

# AVG<sup>®</sup> Business SSO Partner Getting Started Guide

## Table of Contents

Overview.....	2
Getting Started .....	3
Web and OS requirements.....	3
Supported web and device browsers.....	3
Initial Login .....	4
Navigation in the Business SSO Portal.....	7
Cloud Manager.....	7
Overview .....	7
Creating Roles .....	10
<b>To create a role</b> .....	10
Adding and assigning SaaS applications to roles.....	11
<b>To add an application</b> .....	11
Adding mobile applications by using Cloud Manager.....	12
Adding Users .....	13
Assigning users to roles and inviting them to use the cloud service.....	14
<b>To add a user account to a role</b> .....	15
<b>To invite users to log in to the user portal</b> .....	16
Enrolling mobile devices.....	17
Managing mobile devices.....	18
User Portal .....	19
Business SSO user portal overview.....	19
Adding applications through the user portal .....	20
Adding Devices .....	21
Enabling users to enroll devices .....	21
Enrolling a device.....	21

## Overview

Business SSO eliminates barriers to user productivity, and gives AVG partners the tools they need to manage and secure cloud applications and mobile environment across all their customers' devices.

As a proven, secure, scalable service in the enterprise markets, AVG is bringing this service to our channel to manage their multiple SMB customers and end users. Business SSO represents a better to put you back in control of your customers' IT needs, while monetizing a difficult cloud app and mobile market.

This quick start guide is intended to assist our partners with a general overview configuration steps for Business SSO. Just getting started? Follow the sections below to register and setup your cloud account in just a few minutes – quick and easy!

AVG Business SSO is a hosted cloud service, which we encourage you to use for free (NFR) to help you in your own business, with the end goal of selling SSO as a new managed service to your customers.

AVG Business SSO provides the following components:

- An interface to Active Directory Services to manage and authenticate users just the way you do today. If you are not currently using AD, then you can simply use the cloud based identity service to manage user and administrator accounts.
- A partner administrator web portal you open from your browser to assign web applications, manage users, manage devices, and generate reports on cloud service activities.
- A web portal that users open from their browser to open the web applications you assign to them. Users just log in once to the portal, then have single sign on authentication to their applications. For every subsequent log in, the Business SSO cloud service provides silent authentication.
- An extensive catalog of over 2500 ready-to-assign web applications.
- Business SSO mobile applications users can install on their devices to access cloud services from Android and Apple iOS

## Getting Started

### Web and OS requirements

Supported web and device browsers.

This version of AVG Business SSO has been tested with the following web browsers:

- Internet Explorer
  - version 8 on Windows XP and Windows 7– for the Business SSO user portal only
  - version 9 and 10 on Windows 7 and Windows 2008R2 server
  - version 10 on Windows 2012 server and Windows 8
- Mozilla Firefox: version 33 and later
- Google Chrome: version 37 and later
- Apple Safari: 8
  - version 5 on Mac 10.6
  - version 6 on Mac 10.7 and later

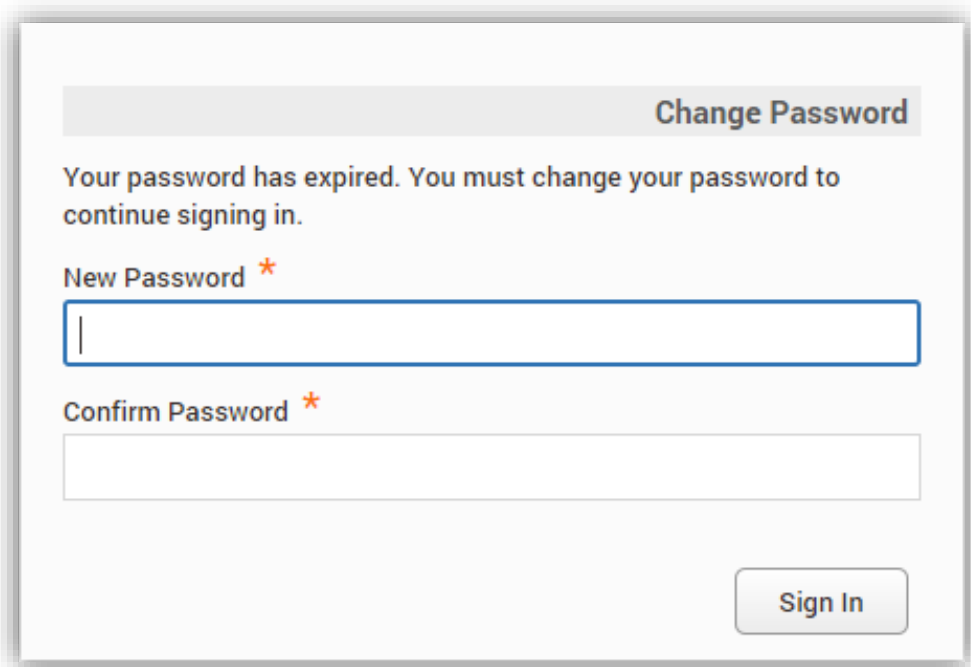
For silent authentication to work correctly, some web browsers need additional configuration or a browser extension.

On devices, the Business SSO application opens the web applications in the native browser unless that application requires a browser extension to provide single sign-on. For these applications only, the Business SSO application opens the application in its built-in browser.

## Initial Login

After registering, you should have received a welcome email with instructions to login to Business SSO. (If not, request access by contacting you AVG Account Manager.)

