

# ZAGG iPad 2 Keyboard Folio

---

If you have been provided with a “ZAGGfolio” keyboard, please follow the below steps:

## Pairing your Keyboard

The Bluetooth keyboard should only need to pair to your iPad once as follows:

1. On the keyboard, slide the power switch to on. The status light illuminates for four seconds, and then turns off
2. On the iPad 2 select **Settings > General > Bluetooth > On**
3. Press the **Connect** button on the keyboard to make it discoverable. The status light flashes on the keyboard and the iPad displays “ZAGG Keyboard” as an available device
4. Select **Zagg Keyboard** on the iPad. The iPad will display a unique code for the keyboard
5. Type the code using the ZAGG keyboard and press the **Enter** button. The keyboard should now be paired to the iPad

# Tylt iPad 2 Keyboard Folio

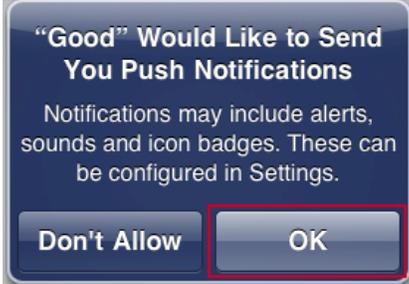
---

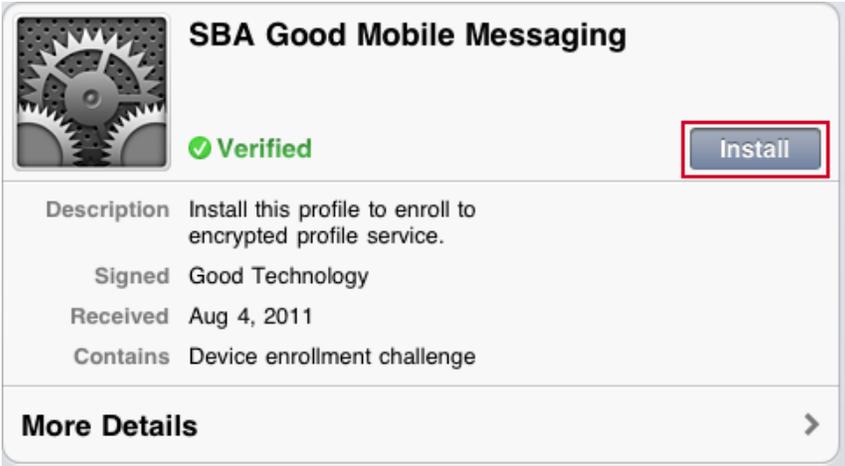
If you have been provided with a “ZAGGfolio” keyboard, please follow the below steps:

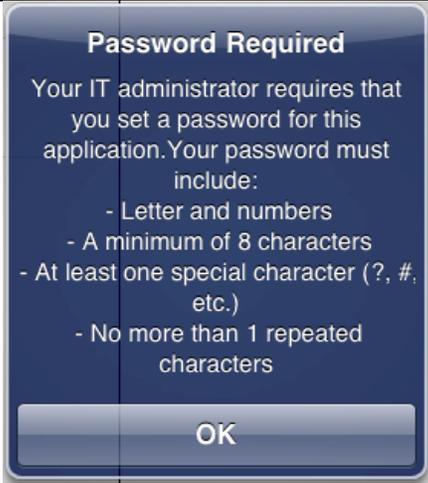
## Pairing your Keyboard

1. Press the “Settings” button
2. Select the “General” tab on the left hand side and then select “Bluetooth”
3. Turn on “Bluetooth”
4. Turn on the keyboard folio by sliding the power switch to the ON position
5. Press the “Bluetooth Pairing Button’ on the keyboard next to the power switch
6. On your device, you will see “Bluetooth Keyboard” has appeared under “Devices”
7. Select the “Bluetooth Keyboard”
8. You will see a pop-up on your screen asking you to enter a 4-digit PIN code. Enter this 4-digit code and press **Enter** on your keyboard
9. You are now connected

