

To create a new administrator in Office 365:

1. Log in to Office 365 with a Global Administrator profile and select the **Admin** option.
2. In the left pane, go to **Users > Active Users**.
3. Click the **+ Add a user** button above the users table to create a new user.
4. Fill in the user’s details.
5. Under **Manage Roles**, select the desired role for the user:
   a. For a web connection, Forcepoint recommends using User admin. You can also use the following admin roles if required: Global admin, Billing admin, Password admin, SharePoint admin, or Service support admin.
   b. For an API connection, **Global admin** is required.
6. Enter an alternate email address.

7. Select the **Product license** for this user.
8. Click **Add**.
9. Select the new user record from the Active users list to edit the user's information.
10. Make sure that **Sign-in status** is set to **Sign-in allowed**.
11. Save and close the user record.

For more information about how to create and configure Office 365 users, refer to Appendix B ("Microsoft Office 365 Reference Images" on page 51).

Enabling audit logging in Office 365

When you configure a new Forcepoint CASB API connection to Office 365, and it is a new Office 365 environment, you must enable Microsoft log generation to receive the audit logs in Forcepoint CASB.

1. Log in to Office 365 with a Global Administrator profile and select the **Admin** option.
2. Open the **Admin centers** menu, then select **Security and Compliance**.
3. Open the **Search** menu, then select **Audit log search**.
4. If audit logging is currently turned off, a banner is displayed at the top of the page indicating that you must turn on auditing to use this feature. Click **Turn on auditing**.
5. Office 365 updates the setting. It may take a few hours for the logs to appear in the Microsoft console. After the logs appear in the console, Forcepoint CASB starts digesting the logs.

Required Azure setup and preparations

Allowing Forcepoint CASB to import data from Microsoft Azure through an API connection requires authorization by an Azure administrator with the Global Administrator profile.

This administrator must have a Monitoring Reader role for every Azure subscription that you would like to monitor:

1. Log in to the Azure portal with a Global Administrator profile and select the **Subscription** option from the left pane. This option may be under **More services** at the bottom of the pane.
2. Select the subscription that you want to audit.
3. Under **Settings**, select **My permissions**.
4. Add one of the following roles: **Owner** or **Monitoring Reader**
5. Save the updated record.

Microsoft Exchange Online

Service supported licenses

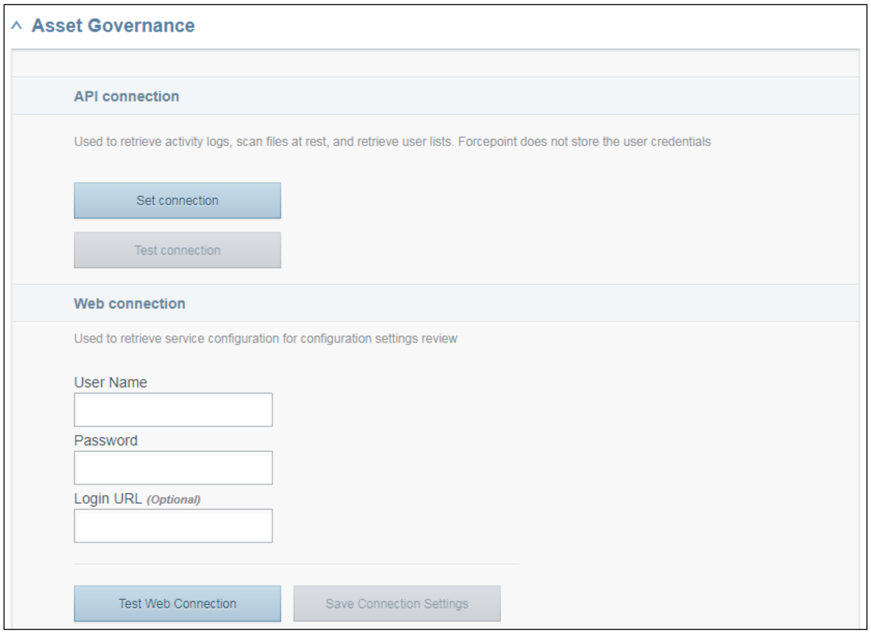
Microsoft Exchange Online API and web connections require one of the following licenses:

- Exchange Online Plan 1
- Exchange Online Plan 2

Supported capabilities summary

- Users and Configuration Governance scanning
- API-based auditing and Anomaly Detection

Configurations and supported capabilities in detail



Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Used to retrieve service configuration for configuration settings review

API connection

Configuration

- Read-Only / Read and Write connection: Configure the API connection to allow read-only access to Office 365 data. Read-only access allows only the Forcepoint CASB Audit Only mitigation action.
- Connect Forcepoint CASB to the Exchange API using an administrator account that has access to relevant data. For more information, see "Required Office 365 setup and preparations" on the next page.

Supported capabilities

Forcepoint CASB uses the Exchange API connection to import:

- User and administrator data for the Forcepoint CASB Users and Configuration Governance report.
- Exchange user and administrator actions for Forcepoint CASB API-based auditing and anomaly detection.

  Note: To import activities, a special license must be purchased for Azure Active Directory. Either of the following two special licenses is sufficient:

  - Enterprise Mobility + Security E5
  - Azure Active Directory Premium P2 (included as part of Enterprise Mobility + Security E5)

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required Office 365 setup and preparations" on the next page.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the Office 365 service is not the default Office 365 URL (login.microsoftonline.com).

Supported capabilities

Forcepoint CASB uses a web connection to import service configurations and settings, such as Password and Authentication, for the Forcepoint CASB Users and Configuration Governance report.

Required Office 365 setup and preparations

Allowing Forcepoint CASB to import data from Exchange through an API connection and/or web connection requires authorization by an Office 365 administrator.

Creating the user and profile

This section explains how to create the Office 365 administrator account. The Office 365 permission model is delivered through User Roles. Forcepoint recommends creating a new dedicated user, connecting it to one of the profiles below:

- **Administrator profile for web connection support only:**
  - **Forcepoint CASB Minimal Permissions Administrator**: Billing admin, Password admin, SharePoint admin, Service support admin, or User admin can be used. Refer to this article for more information.
- **Administrator profile for API and/or web connection support:**
  - **Global Administrator**: When configuring an API connection, you must use an account with a Global Administrator profile. By default, this profile has full administrative permissions on the Office 365 platform.

    If you want the account to only have read-only permissions, select the read-only option on the asset's settings page in the Forcepoint CASB portal. The CASB service then requests a token with the reduced, read-only permissions. The resulting user is a Global Administrator with a token that only includes the read permission.

In both cases, the administrator account must be managed by Cloud Azure Active Directory and have a **@onmicrosoft.com** or **@<TenantName>.com** suffix. The Tenant Name is provided by Microsoft and is based on your organization name.

To create a new admin on Office 365:

1. Log in to Office 365 with a Global Administrator profile and select the **Admin** option.
2. In the left pane, go to **Users > Active Users**.
3. Click the **+ Add a user** button above the users table to create a new user.
4. Fill in the user’s details.
5. Under **Manage Roles**, select the desired role for the user:
   a. For a web connection, Forcepoint recommends using User admin. You can also use the following admin roles if required: Global admin, Billing admin, Password admin,

SharePoint admin, or Service support admin.

b. For an API connection, **Global admin** is required.

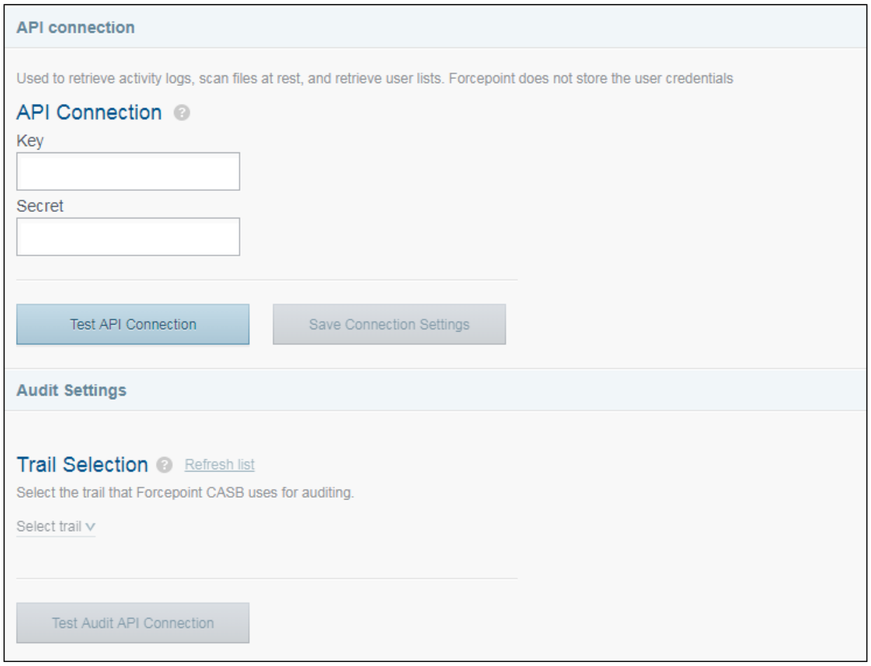
6. Enter an alternate email address.
7. Select the **Product license** for this user.
8. Click **Add**.
9. Select the new user record from the Active users list to edit the user’s information.
10. Make sure that **Sign-in status** is set **to Sign-in allowed**.
11. Save and close the user record.

Amazon Web Services

Supported capabilities summary

- Users and Configuration Governance scanning
- Data Classification scanning on Amazon Web Services (AWS) WorkDocs
- API-based auditing and anomaly detection for AWS CloudTrail

Configurations and supported capabilities in detail



API connection

Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

API Connection

Key

Secret

Audit Settings

Trail Selection

Select the trail that Forcepoint CASB uses for auditing.

API connection

Configuration

Connect Forcepoint CASB to the AWS API using an administrator account with an API Key and Secret available, and has access to relevant data. For more information, see "Required Amazon Web Services setup and preparations" below.

Supported capabilities

Forcepoint CASB uses the AWS API connection to import:

- User, administrator, and AWS account settings and configuration data for the Forcepoint CASB Users and Configuration Governance report.
- API-based auditing and anomaly detection through Amazon CloudTrail. For more information, see "Audit Settings" below.
- Amazon WorkDocs files for Forcepoint CASB Data Classification for data-at-rest.

Audit Settings

Configuration:

Under **Trail Selection**, Forcepoint CASB lists all of the trails available through the above API connection. Select the trail you wish to use for activity auditing, then click **Test Audit API Connection**. If the connection test is successful, enable the activity audit by clicking the **on** button under **Audit Activity**. For more information, see "Required Amazon Web Services setup and preparations" below.

Supported capabilities:

Forcepoint CASB API-based auditing and anomaly detection are done through Amazon CloudTrail.

Important: CloudTrail is an auditing service for AWS. It records user and API activities, and tracks the activities per region. Each event captured through CloudTrail contains information about the associated activity, including who made the request, the service used, the actions performed, the parameters for each action, and the response elements returned by the AWS service.

Required Amazon Web Services setup and preparations

Allowing Forcepoint to import data from AWS requires authorization by an AWS administrator. This section explains how to create the administrator, the relevant IAM policy, and the Amazon CloudTrail for auditing.

Creating the user and profile

AWS uses Policies to define access permissions. Forcepoint recommends using a custom Forcepoint CASB Minimal Permissions profile with a minimum set of read-only permissions. This profile will be attached to an AWS Identity and Access Management (IAM) user, which will be used to pull Cloud Governance data.

To create a new IAM user on AWS:

1. Log in to the AWS Console with a system administrator profile.
2. On the Dashboard, go to **IAM** under the **Security, Identity & Compliance** section.
3. In the left pane, go to **Users**.
4. Click the **Add user** button.
    a. On the **Set user details** page, enter the **User name** and select the **Programmatic access** checkbox.
    b. On the **Permissions** page, set the permissions for the user account, either by adding the user to an existing group, copying permissions for another user, or attaching an existing policy directly.
    c. On the **Review** page, verify that the details are correct, then click **Create user**.
5. Copy the new user's Security Credentials. These will be used later for Cloud Governance API access.

✎ **Note:** If you are creating a user with a CloudTrail IAM policy, then both the new user and the S3 bucket storing the audit trails must be under the same administrator account.

A password must be configured so that the user can access AWS via the Internet. To configure a password for the IAM user:

1. In the **Users** table, click the user created before.
2. Under the **Security credentials** tab, click the **Manage Password** section.
3. Assign a password for the user then click **Apply**.

To configure the IAM user policy:

1. On the Identity & Access Management main page, select **Policies** from the left dashboard.
2. Click **Create policy**.
3. Select the **JSON** tab, copy one of the below security policies into the JSON editor (the JSON is different for each type of policy you are creating), then click **Review policy**.

For Users and Configuration Governance:

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
           "Effect": "Allow",
           "Action": [
              "sns:ListSubscriptionsByTopic",
              "iam:ListSAMLProviders",
              "iam:GenerateCredentialReport",
              "iam:GetAccountPasswordPolicy",
              "iam:GetAccountSummary",
              "iam:GetCredentialReport",
              "iam:ListUsers",
              "iam:listGroups",
              "iam:listGroupsForUser",
              "iam:listPolicyVersions",
              "iam:listAttachedUserPolicies",
              "iam:listUserPolicies",
              "iam:listAttachedGroupPolicies",
              "iam:listGroupPolicies",
              "iam:getGroupPolicy",
              "iam:GetUserPolicy",
              "iam:GetPolicyVersion",
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "s3:GetBucketAcl",
              "s3:GetBucketLogging",
              "s3:GetBucketPolicy",
              "kms:GetKeyRotationStatus",
              "kms:ListKeys",
              "kms:listAliases",
              "config:DescribeConfigurationRecorderStatus",
              "config:DescribeConfigurationRecorders",
              "logs:DescribeMetricFilters",
              "cloudwatch:DescribeAlarms",
              "ds:DescribeDirectories",
              "ec2:DescribeFlowLogs",
              "ec2:DescribeSecurityGroups",
              "ec2:DescribeVpcs",
              "ec2:DescribeRegions"
           ],
           "Resource": [
              "*"
           ]
        }
     ]
}
```

For WorkDocs Data Classification:

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
           "Sid": "WorkDocsAPI",
           "Effect": "Allow",
           "Action": [
              "workdocs:describeUsers",
              "workdocs:describeFolderContents",
              "workdocs:DownloadDocumentVersion",
              "workdocs:getDocumentVersion",
              "workdocs:getDocument",
              "workdocs:describeResourcePermissions",
              "workdocs:getFolderPath",
              "workdocs:getFolder",
              "workdocs:createFolder",
              "workdocs:deleteFolder",
              "workdocs:deleteDocument",
              "workdocs:initiateDocumentVersionUpload",
              "workdocs:abortDocumentVersionUpload",
              "workdocs:updateDocumentVersion",
              "ds:describeDirectories"
           ],
           "Resource": [
              "*"
           ]
        }
     ]
}
```

For activities auditing using CloudTrail:

