Thank you for choosing AT&T Business in a Box® and for allowing us the opportunity to serve you.

AT&T is dedicated to providing you with an exceptional user experience. The AT&T team will work closely with you at every step of the way to help make your experience as easy as possible. Please take a few minutes to review the following information, which includes:

- AT&T Business in a Box® Overview and Important Contact Information
- Customizing your Device(s)

Best Regards,
AT&T

Overview

The AT&T Business in a Box® Converged Networking Router is an intelligent, all-in-one networking solution and provides the following important functions for converged networks:

- A Single Device or Set of Devices and Network Connections that provides combined Voice and Data Service for your business
- Business VoIP (using analog phones, PBX and VoIP Phones)
- Analog Voice Ports
- Outbound Survivability
- LAN ports with Power Over Ethernet (POE) for connecting PC’s, Servers, IP Phones, etc.
- Quality of Service (QoS) for voice and data over the same network
- Several Customer Managed features

Important Contact and Support Information

Once your implementation is complete, you will be supported by AT&T Customer Care.

Phone - 1-877-ATT-VDNA (1-877-288-8362)

Note: If you purchased Managed Router Solution with Business in a Box CPE and AT&T VPN, you will be given a specific phone number to contact for support by your AT&T Project Implementation Manager.

AT&T Business Direct® – https://www.businessdirect.att.com

Additional documentation is available for:

AT&T IP Flexible Reach – http://www.corp.att.com/bvoip/ipflex/

Note: Username and password for both is:
  Username – att
  Password – attvoip

Customer Managed Features Overview

AT&T Business in a Box® includes several features that can be enabled for use. These features can be configured by you to your specifications utilizing this documentation. AT&T support for these features is limited to this Users Guide and the AT&T Tech Support 360SM offer mentioned below.

- Firewall
- Wireless (Wi-Fi) Access Supporting 802.11b/g clients
- Remote access using Point to Point Tunneling Protocol
- IPSec VPN for connecting remote locations

Should additional support for the setup and configuration be required please request your AT&T Sales Team provide details regarding the AT&T Tech Support 360 offer for AT&T Business in a Box Firewall, Wi-Fi and Remote Access.
Contents of the Shipping Box

Please check to ensure all contents are present upon receiving your shipment of AT&T Business in a Box®. Direct any questions about the contents to your AT&T technical contact during the installation.

The contents of the box will include one of the Base Unit devices below.

- 1 Base Unit device (12-port or 24-port PoE)
  - Power adapter
  - Power cable
  - Screws for rack mount brackets
  - Rack mount brackets (with mounting template & instructions)
  - Wi-Fi antenna
  - 14’ brown RJ-11 cable for v.90
  - Gray RJ-45 14’ T1 cable
  - Power Strip
  - Red RJ-45 25’ T1 Crossover cable for PRI/TDM PBX customer orders

In addition, the contents may include these add-ons to support your service:

- 8-port PoE switches, each of which include the following components:
  - Power supply, including power pack and power cord
  - Rack mount brackets (with mounting template & instructions)
  - Screws for rack mount brackets
  - Orange 7’ RJ-45 Ethernet cable

- 24-port PoE switches, each of which include the following components:
  - Black null modem serial cable
  - Power cord
  - Rack mount brackets (with mounting template & instructions)
  - Screws for rack mount brackets
  - Black plastic square feet for desktop installation
  - Orange 7’ RJ-45 Ethernet cable

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
8-port analog expansion modules, each of which includes the following components:

- Power adapter
- Power cable
- Screws for rack mount brackets
- Rack mount brackets (with mounting template & instructions)
- Orange RJ-45 7’ Ethernet cable
- Analog expansion module stencils
- Screws
- Cable tie
- Self adhesive cable tie base

**Caution**

The Erase Button on the back or front of any of the managed devices should never be pressed. Pressing the Erase button will reset the hardware and will fully disable your Voice and Data connectivity which will require either a replacement and/or onsite technician to reconfigure the hardware. Service will be unusable until restored. If the Erase button is pressed, please call AT&T for further support.

