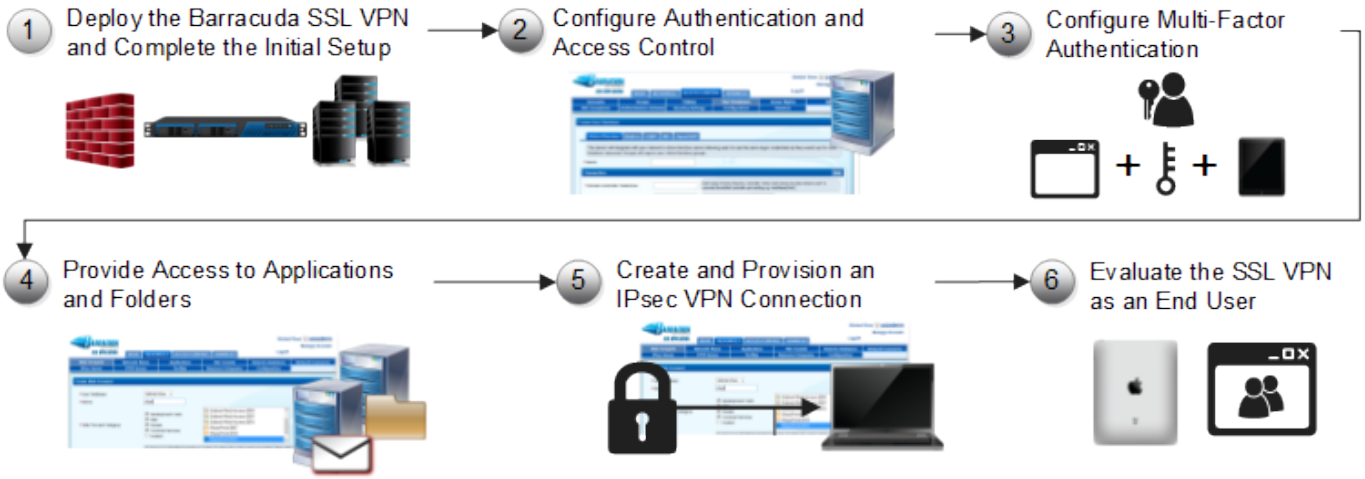
30 Day Evaluation Guide - Barracuda SSL VPN

https://campus.barracuda.com/doc/39822144/

Use this article as a sample roadmap for setting up and testing the Barracuda SSL VPN in your organization's environment.



Before you begin

Some essential information which you should know before you begin to deploy your Barracuda SSL VPN appliance:

- Decide how you want to deploy the Barracuda SSL VPN. It is recommended to use the **direct access deployment** option for the evaluation. For more information on deployment options, see the Deployment page.
  > You can also use the Barracuda SSL VPN online demo at https://sslvpn.barracuda.com. However, the demo does not allow you to save changes.
- The Barracuda SSL VPN provides two administrative web interfaces: the appliance web interface to administer the appliance and the SSL VPN web interface to administer and provide SSL VPN functionality:
  - **Appliance Web Interface**
    - **URL**: https://<IP address for the Barracuda SSL VPN>:8443
    - **Default user**: admin
    - **Default password**: admin
  - **SSL VPN Web Interface**
    - **URL**: https://<IP address for the Barracuda SSL VPN>
    - **Default user**: ssladmin
    - **Default password**: ssladmin
- End users log into the SSL VPN web interface at: https://<IP address for the Barracuda SSL VPN>

- Users on mobile devices are automatically detected and redirected to the mobile portal when using the web interface at: https://<IP address for the Barracuda SSL VPN>

If not stated otherwise, this evaluation guide assumes that you are logged into the SSL VPN web interface as the default **ssladmin** (default password: **ssladmin**) user.

Step 1. Deploy and set up the Barracuda SSL VPN

Depending on whether you are evaluating a hardware or a virtual appliance, complete one of the following sets of instructions:

Hardware appliances

1. Follow the instructions in the Quick Start Guide for Barracuda SSL VPN included with your appliance.
2. (Optional) Complete the Getting Started guide.

