|  |  |
| --- | --- |
|  |  |
| Administrator’s Guide  Integration Framework on Single-Board Computer  Document Version: 1.3 – 2019-12-05 | Public |
| Administrator’s Guide | |

Document History

|  |  |  |
| --- | --- | --- |
| Version | Date | Change |
| 1.0 | 2017-10-24 | First version |
| 1.1 | 2017-11-22 | Enhanced version including screenshots and security information |
| 1.2 | 2018-06-05 | Release to Customer |
| 1.3 | 2019-12-04 | Ported to Raspbian 10 (Buster) , Raspberry Pi 4 hardware platform supported, ported to Tomcat 8 |

Table of Contents

1 Prerequisites 4

1.1 Hardware Requirements 4

1.2 Software Requirements 4

1.3 Infrastructure Requirements 5

2 Preparing the Installation 6

3 Booting Raspbian 8

4 Installation of the Integration Framework 10

4.1 Installing the Integration Framework 10

4.2 Performing Post-Installation Activities 12

4.2.1 Configuring the Host Name 12

4.2.2 Removing Temporary Files 13

4.3 Service Configuration 14

4.4 Shutting Down and Rebooting Raspberry Pi 14

4.5 Uninstalling the Integration Framework 15

5 Service Discovery 17

6 Network Security 18

6.1 Securing Access to Integration Framework 18

6.1.1 Enabling HTTPS 18

6.1.2 Disabling HTTP 20

6.2 Remote Access Through Secure Shell (SSH) 21

6.3 Securing Console Access 22

7 Rollout to Further Devices 24

7.1 Backing Up and Restoring the Installation 24

7.1.1 Backing Up the Installation Using Windows 24

7.1.2 Backing Up the Installation Using Linux 25

7.1.3 Restoring the Backup Using Windows 26

7.1.4 Restoring the Backup Using Linux 26

7.2 Using SD Cards on Further Devices 27

# Prerequisites

## Hardware Requirements

For the installation of the integration framework, Internet of Things (IoT) edition, have the following hardware available:

* Raspberry Pi 3 or 4 compatible with appropriate power supply
* Monitor with HDMI connector and corresponding cabling
* Keyboard
* Mouse
* Network cable (optional)
* A PC running on Windows, Mac or Linux with an SD card writer
* FAT-formatted USB stick
* Micro SD card with up to 32 GB capacity. Raspberry Pi 3 only supports cards with up to 32 GB capacity.

## Software Requirements

Extraction Tools

|  |  |
| --- | --- |
| Operating System | Tool |
| Microsoft Windows | 7-Zip |
| Mac | The Unarchiver |
| Linux | GNU unzip, or any other appropriate extraction tool |

SD Card Imaging Tools

|  |  |
| --- | --- |
| Operating System | Tool |
| Microsoft Windows | Win32 Disk Imager or Etcher |
| Mac | Etcher |
| Linux | dd |

Service Discovery Tools (Optional)

|  |  |
| --- | --- |
| Operating System | Tool |
| iOS | BonjourSearch  Discovery – Bonjour Browser  (available for download from Apple App Store) |
| Android | Bonjour Browser  ZeroConf Browser  Service Browser  (available for download from Google Play Store) |
| Linux | Avahi Zeroconf browser  (Debian and Ubuntu:  sudo apt-get install avahi-utils) |
| Windows | Bonjour Browser (download available at: https://hobbyistsoftware.com/bonjourbrowser)  wxServDisc (download available at: https://sourceforge.net/projects/wxservdisc/) |

## Infrastructure Requirements

* Have access available to a wired or wireless network. A wired network access is preferred.
* The network you connect to must provide a connection to the internet without a proxy or through a transparent proxy.

# Preparing the Installation

Procedure

1. Download Raspbian Jessie from:

https://downloads.raspberrypi.org/raspbian/images/raspbian-2019-09-30/2019-09-26-raspbian-buster.zip

1. For Microsoft Windows and Mac, download and install Etcher from:

<https://etcher.io/>

For Microsoft Windows, choose the Download for Windows x64 option.

1. Depending on your operation system, extract the Raspbian image with an extraction tool of your choice.

* On Windows for example: 7-Zip
* On Mac: The Unarchiver
* On Linux: unzip

1. Insert a micro SD card with 8 to 32 GB capacity into your SD card writer and connect the writer to your PC.
2. Skip the step for all operating systems but Linux.