---

**Customize your device(s)**

The following learning topics in this section will provide you with information on how to log into your AT&T Business in a Box® to then customize to your needs.

**Learning Topics:**

- Overview of the Base Unit router ports
- Logging into your Device
- Configure your Base Unit Router for a secure connection with a VPN Concentrator or other AT&T Business in a Box® device
- Configure your Base Unit Router for secure remote connections
- Configure your Base Unit Router for use with a DMZ
- Configure your Base Unit Router for Port Forwarding
- Configure your Base Unit Router to provide Wireless (Wi-Fi) access

*AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.*
### Overview of the Base Unit Router ports

#### Illustration:
- **Front panel:** Shows the layout of ports.
- **Back panel:** Highlights key components like the power switch and various ports.

#### Table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Cable Provided by</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Port (RJ45)</strong></td>
<td>Port for third-party firewall. NOTE: This port is the only port that can</td>
<td>Customer provided cable (RJ45) to customer owned firewall</td>
</tr>
<tr>
<td></td>
<td>connect with a third-party firewall.</td>
<td></td>
</tr>
<tr>
<td><strong>Ethernet Ports (RJ45)</strong></td>
<td>12 or 24 ports for the LAN on the public segment. Use Ethernet LAN ports</td>
<td>Customer provided cable (RJ45) to IP phones, PC's, servers, printers, etc. or</td>
</tr>
<tr>
<td></td>
<td>to connect to IP phones, PC's, servers, printers, etc. or add on devices</td>
<td>add on devices to the AT&amp;T Business in a Box® base unit. As a Power Over Ethernet</td>
</tr>
<tr>
<td></td>
<td>to the AT&amp;T Business in a Box® base unit. As a Power Over Ethernet (PoE)</td>
<td>(PoE) port, these ports can also transfer electrical power to remote devices.</td>
</tr>
<tr>
<td><strong>Survivability ports (FXO) (RJ11)</strong></td>
<td>Utilized for Outbound Survivability. 2 ports that retain functionalty even in the case of a power outage.</td>
<td>Customer provided cable (RJ11) to jack</td>
</tr>
<tr>
<td><strong>Analog Phone ports (FXS) (RJ11)</strong></td>
<td>6 ports for connecting to voice devices. These ports are normally used for connecting Analog phones, Fax or Key Systems.</td>
<td>Customer provided cable (RJ11) to customer key system</td>
</tr>
<tr>
<td><strong>T1 ports (WAN) (RJ45)</strong></td>
<td>Port that connects to a T1 or NxT1 service demarcation endpoint (SmartJack). Note that if your service requires connecting to a TDM PBX with a PRI interface that one port will be connected to the included RED cable labeled &quot;T1 Crossover cable – TDM PBX&quot;.</td>
<td>AT&amp;T provided cables. Grey cable(s) from SmartJack to grey port. For PRI (TDM PBX) uses RED cable in port #4</td>
</tr>
<tr>
<td><strong>Modem Port</strong></td>
<td>Port that the customer supplied telephone line (POTS line) is connected to for remote access by AT&amp;T Support staff.</td>
<td>AT&amp;T provided cable. Brown cable from POTS jack to brown port</td>
</tr>
<tr>
<td><strong>Wireless Antenna</strong></td>
<td>Antenna for the wireless LAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>Accepts the plug from the supplied power cord to connect the unit to a power source.</td>
<td></td>
</tr>
<tr>
<td><strong>Power Switch</strong></td>
<td>Turns the power off and on.</td>
<td>Please note that there are two USB ports on the router that should not be utilized.</td>
</tr>
</tbody>
</table>
Customizing the Base Unit Router

IMPORTANT: Please note that AT&T does not provide technical support related to completion of the tasks described in this section. Should you require additional assistance with the included Customer Managed Firewall, Wi-Fi or Remote access utilizing Point to Point Tunneling Protocol please contact your AT&T Sales Representative and inquire about AT&T Tech Support 360℠ offer.