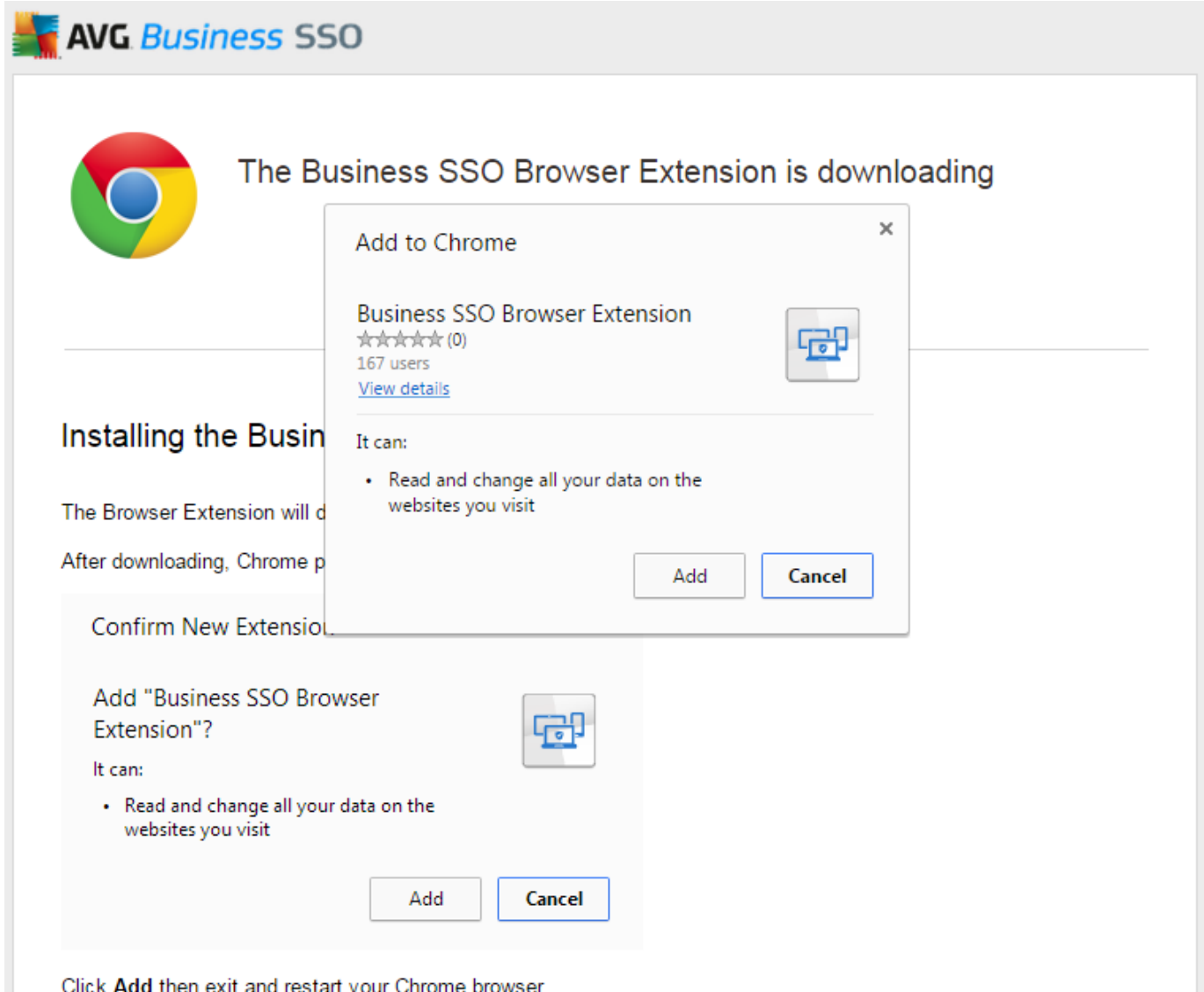
Clicking the link in the email will open a browser window with the initial login screen. As a security measure you will be required to change your password the first time you log in.




The screenshot shows a 'Change Password' form. At the top right, the title 'Change Password' is displayed. Below the title, a message states: 'Your password has expired. You must change your password to continue signing in.' There are two input fields: 'New Password \*' and 'Confirm Password \*'. The 'New Password' field has a blue border and a vertical cursor. The 'Confirm Password' field has a white border. At the bottom right, there is a 'Sign In' button.

The default screen shown after logging in is the user portal where you can view all the applications currently available. In order to view some apps you will be required to install a browser extension. To do so, click the message at the top of the user portal asking permission to install the browser extension. You will be shown the installation screen.

## Browser extension installation – Chrome



**AVG Business SSO**

 The Business SSO Browser Extension is downloading

**Installing the Business SSO Browser Extension**

The Browser Extension will download and install automatically.

After downloading, Chrome will prompt you to add the extension.

**Confirm New Extension**

Add "Business SSO Browser Extension"?

It can:

- Read and change all your data on the websites you visit

**Add** **Cancel**

**Add to Chrome**

Business SSO Browser Extension

☆☆☆☆☆ (0)

167 users

[View details](#)

It can:

- Read and change all your data on the websites you visit

**Add** **Cancel**

Click **Add** then exit and restart your Chrome browser.