On Linux, enter the following statement on your PC to determine the device name of the SD card:

tail -f /var/log/syslog

Your system displays [sdx] Attached SCSI removable disk and sdx: sdx1 sdx2 …

sdx is the device name that we need later.

The number indicates a mounted partition, if the SD card contains mountable partitions.

1. Copy the Raspbian image to the SD card:

|  |  |
| --- | --- |
| Operating System | Tool |
| Microsoft Windows and Mac | To run Etcher:   1. In Etcher, select the image you extracted from the download and click Flash. 2. Answer the question, whether you allow Etcher to make changes to your system with Yes. 3. Wait until Etcher finished writing the image to your SD Card |
| Linux | 1. Change to the directory where you extracted the image. 2. If your system mounted the SD card automatically, unmount the SD card:   unmount /dev/[device][number]  [device] is the device name detected in step 5  [number] is the device number of the mounted partition   1. Repeat the procedure for each detected partition. 2. Alternatively, use the capabilities of your desktop environment. All modern desktop environments such as KDE, Gnome, MATE, Unity, and so on, provide the ability to unmount SD cards using the file manager. 3. To write the image to your SD card, enter the following statements:   sudo dd bs=4M if=/path/to/image of=/dev/[device] conv=fsync  Make sure to address the correct device. Choosing the wrong device can seriously damage your PC operating system.   1. To have a progress indicator available during the write operation, enter the following statements:   sudo su; dd bs=4M if=/path/to/image | pv | dd of=/dev/[device] conv=fsync  Make sure to address the correct device. Choosing the wrong device can seriously damage your PC operating system.   1. Wait until dd returns. |

Result

Raspbian is installed on your SD card. Depending on your operating system, safely remove or unmount the SD card from your system.

# Booting Raspbian

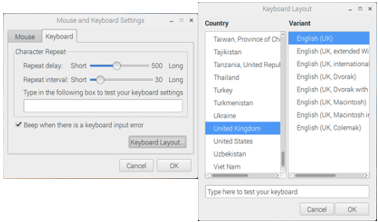
Procedure

1. Connect the Raspberry Pi to a monitor, keyboard, mouse and to a network. Do not yet connect the Raspberry Pi to the power supply.
2. Put the micro SD card into the Raspberry Pi.
3. Connect the Raspberry Pi to the power supply and monitor the initial booting of Raspbian.

The procedure automatically logs you in as the pi user.

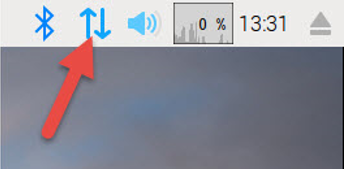
1. By default, Raspbian is preconfigured with the UK or US keyboard layout. To adjust the keyboard layout to your region, choose the Start Menu in the upper left corner of the desktop.
2. Choose Preferences → Mouse and Keyboard Settings, select Keyboard and click Keyboard Layout… .
3. In Keyboard Layout, select a keyboard layout of your choice and click OK.

The changes take immediate effect. Note that the procedure depends on the type of graphical user interface or desktop environment that you use on your Raspberry Pi.



Keyboard Settings

1. If the wired network that the Raspberry Pi connects to provides automatic network configuration via Dynamic Host Configuration Protocol (DHCP), you are already connected to your network. If you prefer using a wireless network and you do not have access to the desktop of the Raspberry Pi, follow the instructions to start the wireless network: https://www.raspberrypi.org/documentation/configuration/wireless/wireless-cli.md
2. To connect to a wireless network while having access to the desktop, click the network symbol in the upper right corner of your desktop. The desktop displays a list of wireless networks. Note that the procedure depends on the type of graphical user interface or desktop environment that you use on your Raspberry Pi.

  
Wireless Network Selection

1. To connect to a wireless network, select a wireless network and enter the secret.

Alternatively, open a shell and start the raspi-config general purpose configuration tool. The tool also allows you to change the keyboard layout and to attach out Raspberry Pi to a network.