Logging into the Base Unit Router

1. Connect a PC via Ethernet to any port other than LAN port 2 on the Base Unit Router (LAN port 2 is reserved for an external firewall if required).

2. Launch a web browser on the PC and enter the following URL: http://192.168.4.1/

   Note: If you have not received an IP address for your connected device via DHCP, you must statically assign your IP address to 192.168.4.2

3. A login window similar to the following should appear:

4. Enter “custadmin” in the User name field and the last six characters of the MAC address in the Password field.

   You can locate the MAC address on the bottom side of the base unit router, as shown in the following figure:

   Example Password: 25BACE

   IMPORTANT: When entering the MAC address, always use uppercase characters.

5. Upon successful login, the web configuration GUI appears. You will see the Configuration Menu on the left hand side of the screen which you will use in the customization of your device.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
Configure the LAN of the Base Unit Router for remote access

Prerequisite task: Log on to the base unit router as described in Configure the Base Unit Router.

1. Choose **Firewall > Customer Networks**.

   Select the PPTP Server address dropdown and choose from the available IP addresses. For this example 12.105.153.43 has been chosen already. Your options will be different and will be based upon the IP address range provided with your service. Once you select an available IP address, then press the **Submit** button to save your changes.

2. Write down the IP address you chose above for the **PPTP Server Address**.

3. From the **Configuration Menu** select **PPTP Server**.

4. Select **Enable PPTP Server** Checkbox.
   
   The **IP Range** should be populated for you. Populate the **WINS** section if needed and **PPTP Authentication Mode** may be changed if appropriate. Select **Submit** when complete.
5. Select **Usernames** under the **PPTP Server** Configuration Menu.

6. Enter the **Username** that the remote user will use to access the **PPTP server** and to connect to the LAN. Enter and confirm the **Password** for the remote user. Select **Add** when complete and the new User will show up under **PPTP Usernames** below. Perform this step for each user that should be added for remote access. For the example below the User “Scott” is being added.

On the computer or device you wish to use to connect remotely, configure per the specifications of that device. In the configuration, specify the PPTP Server Address you selected in the steps above as the server, and specify the authentication settings using the Username and Password created above as well.

Test your devices ability to connect to the PPTP Server and your LAN resources.

---

**Configure the Base Unit Router for use with a DMZ**

Prerequisite task: Log on to the base unit router as described in Configure the Base Unit Router.

1. Choose **Firewall**. The following screen appears:

2. Make sure that **Allow HTTP access through Firewall** is selected.

3. Click **Submit**.

4. If all traffic will be redirected to a third party firewall that is not physically connected to the Base Unit Router, complete the following steps:

---

**AT&T Proprietary:** The information contained herein is for use by authorized persons only and is not for general distribution.
i. Choose **Firewall > Assigned LAN Addresses.**
The following screen appears:

ii. In the **Hostname** field, specify a hostname by which the Base Unit Router will recognize the third-party firewall.

iii. In the **IP Address** field, specify the IP address of the third-party firewall.

iv. Click **Add.**

5. Choose **Firewall > Port Forwarding.**
The following screen appears:

6. In the **Select a system** drop down window, select the firewall for your DMZ.

Note: If you have assigned a LAN address to a third-party firewall that is not connected to the Base Unit Router, it should appear in this drop down menu.

7. Select the radio button next to **Allow the Selected Applications to access the System.**

8. Specify which applications should be allowed to access the LAN through the firewall.

9. Click **Submit.**

The DMZ is ready for use by devices connected to the LAN.
Configure the Base Unit Router for Port Forwarding

In this example we will allow a Web Server that utilizes HTTPS on the Private LAN to be accessed remotely. The example assumes the Server is already connected and working as expected on the LAN and utilizes TCP port 443 for access. Your information is expected to be different so changes to the information entered in your specific scenario will be different. There are numerous other built-in examples under Available Applications which could be selected as well.