Virtual appliances

1. Download the Barracuda SSL VPN Vx image for your hypervisor from the Barracuda Networks Virtual Appliance Download page.
2. Deploy and install the Barracuda SSL VPN Vx. For instructions, see Virtual Deployment.
3. Complete the Barracuda SSL VPN Vx Quick Start Guide.
4. (Optional) Complete the Getting Started guide.

Step 2. Configure authentication and access control

The Barracuda SSL VPN is very flexible when handling access control and authentication. You can combine different authentication modules with various external user directory services to configure a custom login process. In the web interface, login processes are referred to as authentication schemes. Lists of users and groups are stored in policies. The remote user directory (e.g., AD, LDAP, and RADIUS) or local user directory is stored in a user database. The Barracuda SSL VPN 380 and above support multiple user databases.

Configure your Active Directory server on the **ACCESS CONTROL > User Databases** page. Click the **Active Directory** tab to enter the settings. Test the connection setting by clicking **Test** before adding the server. If you are evaluating the Barracuda SSL VPN 180 or 280, edit the default user database to configure an external Active Directory server.

If you do not have an external user directory service or do not want to use it in combination with your Barracuda SSL VPN, you can also use the internal user database.

You can control access to the SSL VPN's resources by defining criteria (e.g., time, operating system, updates installed, browser version) that must be met by users. To configure NAC settings, go the **Manage System > ACCESS CONTROL > NAC** page.

Related articles and help

For more information on authentication and access control, see these articles and online help:

- **User Databases** – How to Configure User Databases and Example - Create a User Database with Active Directory.
- **Policies** – How to Configure Policies.
- **NAC** – Go to the **Manage System > ACCESS CONTROL > NAC** page.

Step 3. Configure multi-factor authentication schemes

Authentication schemes contain a configurable list of authentication modules and policies. Create an authentication scheme on the **ACCESS CONTROL > Authentication Schemes** page. If multiple user databases are defined, users can select a user database by clicking **More** before logging in. Hardware token authentication is available for the Barracuda SSL VPN 380 and above.

Available authentication modules

The following table lists all of the authentication modules that you can configure on the Barracuda SSL VPN. Secondary authentication modules must be combined with a primary authentication module, like password, for example, and can not be placed first in the authentication scheme configuration. Barracuda Networks recommends using at least two authentication modules for an authentication scheme.

Authentication Module	Type
Client Certificate	Primary/Secondary
IP Address	Primary/Secondary
Password	Primary/Secondary
PIN	Primary/Secondary
Public Key	Primary/Secondary
RADIUS	Primary/Secondary
Google Authenticator	Primary/Secondary

OTP (One-Time Passwords)	Secondary
Personal Questions	Secondary

RADIUS authentication and hardware token support is included with the Barracuda SSL VPN 380 and above.

Step 4. Provide access to applications and folders

The Barracuda SSL VPN gives users secure access to applications and network file shares in the corporate network. You can specify who can use a resource by assigning one or more policies to every resource. Choose the type of resource depending on what type of network service you want to share.

Microsoft Exchange

If you are using Microsoft Exchange, go to the **RESOURCES > Web Forwards** page and create a Web Forward using the Microsoft Exchange template.

Step 1. Create the Web Forward for OWA

Configure a Path-Based Reverse Proxy type of Web Forward for OWA.

1. Log into the SSL VPN web interface.
2. Go to the **Manage System > RESOURCES > Web Forwards** page.
3. In the upper right, verify that you have selected the correct user database.
4. In the **Create Web Forward** section, configure these settings:
   - **User Database** – Select the database that the users reside in.
   - **Name** – Enter a name to help end users identify the Web Forward. For example, `Outlook Web Access` .
   - **Web Forward Category** – Select the **Mail** check box, and then select **Outlook Web Access 2010**.
   - **Hostname** – Enter the hostname or IP address of the web server that you want to connect to.
5. To save authentication time, enable **Provide Single Sign On** .
6. From the **Available Policies** list, add the policies that you want to apply to the Web Forward.
7. To add the Web Forward to the default Resource Category, enable **Add to My Favorites**.
8. Click **Add**.