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
           "Sid": "VisualEditor0",
           "Effect": "Allow",
           "Action": [
              "s3:GetObject",
              "s3:ListBucket"
           ],
           "Resource": [
              "arn:aws:s3:::<s3-bucket-name>",
              "arn:aws:s3:::<s3-bucket-name>/*"
           ]
        },
        {
           "Sid": "VisualEditor1",
           "Effect": "Allow",
           "Action": "s3:GetBucketLocation",
           "Resource": [
              "arn:aws:s3:::<s3-bucket-name>"
           ]
        },
        {
           "Sid": "VisualEditor2",
           "Effect": "Allow",
           "Action": [
              "cloudtrail:LookupEvents",
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "s3:ListAllMyBuckets"
           ],
           "Resource": "*"
        }
     ]
}
```

Where **<s3-bucket-name>** is the name of the S3 bucket where the trail delivers the log files. You specify the bucket name when you create the trail. For more information, see "Creating the CloudTrail" below.

The S3 bucket storing the trails and the user record must be under the same administrator account. If the stored trails and user record are under different accounts, the trails are not accessible to the user.

4. On the **Review policy** page, specify a **Name** and **Description** for the policy, then click **Create policy**.
5. Create the policy.
6. In the Policies table, select the new policy and open the **Attached entities** tab.
7. Click **Attach**.
8. Select the user created before, then click **Attach policy**.

After the policy is applied, you can use the Security Credentials of the IAM user for API access (see image 13 in Appendix C: "Amazon Web Services Reference Images" on page 53).

For more information about creating and configuring IAM users on AWS, refer to Appendix C ("Amazon Web Services Reference Images" on page 53).

Creating the CloudTrail

1. Log in to the AWS Console with a system administrator profile.
2. On the Dashboard, go to **CloudTrail** under the **Management Tools** section.
3. Click **Get Started** to create your first trail.
   a. Type the **Trail name**.
   b. Select **Yes** for **Apply trail to all regions**.
   c. To create a new S3 bucket to store your logs, select **Yes** for **Create a new S3 bucket**, then type the name of the new **S3 bucket**. To store the log files in an existing S3 bucket, select **No** for **Create a new S3 bucket**, then type the name of the existing **S3 bucket**.
   d. Click **Turn On**.
4. The new trail appears in the list of trails.
5. To create another trail, click **Add new trail** above the list.
6. Complete the procedures in "Creating the user and profile" on page 22, using the CloudTrail JSON in the policy.

✎ **Note:** CloudTrail delivers events within 15 minutes of an API call. If you set up an S3 bucket, CloudTrail delivers the log files to the bucket every 5 minutes.

CloudTrail does not deliver log files unless an API call is made on the account.

By default, CloudTrail stores the log files indefinitely. If you want to define your own log retention policy, you can set it up through the Amazon S3 object lifecycle management rules.

Google G Suite

Service supported licenses

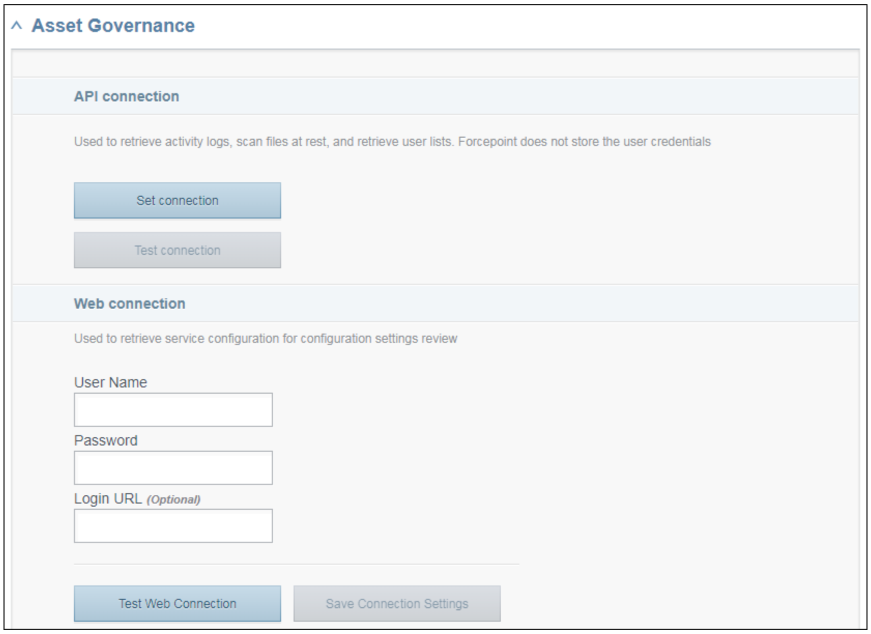
Google G Suite API and web connections require one of the following licenses:

- G Suite Business
- G Suite for Education
- G Suite Enterprise

Supported capabilities summary

- Users and Configuration Governance scanning
- Data Classification scanning on Google Drive
- API-based auditing and anomaly detection

Configurations and supported capabilities in detail



Asset Governance

API connection

Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Web connection

Used to retrieve service configuration for configuration settings review

API connection

Configuration

Connect Forcepoint CASB to the Google G Suite API using an administrator account that has access to relevant data. For more information, see "Required G Suite setup and preparations" below.

Supported capabilities

Forcepoint CASB uses the G Suite API Connection to import:

- User and administrator data for the Forcepoint CASB Users and Configuration Governance report.
- Event logs of user and administrator activities for Forcepoint CASB API-based auditing and anomaly detection.
- Google Drive files for Forcepoint CASB Data Classification for data-at-rest and near real time data-in-motion. Forcepoint CASB applies corrective (mitigation) actions if needed.

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required G Suite setup and preparations" below.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the G Suite service is not the default G Suite URL.

Supported capabilities

Forcepoint CASB uses the web connection to import service configurations and settings, such as Password, Authentication and Collaboration settings, for the Forcepoint CASB Users and Configuration Governance report.

Required G Suite setup and preparations

- Allowing Forcepoint CASB to import users and configurations from G Suite through an API connection and/or web connection requires authorization by a Google administrator. You must also disable Google Security Verifications. For more information, see "Creating the user and profile" on the facing page.
- Allowing Forcepoint CASB to import activities and files from Google Drive through an API connection requires authorization for the Forcepoint CASB Google app. For more information, see "Authorization to access user data" on page 32.

Creating the user and profile

G Suite allows the creation of custom roles. Forcepoint recommends creating a Forcepoint CASB Minimal Permission role and assigning it to the designated user. This role requires very limited read privileges; however, they are sufficient for pulling governance data.

To configure a role on G Suite:

1. Log in to Google's **Admin Console** with an Administrator profile.
2. On the dashboard, click **Admin roles**.
3. Click the **Create a new role** button.
4. Select the required privileges according to the specification in Appendix D ("Google G Suite Reference Images" on page 59).
5. Save the changes.

To create and configure a user on G Suite:

1. Log in to Google's Admin Console with an Administrator profile.
2. On the dashboard, click **Users**.
3. Click the + sign on the top right to add a user.
4. You can either invite or create a new user.
5. Select the newly created user from the users table.
6. On the user page, click **Show more**.
7. Select **Admin roles and privileges**.
8. In the opened menu, click **Manage roles**.
9. Add the Forcepoint Minimal Permissions profile to the user's roles.

Please make sure to log in with the user at least once before using it for Governance.

For further information about roles and users creation and configuration, see Appendix D ("Google G Suite Reference Images" on page 59).

Disabling Google Security Verifications

Google has implemented multiple precautions to secure your Google account from suspicious login attempts. For Forcepoint CASB to properly scan the account, you must disable both the Google Login Challenge and CAPTCHA on the administrator account before setting up either the API or web connection in Forcepoint CASB.

Disabling the Google Login Challenge:

At times, Google may identify a login attempt as suspicious and present a “Login Challenge” in the form of a code sent to the email address or phone associated with the account. To allow for Users and Configuration Governance scanning, the Login Challenge should be temporarily disabled.

To disable the Login Challenge:

1. Log in to Google’s Admin Console with an Administrator profile.
2. Find the user account.
3. Click the row for the user account to display the user information page.
4. Click **Security**.
5. Click **Disable Login Challenge**.

The challenge is disabled for 10 minutes and a Governance scan can be manually executed. Unfortunately, the Login Challenge can only be turned off temporarily for 10 minutes and cannot be completely disabled. Also, the Login Challenge can only be disabled on a per-user basis and cannot be disabled for the entire domain.

Disabling CAPTCHA:

Google might try to prevent Forcepoint CASB from accessing the administrator account the first time it attempts to log in to the account. To enable access, you must disable CAPTCHA:

1. Open a new private or incognito browser window.
2. Browse to **https://www.google.com/accounts/UnlockCaptcha**.
3. Log in with an Administrator profile.
4. Follow the instructions on the web page(s).

   CAPTCHA is disabled for 10 minutes.
5. In Forcepoint CASB, re-test the web connection.

   When you log in to the account through Forcepoint CASB within 10 minutes of disabling CAPTCHA, Google remembers Forcepoint CASB after it logs on and allows Forcepoint CASB to access the account in the future as long as it uses the correct password.

Authorization to access user data

To allow Forcepoint CASB to access your user data through the API connection for service provider logs and data classification (data at rest) scans, you must add the Forcepoint CASB client name (OAuth consumer key) in the Admin Console. If you do not complete this procedure, the data classification connection test might fail after you enter the API connection credentials and click **Test Connection**.

1. Log in to Google’s Admin Console with an Administrator profile.
2. From the dashboard, go to **Security > Access and data control > API controls**.
3. Under **App Access Control**, click **Manage Third-Party App Access**.
4. Click **Add app**, then select **OAuth App Name or Client ID**.
5. In the search field, enter the Forcepoint CASB client ID:

   `110037928920341175583`
6. Click **Search**, then select the Forcepoint CASB app.
7. Select the Client ID from the table, then click **Select**.
8. For app access, click the **Trusted** option, then click **Configure**.
9. Return to **API Controls**, then select **Manage Domain Wide Delegation**.
10. Click **Add new**.
11. In the **Client ID** field, enter the Forcepoint CASB client name:

    `110037928920341175583`
12. In the **OAuth Scopes** field, enter:

    `https://www.googleapis.com/auth/drive`
13. Click **Authorise**.

Dropbox

Service supported licenses