## Browser extension installation - Internet Explorer

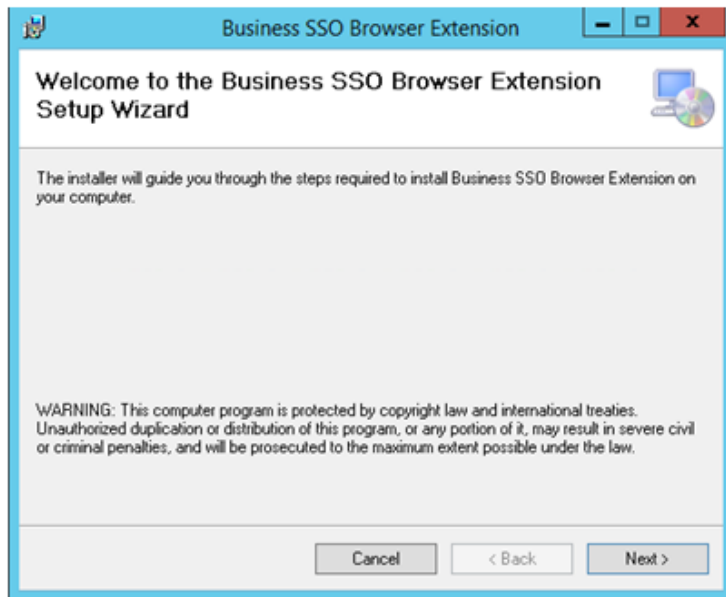
### Installing the Business SSO Browser Extension

The Browser Extension will download automatically. If it doesn't, click [here](#)

After downloading, Internet Explorer prompts you to run or save the installer file. Click **Run**.

Complete the setup wizard, then exit and restart Internet Explorer.

**Note: You must be an administrator to install the Business SSO Browser Extension for Internet Explorer.**

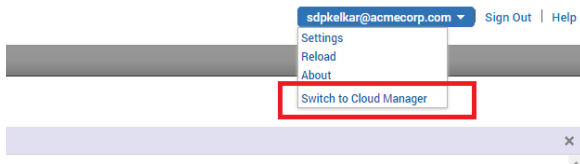


© 2015 AVG Corporation.

After installing the extension, restart the browser and you can access all the applications available in the dashboard.

## Navigation in the Business SSO Portal

The default view shown in the first login is the User Portal. To access the Cloud Manager Administrator dashboard, click on your user name link in the top right corner. This will bring up a drop down menu in which you can switch between the User Portal and the Cloud Manager that you as the partner administrator will use to manage your customers and end users.



## Cloud Manager

### Overview

The Cloud Manager is your administrator tool for managing the Business SSO cloud service applications, users, policies, and devices.


You use Cloud Manager to configure the Business SSO cloud service and to perform the day-to-day administrative tasks. For example, you use Cloud Manager to perform the following tasks:


- Assign applications to users
- Create roles for users and administrators and assign cloud service permissions
- Manage enrolled devices
- Create policy sets for the Business SSO policy service
- Monitor Business SSO cloud service activity
- Configure the Business SSO cloud service settings
- Generate reports

You manage each aspect of the cloud service—users, applications, devices, policies, roles, and Business SSO cloud service settings—using the tabs across the top of the page. Another tab is provided for generating and creating reports.

The Business SSO startup wizard will be launched by default whenever the Cloud manager is accessed. This wizard allows you to get up and running with minimal effort and consists of five steps:


1. Managing Devices
2. Adding Web application
3. Adding Mobile applications
4. Adding Users
5. Sending Invites to users



 **AVG Business SSO**

## Welcome to AVG Business SSO

One simple login for users.  
One unified identity infrastructure for IT.



This wizard will help with the initial configuration of AVG Business SSO.

You can run this wizard again at any time from Getting Started dashboard.

Don't show this to me again.



### Quick Start Wizard

1 Manage Devices   2 Add Web Apps   3 Add Mobile Apps   4 Add Users   5 Invite Users

## Manage Devices

Setup device management (click next to skip).

Use AVG for mobile device management of Android, Samsung KNOX and iOS devices.

- Enable Mobile Device Management
- Manage iOS Devices ⓘ

Your Apple Push Notification Service is configured  
Expiration Date: December 1, 2015

[Create New](#)

< Back   Next >

## Creating Roles

Roles control which SaaS and mobile applications are assigned to which users and the administrative rights available to the role members.

There are two default roles when you first open the Roles page:

**sysadmin:** This is the role for cloud service system administrators. Members have full access to all Cloud Manager tabs and are the only administrators who can perform the following tasks:

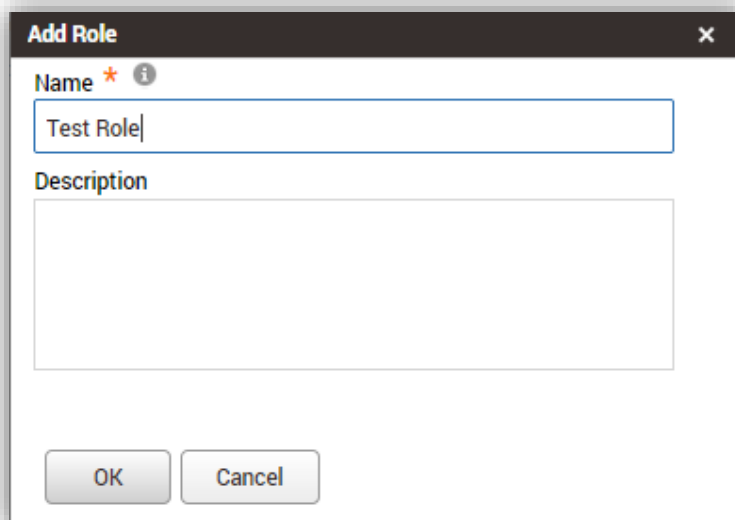
- Add users to or remove them from the sysadmin role.
- Customize Cloud Manager and user portal pages user interfaces.
- Modify the cloud proxy server settings and generate activation codes for additional cloud proxy servers.

**Everybody:** By default, Cloud Manager adds all cloud service users to this role. Applications you assign to this role can be opened by all cloud service users.

We recommend creating different types of administrative roles based on the best practices set forth by the Information Technology Infrastructure Library (ITIL) service strategy for production deployments.