The Web Forward then appears in the **Web Forwards** section.

Step 2. Edit the Web Forward settings

If you want to configure additional options for the OWA Web Forward (e.g., **Multiple Services On Destination Host** and **Authentication Type**), edit its settings.

1. In the **Web Forwards** section, click **Edit** next to the entry for the OWA Web Forward.
2. To use OWA form-based authentication, enable **Multiple Services On Destination Host** .
3. If required, configure the remaining settings.
4. Click **Save**.

Step 3. Launch the Web Forward

Add a resource category to the Web Forward to make it available to users on their **My Resources** page.

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. In the **Edit Web Forward** window, scroll to the **Resource Categories** section, and add the available categories that you want to apply to the Web Forward.
3. If you want the Web Forward to automatically launch whenever users log into the Barracuda SSL VPN, scroll to the **Details** section and enable **Auto-Launch**.
4. Click **Save**.

Microsoft SharePoint

If you are using Microsoft SharePoint, go to the **RESOURCES > Web Forwards** page and create a Web Forward using the Microsoft SharePoint template.

Using SharePoint 2007 and 2010

- When using SharePoint 2010, the end user must disable the **Trusted Documents** setting to allow the editing of documents on a SharePoint 2010 server using Office 2010.
- When using SharePoint 2007, be aware that the SharePoint 2007 template only allows site navigation, limited editing of the SharePoint site, and the uploading and downloading of

documents.

Step 1. Configure the SharePoint server

On the SharePoint server, add alternate access mappings. Then restart the IIS server.

Step 1.1 Add alternate access mappings

1. Go to the SharePoint 2013 Central Administration console (this might be set up on *your SharePoint server* :1317). If it is not available, log into the system that IIS is running on and go to **Start > SharePoint 2013 Central Administration**.
2. On the **Central Administration** page, click **Configure alternate access mappings** in the **System Settings** section.
3. Click **Edit Public URLs**.
4. From the **Alternate Access Mapping Collection** list, select **SharePoint - 80**.
5. Add the following entries:
   - **Default**: `http://your SharePoint server`
   - **Intranet**: `http://your fully qualified SharePoint server`
   - **Internet**: `http://your fully qualified Barracuda SSL VPN`
   - **Extranet**: `https://your fully qualified Barracuda SSL VPN`

Step 1.2 Restart the IIS server

1. Go to **Start > Internet Information Services (IIS) Manager** .
2. In the left pane, click **SHAREPOINT**.
3. In the right pane under **Manage Server**, click **Restart**.

Step 2. Create the Web Forward for SharePoint

Configure the Web Forward with the information for the SharePoint server, and add policies for the users and groups who are allowed to use it.

1. Log into the SSL VPN web interface.
2. Int the upper right, verify that you have selected the correct user database.
3. Go to the **Manage System > RESOURCES > Web Forwards** page.
4. In the **Create Web Forward** section, configure these settings:
   - **User Database** – Select the database that the users reside in.
   - **Name** – Enter a name to help end users identify the Web Forward. For example, `SharePoint`.
   - **Web Forward Category** – Select the **Portals** check box, and then select **SharePoint 2013**.

- **Hostname** – Enter the hostname or IP address of the server that you want to connect to.
- **Domain** – Enter the domain that the SharePoint server belongs to.

5. From the **Available Policies** list, add the policies that you want to apply to the Web Forward.
6. To add the Web Forward to the default Resource Category, enable **Add to My Favorites**.
7. Click **Add**.

The SharePoint 2013 Web Forward appears in the **Web Forwards** section.

Step 3. Launch the Web Forward

Add a resource category to the Web Forward to make it available to users on their **My Resources** page.