You may want to assign a static IP address to your device you will be using to Port Forward to.

1. Select Firewall, then select Assigned LAN Addresses
2. Under Add an Assigned LAN Address, enter a Hostname and IP Address (from your private IP from your LAN IP address block)
3. Click Add

Prerequisite task: Log on to the base unit router as described in Configure the Base Unit Router.

1. Select Firewall. The following screen appears:
2. Make sure that Allow HTTP access through Firewall is selected.
3. Click Submit.
4. Select **Port Forwarding** under **Firewall** on the Configuration Menu. The following Screen appears.

5. In the **Select a system** dropdown, select your Web Server from the list. Next under **Available Applications** select **HTTPS Server** and click the + symbol to the right which will add this to the list of **Allowed Applications**. When you do so, **Maximum Protection** is then automatically changed to **Allow the selected applications**.

6. Click **Submit**

Your Secure Web Server using HTTPS should now be available from the Internet.

Note: If the specific requirements you have are not listed in the **Available Applications** section you can add custom applications/protocols by clicking **Manage User-defined applications/protocols** which is directly under the **Available Applications** slider. You can then add a **Name** of the application/protocol, **Protocol type** (TCP/UDP) and **Public Port/Server Port** which will then be available to select from the Available Applications for your device.
Configure the wireless (Wi-Fi) settings of the Base Unit Router

Prerequisite task: Log on to the base unit router as described in Configure the Base Unit Router.

1. Select **Wireless**.

2. The following screen appears

3. Select the checkbox at the top of the screen to enable wireless capabilities.

4. Modification can be made to each of the dropdown options listed above to fit the needs of your location. Click **Submit**.

5. Wi-Fi is ready for use by devices to connect to the LAN.

6. On your Computer or other device that will utilize Wireless, utilize the devices configuration utility for Wireless. The configuration utility should display the wireless network SSID as described above. In the Password field, enter the Pre-Shared Key (PSK) which is also commonly known as the password set above.

7. Once complete, you should be connected to the Base Unit router via Wi-Fi. Test your connection with your devices web browser to ensure connectivity.
Configure the LAN of a local Base Unit Router for a secure connection with the LAN of a remote third-party VPN concentrator or other Base Unit Router

IMPORTANT: Determine the following values that will be shared between the local and remote VPN device (such as another AT&T Business in a Box® router or third-party VPN concentrator) before starting this procedure:

- The shared secret, a field consisting of up to 32 alphanumeric characters (excluding the character “$”), to be shared between the local and remote Base Unit Router.

- The encryption settings, including the Diffie-Helman Group (DH Group) to use for Phase 1 and Phase 2 of encryption, the cipher, hash algorithms and times to use Phase 1 and Phase 2 of encryption, and whether or not your VPN tunnel will employ Perfect Forward Secrecy. Perfect Forward Secrecy is a security measure which ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

- The IPsec server address and network mask of the Customer Data VLAN, located on the Customer Networks (choose Firewall > Customer Networks to view the Base Units configuration) page of the Base Unit Routers.

Prerequisite task: Log on to the local base unit router.

1. Select **VPN**
2. Select the checkbox next to **Enable the VPN module**
3. Click **Submit**
4. Click **Add Tunnel**
The following screen appears:

1. In the **Name** field, enter a name for this VPN connection.

2. In the **Remote VPN Gateway** field, enter the IPsec server address of the remote Base Unit Router or the third-party VPN concentrator.

3. In the **Protected Remote Network** field, enter the Customer Data VLAN of the alternate Base Unit Router or the third-party VPN concentrator.

4. Enter the shared Secret, and confirm the DH Group, Phase 1, Phase 2, Phase 1 Lifetime and Phase 2 Lifetime settings.

   Important: Ensure that these fields contain the same values on both the local and the remote Base Unit Router.

5. Select the checkbox next to **Perfect Forward Secrecy** if it will be used on both the local and remote Base Unit Router.