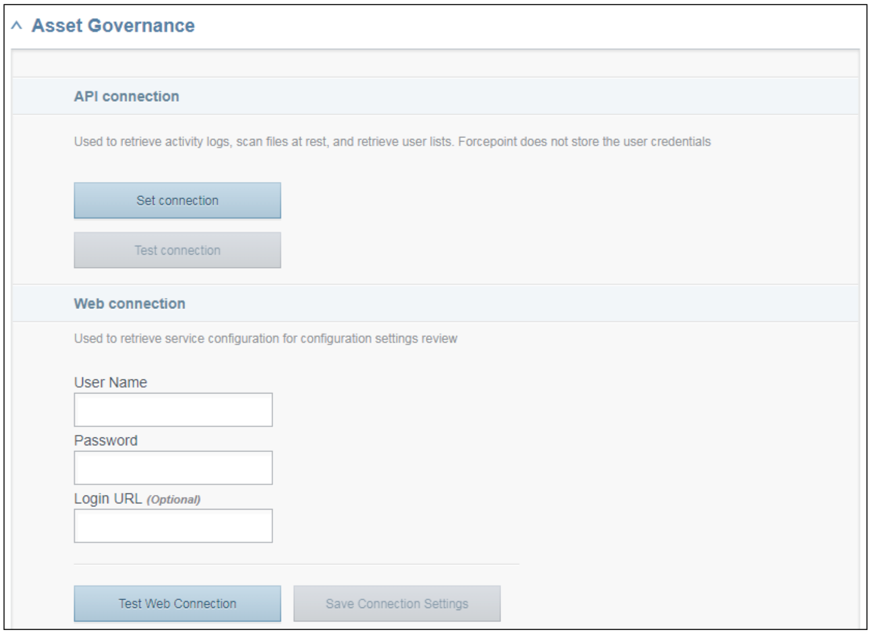
Dropbox API and web connections require one of the following licenses:

- Dropbox Business Standard
- Dropbox Business Advanced
- Dropbox Business Enterprise

Supported capabilities summary

- Users and Configuration Governance scanning
- Data Classification scanning

Configurations and supported capabilities in detail



Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Used to retrieve service configuration for configuration settings review

API connection

Configuration

Connect Forcepoint CASB to the Dropbox API using an administrator account to grant permissions for the Forcepoint CASB Dropbox app. For more information, see "Required Dropbox setup and preparations" below.

Supported capabilities

Forcepoint CASB uses the Dropbox API connection to import Dropbox files for Forcepoint CASB Data Classification for data-at-rest. Forcepoint CASB applies corrective (mitigation) actions if needed.

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required Dropbox setup and preparations" below.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the Dropbox service is not the default Dropbox URL.

Supported capabilities

Forcepoint CASB uses the web connection to import user and administrator data and service configurations and settings for the Forcepoint CASB Users and Configuration Governance report.

Required Dropbox setup and preparations

Allowing Forcepoint to import users and configurations from Dropbox through a web connection requires authorization by a Dropbox administrator. Dropbox does not allow profile and role customization; therefore, an existing native administrator or a new one is required.

The following section explains how to create such an administrator.

Creating the user and profile

In Dropbox, it is not possible to create users. Instead, users are invited to use the service. Once a user accepts an invitation, they become active on Dropbox and their permissions can be changed. To invite and configure a user in Dropbox:

1. Log in to your Dropbox account with an Administrator profile.
2. In the left pane, click **Admin Console**.

3. In the top right corner, click **Invite Members** and specify the email address of the user you wish to invite.
4. Log in with the invited user to activate the account.
5. Using the Administrator profile, return to the Members page.
6. In the new user’s record, click the gray wheel on the right and select **Add admin permissions**.

For more information about creating and configuring a Dropbox user, see Appendix E ("Dropbox Reference Images" on page 64).

Box

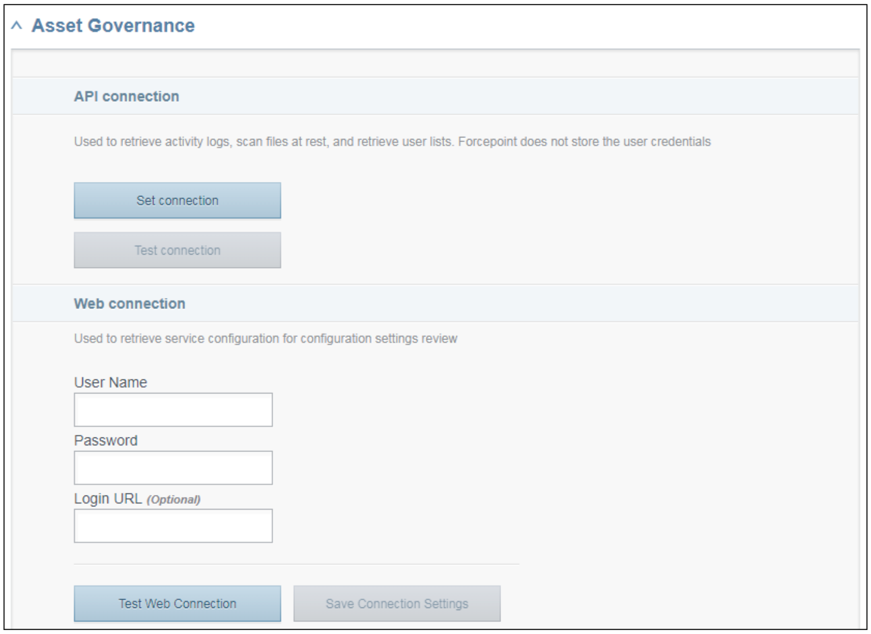
Service supported licenses

Box API and web connections require that you have a valid Box Business plan license.

Supported capabilities summary

- Users and Configuration Governance scanning
- Data Classification scanning
- API-based auditing and anomaly detection

Configurations and supported capabilities in detail



Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

Used to retrieve service configuration for configuration settings review

API connection

Configuration

Connect Forcepoint CASB to the Box API using an administrator account to grant permissions for the Forcepoint CASB Box app. For more information, see "Required Box setup and preparations" below.

Supported capabilities

Forcepoint CASB uses the Box API connection to import:

- User and administrator data for the Forcepoint CASB Users and Configuration Governance report.
- Event logs of user and administrator activities for Forcepoint CASB API-based auditing and anomaly detection.
- Box files for Forcepoint CASB Data Classification for data-at-rest and near real time data-in-motion. Forcepoint CASB applies corrective (mitigation) actions if needed.

Web connection

Configuration

- User name and password of an administrator account that has access to relevant data. For more information, see "Required Box setup and preparations" below.
- The **Login URL** parameter should be used in case the login URL that is used by the organization to enter the Box service is not the default Box URL.

Supported capabilities:

Forcepoint CASB uses the web connection to import service configurations and settings for the Forcepoint CASB Users and Configuration Governance report.

Required Box setup and preparations

Allowing Forcepoint CASB to import users, settings, and configurations from Box through an API connection and/or web connection requires authorization by a Box administrator.

Box allows the creation of a Co-Admin user with various permissions to Users and Groups, Files and Folders, and Reports and Settings. Forcepoint recommends creating a new user and connecting it to one of the two profiles below:

- **Box Administrator**: A native Box administrator.
- **Forcepoint CASB Minimal Permissions Administrator**: A Box Co-Admin with a

minimum set of view permissions. This user cannot view, download, or modify a user's files and folders. It also cannot grant permissions to other users.

Creating the user and profile

To create and configure a new user on Box with a Forcepoint CASB Minimal Permissions profile:

1. Log in to Box with an Administrator profile.
2. In the top pane, click **Admin Console**, then click the Users and Groups icon.
3. Click the **+ Users** button to create a new user.
4. Specify a user name and password for the user and remove all access permissions.
5. After the user is created, click the triangle drop-down menu in the user’s context, open its settings, and select **Change User Settings**.
6. Under the **Edit User Access permissions** section, select the **Co-Admin** checkbox, then select the following permissions:
   a. Users and Groups
      i. Manage users
      ii. Manage groups
   b. Files and Folders

      Note: Granting this permission will not allow the user to view other users’ files and folders.

      i. View users’ content
   c. Reports and Settings
      i. View settings for your company
      ii. Edit settings for your company
      iii. Run new reports and access existing reports
7. Save your changes.

A confirmation email is sent to the specified email address. Log in once and create a password before using this user for Governance.

For more information about how to create and configure a Box user, see Appendix F ("Box Reference Images" on page 66).

ServiceNow

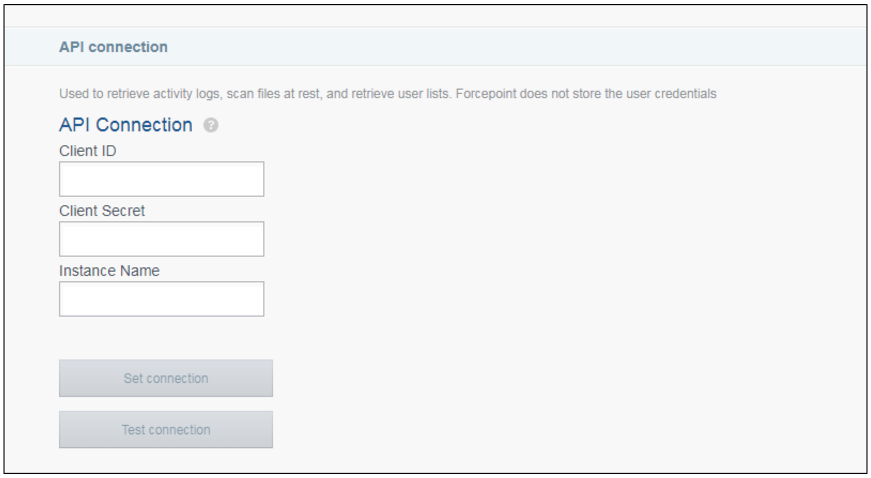
Service supported licenses

ServiceNow API connections do not require a specific license. Any ServiceNow license can be used.

Supported capabilities summary

- Data Classification scanning
- API-based auditing and anomaly detection

Configurations and supported capabilities in detail



API connection

Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

API connection

Configuration

- Connect Forcepoint CASB to the ServiceNow API using the **Client ID** and **Client Secret** of a new dedicated ServiceNow Application Registry for Forcepoint CASB. For more information, see "Required ServiceNow setup and preparations" on the facing page.
- **Instance Name**: Each customer has a unique instance name. The Instance Name is part of

the ServiceNow portal URL (**https://<instance-name>.servicenow.com**). Forcepoint CASB requires the Instance Name here to establish the API connection.

Supported capabilities

Forcepoint CASB uses the ServiceNow API connection to import:

- Event logs of user and administrator activities for Forcepoint CASB API-based auditing and anomaly detection.
- ServiceNow attachments for Forcepoint CASB Data Classification for data-at-rest and near real time data-in-motion. Forcepoint CASB applies corrective (mitigation) actions if needed.

Required ServiceNow setup and preparations

Allowing Forcepoint CASB to import activities and attachments from ServiceNow through an API connection requires that a ServiceNow user with an Administrator role create and register a new third-party OAuth application in the ServiceNow instance and grant API permissions to this application.

To create a new ServiceNow user with an Administrator role:

1. Log in to your ServiceNow instance (**https://<instance-name>.servicenow.com**) with an Administrator account.
2. In the navigation pane, go to **User Administrator > Users**.
3. In the top menu, click the **New** button.
4. Enter the new user 's detailed information, then click **Submit**.
5. At the bottom of the page, go to the **Roles** tab, then click **Edit**.
6. Assign the **admin** permission to the user by moving it from the left pane to the right pane, then click **Save**.
7. On the user's details page, click **Update**.

To create a new OAuth application in ServiceNow:

1. Log in to your ServiceNow instance (**https://<instance-name>.servicenow.com**) with an Administrator account.
2. In the navigation pane, go to **System OAuth > Application Registry**.
3. On the Application Registries dashboard, click **New**.
4. Select **Create an OAuth API endpoint for external clients**.

5. In the new record form, enter the following:
   a. **Name**: A unique name. For example: **Forcepoint CASB API Endpoint**.
   b. **Client ID**: This field is automatically generated by the ServiceNow OAuth server.
   c. **Client Secret**: Either enter a unique client secret, or leave the field empty for auto-generation.
   d. **Access Token Lifespan**: Time in seconds that the access token should be valid. This must be set to **3,600**.
   e. **Redirect URL**: The URL to which the authorization service redirects. This must be set to one of the following Forcepoint CASB URLs, depending on your Forcepoint CASB portal region:
      - For US: https://my.skyfence.com/cm/offline/prepareSaveToken/
      - For EU: https://my-eu1.skyfence.com/cm/offline/prepareSaveToken/
6. Click **Submit**.

Cisco Webex

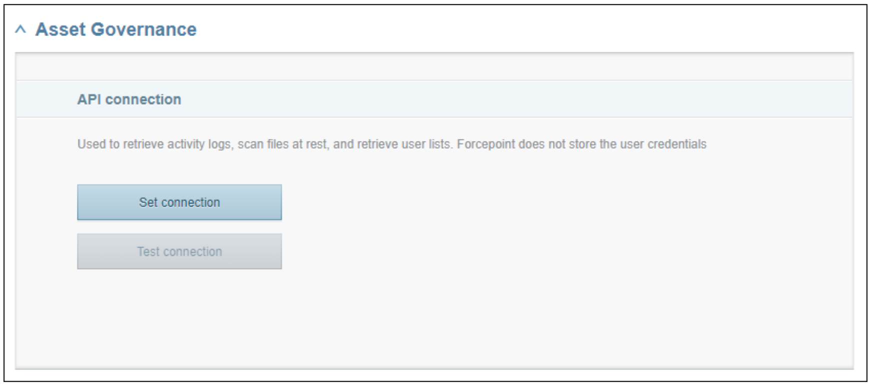
Service supported licenses

Cisco Webex API connections do not require a specific license. Any Webex license can be used.

Supported capabilities summary

- API-based auditing and anomaly detection

Configurations and supported capabilities in detail



Asset Governance

API connection

Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

API connection

Configuration