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. In the **Edit Web Forward** window, scroll to the **Resource Categories** section, and add the available categories that you want to apply to the Web Forward.
3. If you want the Web Forward to automatically launch whenever users log into the Barracuda SSL VPN, scroll to the **Details** section and enable **Auto-Launch**.
4. Click **Save**.

Network places

Network places grant access to network file shares. With the web interface, you can download and upload files up to 2 GB in size. To create a resource for accessing a network file share, go to the **RESOURCES > Network Places** page. All files uploaded to the share are scanned for malware by the Barracuda SSL VPN.

Step 1. Create the Network Place

1. Log into the SSL VPN web interface.
2. Go to the **RESOURCES > Network Places** page.
3. Verify that you have selected the correct user database on the top right of the page.
4. In the **Create Network Place** section, select the desired database from the **User Database** drop down list.
5. Enter the name of the Network Place in the **Name** field.
6. In the **Path** field, specify the path to the Network Place, for example: *sales**public*.
7. In the **Username** and **Password** fields, enter the username and password, or leave them

blank if you want the user to provide credentials when the application is launched. If you are using session variables:

1. Select *session:username* in the **Username** field.
   > You might have to enter the domain as well as the **Username** session variable, using the following format: *domain\${session:username}*
2. In the **Password** field, select *session:password*.

8. In the **Available Policies** section, select the policies that you want to apply to the Network Place and c lick **Add >>**
   > If the policy that you want to add is not available in the **Available Policies** section, make sure that the appropriate user database is selected from the pull-down menu in the upper right of the page, or select the *Global View* user database to list all of the available policies from all the user databases.
9. Click **Add** to create the network place.

The Network Place resource is now created and displayed in the **Network Places** section.

Step 2. Edit the Network Place

You can configure additional settings such as host and folder options by completing the following steps:

1. In the **Network Places** section, click the **Edit** link associated with the Network Place. The **Edit Network Places** page opens.
2. Configure the settings as required.
3. When you are finished configuring your options, click **Save** at the bottom of the page.
4. Click **Save**.

Step 3. Launch the Network Place

To test the Network Place, go to the **Network Places** section, click the name of the Network Place or the **Launch** link associated with it. Make sure that you also test a user account that has the appropriate access rights with a connection outside your intranet.

Step 4. Add the Network Place

When you are ready to make the Network Place available to your users, apply a resource to it.

1. In the **Network Places** section, click the **Edit** link associated with the new Network Place.

2. In the **Categories Resource** section, select the resource categories that you want to apply to the Network Place, then click **Add>>** .
3. Click **Save**.

Available resource types

The following table lists all of the resource types that you can configure on the Barracuda SSL VPN.

Resource Type	Description	Link
Web Forwards	Access to intranet websites and internal web-based applications.	Web Forwards
Applications	Predefined and custom client/server applications within the secured network.	Applications
Network Connector	Full TCP/IP access into the secured network.	Network Connector
Network Places	Network shares on the internal network.	Network Places
SSL Tunnels	Create SSL tunnels to secure unencrypted intranet services.	SSL Tunnels

Step 5. Create and provision an IPsec VPN connection

Some users, applications, or devices require full routed access to the network. The Barracuda SSL VPN supports VPN access via IPsec server for Windows, macOS, and Linux computers, as well as mobile devices. The end user does not have to configure the VPN client because an applet in the end user portal completes this task automatically. iOS users can also use the custom device setup in the mobile portal to automatically configure the VPN connections.

To create an IPsec VPN, go to the **RESOURCES > IPsec Server** page.