### To create a role

1. Click the Roles tab.
2. Click Add Role.
3. Enter a name (for example Engineers) and a description for the role.
4. Click OK.



**Add Role** [X]

Name \* ⓘ  
Test Role

Description

OK Cancel

## Adding and assigning SaaS applications to roles

When using Business SSO for single sign-on to SaaS applications, you use Cloud Manager to add SaaS and/or mobile applications and assign them to one or more roles. The users in those roles can then open the applications from the User portal and mobile devices.

Business SSO provides comprehensive, application-specific help for adding a wide variety of SaaS applications, see [AVG Application Configuration Help](#). If you are adding an application that uses SAML, please see [Creating a custom SAML application profile](#) for details.

### To add an application

1. Click the Apps tab
2. Click Add App
3. Type the name of the app that you want to add into the search box
4. Click the desired app (a check will appear)
5. Click Add App
6. Click User Access and select the Role(s) that you want to make the app available for
7. Click Application Help for specifics on configuring that app.
8. Click Save.

See instructions: [Adding web applications](#)

If the app you want is not in the app catalog, you can add it yourself. [See Adding web applications by using Business SSO Infinite Apps](#)

## Adding mobile applications by using

## Cloud Manager

This section describes adding and deploying mobile applications by

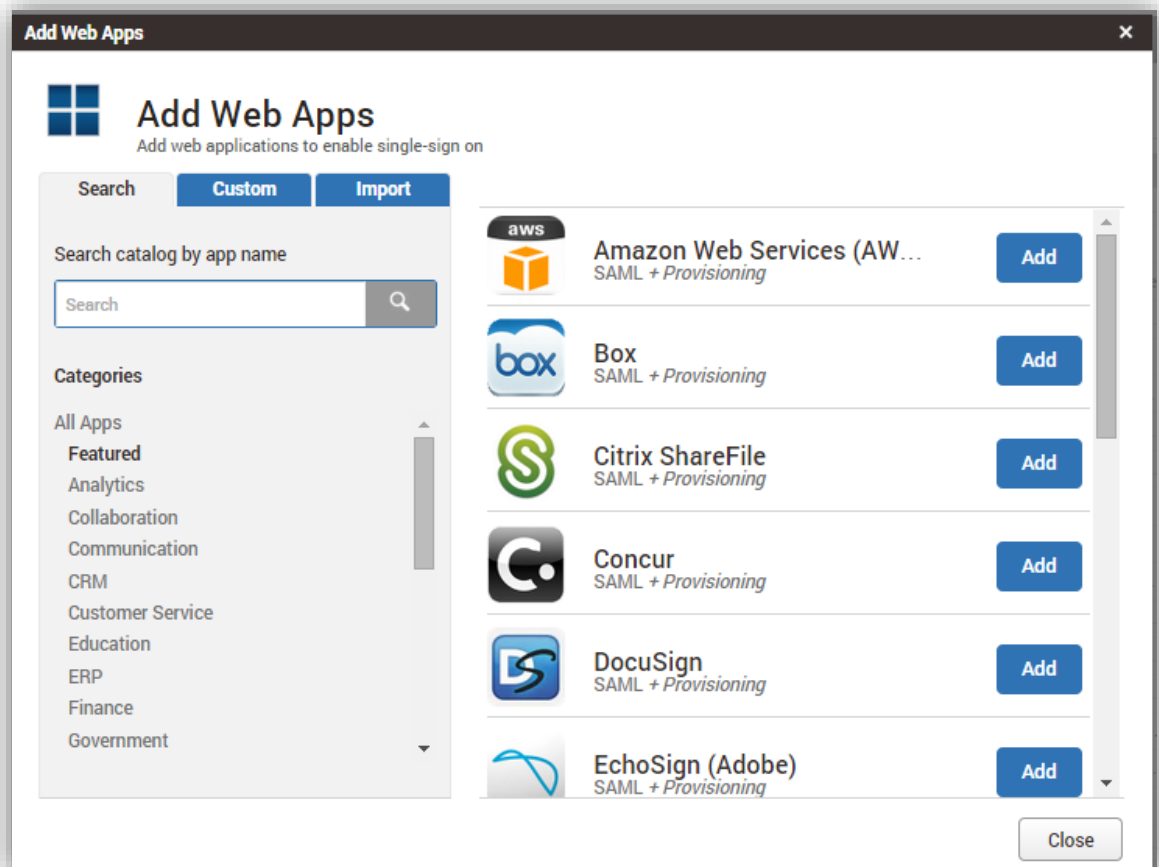
using Cloud Manager from the conceptual level. See [Application Configuration](#) Help for complete, application-specific configuration and deployment instructions.

You deploy native device mobile applications to sets of users based on their roles. For Android devices, you can deploy any free application from Google play or an Android application for which you have the binary—the .APK—file.

Note: If you are deploying applications to Samsung Workspace devices with KNOX mode version 1 containers, the application must be wrapped to be installed in the container.