# Installation of the Integration Framework

## Installing the Integration Framework

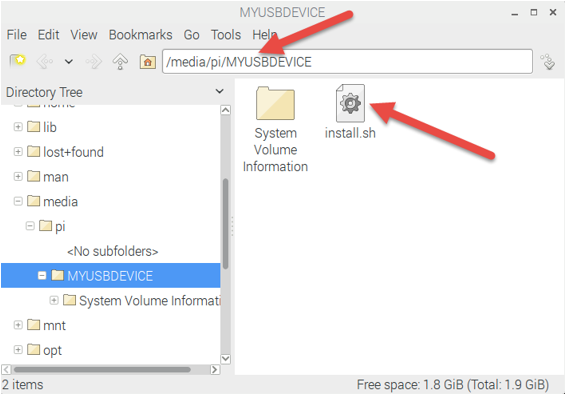
Prerequisites

You have the integration framework installation program available.

Procedure

1. On your PC, download the integration framework installation to a USB stick.
2. Remove the USB stick and connect the stick to the Raspberry Pi.
3. Raspberry Pi requests the action for the new device. Select the Open in File Manager option.

The system displays the File Manager window displaying the USB stick content and the mounted path. Note that the procedure depends on the type of graphical user interface or desktop environment that you use on your Raspberry Pi.

  
File Manager Window and Content

1. To open a terminal, click the Terminal icon in the upper left corner of the desktop.

Alternatively, choose Start → Accessories.

  
Open Terminal

1. In the terminal window, change to the directory displayed in the file manager.

  
Terminal Window

1. Enter the following commands that copy the installation to the tmp directory, call the installation program and call the integration framework:

* cp install.sh /tmp/
* cd /tmp
* chmod +x install.sh
* sudo ./install.sh
* chromium-browser <http://127.0.0.1:8080/B1iXcellerator/>

## Performing Post-Installation Activities

### Configuring the Host Name

By default, the host name of a new Raspbian system is raspberry. During boot time, the host name is broadcasted to the network that the system is connected to. It allows other computers in the same network segment to contact the Raspberry Pi by using the name rather than the IP address. The approach works if there is only one device called raspberry connected to the network. If you want to run more devices in the same network, assign a distinct host name to each device to avoid naming collisions in the network. You have the following alternatives:

* Configuring the host name on the client
* Managing the host name on the server

#### Configuring the Host Name on the Client

Raspbian provides a user-friendly user interface tool to change several system parameters. Use the tool to change the system host name.

Procedure

1. Click the icon in the upper left corner of your desktop to open the start menu.
2. Select Preferences and in the submenu, select Raspberry Pi Configuration.
3. Select the System tab, to change the system host name, click OK and reboot the system.
4. If you do not have access to the graphical desktop of your Raspbian system, change two files in the following way in a terminal:

* sudo nano /etc/hosts
* Find the line that contains 127.0.0.1 raspberry and replace the term raspberry with the name you want to assign.
* Enter CTRL-x followed by y to exit nano by saving the file.
* sudo nano /etc/hostname
* Replace again the term raspberry with the name you want to assign.
* Enter CTRL-x followed by y to exit nano by saving the file.
* sudo reboot

Result

When the system is available, you can reach the system using the new host name in the network.

#### Managing the Host Name on the Server

During boot time, the network configuration of most devices is negotiated between the client and the network by Dynamic Host Configuration Protocol (DHCP). DHCP allows a client such as the Raspberry Pi, to request a host name from the network. This is very convenient when setting up a larger number of devices in the same network. You do not have to perform the host name configuration on each device.

Prerequisites

The DHCP server in the network must support the feature to provide a host name upon request. Not all DHCP servers support the feature. Some DHCP servers require server-side configuration to support the feature. If you are not sure, ask your IT staff or try it out.

Procedure

1. To enable the function on Raspbian, open a terminal or login via Secure Shell (SSH).
2. Enter sudo nano /etc/dhcp/dhclient.conf
3. Find the line that contains send host-name = gethostname();
4. Comment out the line by prepending it with a #.
5. Find the line that starts with request.
6. Make sure the comma-separated list behind request contains the host-name term.
7. Enter CTRL-x followed by y to exit nano by saving the file.
8. Enter sudo reboot

Result

After reboot, you can reach your Raspberry Pi through the network by an automatically assigned host name. If the feature is not available, contact your IT.

### Removing Temporary Files

Procedure

After successful installation, enter rm /tmp/install.sh to delete install.sh.

## Service Configuration

During the setup procedure, the SSH Daemon was enabled on your Raspberry Pi to allow remote logins when running headless without connection to a monitor. This is the usual way to run your Raspberry Pi in an IoT setup. To secure the service, change the password of the pi user.