Related articles

For more information on configuring IPsec VPN connections, see these articles:

- How to Configure IPsec
- Provisioning Client Devices
- Custom Device Setup for iOS Devices

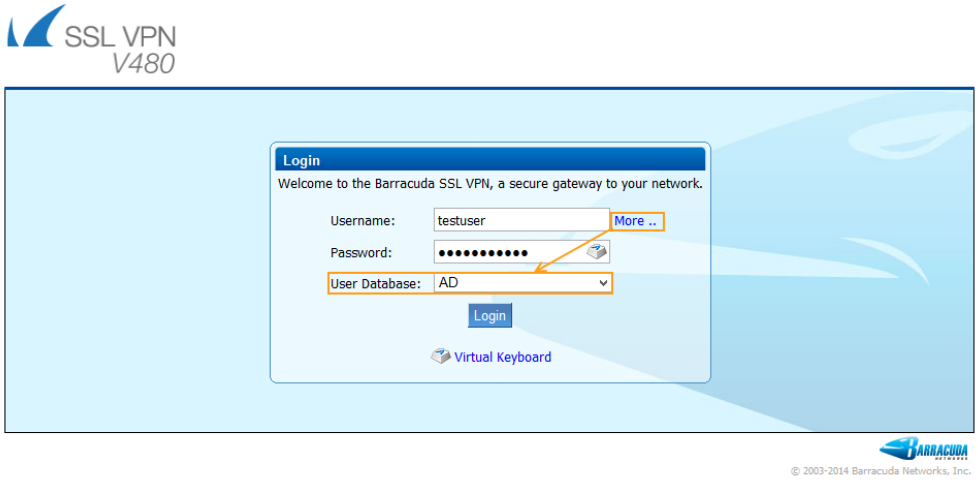
Step 6. Evaluate the Barracuda SSL VPN as an end user

Log in using a desktop computer

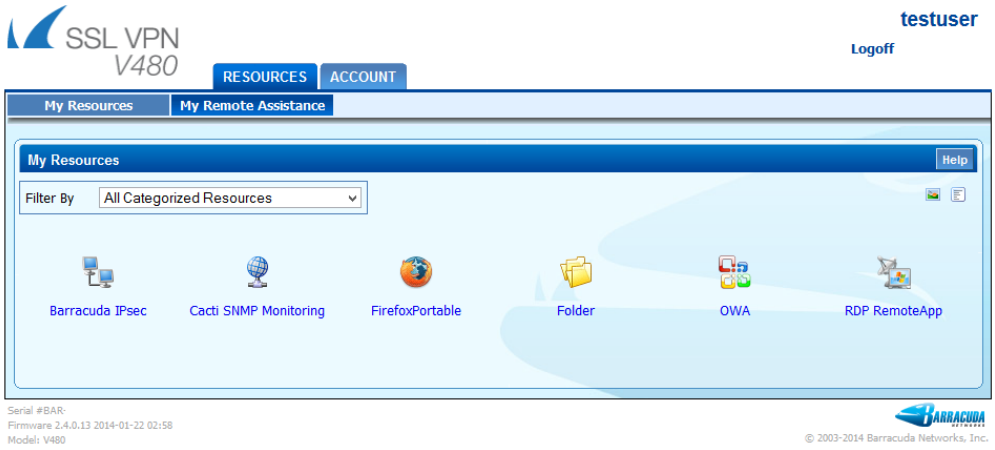
With an end user account, log into the SSL VPN end-user portal to view and evaluate the previously configured resources.

https://<IP address for the Barracuda SSL VPN>

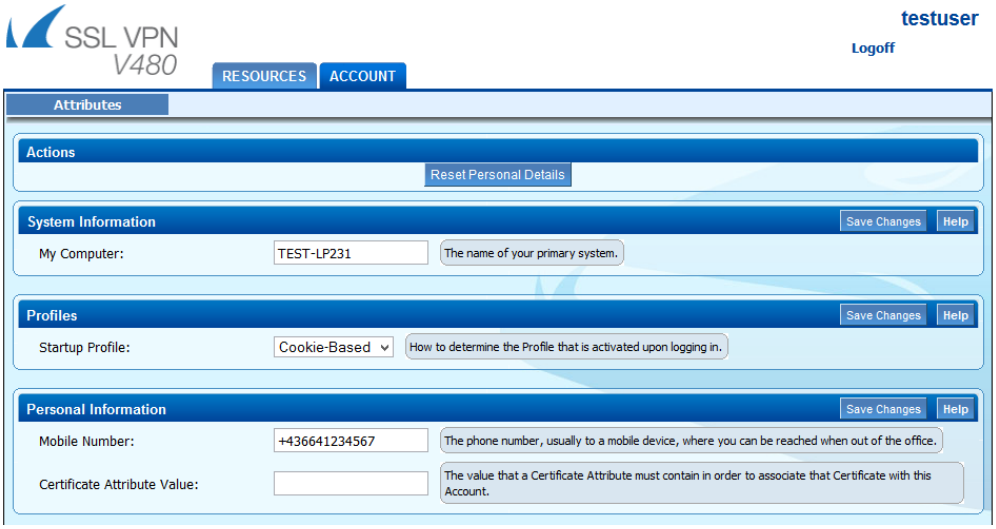
If more than one user database is configured (available on the Barracuda SSL VPN 380 and above), click **More** to select the correct user database before logging in.