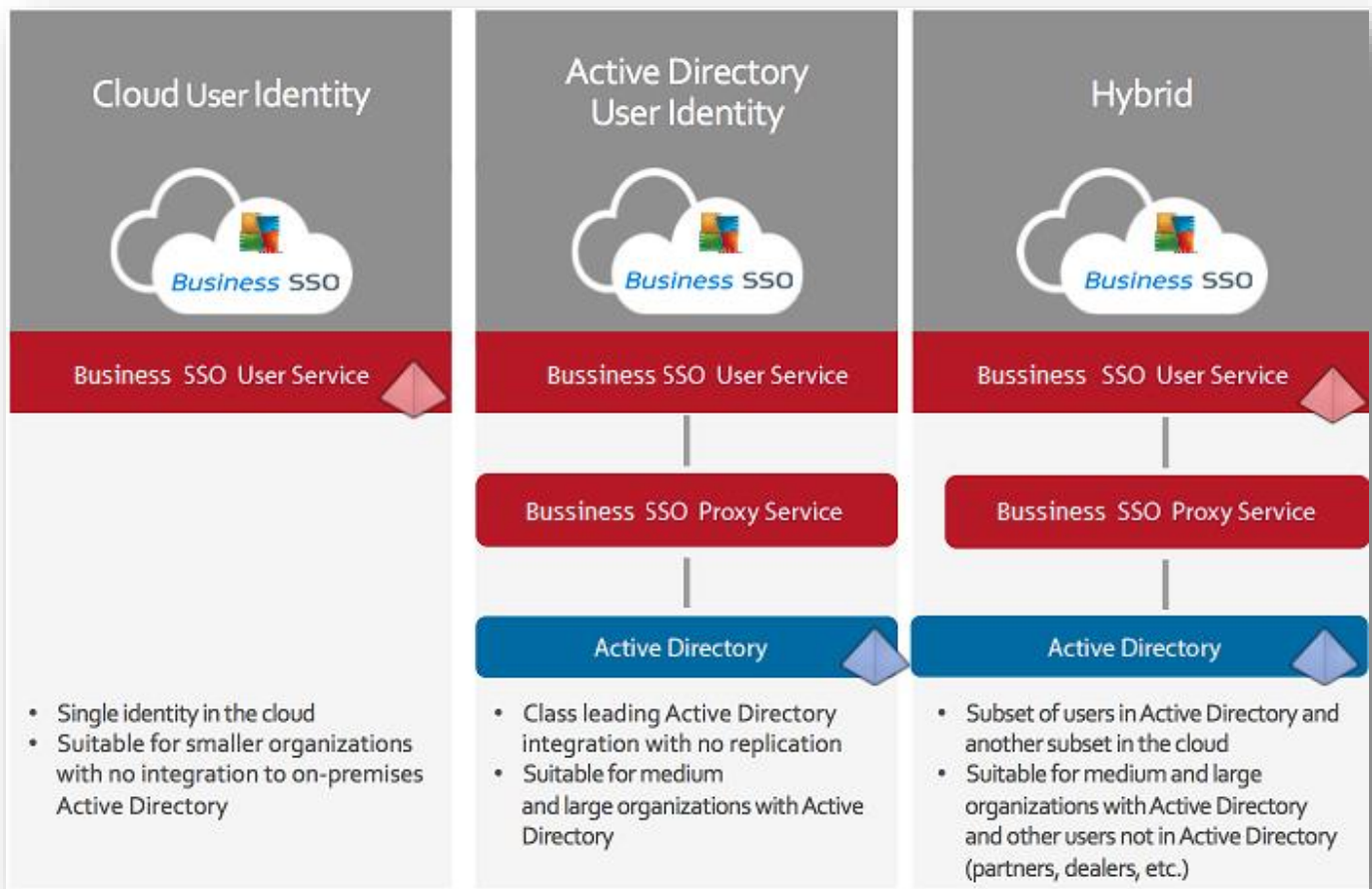
For iOS devices, you can deploy any free application from the Apple App Store or an iOS application for which you have the binary—the .IPA—file. See [Installing mobile applications](#) on iOS devices for the details.

The mobile applications you add are displayed on the Apps page. In addition, the mobile applications that have been installed by the user on a device are listed in the “Installed Applications” list when you open the device details page.



## Adding Users

Business SSO supports three deployment models for user identities:



The Users page in Cloud Manager lists all of the cloud service users. You can add user accounts one at-a-time or use the Bulk User Import wizard to create multiple accounts from a CSV file or Excel spreadsheet.

The cloud service also lets you reference existing accounts in Active Directory. In this case, Active Directory users are automatically linked to the cloud service when they log in to the user portal or enroll a device. If you would like to enable Active Directory users, you will need to install a cloud proxy server on your network. You can download the proxy server package from the Proxies tab under Settings. See [Installing and configuring cloud proxy servers](#) in Help for the proxy server installation instructions.

## Assigning users to roles and inviting them to use the cloud service

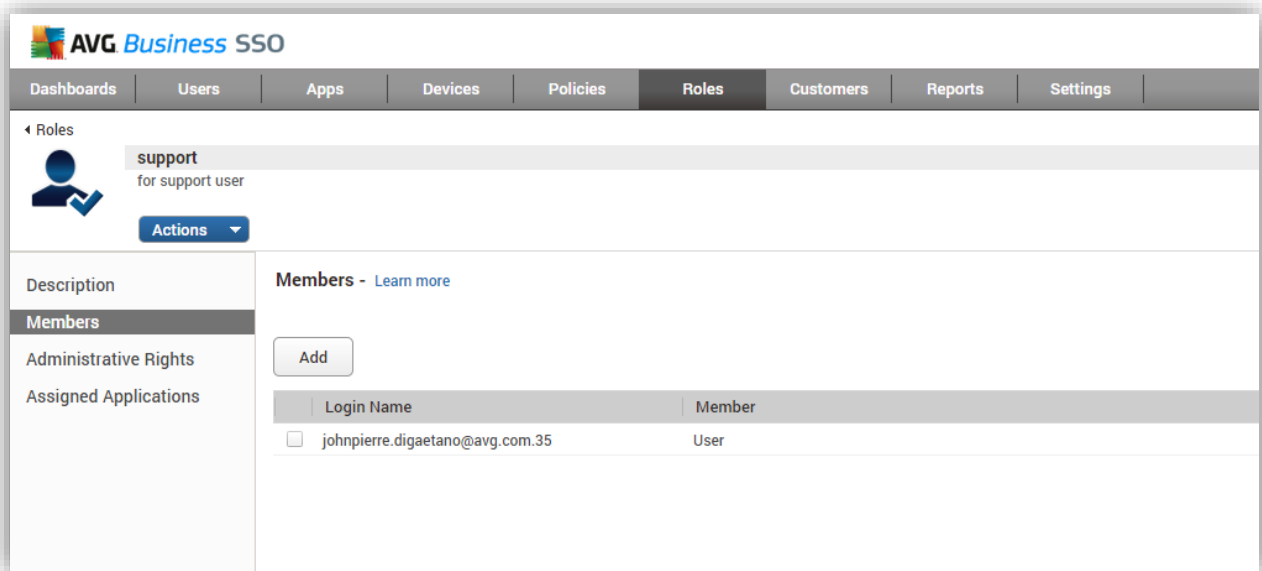
The cloud service assigns applications and, for mobile device management, installs mobile device policies based on the roles in which the user is a member. Once you have added users to the