Connect Forcepoint CASB to the Webex Teams API using the credentials for a dedicated administrator role. For more information, see "Required Webex setup and preparations" below.

Supported capabilities

Forcepoint CASB uses the Webex Teams API connection to import event logs of user and admin console activities for Forcepoint CASB API-based auditing and anomaly detection.

Required Webex setup and preparations

Allowing Forcepoint CASB to import activities and attachments from Webex through an API connection requires the creation of a Webex administrator account with the **Full Administrator** and **Compliance Officer** roles.

To create a new Webex user with an Administrator role, follow the procedures on the Webex site:

- **Ways to Add Users to your Control Hub Organization**: Add the new administrator to your Webex account.
- **Assign Organization Account Roles in Control Hub**: For the Webex integration with Forcepoint CASB, assign both the **Full Administrator** and **Compliance Officer** roles. See "Cisco Webex Reference Images" on page 71 for an example screenshot.

After you configure the new administrator role, use the credentials for this new administrator to set up the API connection for the Cisco Webex asset in Forcepoint CASB. For more information about creating and configured assets, see the **Forcepoint CASB Administration Guide**.

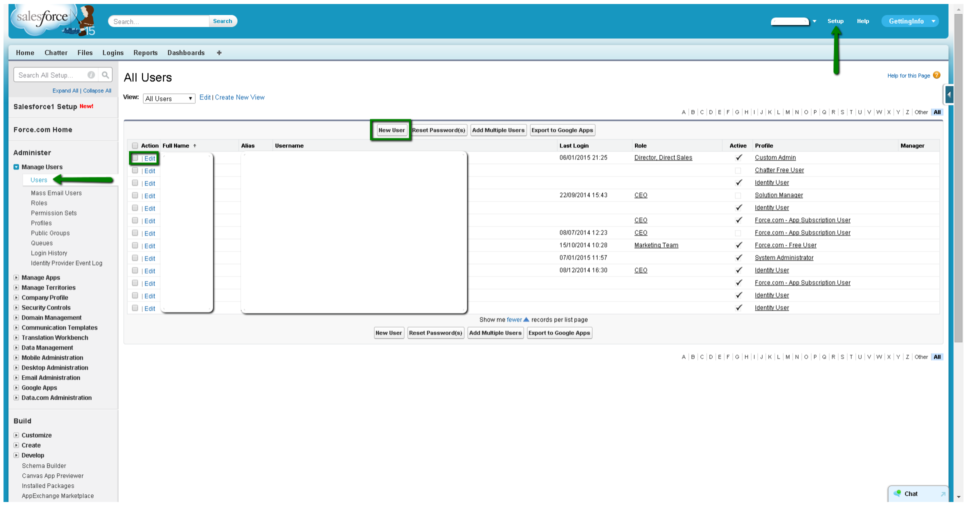
APPENDIX A

Salesforce Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Salesforce Images

Image 1: Create new user

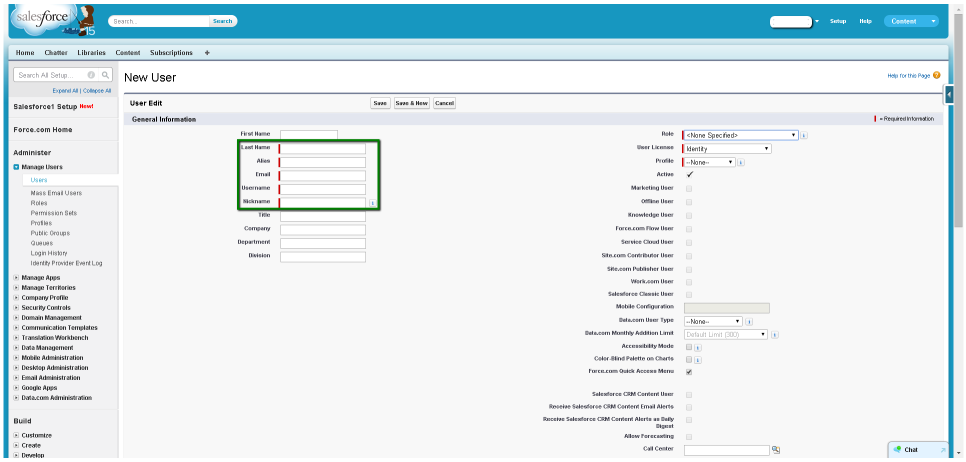


All Users

View: All Users ▾ Edit | Create New View

Action	Full Name ↑	Alias	Username	Last Login	Role	Active	Profile	Manager
☐ | Edit	[redacted]	[redacted]	[redacted]	06/01/2015 21:25	Director, Direct Sales	✓	Custom Admin	
☐ | Edit	[redacted]	[redacted]	[redacted]			☐	Chatter Free User	
☐ | Edit	[redacted]	[redacted]	[redacted]			✓	Identity User	
☐ | Edit	[redacted]	[redacted]	[redacted]	22/09/2014 15:43	CEO	☐	Solution Manager	
☐ | Edit	[redacted]	[redacted]	[redacted]			✓	Identity User	
☐ | Edit	[redacted]	[redacted]	[redacted]		CEO	✓	Force.com - App Subscription User	
☐ | Edit	[redacted]	[redacted]	[redacted]	08/07/2014 12:23	CEO	☐	Force.com - App Subscription User	
☐ | Edit	[redacted]	[redacted]	[redacted]	15/10/2014 10:28	Marketing Team	✓	Force.com - Free User	
☐ | Edit	[redacted]	[redacted]	[redacted]	07/01/2015 11:57		✓	System Administrator	
☐ | Edit	[redacted]	[redacted]	[redacted]	08/12/2014 16:30	CEO	✓	Identity User	
☐ | Edit	[redacted]	[redacted]	[redacted]			✓	Force.com - App Subscription User	
☐ | Edit	[redacted]	[redacted]	[redacted]			✓	Identity User	
☐ | Edit	[redacted]	[redacted]	[redacted]			✓	Identity User	

Show me fewer ▲ records per list page



New User

User Edit

Save | Save & New | Cancel

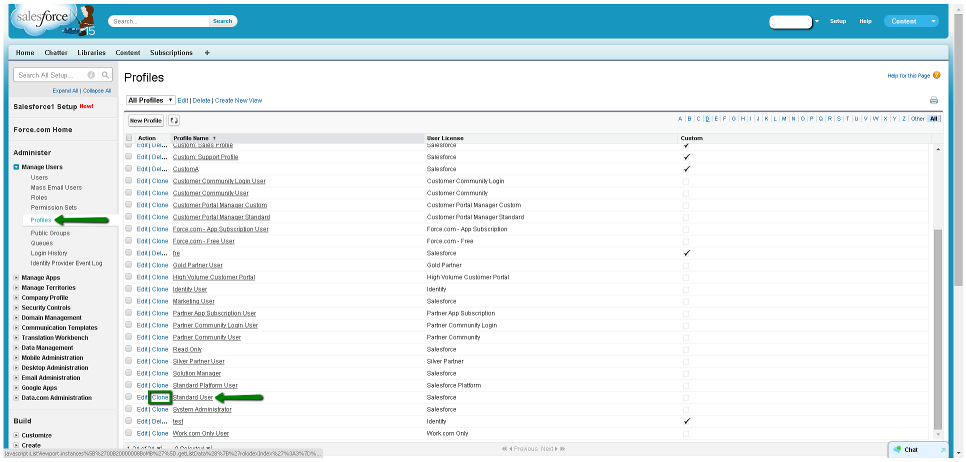
General Information

| = Required Information

First Name	
Last Name	
Alias	
Email	
Username	
Nickname	
Title	
Company	
Department	
Division	

Role	<None Specified>
User License	Identity
Profile	--None--
Active	✓
Marketing User	□
Offline User	□
Knowledge User	□
Force.com Flow User	□
Service Cloud User	□
Site.com Contributor User	□
Site.com Publisher User	□
Work.com User	□
Salesforce Classic User	□
Mobile Configuration	
Data.com User Type	--None--
Data.com Monthly Addition Limit	Default Limit (300)
Accessibility Mode	□
Color-Blind Palette on Charts	□
Force.com Quick Access Menu	☑
Salesforce CRM Content User	□
Receive Salesforce CRM Content Email Alerts	□
Receive Salesforce CRM Content Alerts as Daily Digest	□
Allow Forecasting	□
Call Center	

Image 2: Clone profile



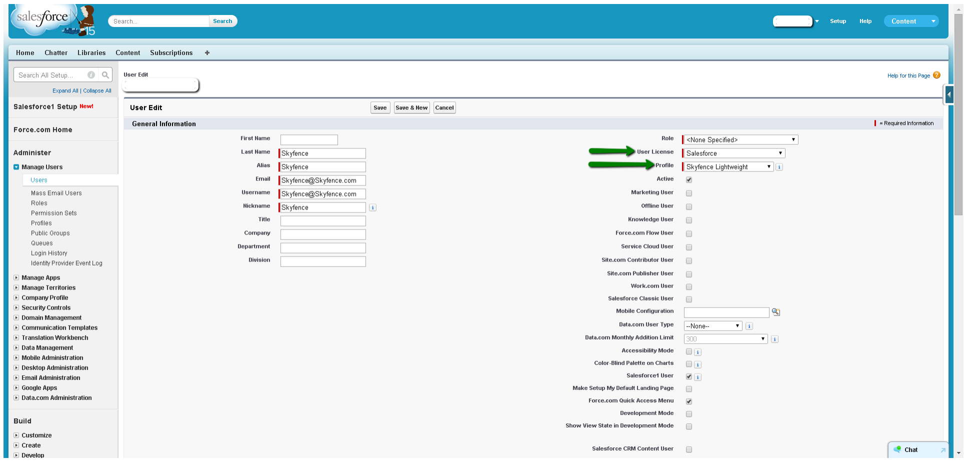
Profiles

All Profiles | Edit | Delete | Create New View

New Profile

Action	Profile Name ↑	User License	Custom
Edit | Del...	Custom: Sales Profile	Salesforce	✓
Edit | Del...	Custom: Support Profile	Salesforce	✓
Edit | Del...	CustomA	Salesforce	✓
Edit | Clone	Customer Community Login User	Customer Community Login	□
Edit | Clone	Customer Community User	Customer Community	□
Edit | Clone	Customer Portal Manager Custom	Customer Portal Manager Custom	□
Edit | Clone	Customer Portal Manager Standard	Customer Portal Manager Standard	□
Edit | Clone	Force.com - App Subscription User	Force.com - App Subscription	□
Edit | Clone	Force.com - Free User	Force.com - Free	□
Edit | Del...	fre	Salesforce	✓
Edit | Clone	Gold Partner User	Gold Partner	□
Edit | Clone	High Volume Customer Portal	High Volume Customer Portal	□
Edit | Clone	Identity User	Identity	□
Edit | Clone	Marketing User	Salesforce	□
Edit | Clone	Partner App Subscription User	Partner App Subscription	□
Edit | Clone	Partner Community Login User	Partner Community Login	□
Edit | Clone	Partner Community User	Partner Community	□
Edit | Clone	Read Only	Salesforce	□
Edit | Clone	Silver Partner User	Silver Partner	□
Edit | Clone	Solution Manager	Salesforce	□
Edit | Clone	Standard Platform User	Salesforce Platform	□
Edit | Clone	Standard User	Salesforce	□
Edit | Clone	System Administrator	Salesforce	□
Edit | Del...	test	Identity	✓
Edit | Clone	Work.com Only User	Work.com Only	□

Image 3: Associate a profile with the user



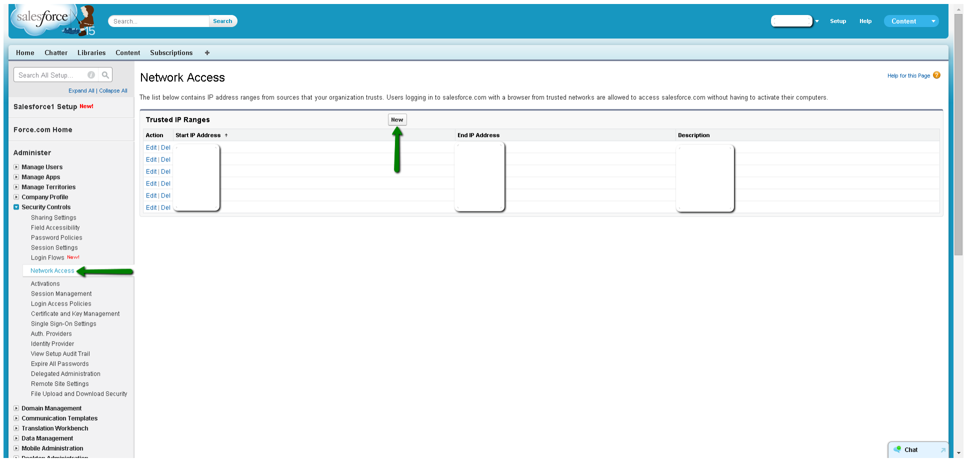
User Edit

User Edit Save | Save & New | Cancel

General Information = Required Information

First Name		Role	<None Specified>
Last Name	Skyfence	User License	Salesforce
Alias	Skyfence	Profile	Skyfence Lightweight
Email	Skyfence@Skyfence.com	Active	☑
Username	Skyfence@Skyfence.com	Marketing User	☐
Nickname	Skyfence	Offline User	☐
Title		Knowledge User	☐
Company		Force.com Flow User	☐
Department		Service Cloud User	☐
Division		Site.com Contributor User	☐
		Site.com Publisher User	☐
		Work.com User	☐
		Salesforce Classic User	☐
		Mobile Configuration	
		Data.com User Type	--None--
		Data.com Monthly Addition Limit	300
		Accessibility Mode	☐
		Color-Blind Palette on Charts	☐
		Salesforce1 User	☑
		Make Setup My Default Landing Page	☐
		Force.com Quick Access Menu	☑
		Development Mode	☐
		Show View State in Development Mode	☐
		Salesforce CRM Content User	☐

Image 4: Device activation - Add new device



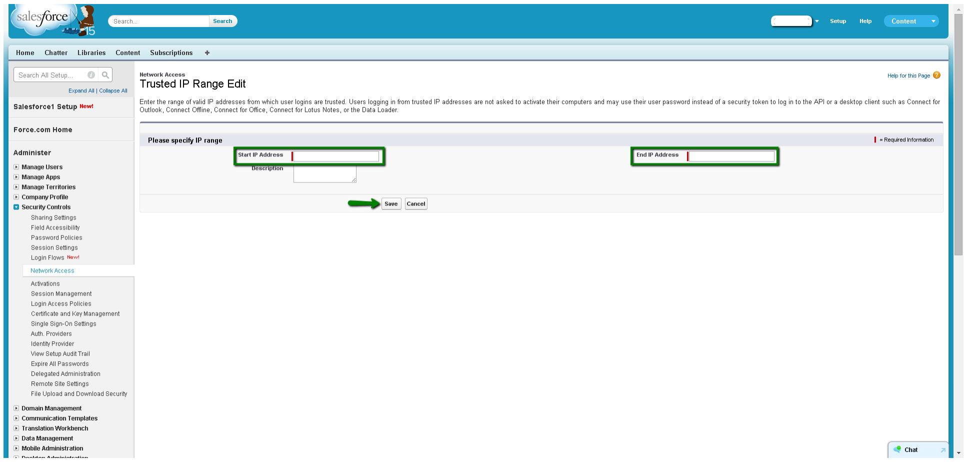
Network Access

The list below contains IP address ranges from sources that your organization trusts. Users logging in to salesforce.com with a browser from trusted networks are allowed to access salesforce.com without having to activate their computers.

Trusted IP Ranges New

Action	Start IP Address ↑	End IP Address	Description
Edit | Del			
Edit | Del			
Edit | Del			
Edit | Del			
Edit | Del			
Edit | Del			

Image 5: Device activation - Configure device



Network Access

Trusted IP Range Edit

Enter the range of valid IP addresses from which user logins are trusted. Users logging in from trusted IP addresses are not asked to activate their computers and may use their user password instead of a security token to log in to the API or a desktop client such as Connect for Outlook, Connect Offline, Connect for Office, Connect for Lotus Notes, or the Data Loader.

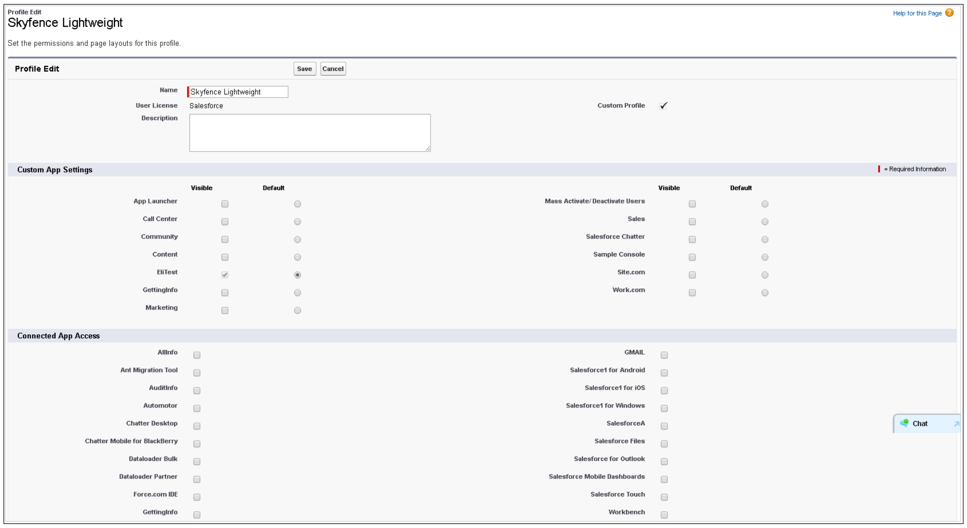
Please specify IP range | = Required Information

Start IP Address

Description

End IP Address

Image 6: Lightweight profile (image 1 of 5)



Profile Edit

Skyfence Lightweight

Set the permissions and page layouts for this profile.

Profile Edit

Name	Skyfence Lightweight		
User License	Salesforce	Custom Profile	✓
Description			

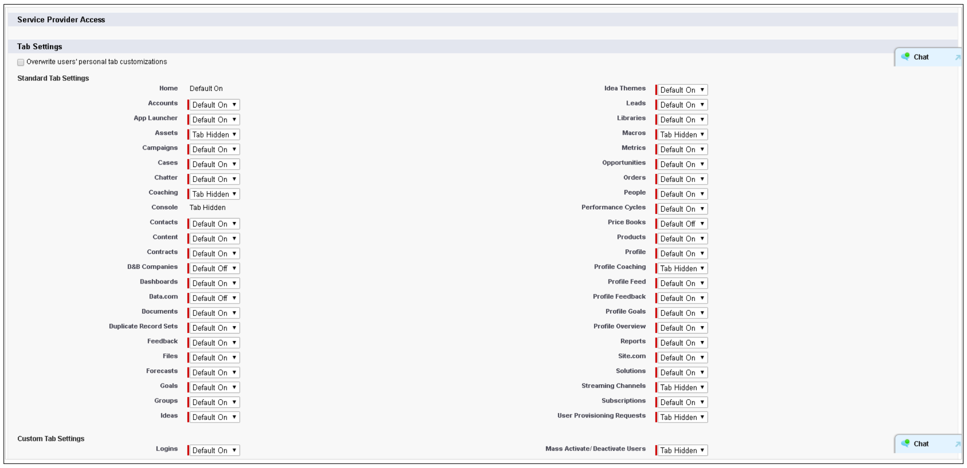
Custom App Settings | = Required Information

	Visible	Default		Visible	Default
App Launcher	□	○	Mass Activate/ Deactivate Users	□	○
Call Center	□	○	Sales	□	○
Community	□	○	Salesforce Chatter	□	○
Content	□	○	Sample Console	□	○
EliTest	☑	●	Site.com	□	○
GettingInfo	□	○	Work.com	□	○
Marketing	□	○			

Connected App Access

AllInfo	□	GMAIL	□
Ant Migration Tool	□	Salesforce1 for Android	□
AuditInfo	□	Salesforce1 for iOS	□
Automotor	□	Salesforce1 for Windows	□
Chatter Desktop	□	SalesforceA	□
Chatter Mobile for BlackBerry	□	Salesforce Files	□
Dataloader Bulk	□	Salesforce for Outlook	□
Dataloader Partner	□	Salesforce Mobile Dashboards	□
Force.com IDE	□	Salesforce Touch	□
GettingInfo	□	Workbench	□

Image 7: Lightweight profile (image 2 of 5)



Service Provider Access

Tab Settings

□ Overwrite users' personal tab customizations

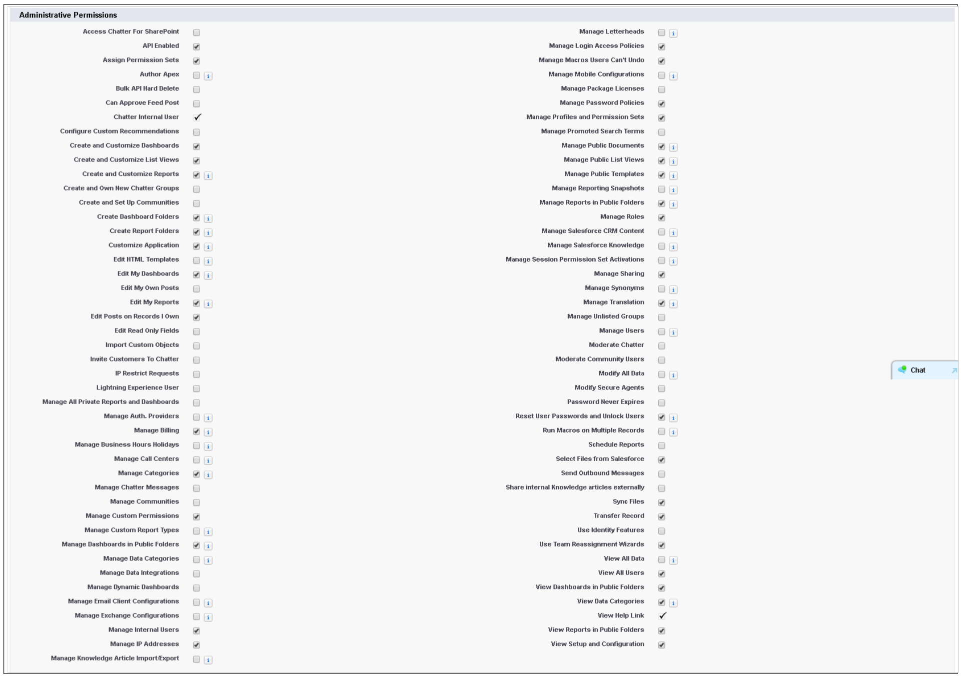
Standard Tab Settings

Home	Default On	Idea Themes	Default On ▼
Accounts	Default On ▼	Leads	Default On ▼
App Launcher	Default On ▼	Libraries	Default On ▼
Assets	Tab Hidden ▼	Macros	Tab Hidden ▼
Campaigns	Default On ▼	Metrics	Default On ▼
Cases	Default On ▼	Opportunities	Default On ▼
Chatter	Default On ▼	Orders	Default On ▼
Coaching	Tab Hidden ▼	People	Default On ▼
Console	Tab Hidden	Performance Cycles	Default On ▼
Contacts	Default On ▼	Price Books	Default Off ▼
Content	Default On ▼	Products	Default On ▼
Contracts	Default On ▼	Profile	Default On ▼
D&B Companies	Default Off ▼	Profile Coaching	Tab Hidden ▼
Dashboards	Default On ▼	Profile Feed	Default On ▼
Data.com	Default Off ▼	Profile Feedback	Default On ▼
Documents	Default On ▼	Profile Goals	Default On ▼
Duplicate Record Sets	Default On ▼	Profile Overview	Default On ▼
Feedback	Default On ▼	Reports	Default On ▼
Files	Default On ▼	Site.com	Default On ▼
Forecasts	Default On ▼	Solutions	Default On ▼
Goals	Default On ▼	Streaming Channels	Tab Hidden ▼
Groups	Default On ▼	Subscriptions	Default On ▼
Ideas	Default On ▼	User Provisioning Requests	Tab Hidden ▼

Custom Tab Settings

Logins	Default On ▼	Mass Activate/ Deactivate Users	Tab Hidden ▼

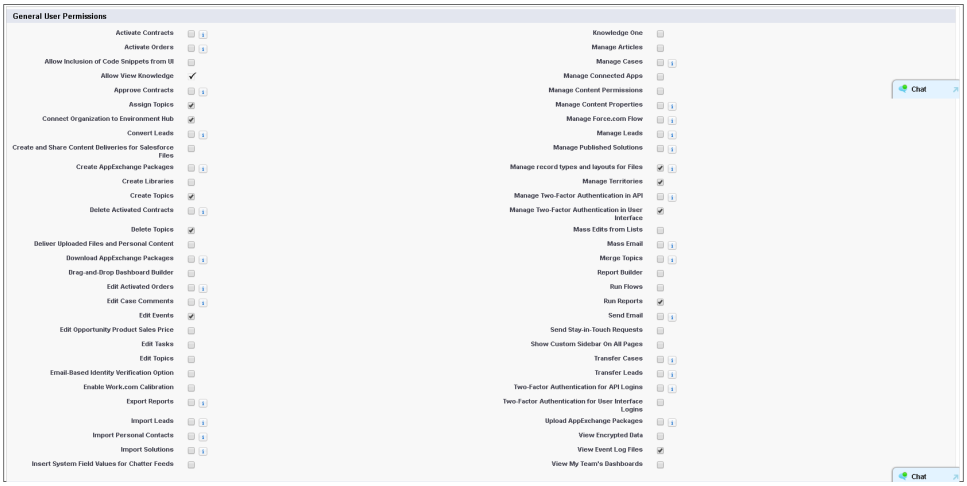
Image 8: Lightweight profile (image 3 of 5)



Administrative Permissions

Access Chatter For SharePoint	□	Manage Letterheads	□ i
API Enabled	☑	Manage Login Access Policies	☑
Assign Permission Sets	☑	Manage Macros Users Can't Undo	☑
Author Apex	□ i	Manage Mobile Configurations	□ i
Bulk API Hard Delete	□	Manage Package Licenses	□
Can Approve Feed Post	□	Manage Password Policies	☑
Chatter Internal User	✓	Manage Profiles and Permission Sets	☑
Configure Custom Recommendations	□	Manage Promoted Search Terms	□
Create and Customize Dashboards	☑	Manage Public Documents	☑ i
Create and Customize List Views	☑	Manage Public List Views	☑ i
Create and Customize Reports	☑ i	Manage Public Templates	☑ i
Create and Own New Chatter Groups	□	Manage Reporting Snapshots	□ i
Create and Set Up Communities	□	Manage Reports in Public Folders	☑ i