From the **RESOURCES** tab, you can launch the previously configured resources.



From the **ACCOUNT** tab, you can change personal or user-specific information.

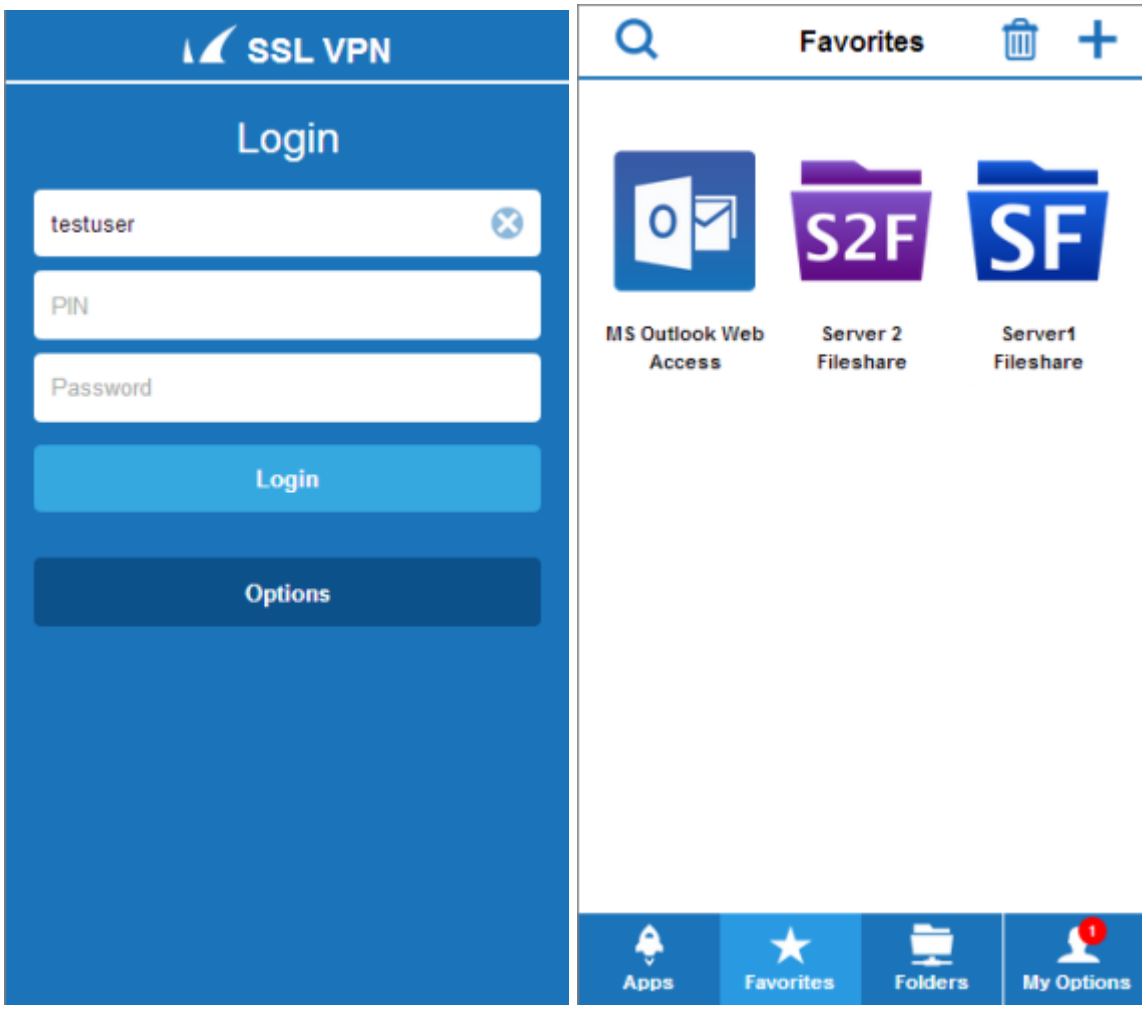


Log in using a mobile device

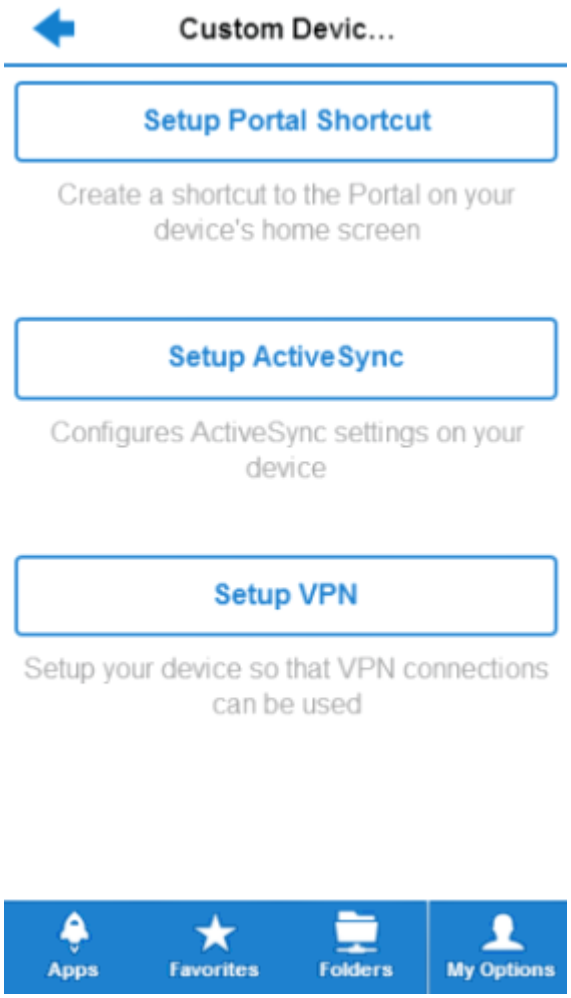
Use a mobile device (cell phone, tablet) to login to the Barracuda SSL VPN:

https://<IP address for the Barracuda SSL VPN>

You are automatically redirected to the mobile portal. There, you can use the **Apps** (Resources), **Favorites**, and **Folders** (Network Places) you configured previously.



If you are using an Apple iOS device the mobile portal offers a **Custom Device Setup** for VPN, Active Sync and the ability to create a shortcut on your home screen.



Related articles

For more information on the mobile portal see these articles:

- Mobile Portal User Guide
- Custom Device Setup for iOS Devices

Additional features to explore

The Barracuda SSL VPN contains many features that make it easy to use and deploy.

- The **User Activity Log** (**BASIC > User Activity Logs**) helps you identify who is using the SSL VPN and when they are interacting with the network.
- The **Audit Log** (**BASIC > Audit Logs**) records any changes to resources, access controls, and access rights.
- **Reports** (**BASIC > Reports**) are generated based upon the VPN Connection and Logon

Attempts log files.

- **Integrated Virus Scanning** on the portal ensures that web traffic and uploaded files do not contain malware.
- **Remote Assistance** lets you remotely control the computers of end users.
- **Server Agents** let you include resources from remote networks that cannot be reached directly by the Barracuda SSL VPN.

Figures