Cloud service, or have referenced users from Active Directory, you will need to assign those users to a role (or roles).

## To add a user account to a role

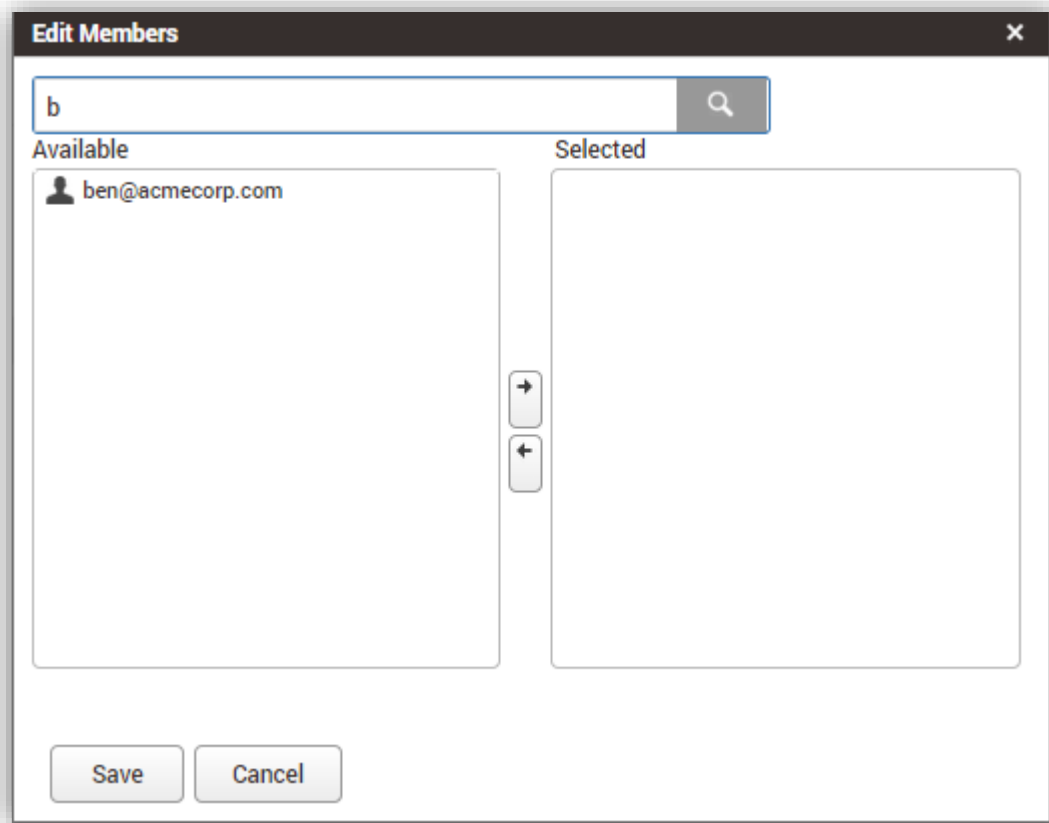
1. Click the **Roles** tab
2. Select the Role that you would like to add the User to
3. Click the **Members** Edit button
4. Enter the **User name** (AD Group or another cloud service role) that you would like to add to the Role in the search box
5. Move the desired User or Group from the **Available** pane to the **Selected** pane (you can do this by double-clicking, dragging or selecting the name and clicking the arrow)
6. Click **OK**.

**Note:** When adding users in bulk, you can automate role assignment by specifying the roles in the CSV or Excel file. See instructions: [Adding and removing users and groups to and from roles](#).



The screenshot shows the AVG Business SSO interface. The top navigation bar includes tabs for Dashboards, Users, Apps, Devices, Policies, Roles (selected), Customers, Reports, and Settings. The main content area is titled 'Roles' and shows a role named 'support' for support user. Below the role name is an 'Actions' dropdown menu. The 'Members' section is active, showing an 'Add' button and a table with one member: 'johnpierre.digaetano@avg.com.35' with the role 'User'. The left sidebar contains links for Description, Members, Administrative Rights, and Assigned Applications.

After you add the users to roles, you can invite users to log in to the user portal and open the web applications you assigned to them.



### To invite users to log in to the user portal

1. Click the **Users** tab
2. Right-click the user you want to invite to the service
3. Click **Email Invite**.

**Note:** If you will be using the mobile device management features, you should do this step last. See instructions: [Getting users started](#).