Create Dashboard Folders	☑ i	Manage Roles	☑
Create Report Folders	☑ i	Manage Salesforce CRM Content	□ i
Customize Application	☑ i	Manage Salesforce Knowledge	□ i
Edit HTML Templates	□ i	Manage Session Permission Set Activations	□ i
Edit My Dashboards	☑ i	Manage Sharing	☑
Edit My Own Posts	□	Manage Synonyms	□ i
Edit My Reports	☑ i	Manage Translation	☑ i
Edit Posts on Records I Own	☑	Manage Unlisted Groups	□
Edit Read Only Fields	□	Manage Users	□ i
Import Custom Objects	□	Moderate Chatter	□
Invite Customers To Chatter	□	Moderate Community Users	□
IP Restrict Requests	□	Modify All Data	□ i
Lightning Experience User	□	Modify Secure Agents	□
Manage All Private Reports and Dashboards	□	Password Never Expires	□
Manage Auth. Providers	□ i	Reset User Passwords and Unlock Users	☑ i
Manage Billing	☑ i	Run Macros on Multiple Records	□ i
Manage Business Hours Holidays	□ i	Schedule Reports	□
Manage Call Centers	□ i	Select Files from Salesforce	☑
Manage Categories	☑ i	Send Outbound Messages	□
Manage Chatter Messages	□	Share internal Knowledge articles externally	□
Manage Communities	□	Sync Files	☑
Manage Custom Permissions	☑	Transfer Record	☑
Manage Custom Report Types	□ i	Use Identity Features	□
Manage Dashboards in Public Folders	☑ i	Use Team Reassignment Wizards	☑
Manage Data Categories	□ i	View All Data	□ i
Manage Data Integrations	□	View All Users	☑
Manage Dynamic Dashboards	□	View Dashboards in Public Folders	☑
Manage Email Client Configurations	□ i	View Data Categories	☑ i
Manage Exchange Configurations	□ i	View Help Link	✓
Manage Internal Users	☑	View Reports in Public Folders	☑
Manage IP Addresses	☑	View Setup and Configuration	☑
Manage Knowledge Article Import/Export	□ i		

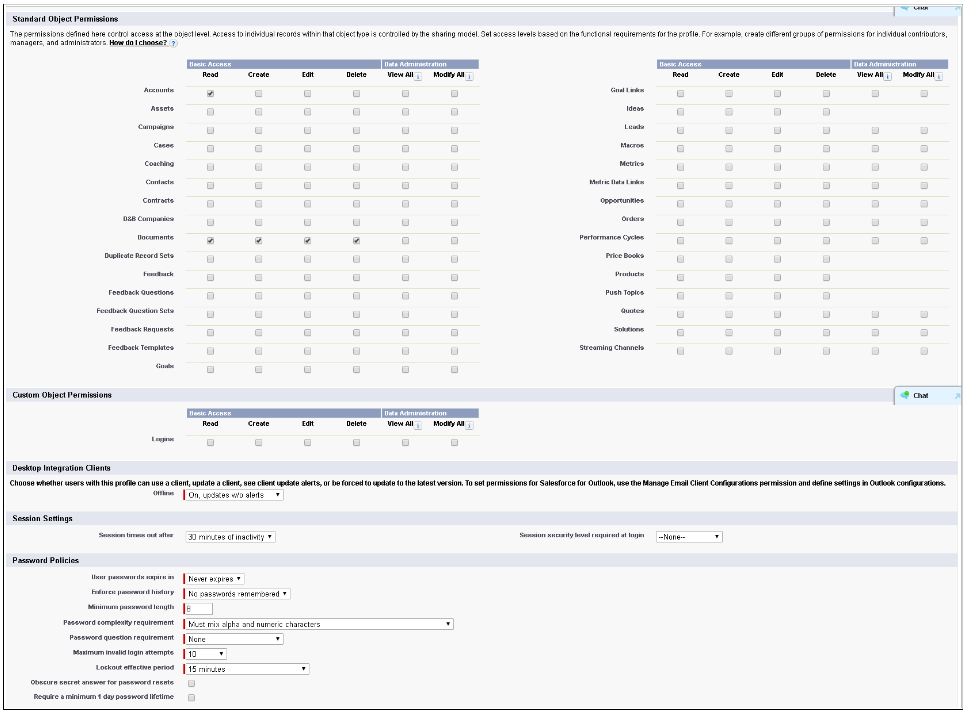
Image 9: Lightweight profile (image 4 of 5)



General User Permissions

Activate Contracts	☐	Knowledge One	☐
Activate Orders	☐	Manage Articles	☐
Allow Inclusion of Code Snippets from UI	☐	Manage Cases	☐
Allow View Knowledge	✓	Manage Connected Apps	☐
Approve Contracts	☐	Manage Content Permissions	☐
Assign Topics	☑	Manage Content Properties	☐
Connect Organization to Environment Hub	☑	Manage Force.com Flow	☐
Convert Leads	☐	Manage Leads	☐
Create and Share Content Deliveries for Salesforce Files	☐	Manage Published Solutions	☐
Create AppExchange Packages	☐	Manage record types and layouts for Files	☑
Create Libraries	☐	Manage Territories	☑
Create Topics	☑	Manage Two-Factor Authentication in API	☐
Delete Activated Contracts	☐	Manage Two-Factor Authentication in User Interface	☑
Delete Topics	☑	Mass Edits from Lists	☐
Deliver Uploaded Files and Personal Content	☐	Mass Email	☐
Download AppExchange Packages	☐	Merge Topics	☐
Drag-and-Drop Dashboard Builder	☐	Report Builder	☐
Edit Activated Orders	☐	Run Flows	☐
Edit Case Comments	☐	Run Reports	☑
Edit Events	☑	Send Email	☐
Edit Opportunity Product Sales Price	☐	Send Stay-in-Touch Requests	☐
Edit Tasks	☐	Show Custom Sidebar On All Pages	☐
Edit Topics	☐	Transfer Cases	☐
Email-Based Identity Verification Option	☐	Transfer Leads	☐
Enable Work.com Calibration	☐	Two-Factor Authentication for API Logins	☐
Export Reports	☐	Two-Factor Authentication for User Interface Logins	☐
Import Leads	☐	Upload AppExchange Packages	☐
Import Personal Contacts	☐	View Encrypted Data	☐
Import Solutions	☐	View Event Log Files	☑
Insert System Field Values for Chatter Feeds	☐	View My Team's Dashboards	☐

Image 10: Lightweight profile (image 5 of 5)



Standard Object Permissions

The permissions defined here control access at the object level. Access to individual records within that object type is controlled by the sharing model. Set access levels based on the functional requirements for the profile. For example, create different groups of permissions for individual contributors, managers, and administrators. **How do I choose?**

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Accounts	☑	☐	☐	☐	☐	☐
Assets	☐	☐	☐	☐	☐	☐
Campaigns	☐	☐	☐	☐	☐	☐
Cases	☐	☐	☐	☐	☐	☐
Coaching	☐	☐	☐	☐	☐	☐
Contacts	☐	☐	☐	☐	☐	☐
Contracts	☐	☐	☐	☐	☐	☐
D&B Companies	☐	☐	☐	☐	☐	☐
Documents	☑	☑	☑	☑	☐	☐
Duplicate Record Sets	☐	☐	☐	☐	☐	☐
Feedback	☐	☐	☐	☐	☐	☐
Feedback Questions	☐	☐	☐	☐	☐	☐
Feedback Question Sets	☐	☐	☐	☐	☐	☐
Feedback Requests	☐	☐	☐	☐	☐	☐
Feedback Templates	☐	☐	☐	☐	☐	☐
Goals	☐	☐	☐	☐	☐	☐

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Goal Links	☐	☐	☐	☐	☐	☐
Ideas	☐	☐	☐	☐		
Leads	☐	☐	☐	☐	☐	☐
Macros	☐	☐	☐	☐	☐	☐
Metrics	☐	☐	☐	☐	☐	☐
Metric Data Links	☐	☐	☐	☐	☐	☐
Opportunities	☐	☐	☐	☐	☐	☐
Orders	☐	☐	☐	☐	☐	☐
Performance Cycles	☐	☐	☐	☐	☐	☐
Price Books	☐	☐	☐	☐		
Products	☐	☐	☐	☐		
Push Topics	☐	☐	☐	☐		
Quotes	☐	☐	☐	☐	☐	☐
Solutions	☐	☐	☐	☐	☐	☐
Streaming Channels	☐	☐	☐	☐	☐	☐

Custom Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Logins	☐	☐	☐	☐	☐	☐

Desktop Integration Clients

Choose whether users with this profile can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesforce for Outlook, use the Manage Email Client Configurations permission and define settings in Outlook configurations.

Offline: On, updates w/o alerts ▾

Session Settings

Session times out after: 30 minutes of inactivity ▾

Session security level required at login: --None-- ▾

Password Policies

User passwords expire in: Never expires ▾

Enforce password history: No passwords remembered ▾

Minimum password length: 8

Password complexity requirement: Must mix alpha and numeric characters ▾

Password question requirement: None ▾

Maximum invalid login attempts: 10 ▾

Lockout effective period: 15 minutes ▾

Obscure secret answer for password resets: ☐

Require a minimum 1 day password lifetime: ☐

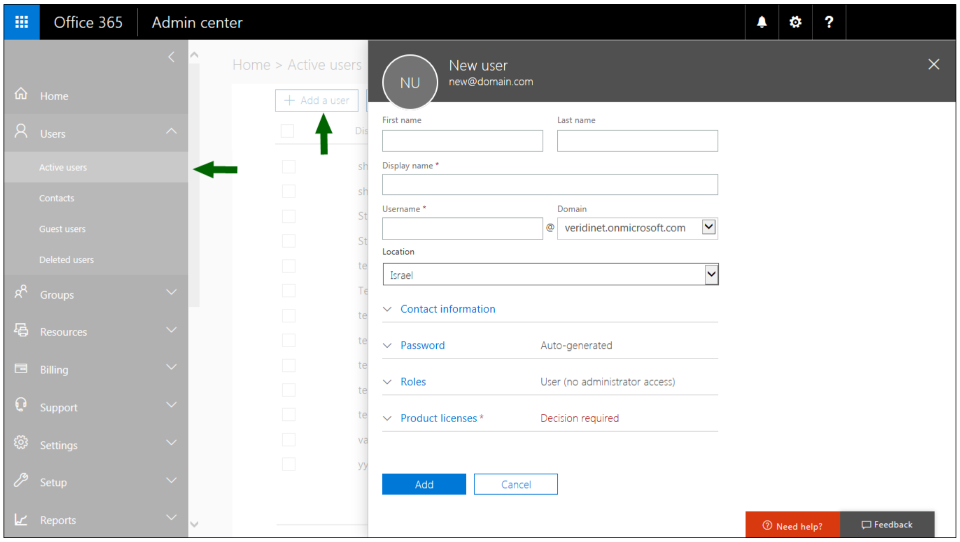
APPENDIX B

Microsoft Office 365 Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Microsoft Office 365 Images

Image 1: Create new user

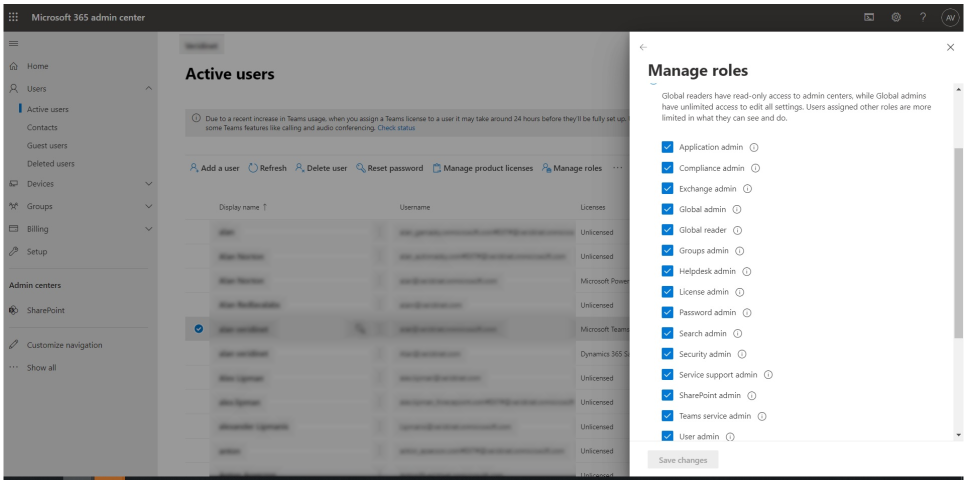


New user
new@domain.com

First name
Last name
Display name *
Username * @
Domain: veridinet.onmicrosoft.com
Location: Israel

Contact information
Password: Auto-generated
Roles: User (no administrator access)
Product licenses *: Decision required

Image 2: Set user role



Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. some Teams features like calling and audio conferencing. Check status

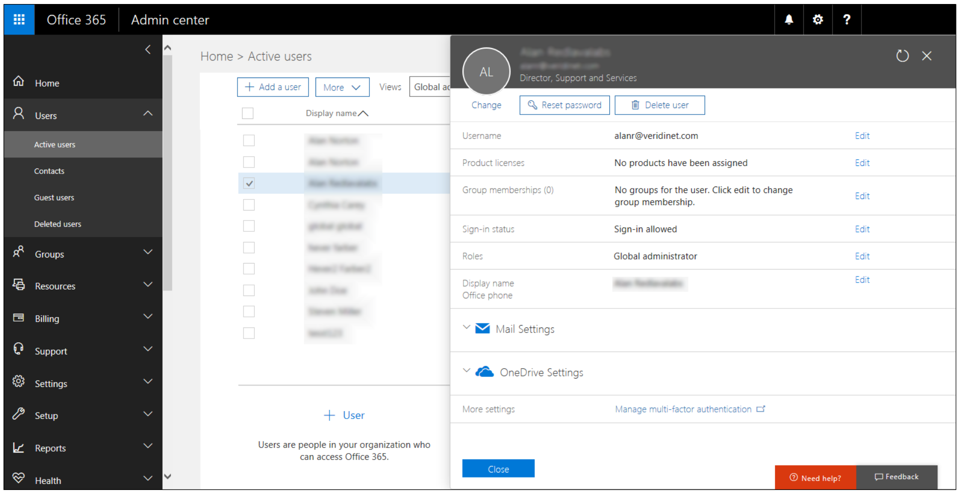
Display name	Username	Licenses
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Microsoft Power
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Microsoft Teams
[redacted]	[redacted]	Dynamics 365 S
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed

Manage roles

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- ☑ Application admin
- ☑ Compliance admin
- ☑ Exchange admin
- ☑ Global admin
- ☑ Global reader
- ☑ Groups admin
- ☑ Helpdesk admin
- ☑ License admin
- ☑ Password admin
- ☑ Search admin
- ☑ Security admin
- ☑ Service support admin
- ☑ SharePoint admin
- ☑ Teams service admin
- ☑ User admin

Image 3: Edit user



Users are people in your organization who can access Office 365.

[redacted]
Director, Support and Services

Username	alanr@veridinet.com	Edit
Product licenses	No products have been assigned	Edit
Group memberships (0)	No groups for the user. Click edit to change group membership.	Edit
Sign-in status	Sign-in allowed	Edit
Roles	Global administrator	Edit
Display name Office phone	[redacted]	Edit

Mail Settings

OneDrive Settings

More settings: Manage multi-factor authentication

APPENDIX C

Amazon Web Services Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Amazon Web Services Images

Image 1: Create an IAM user (image 1 of 5)

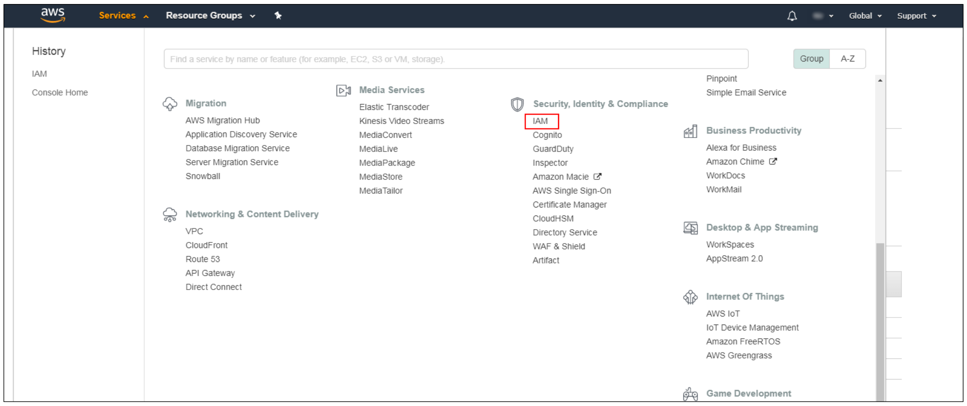
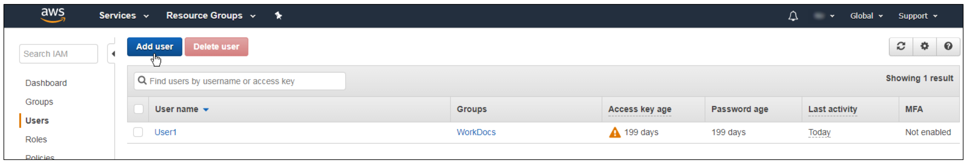
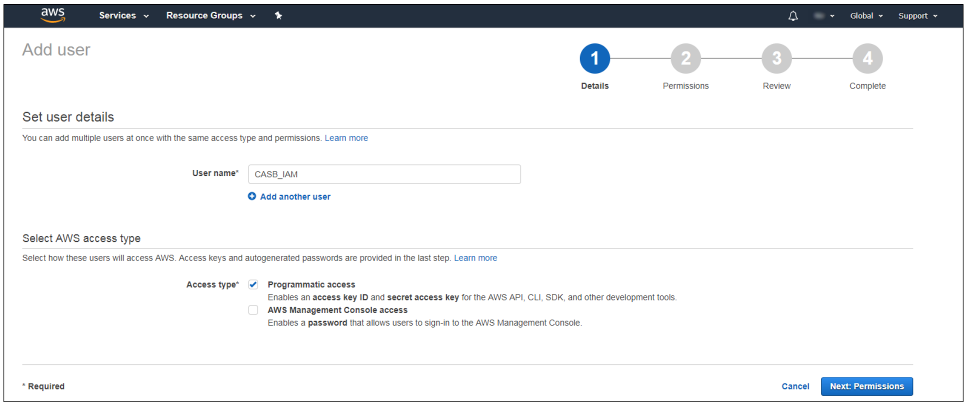


Image 2: Create an IAM user (image 2 of 5)



	User name	Groups	Access key age	Password age	Last activity	MFA
□	User1	WorkDocs	⚠ 199 days	199 days	Today	Not enabled

Image 3: Create an IAM user (image 3 of 5)



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* CASB_IAM

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

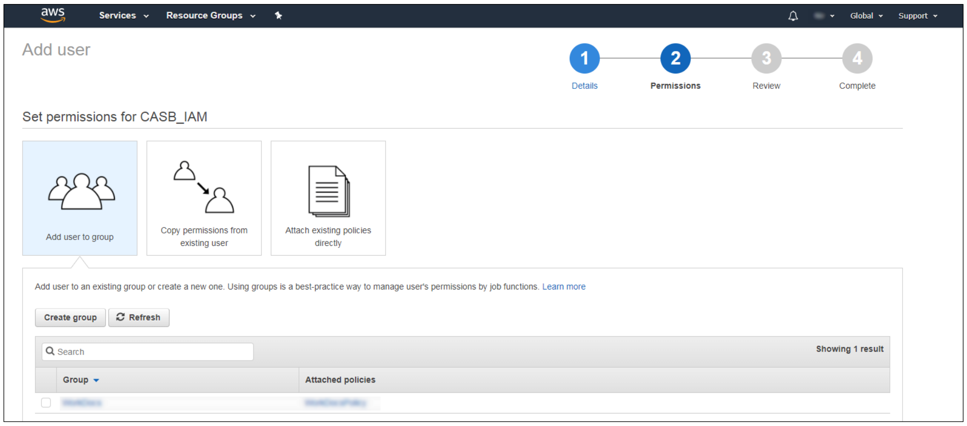
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Cancel | Next: Permissions

Image 4: Create an IAM user (image 4 of 5)



Add user

Set permissions for CASB_IAM

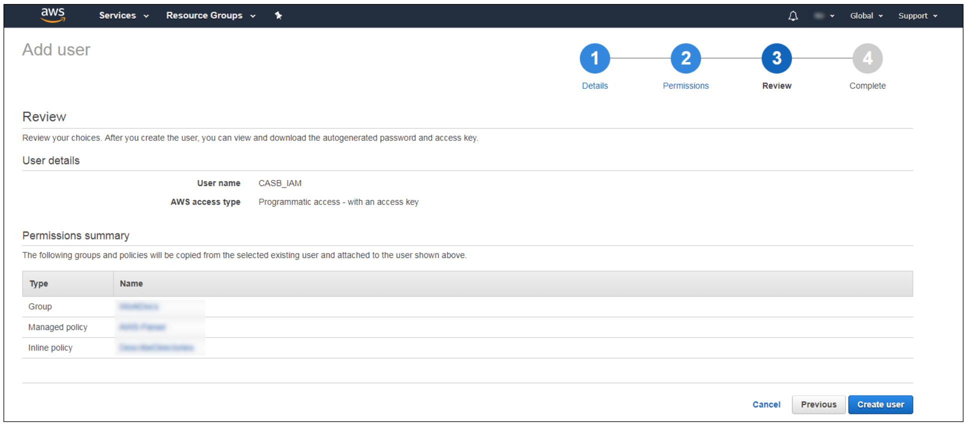
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Create group | Refresh

Search | Showing 1 result

	Group	Attached policies
☐	[redacted]	[redacted]

Image 5: Create an IAM user (image 5 of 5)



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

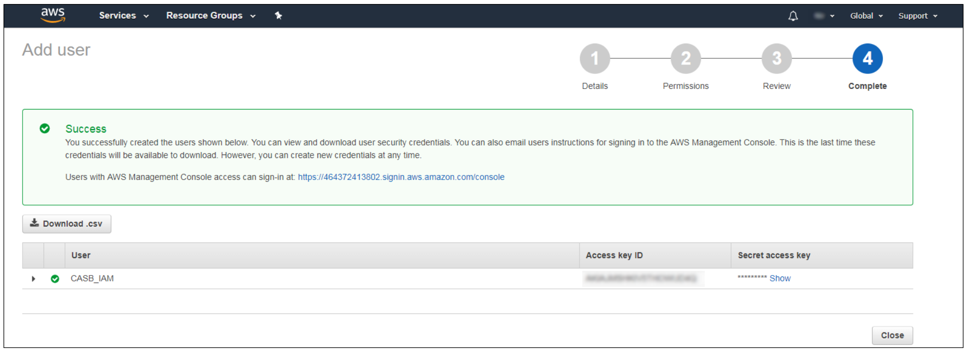
User name	CASB_IAM
AWS access type	Programmatic access - with an access key

Permissions summary

The following groups and policies will be copied from the selected existing user and attached to the user shown above.

Type	Name
Group	[redacted]
Managed policy	[redacted]
Inline policy	[redacted]

Image 6: Copy security credentials



Add user

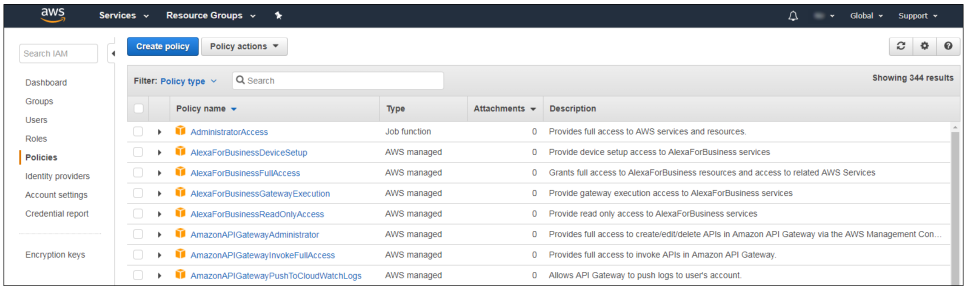
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://464372413802.signin.aws.amazon.com/console

		User	Access key ID	Secret access key
▸	✓	CASB_IAM	[redacted]	********* Show

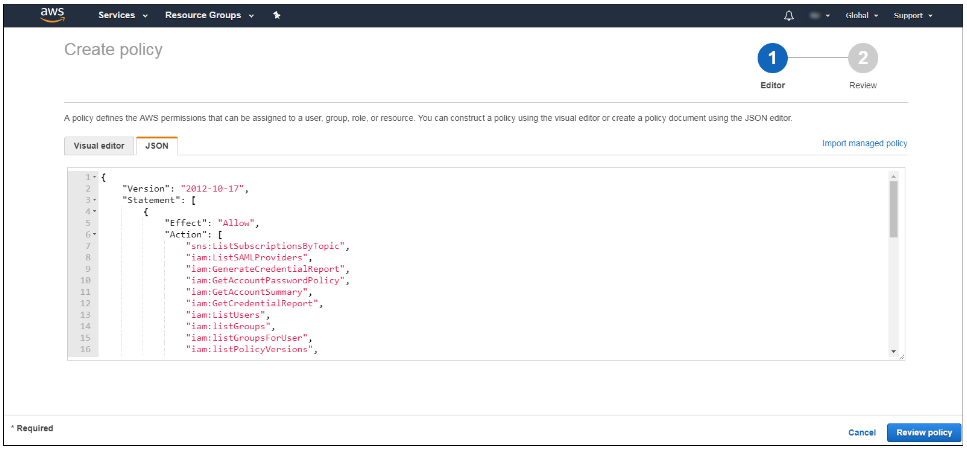
Image 7: Create custom policy (image 1 of 3)



Showing 344 results

	Policy name	Type	Attachments	Description
□	AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
□	AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
□	AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to related AWS Services
□	AlexaForBusinessGatewayExecution	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
□	AlexaForBusinessReadOnlyAccess	AWS managed	0	Provide read only access to AlexaForBusiness services
□	AmazonAPIGatewayAdministrator	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Con…
□	AmazonAPIGatewayInvokeFullAccess	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
□	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0	Allows API Gateway to push logs to user's account.

Image 8: Create custom policy (image 2 of 3)



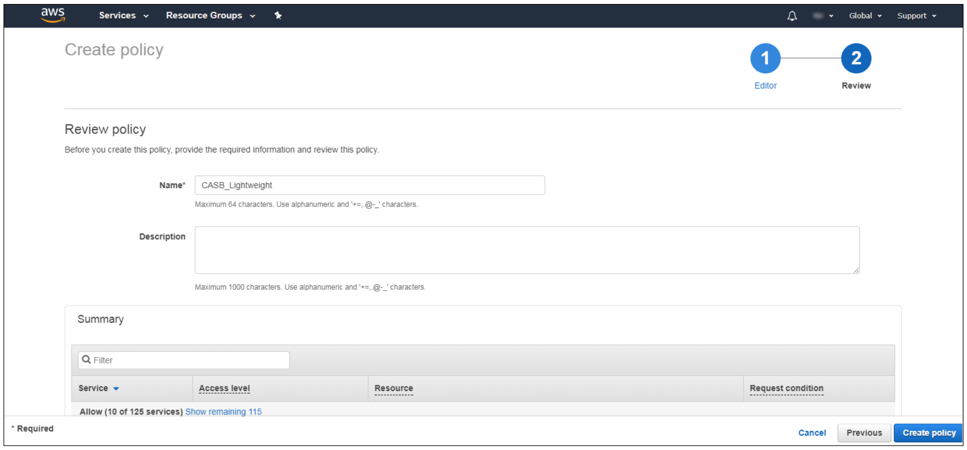
Create policy

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListSubscriptionsByTopic",
                "iam:ListSAMLProviders",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:ListUsers",
                "iam:listGroups",
                "iam:listGroupsForUser",
                "iam:listPolicyVersions",
```