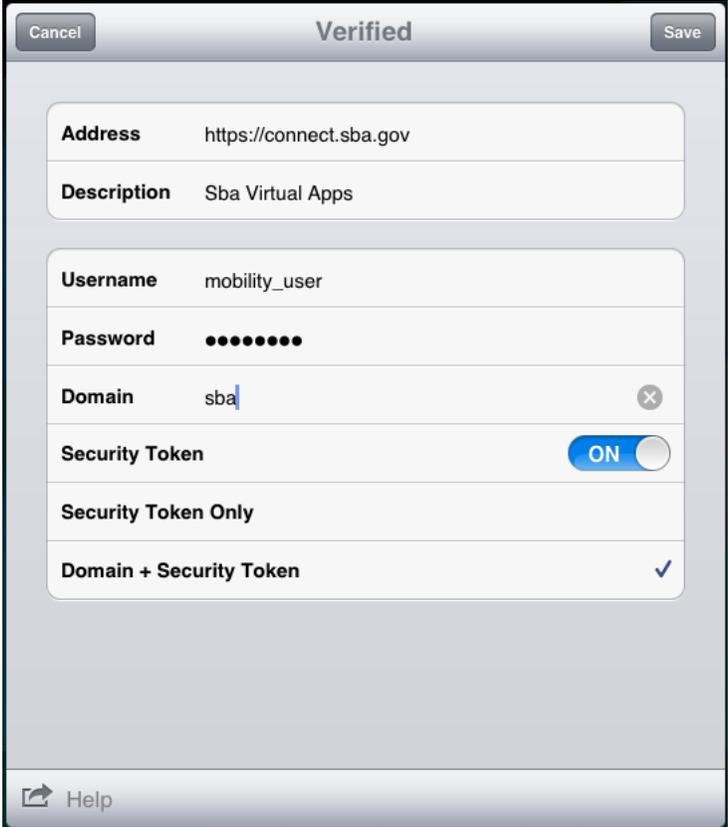
To set up your SBA-issues iPad with *Good for Enterprise*:

<i>Instructions</i>	<i>Example</i>
<p>1. Before you begin your setup of <i>Good for Enterprise</i>, please ensure that you have received an e-mail from “Good Admin” which contains your e-mail address, and your PIN number.</p> <p><b>Please note:</b> PIN numbers expire after two (2) days. Contact the SBA Service Desk at 202-205-6400 if your PIN number has expired and a new one can be sent to you.</p>	
<p>2. Make sure that your iPad is fully charged and your wireless or 3G connection is active</p>	
<p>3. Tap on the <b>Good</b> icon located at the bottom of your iPad’s screen</p>	
<p>4. Tap on the <b>OK</b> button to allow <i>Good for Enterprise</i> to send you “Push Notifications”</p>	
<p>5. Tap the <b>Start</b> button once the information screen is displayed</p>	
<p>6. Tap as necessary to accept the <i>Good</i> license information</p>	

7.	Enter your e-mail address and PIN number in the setup screen. The <i>Good for Enterprise</i> installation begins	
8.	As configuration policies have been established for your iPad, you will need to complete the following steps. When the “Profile Required” dialog window appears, tap the <b>Install Now</b> button. The <i>Good</i> installer exits and the iPad’s <i>Safari</i> browser launches to perform a check	
9.	When the “Install Profile” dialog window appears, tap the <b>Install</b> button, then tap on <b>Install Now</b>	
10.	When prompted, enter your iPad’s passcode and then tap the <b>OK</b> button	
11.	Tap the <b>Done</b> button once the installation is complete	
12.	Tap the <b>Done</b> button once the <i>Good for Enterprise</i> installation is complete	

<p>13.</p>	<p>You will now need to enter a password for access to <i>Good for Enterprise</i> using the guidelines shown on the right</p>	
<p>14.</p>	<p><i>Good for Enterprise</i> will now automatically synchronize your iPad with information from your SBA Microsoft Exchange account. When synchronization is complete, the "Welcome to Good for Enterprise" message you received previously, will appear in your iPad e-mail Inbox (located within Good), along with the 100 most recent e-mails contained in your Inbox</p>	