6. Click **Submit**.

7. Repeat the preceding steps on both the local and remote Base Unit Routers.

8. On the local Base Unit Router, choose **Firewall**.

   The following screen appears:

9. Make sure that **Allow HTTP access through Firewall** is selected.

10. Click **Submit**.
11. Choose **Firewall > Trusted Hosts**. The following screen appears:

12. Enter the IP address of the remote Base Unit Router in the **IP/Network Address** field.

13. Enter the Netmask of the remote Base Unit Router or the third-party VPN concentrator in the **Netmask** field. Click **Add**.

After having configured both devices as shown above, the local and remote routers are now securely connected.
### AT&T Business in a Box® CPE specifications

<table>
<thead>
<tr>
<th><strong>WAN Ports</strong></th>
<th>4xT1 CSU/DSU</th>
</tr>
</thead>
</table>
| **LAN Ports** | • 12 or 24x10/100/1000 Mbps Power Over Ethernet (POE) ports  
• Add-on POE module options available with either 8x10/100 Mbps POE ports or 24x10/100 Mbps POE ports |
| **Phone/FXS** | • 6xRJ11 connectors  
• Note: Additional option for Add-on Analog port expansion module with 8xFXS (RJ11) |
| **Line/FXO** | 2xRJ11 connectors |
| **Environmental** | Operating Temperature: 41° to 104° F  
Humidity: 20% to 80%, non-condensing |

---

### 8 Port POE Module – Power and Dimension Specifications

| **Power Supply (AC)** | 100-240V, 3.0A |
| **Power Support** | IEEE 802.3af with a maximum of 15.4W per port and a total of 70W for the switch |
| **Dimensions (H/W/D)** | 1.73”/10.35”/6.69” |
| **Weight** | 2.9 lbs |
| **Regulatory** | CE Mark, FCC Class A, CISPR Class A, EN 6100-4-2/3/4/5/6/8/11, UL/CUL (UL 60950-1, CSA 22.2 No. 60950-1), CB (IEC60950-1, EN60950-1) |

### 24 Port POE Module – Power and Dimension Specifications

| **Power Supply (AC)** | 100-240V, 7.0A |
| **Power Support** | IEEE 802.3af with a maximum of 15.4W per port and a total of 180W for the switch |
| **Dimensions (H/W/D)** | 1.69”/17.32”/16.14” |
| **Weight** | 12.7 lbs |
| **Regulatory** | CE Mark, FCC Class A, VCCI Class A, CISPR Class A, TUV/GS(EN60950), CB, CSA/NRTL(CSA 22.2 No. 60950) |

### Base Unit 12 or 24 (4608PoE version as noted on bottom of router) – Power and Dimension Specifications

| **Power Supply (AC)** | 100-240V, 2.5A, 50-60 Hz |
| **Power Supply (DC)** | 48V, 3.75A |
| **Total Power** | 200W (12 port & 24 port) |
| **Switch Power** | 120W |
| **Power per Port (avg.)** | 10W (12 port) 5W (24 port) |
| **Power per Port (max)** | 14W |
| **Dimensions (H/W/D)** | 1.75”/16.93”/13.19” |
| **Weight** | 16.09 lbs |
| **Regulatory** | UL, CE, FCC Part 68, FCC Part 15, Industry Canada, CB |

### 8 Port Analog Expansion Module (4570 version as noted on bottom of router) – Power and Dimension Specifications

| **Power Supply (DC)** | 12V, 3.0A |
| **Dimensions (H/W/D)** | 1.7”/10”/7” |
| **Weight** | 2.0 lbs |
Legal Notice

This AT&T Business in a Box® User Guide ("Guide") is offered as a convenience to AT&T’s customers. The specifications and information regarding the product in this Guide are subject to change without notice. All statements, information, and recommendations in this Guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this Guide.

In no event shall AT&T or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this Guide, even if AT&T or its suppliers have been advised of the possibility of such damage.