* Required

Image 9: Create custom policy (image 3 of 3)



Create policy

Review policy

Before you create this policy, provide the required information and review this policy.

Name*: CASB_Lightweight

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description:

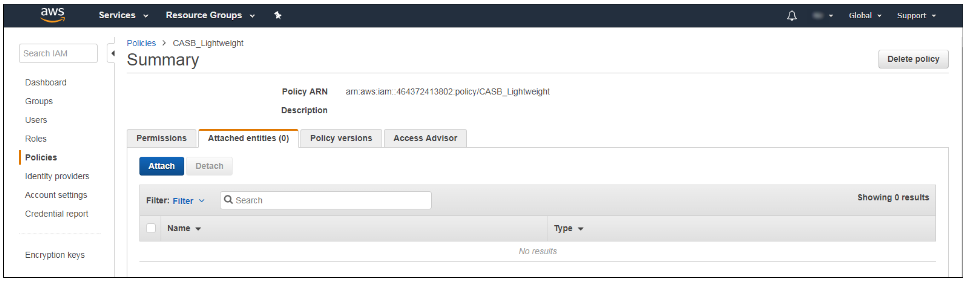
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (10 of 125 services) Show remaining 115			

* Required

Image 10: Attach IAM policy (image 1 of 3)



Summary

Policy ARN arn:aws:iam::464372413802:policy/CASB_Lightweight

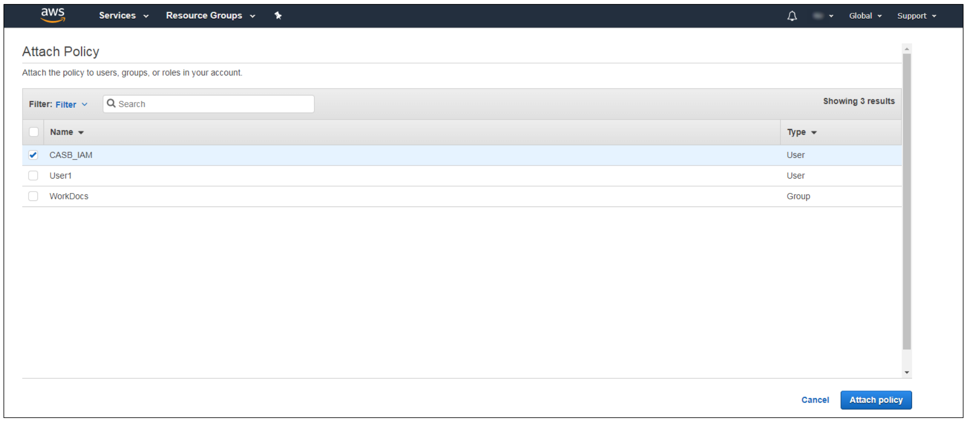
Description

Showing 0 results

Name	Type

No results

Image 11: Attach IAM policy (image 2 of 3)



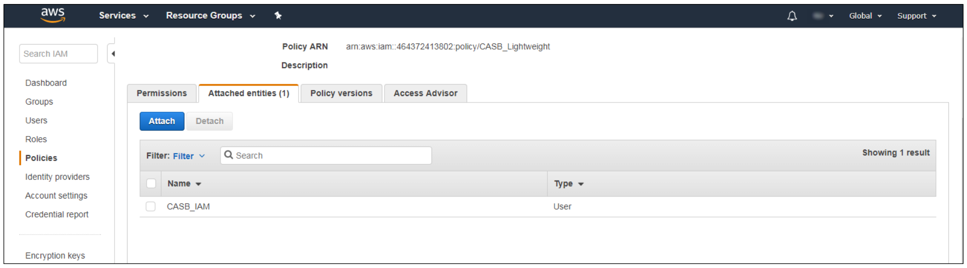
Attach Policy

Attach the policy to users, groups, or roles in your account.

Showing 3 results

	Name	Type
☑	CASB_IAM	User
□	User1	User
□	WorkDocs	Group

Image 12: Attach IAM policy (image 3 of 3)



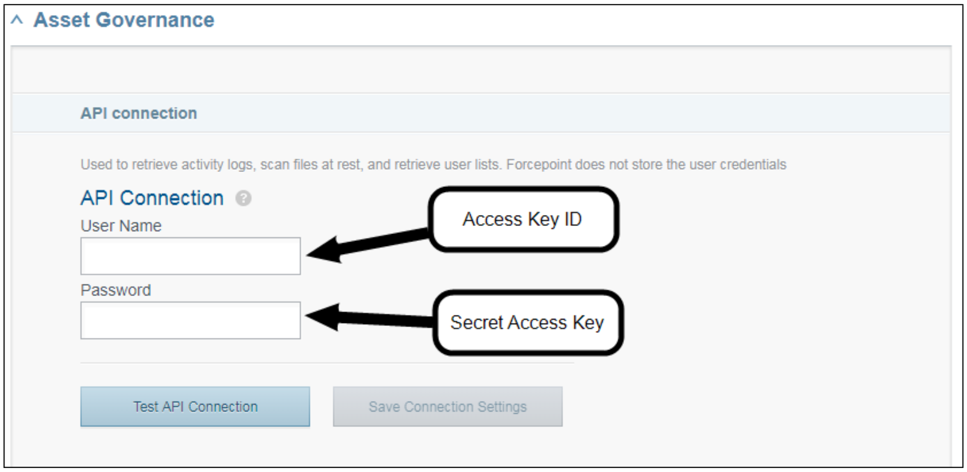
Policy ARN arn:aws:iam::464372413802:policy/CASB_Lightweight

Description

Showing 1 result

	Name	Type
□	CASB_IAM	User

Image 13: AWS credentials on Forcepoint CASB management portal



Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

APPENDIX D

Google G Suite Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

G Suite Images

Images 1-7: Setting up a role

Image 1: Open Admin roles

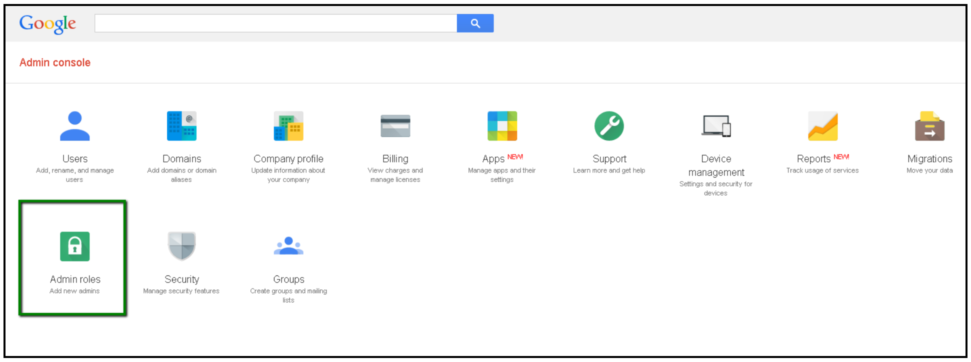
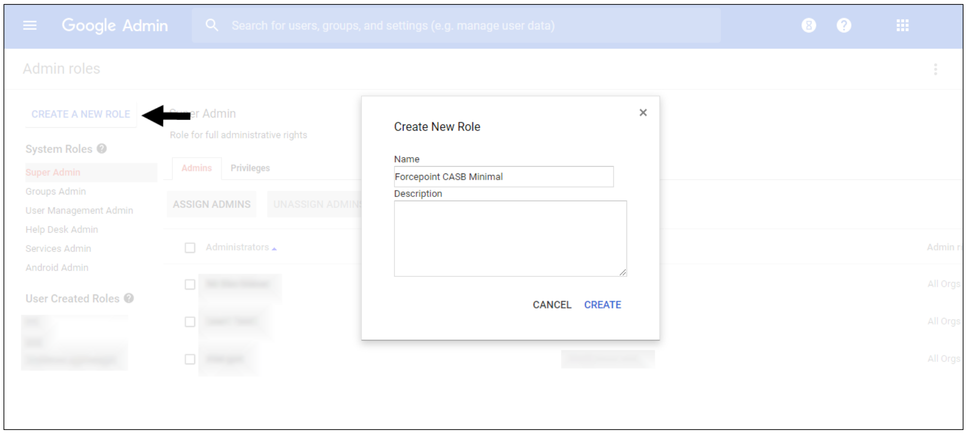


Image 2: Create new role

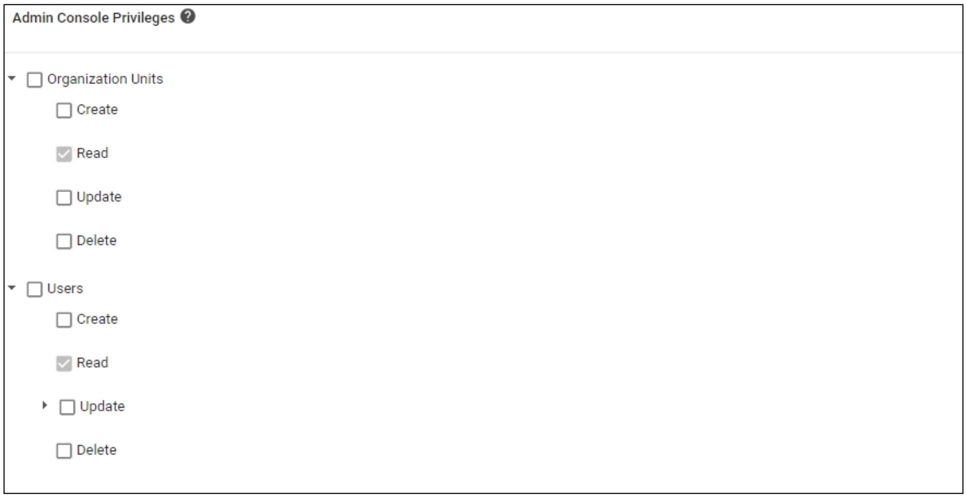


Create New Role

Name: Forcepoint CASB Minimal

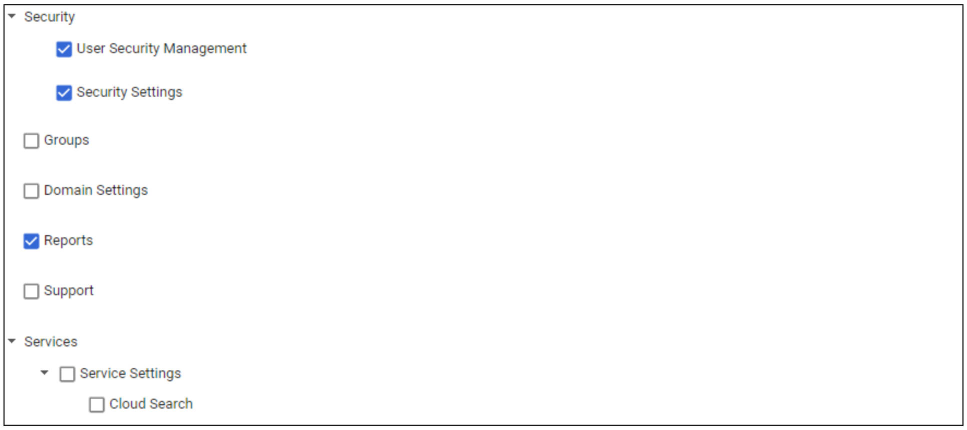
Description:

Images 3-7: Select privileges as displayed in the images below

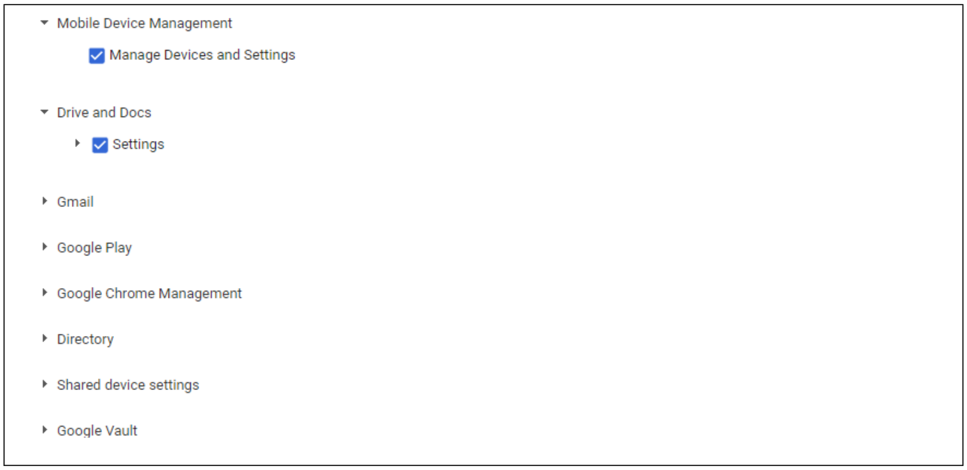


Admin Console Privileges

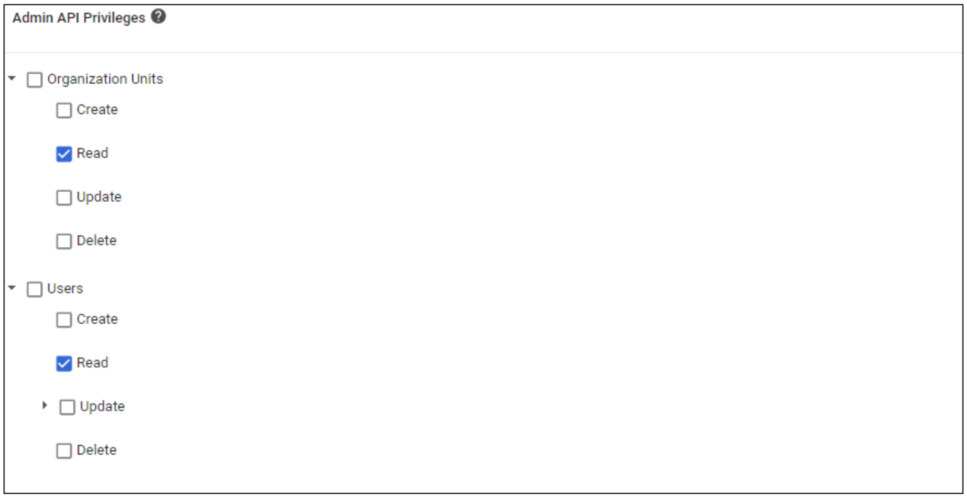
- ☐ Organization Units
  - ☐ Create
  - ☑ Read
  - ☐ Update
  - ☐ Delete
- ☐ Users
  - ☐ Create
  - ☑ Read
  - ☐ Update
  - ☐ Delete



- ▾ Security
  - ☑ User Security Management
  - ☑ Security Settings
- □ Groups
- □ Domain Settings
- ☑ Reports
- □ Support
- ▾ Services
  - ▾ □ Service Settings
    - □ Cloud Search