Follow the instructions below to set up *Citrix Receiver*

	<i>Instructions</i>	<i>Example</i>
1.	From the home screen, tap on the Citrix Receiver icon	
2.	Tap on the <b>Add Account</b> button	
3.	In the <i>Address</i> field enter <b>connect.sba.gov</b>	
4.	Enter Username, password, domain. Turn Security Token On. Ensure Domain + Security Token is checked. Tap save.	

5.	Enter your token (and password if you did not already enter) to authenticate. Tap the <b>OK</b> button when completed	

# BOLT: MOBILITY PROJECT – PILOT USERS AGREEMENT

## **Pilot Background**

This pilot seeks to explore the use of tablet-based computers within the SBA enterprise. This technology represents a new technology within SBA. As such, we need to assess the functionality, security, and manageability of these devices. As a participant in this pilot, you must accept and adhere to the following rules and guidelines:

## **Functionality**

This pilot intends to demonstrate that this tool is a meaningful addition to the SBA technology platform. Tablet devices may represent a significant cost savings over currently implemented mobile devices. It is important to understand that as this is new technology, some functionality may not work as expected, and we ask that you remain patient as any problems are resolved. As a pilot user, you will:

- Participate in pilot specific surveys, assessments and working sessions
- Assess the device's capabilities in the context of your daily work
- Consider potential new uses

## **Management**

A successful pilot must also reveal the capabilities of managing these devices from an enterprise perspective. As a pilot user, you shall:

- Try to use the tablet as a replacement for your laptop or desktop
- Respond to queries from the Pilot Team
- Immediately notify the Pilot Team concerning theft or loss of device
- Not lend the device to non-SBA employees
- Acknowledge that the device can be remotely disabled at any time
- Understand that the tablet device can be retrieved at any time

## **Security**

Security is paramount. Without a secure platform, the pilot will not be successful. Thus, as a pilot user, you must agree to the provisions set forth in the separate security agreement.

## **Duration**

The pilot will begin on 16 NOV 2011 and will conclude on 16 MAR 2011.

I have read, understood and accepted the terms outlined above and agree to be part of the BOLT: Mobility Pilot project.

---

Name

---

Signature

---

Date

## **BOLT: MOBILITY PROJECT – PILOT USERS SECURITY AGREEMENT**

The SBA is committed to ensuring government information is properly secured and protected. This requirement is of particular importance with the Mobility Pilot. As the device is portable, it can be easily lost or stolen. With the integration of new technologies, additional risk is assumed. Finally, when combined with access to SBA data, our overall risk profile is elevated. Thus, it is incumbent on our pilot users to ensure the device is properly secured and be diligent in following our policies.

Specifically, the pilot user must heed the following guidelines. Failure to do so will result in your removal from the pilot.

Follow currently implemented rules for acceptable use. (SOP 90.49.1 and 90.47.2)

Receive permission from the pilot team before you download software.

Not use the device outside of the United States.

Beware of roaming charges.

Maintain an appropriate password.

Not share your password.

Immediately notify the pilot team of theft or loss.

Not lend the device to non-SBA employees.

Not participate in prohibited activities to include:

- Gambling.

- Intentionally visiting and downloading material from pornographic Web sites.

- Lobbying Congress or any government agency.

- Campaigning – political activity.

- Any type of continuous audio or video streaming from commercial, private, news, or financial organizations, except as expressly authorized by management.

- Activities that are connected with any type of outside employment.

- Endorsement of any non-government products, services, or organizations.

As part of the OCIO's comprehensive approach to manage and secure this device, this device will be subject to monitoring and oversight. Some of these capabilities will include:

- Remotely wiping the tablet of all data and applications

- Remotely accessing the device by support personnel

- Remotely identifying which applications have been installed

- Blacklisting applications.