## Enrolling mobile devices

Users can enroll their devices in the cloud service to get SSO access to their SaaS applications on their devices too. If you use the cloud service for mobile device management, you can also use Cloud Manager to deploy policies to enrolled devices, send MDM commands, such as lock and wipe, and deploy native applications.

To enroll the device, users install the free Business SSO application from either Google Play or the Apple App Store on the device. Users can also enroll the device by logging into the User Portal, clicking the Devices tab and following the on-screen instructions.

### Supporting iOS Devices

If your users will be enrolling an iOS-based device, you need to upload an Apple Push Notification Service (APNS) certificate in the cloud service.

To upload an APNS certificate click the Start Wizard button (if available to you), or manually upload the certificate by following these instructions:

1. Click the **Settings** tab
2. Click **APNS Certificate**
3. Follow the procedures described on that page.

See instructions: [Generating your APNS certificate for iOS devices](#)

### Supporting Samsung KNOX

If your organization uses Samsung KNOX Workspace devices, see the document [AVG for Samsung KNOX Administrator's Guide](#) to get started with the Business SSO installation and configuration.

### Configuring the cloud service for single sign-on only

If you plan to use the cloud service for SSO alone—and not for managing mobile device policies, you need to disable deploying device management policies by using the following procedure.

#### To select single sign-on only

1. Click the **Settings** tab
2. Click **Mobile Device Management**
3. **Uncheck** the check box
4. Click **Save**.

See instructions: [Configuring mobile device management or single sign-on only](#)

## Managing mobile devices

If you are using the Business SSO for mobile device management, the cloud service provides three primary device management functions:

- Device management commands.

The commands available vary, depending upon the type of device and whether or not you are using the cloud service for mobile device management. For example, if you are using the cloud service for mobile device management, you can send commands such as remote lock, remote wipe, and update policies. However, if you are using the cloud service for single sign-on only, you can only send enable SSO and disable SSO commands.

See [Using the cloud service commands](#) for the descriptions of all the commands.

- Mobile device policy enforcement.

The Business SSO includes a comprehensive set of mobile device policies. You create policy sets in Cloud Manager to turn policies on and off and set parameters. The cloud service installs the policies when the user enrolls the device and automatically updates them after you make a change.

See [Managing mobile device policies](#) for a description of the policies available for Android, iOS, and Samsung KNOX devices. If you are using Active Directory, you can also use the Group Policy Management Editor to set policies for devices that belong to users with Active Directory accounts.

- Mobile native applications deployment.

You can deploy free applications from Google Play and the Apple App Store and custom in-house applications for which you have the binary. The cloud service deploys the mobile application to the users' devices for installation by the user.

See [Deploying mobile applications](#) for the details.

## User Portal

### Business SSO user portal overview

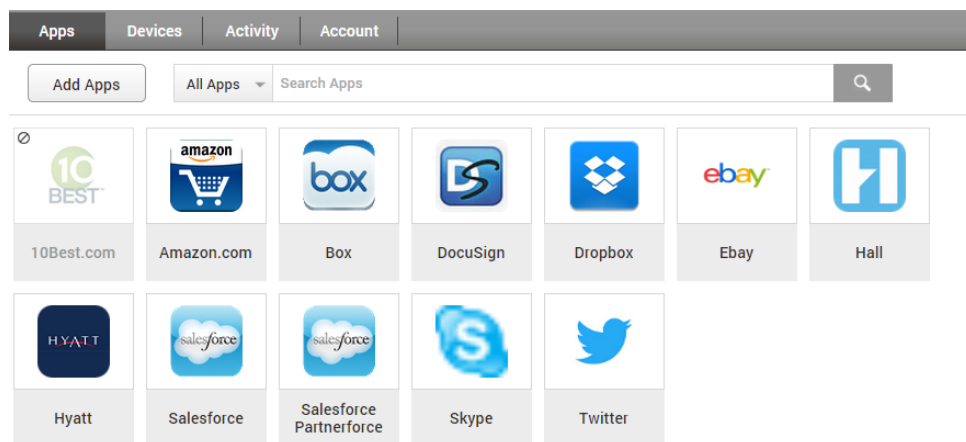
Users open the Business SSO user portal to launch the web applications you assign to them. In addition, they can use it to add web applications on their own (this feature is policy-controlled, however, and you can deny it to some or all users), review their cloud service activities, and, if you use the Business SSO cloud service for mobile device management, manage their devices. See the [user web portal online help](#) for an overview.

The user portal help also provides the user instructions for installing the Business SSO application on devices and enrolling devices in the Business SSO cloud service.

Users open the Business SSO user portal by entering the following URL in their web browser:

<https://sso.avg.com/my>

The user portal prompts them to enter their credentials and opens to the Apps page, which lists all of the web applications you have assigned to this user. The following picture illustrates the Apps page in the user portal populated with web applications.



Users click Help to open the online help and use the drop-down menu to reload privileges and, in Settings, select the default applications filter and turn off device tracking for devices.

**Note:** For administrator accounts only, the drop-down menu also includes an item you can use to switch from the user portal to the admin portal.

## Adding applications through the user portal

The Business SSO User Portal application is the cloud service user portal. By default, it is added to the Apps page and deployed to the Everybody role. (When you open the Apps page for the first time, you see Business SSO User Portal, and the Status is deployed.) This application, however, does not appear on the Apps page in the user portal nor in the Web Apps screen on devices.