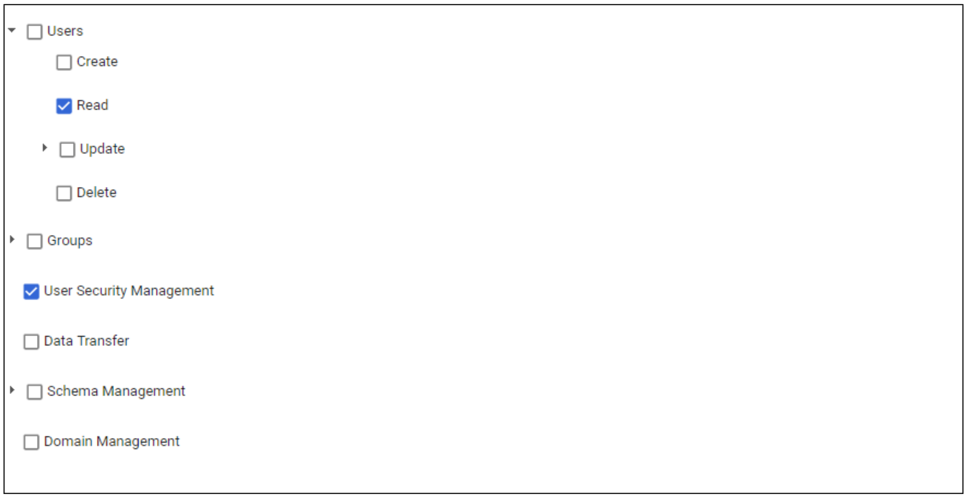


- ▾ Mobile Device Management
  - ☑ Manage Devices and Settings
- ▾ Drive and Docs
  - ▸ ☑ Settings
- ▸ Gmail
- ▸ Google Play
- ▸ Google Chrome Management
- ▸ Directory
- ▸ Shared device settings
- ▸ Google Vault



Admin API Privileges

- ▾ □ Organization Units
  - □ Create
  - ☑ Read
  - □ Update
  - □ Delete
- ▾ □ Users
  - □ Create
  - ☑ Read
  - ▸ □ Update
  - □ Delete



- □ Users
  - □ Create
  - ☑ Read
  - □ Update
  - □ Delete
- □ Groups
- ☑ User Security Management
- □ Data Transfer
- □ Schema Management
- □ Domain Management

Images 8-10: Create user and assign role

Image 8: Open Users

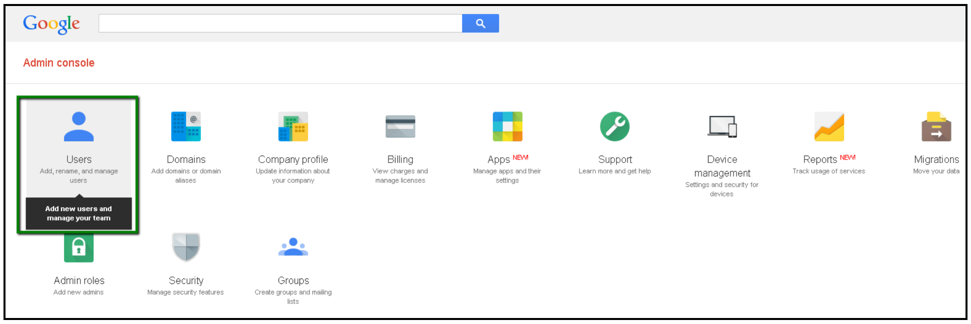
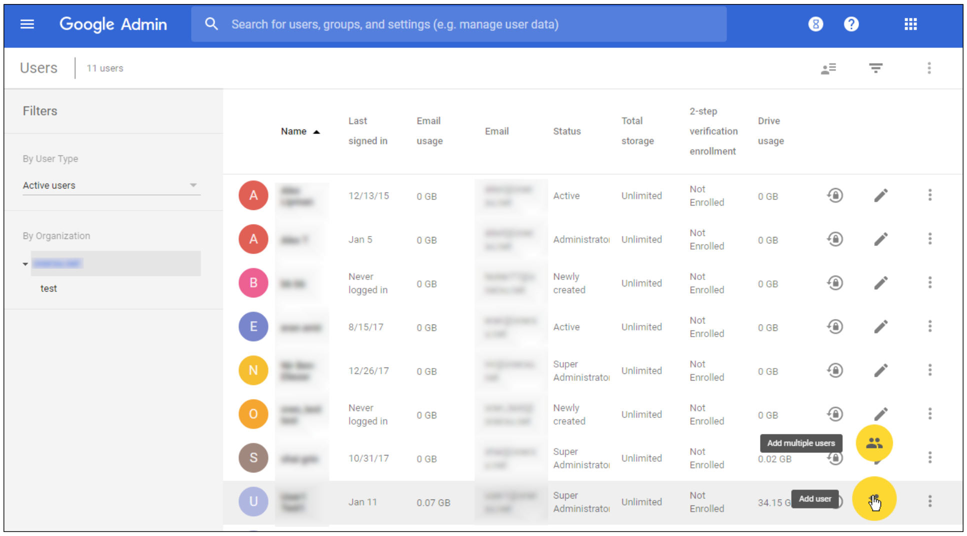
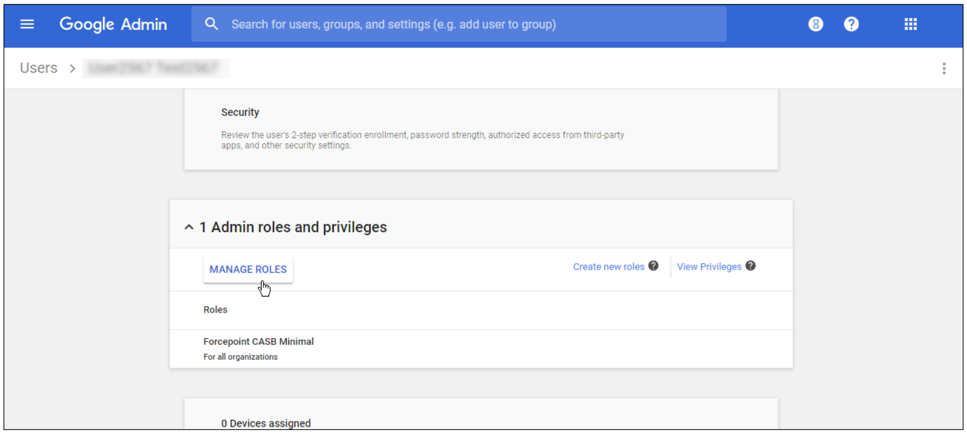

Google
Admin console
Users
Add, rename, and manage users
Add new users and manage your team
Domains
Add domains or domain aliases
Company profile
Update information about your company
Billing
View charges and manage licenses
Apps NEW
Manage apps and their settings
Support
Learn more and get help
Device management
Settings and security for devices
Reports NEW
Track usage of services
Migrations
Move your data
Admin roles
Add new admins
Security
Manage security features
Groups
Create groups and mailing lists

Image 9: Add a user



	Name ▲	Last signed in	Email usage	Email	Status	Total storage	2-step verification enrollment	Drive usage
A	[redacted]	12/13/15	0 GB	[redacted]	Active	Unlimited	Not Enrolled	0 GB
A	[redacted]	Jan 5	0 GB	[redacted]	Administrator	Unlimited	Not Enrolled	0 GB
B	[redacted]	Never logged in	0 GB	[redacted]	Newly created	Unlimited	Not Enrolled	0 GB
E	[redacted]	8/15/17	0 GB	[redacted]	Active	Unlimited	Not Enrolled	0 GB
N	[redacted]	12/26/17	0 GB	[redacted]	Super Administrator	Unlimited	Not Enrolled	0 GB
O	[redacted]	Never logged in	0 GB	[redacted]	Newly created	Unlimited	Not Enrolled	0 GB
S	[redacted]	10/31/17	0 GB	[redacted]	Super Administrator	Unlimited	Not Enrolled	0.02 GB
U	[redacted]	Jan 11	0.07 GB	[redacted]	Super Administrator	Unlimited	Not Enrolled	34.15 G

Image 10: Open Admin roles and privileges on the user's page. Select **Manage Roles** and assign the new role (from Image 2 above)



Security

Review the user's 2-step verification enrollment, password strength, authorized access from third-party apps, and other security settings.

1 Admin roles and privileges

Roles

Forcepoint CASB Minimal
For all organizations

0 Devices assigned

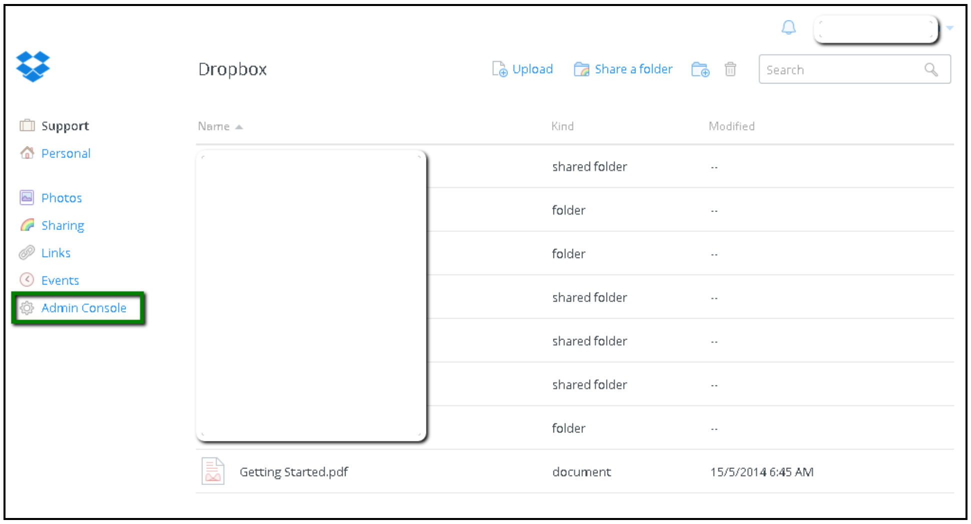
APPENDIX E

Dropbox Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Dropbox images

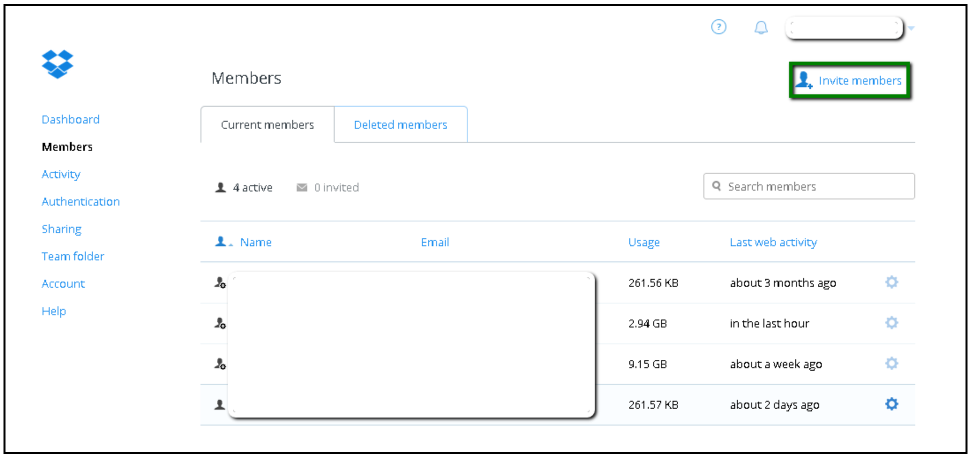
Image 1: Open the Admin Console



Dropbox

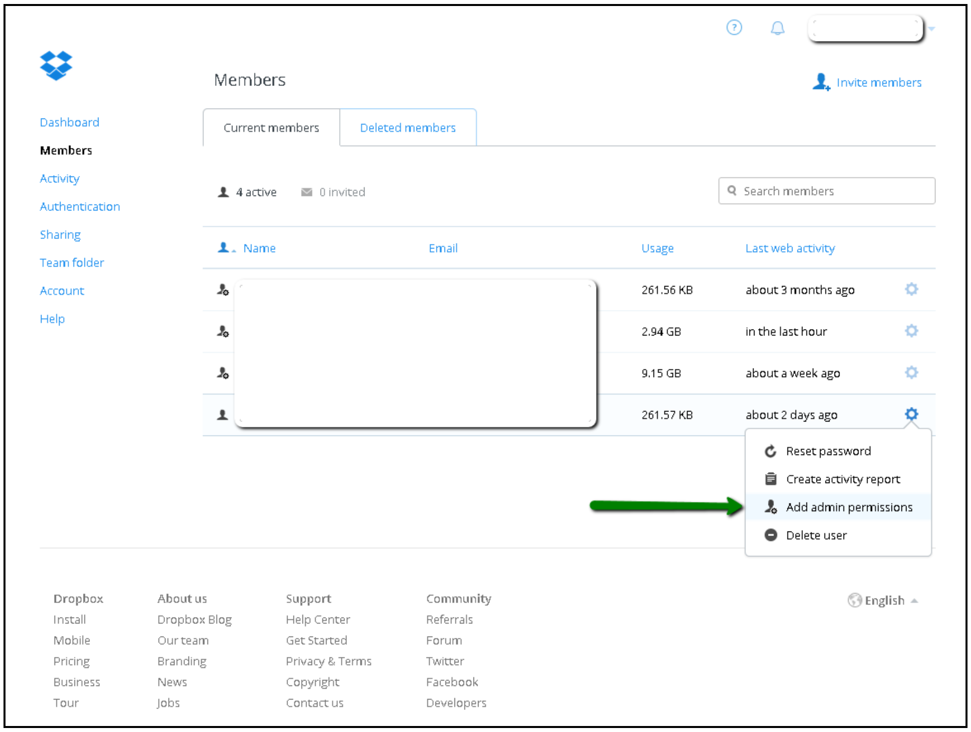
Name	Kind	Modified
	shared folder	--
	folder	--
	folder	--
	shared folder	--
	shared folder	--
	shared folder	--
	folder	--
Getting Started.pdf	document	15/5/2014 6:45 AM

Image 2: Invite member



Name	Email	Usage	Last web activity
[redacted]	[redacted]	261.56 KB	about 3 months ago
[redacted]	[redacted]	2.94 GB	in the last hour
[redacted]	[redacted]	9.15 GB	about a week ago
[redacted]	[redacted]	261.57 KB	about 2 days ago

Image 3: Set member as Admin



Name	Email	Usage	Last web activity
[redacted]	[redacted]	261.56 KB	about 3 months ago
[redacted]	[redacted]	2.94 GB	in the last hour
[redacted]	[redacted]	9.15 GB	about a week ago
[redacted]	[redacted]	261.57 KB	about 2 days ago

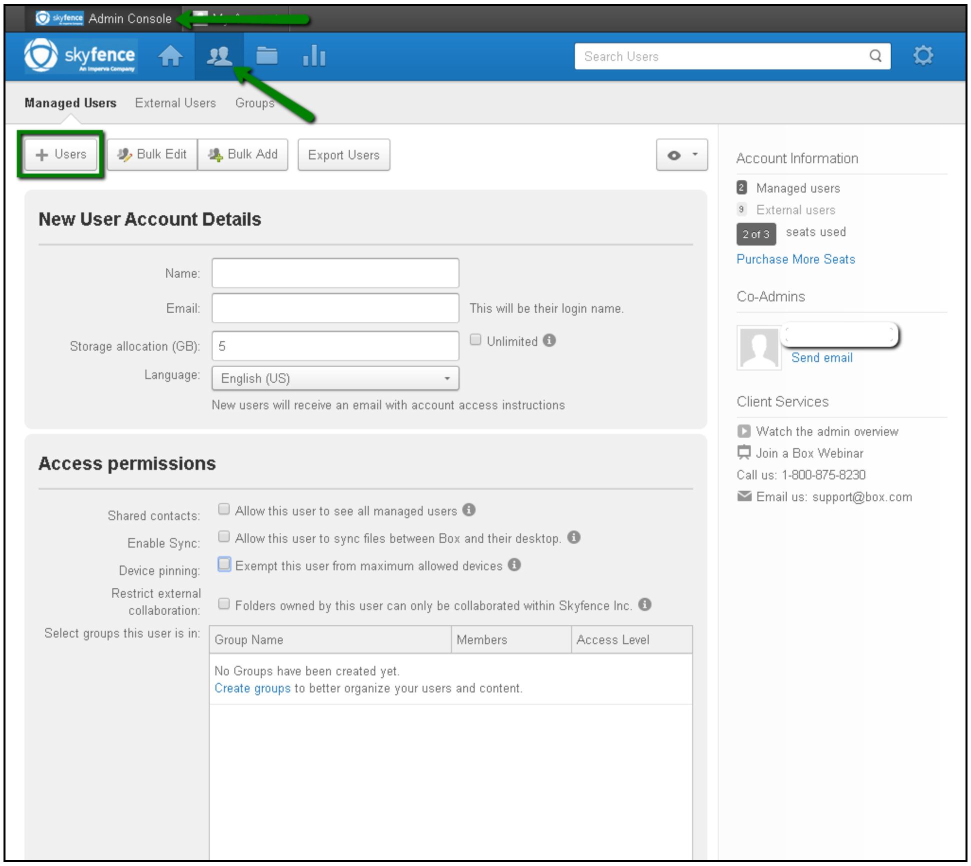
APPENDIX F

Box Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Box images

Image 1: Create user



New User Account Details

Name:

Email: This will be their login name.

Storage allocation (GB): 5 □ Unlimited

Language: English (US)

New users will receive an email with account access instructions

Access permissions

Shared contacts: □ Allow this user to see all managed users

Enable Sync: □ Allow this user to sync files between Box and their desktop.

Device pinning: □ Exempt this user from maximum allowed devices

Restrict external collaboration: □ Folders owned by this user can only be collaborated within Skyfence Inc.

Select groups this user is in:

Group Name	Members	Access Level
No Groups have been created yet. Create groups to better organize your users and content.		