- Resetting passwords.

- Monitoring usage

Existing controls and agreements will also be in place. These include:

- Filtering to prevent inappropriate and offensive messages from passing through SBA email gateways.

Prohibiting the forwarding of official SBA email to private email addresses

Prohibiting the use of SBA IT resources to send, receive, retain, or proliferate any messages or material that is fraudulent, inappropriate, offensive, harassing, or is of a sexual nature.

Following established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards.

Following established channels for requesting and disseminating information.

Accessing only those files, directories, and applications for which access authorization by the system administrator has been granted.

Using government equipment only for approved purposes.

Users shall NOT:

Give information to other employees or outside individuals who do not have access authority.

Store sensitive or confidential information on a system unless access control safeguards are used.

Use their trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.

Browse files (i.e., what can be accessed).

Users are accountable for actions related to information resources entrusted to them. Users shall:

Behave in an ethically, technically proficient, informed, and trustworthy manner when using systems.

Be alert to threats and vulnerabilities such as malicious programs and viruses.

Comply with all software licensing agreements, and not violate Federal copyright laws.

Know that there may be monitoring and that there is no expectation of privacy on SBA IT resources.

Access to confidential or sensitive information must be restricted to authorized individuals who need it to perform their jobs. This entails refraining from intentional disclosure and using measures to guard against accidental disclosure. Users shall:

Protect confidential or sensitive information by using encryption, and limiting the collection, disclosure, sharing and use of PII data. Never access or disclose personal information or other sensitive data unless it is necessary to perform official duties.

Not send highly sensitive or classified information

Not store or transmit confidential information on public access systems, such as email or the Internet.

Ensure that the tablet screen is not viewed by unauthorized persons.

Users must protect the integrity and quality of information. This includes, but is not limited to:

Protecting information against viruses and similar malicious code by discontinuing use of a system at the first sign of virus infection.

Never knowingly entering unauthorized, inaccurate, or false information into a system.

Computer systems and media must be protected from environmental hazards such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling. Users shall:

Users are responsible and accountable for any actions taken under their user ID. Users shall:

Protect passwords from access by other individuals.

Never give a password to another person, including a supervisor or a computer support person.

Construct effective passwords by following SBA password policy for complex passwords.

Users must protect computer equipment from damage, abuse, theft, and unauthorized use. Users shall:

Protect computer equipment from hazards such as:

Extreme temperatures;

Electrical storms;

Water and fire;

Static electricity;

Spills from food and drink;

Dropped objects;

Excessive dusty environments; and

Combustible materials.

Not leave computer equipment in a parked car or in an unsecured location where it might be stolen.

Not alter the configuration,

Notify management before relocating computing resources.

When possible, use physical locking devices for laptop computers and use special care for other portable devices.

Do not install non-authorized software without approval from the appropriate management official. Computer users must protect SBA owned software and equipment from malicious software. Users shall NOT:

Use SBA purchased software on personally owned or non-SBA computers unless authorized.

Alter the configuration, including installing software or peripherals, on government computer equipment unless authorized.

Comply with all software licensing agreements and Federal copyright laws.

Not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system unless otherwise expressly authorized."

Users are prohibited from using Peer-to-peer (P2P) file sharing. P2P file sharing poses a threat to IT security. It allows employees to transfer files between computers without proper security controls. These programs can be used to distribute inappropriate materials, violate copyright law and put government information at risk.

There are no exceptions to the requirement that all employees, contractors, partners, and volunteers comply with these rules of behavior. If you are not sure whether your intended computer use is prohibited, you should NOT do it. Consult with Mobile Project team with questions.

SBA requires employees, contractors, partners, and volunteers to acknowledge that they understand their responsibilities and accountability for using SBA information and resources.

I have read, understood and accepted the security terms above and agree to be part of the BOLT: Mobility Project pilot.

\_\_\_\_\_

Name

\_\_\_\_\_

Signature

\_\_\_\_\_

Date