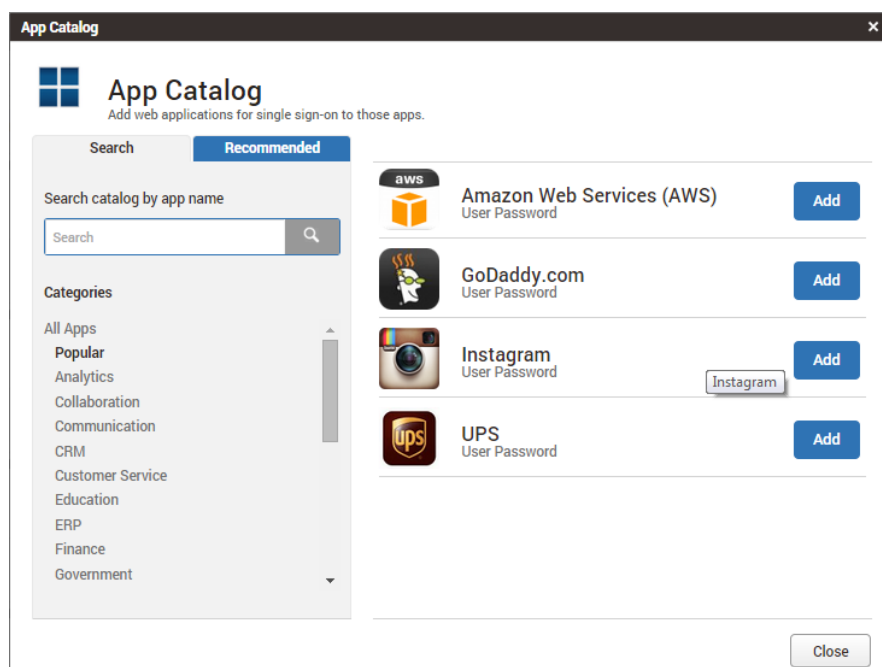
In some ways, Business SSO User Portal is like any web application. That is, you can modify the default settings. For example, you can set the Policy to “Intranet only” so that users outside your organization’s intranet cannot log in to the user portal. In addition, you can change the User Access settings to add and remove roles. However, Business SSO User Portal cannot be deleted, cloned, or exported; nor can you add it from the Business SSO app catalog.

### Notes

Business SSO User Portal must be assigned to any of a user’s roles before the user can open the user portal. If it is not, the cloud service displays “Not Authorized” in a pop up window with instructions to contact their administrator when the users log in.

The role specified in the **Invite Users** button ([see Using the Invite Users button](#)) is automatically selected in the User Access settings for Business SSO User Portal.

Users can add apps by clicking Apps > Add Apps. This brings up the App Catalog from which users can select the applications to be added for Single Sign On.



## Adding Devices

### Enabling users to enroll devices

You must be using the Business SSO cloud service for mobile device management (see [Configuring mobile device management or single sign-on only](#)) for users to enroll devices in the Business SSO cloud service. When devices are enrolled in the cloud service, you can manage them in Cloud Manager, install mobile device policies, and deploy mobile applications to select sets of devices.

User accounts in both the Business SSO user service and Active Directory must be enabled before the user can enroll a device. There are two options to enable accounts:

Create a cloud service role, configure the Device Enrollment Settings, and add the user as a member to this role.

You must use this option when you use the Business SSO policy service for device policy management (see [Selecting the Business SSO policy service or Active Directory group policy management to set device policies](#)).

You can add individual Business SSO user service accounts, other roles, Active Directory user accounts, and Active Directory groups to the role. (You must have a cloud connector installed to add Active Directory accounts and groups.)

See [Device Enrollment Settings - Enabling users to enroll devices](#) for the details.

Add the user's Active Directory group to the groups that are allowed to enroll devices in the Business SSO cloud connector.

You should use this option only if you have a simple configuration of Active Directory domains in a trusted domains configuration. Otherwise, you should use cloud service roles to enable Active Directory users to enroll devices.

### Enrolling a device

The Business SSO cloud service requires the device owners to enroll the device regardless of whether it is used for single sign-on or mobile device management.

Before they can enroll a device, however, the users' account must have the enroll device permission. Users enroll their devices using the following methods:

**For Android devices:** Users install the Business SSO application for Android on the device.

Users with Samsung KNOX Workspace devices that have the Universal MDM Client (UMC) installed can enroll their devices by entering just their user name and password—[see Enabling Samsung KNOX UMC login suffix updates](#) for an overview of the UMC.

**For iOS devices:** Users install the Business SSO application for iOS on the device.

If your organization is using the Apple Device Enrollment Program, you can have the Business SSO application installed automatically on the device. If you use this program, however, you cannot unenroll the device. See [Linking to the Apple Device Enrollment Program](#) for the details.

**For OS X computers:** Users enroll from the Business SSO user portal.

If you plan to enroll a computer in the Business SSO cloud service that is already joined to Active Directory, see [Working with Samsung KNOX devices](#) first.


Users can get the Business SSO application from a number of places. For example:

They can click Add Devices from the Business SSO user portal. From the pop up window, users can use a QR reader to download the application from Google Play or the Apple App Store, send an SMS message to the device with a link that downloads the application, or get a link they can enter in the device's browser to download the application.

- You can send them an SMS message using the SMS Invite command (see using a SMS Invite).
- You can email the same link or download the Business SSO application and email it to your users.
- Users enroll from the Business SSO user portal.

**Add Devices** ✕

Choose an option below to send an enrollment link to your device.

<p><b>Send SMS</b> ⓘ</p> <input type="text"/> <input type="button" value="Send"/>	<p>or</p>	<p><b>Send email to device</b></p> <input type="text" value="mukul.hinge@avg.com"/> <input type="button" value="Send"/>	<p>or</p>	<p><b>Scan QR code on your device</b></p> 
--	-----------	--	-----------	---

Type this address into your mobile browser

See the user portal help for the Business SSO application installation and enrollment instructions for each device.