Account Information

2 Managed users

9 External users

2 of 3 seats used

Purchase More Seats

Co-Admins

Send email

Client Services

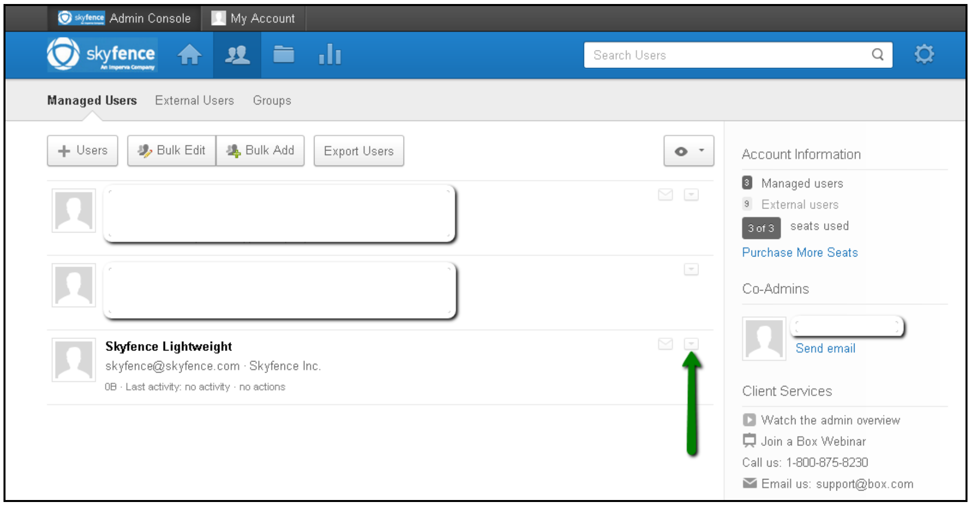
Watch the admin overview

Join a Box Webinar

Call us: 1-800-875-8230

Email us: support@box.com

Image 2: Configure User Settings (image 1 of 2)



[redacted]

[redacted]

Skyfence Lightweight
skyfence@skyfence.com · Skyfence Inc.
0B · Last activity: no activity · no actions

Account Information

3 Managed users
9 External users
3 of 3 seats used
Purchase More Seats

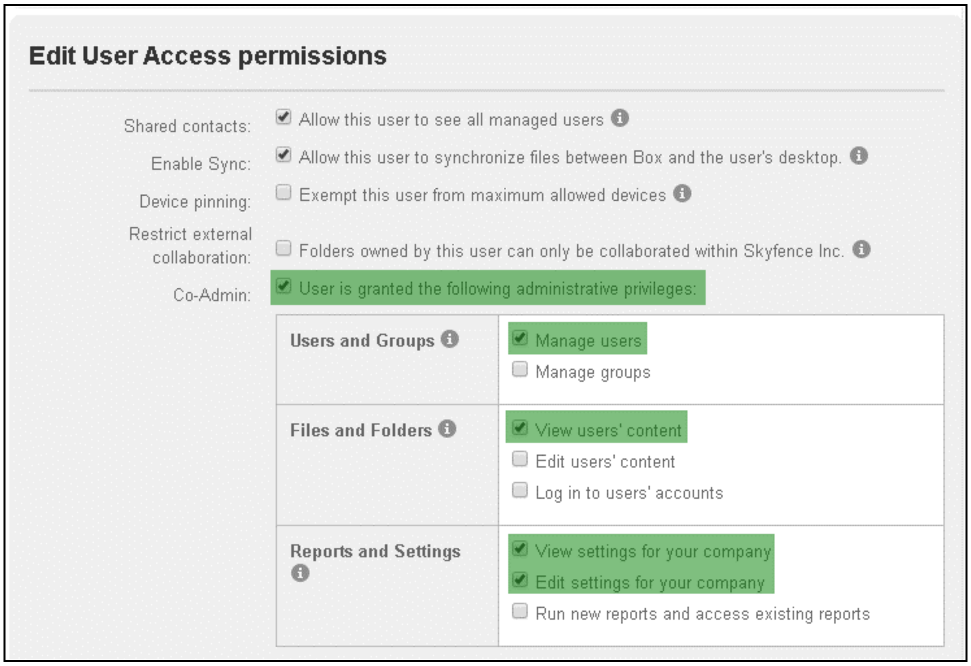
Co-Admins

[redacted]
Send email

Client Services

Watch the admin overview
Join a Box Webinar
Call us: 1-800-875-8230
Email us: support@box.com

Image 3: Configure User Settings (image 2 of 2)



Edit User Access permissions

Shared contacts: ☑ Allow this user to see all managed users

Enable Sync: ☑ Allow this user to synchronize files between Box and the user's desktop.

Device pinning: □ Exempt this user from maximum allowed devices

Restrict external collaboration: □ Folders owned by this user can only be collaborated within Skyfence Inc.

Co-Admin: ☑ User is granted the following administrative privileges:

Users and Groups	☑ Manage users □ Manage groups
Files and Folders	☑ View users' content □ Edit users' content □ Log in to users' accounts
Reports and Settings	☑ View settings for your company ☑ Edit settings for your company □ Run new reports and access existing reports

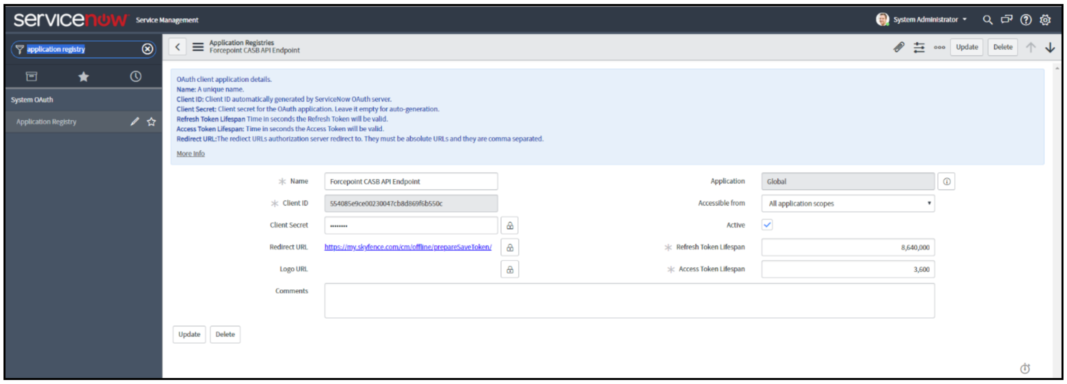
APPENDIX G

ServiceNow Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

ServiceNow images

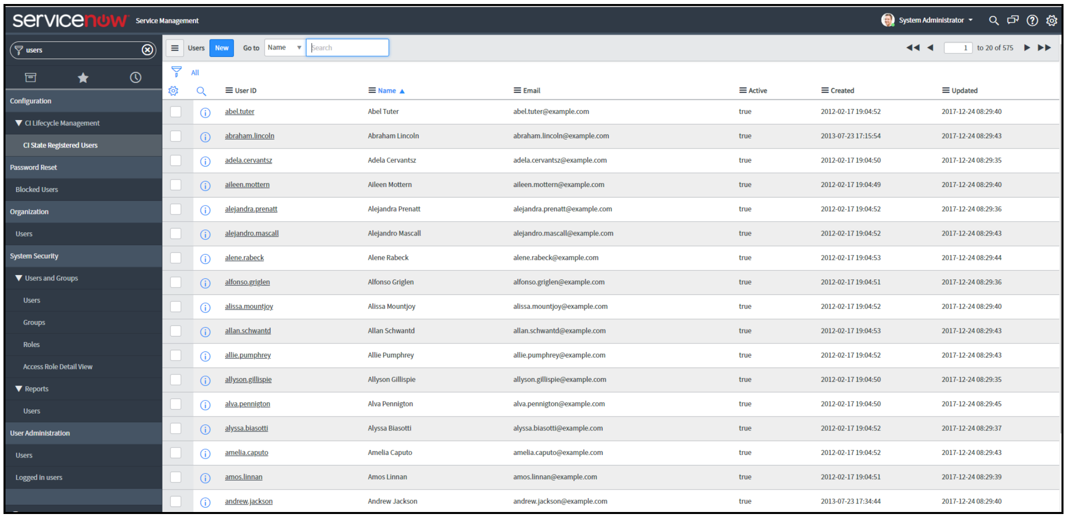
Image 1: Create OAuth Client Application



OAuth client application details.
Name: A unique name.
Client ID: Client ID automatically generated by ServiceNow OAuth server.
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 rediect URLs authorization server redirect to. They must be absolute URLs and they are comma separated.

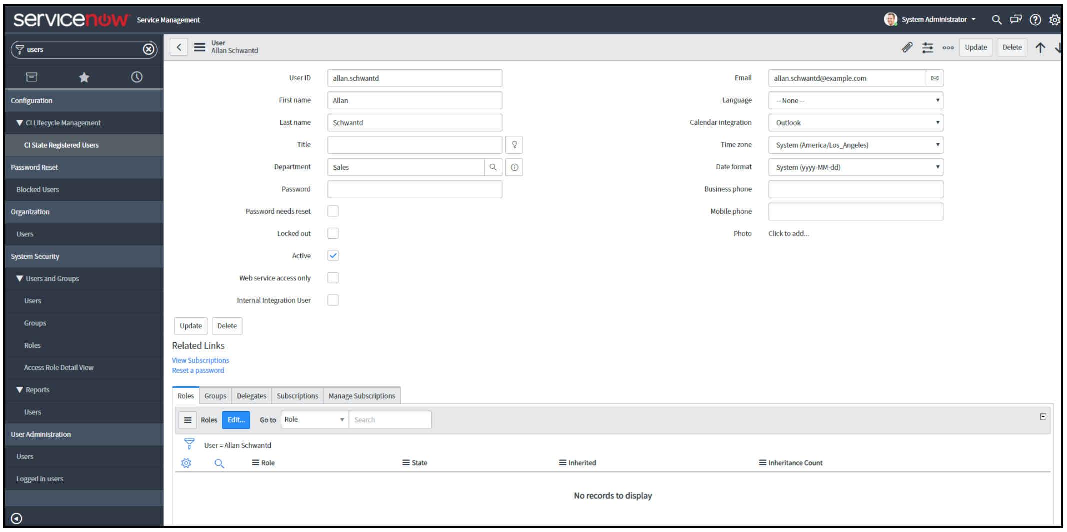
* Name	Forcepoint CASB API Endpoint	Application	Global
* Client ID	554085e9ce00230047cb8d869f6b550c	Accessible from	All application scopes
Client Secret	••••••••	Active	☑
Redirect URL	https://my.skyfence.com/cm/offline/prepareSaveToken/	* Refresh Token Lifespan	8,640,000
Logo URL		* Access Token Lifespan	3,600
Comments			

Image 2: User list



User ID	Name ▲	Email	Active	Created	Updated
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:40
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-23 17:15:54	2017-12-24 08:29:43
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	2012-02-17 19:04:50	2017-12-24 08:29:35
aileen.mottern	Aileen Mottern	aileen.mottern@example.com	true	2012-02-17 19:04:49	2017-12-24 08:29:40
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:36
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:43
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-17 19:04:53	2017-12-24 08:29:44
alfonso.griglen	Alfonso Griglen	alfonso.griglen@example.com	true	2012-02-17 19:04:51	2017-12-24 08:29:36
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:40
allan.schwantd	Allan Schwantd	allan.schwantd@example.com	true	2012-02-17 19:04:53	2017-12-24 08:29:43
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:43
allyson.gillispie	Allyson Gillispie	allyson.gillispie@example.com	true	2012-02-17 19:04:50	2017-12-24 08:29:35
alva.pennigton	Alva Pennigton	alva.pennigton@example.com	true	2012-02-17 19:04:50	2017-12-24 08:29:45
alyssa.biasotti	Alyssa Biasotti	alyssa.biasotti@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:37
amelia.caputo	Amelia Caputo	amelia.caputo@example.com	true	2012-02-17 19:04:52	2017-12-24 08:29:43
amos.linnan	Amos Linnan	amos.linnan@example.com	true	2012-02-17 19:04:51	2017-12-24 08:29:39
andrew.jackson	Andrew Jackson	andrew.jackson@example.com	true	2013-07-23 17:34:44	2017-12-24 08:29:40

Image 3: Adding a new user



User
Allan Schwantd

User ID	allan.schwantd	Email	allan.schwantd@example.com
First name	Allan	Language	-- None --
Last name	Schwantd	Calendar integration	Outlook
Title		Time zone	System (America/Los_Angeles)
Department	Sales	Date format	System (yyyy-MM-dd)
Password		Business phone	
Password needs reset	□	Mobile phone	
Locked out	□	Photo	Click to add...
Active	☑		
Web service access only	□		
Internal Integration User	□		

Related Links

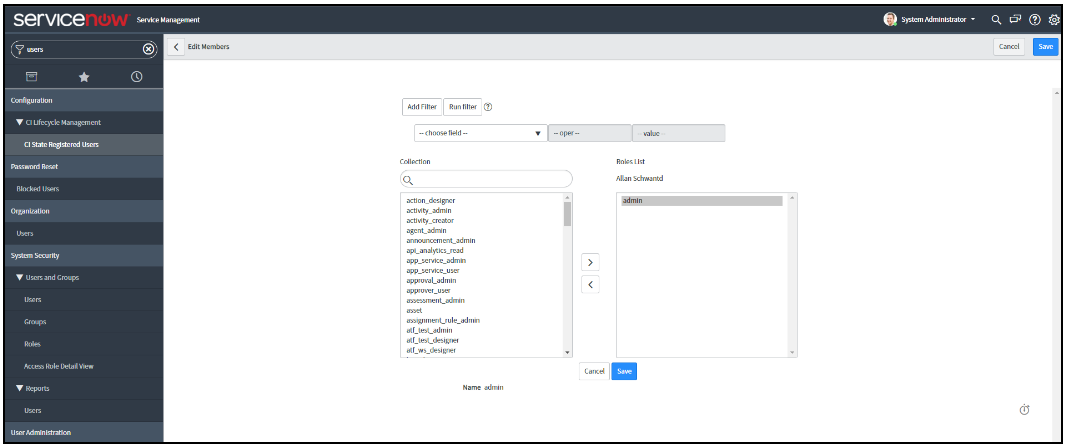
View Subscriptions
Reset a password

User = Allan Schwantd

Role	State	Inherited	Inheritance Count

No records to display

Image 4: Updating roles



Collection

action_designer
activity_admin
activity_creator
agent_admin
announcement_admin
api_analytics_read
app_service_admin
app_service_user
approval_admin
approver_user
assessment_admin
asset
assignment_rule_admin
atf_test_admin
atf_test_designer
atf_ws_designer

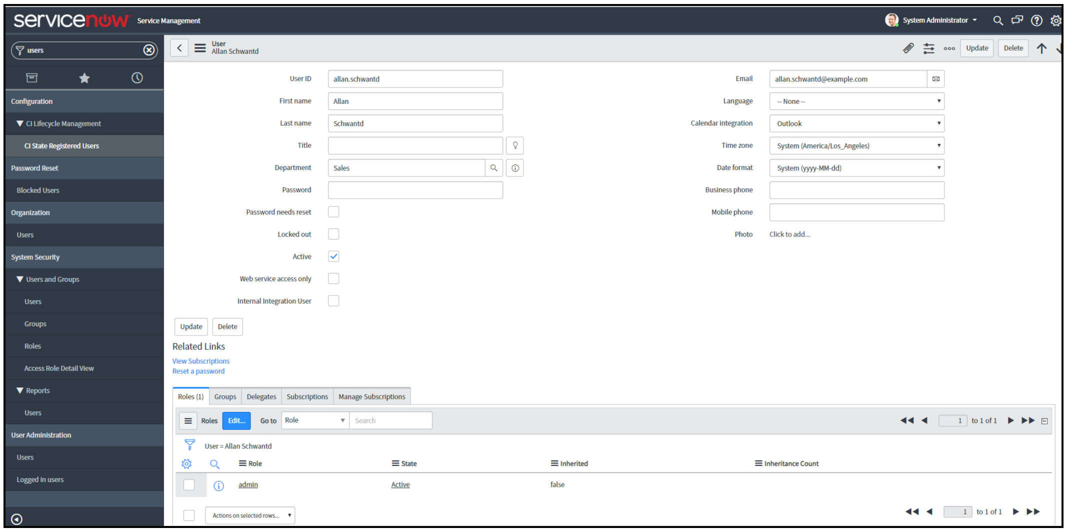
Roles List

Allan Schwantd

admin

Name admin

Image 5: Updated user record with admin role



User
Allan Schwantd

User ID	allan.schwantd	Email	allan.schwantd@example.com
First name	Allan	Language	-- None --
Last name	Schwantd	Calendar integration	Outlook
Title		Time zone	System (America/Los_Angeles)
Department	Sales	Date format	System (yyyy-MM-dd)
Password		Business phone	
Password needs reset	□	Mobile phone	
Locked out	□	Photo	Click to add...
Active	☑		
Web service access only	□		
Internal Integration User	□		

Go to Role

User = Allan Schwantd

Role	State	Inherited	Inheritance Count
admin	Active	false	

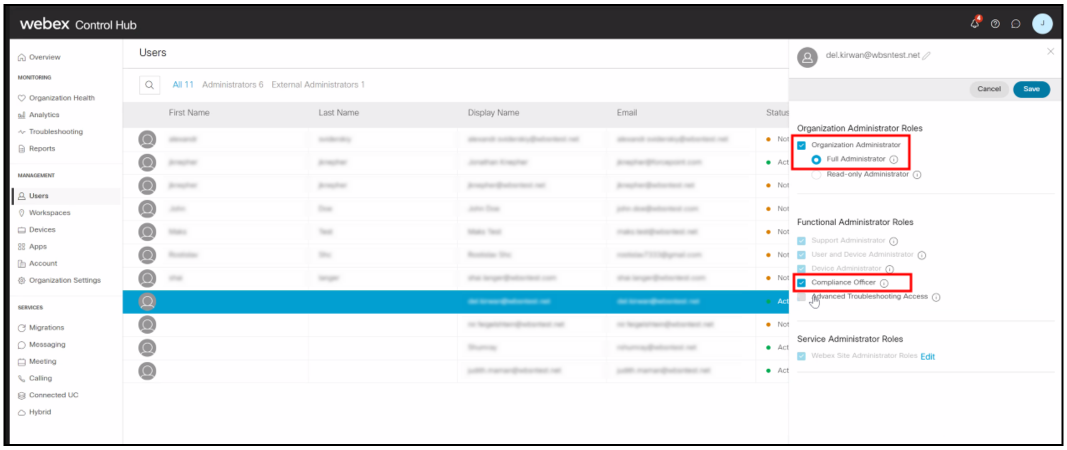
APPENDIX H

Cisco Webex Reference Images

Important: This appendix contains screenshots taken directly from the cloud service. The cloud service can change the appearance or workflow of these pages at any time. Forcepoint makes every effort to keep these images up-to-date, but they might differ from what is available from the cloud service. These images should be used as a reference only.

Cisco Webex images

Image 1: Administrator permissions



del.kirwan@wbsntest.net

Organization Administrator Roles

☑ Organization Administrator

● Full Administrator

○ Read-only Administrator

Functional Administrator Roles

☑ Support Administrator

☑ User and Device Administrator

☑ Device Administrator

☑ Compliance Officer

□ Advanced Troubleshooting Access

Service Administrator Roles

☑ Webex Site Administrator Roles Edit