Procedure

1. Login with the pi user.
2. In a terminal or in the command line, enter: sudo passwd pi
3. The system asks you to enter and confirm a new password for the pi user.

It is essential for the security of your IoT infrastructure to enter a secure password and to keep it a secret.

## Shutting Down and Rebooting Raspberry Pi

Several options are available to shut down and to reboot the system.

Procedure

With access to the desktop environment:

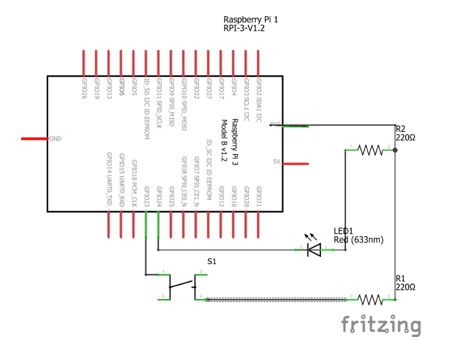
1. Click the icon in the upper left corner to open the start menu.
2. In the menu, select shutdown.

With access to command prompt in the terminal or through SHH:

Enter sudo shutdown and sudo poweroff

Without access to the desktop or command prompt:

1. Connecting GPIO Pin 23 and 3.3V for six seconds triggers the graceful power shutdown.
2. To avoid shortcutting the pins, use a circuit containing a resistor.
3. Display the status of the systems by connecting the anode of a led through a protective resistor to Pin 1 and the cathode to Pin 24.

  
Raspberry Pi Pins

Result

Unplugging and reconnecting the power plug of the Raspberry Pi triggers a reboot.

Never unplug the power supply while the operating system is running. It can cause serious damage to the file system of the SD card and can severely harm the database system of the integration framework.

Make sure that you always gracefully shut down the system by using one of the above methods before unplugging the power supply or draining a buffered power supply to empty. A buffered power supply could signal a graceful shutdown via GPIO Pin 23 before its supplied voltage for the Raspberry Pi significantly drops below 5V.

## Uninstalling the Integration Framework

Procedure

1. Open a terminal or remotely connect to your system using SSH.
2. In the command prompt enter following command:

sudo dpkg –-remove b1i-iot-raspi

Result

The procedure removes the integration framework from your system and deletes all data.

# Service Discovery

After integration framework installation, the system offers two services through the network:

* The integration framework
* SSH allowing remote connections to the system to perform maintenance and configuration tasks in headless operation

The integration framework is available:

* Through HTTP by pointing a Web browser or other client programs to <http://raspberry:8080/B1iXcellerator/>
* Through HTTPS by pointing a Web browser or other client programs to <https://raspberry:8443/B1iXcellerator/>

raspberry is the host name assigned to the device by default. If you changed the host name, replace raspberry with the term you chose.

Especially in headless operation, there can be situations, in which the assigned host name is not known. For more information, refer to Configuring the Host Name section

To handle such situations and to allow automatic service discovery, the integration framework uses zero-configuration networking (zeroconf). For more information, refer to https://en.wikipedia.org/wiki/Zero-configuration\_networking. The integration framework broadcasts its services using zeroconf as Integration framework on <hostname>.

Although zeroconf is primarily designed for direct machine to machine configuration, there are several browser programs available that allow gathering information about what services are available on the network.

Find a list of browser tools in the Software Requirements section of this guide under Service Discovery Tools.

To integrate automatic configuration of services provided by the integration framework, there are also several client libraries available for Java, C, C#, python and other languages.

Using the function, it is easy to integrate headless IoT devices running integration framework into a Service-Oriented or a Microservice Architecture.

# Network Security

## Securing Access to Integration Framework

### Enabling HTTPS

To secure communication between the integration framework and a connected client application, HTTPS respectively SSL is used. The integration framework on Raspberry Pi runs inside the Apache Tomcat Web container. To encapsulate the communication with the integration framework, the crypto capabilities of Tomcat and Java are used. The following sections describe how to ensure secure communication for the integration framework.

#### Some Background Information about Secure Sockets Layer (SSL)

HTTP using SSL is called HTTPS. The protocol provides the following functions to secure communication over untrusted networks.

* Secure encoding by cryptographic algorithms
* Secure server identification
* Secure client identification

The guide focuses on the first point. It is the most important point and must be in place. Once secure communication is set up, it is possible to exchange data between server and client applications without anyone being able to easily read the content of the communication while it passes the wire.

Nevertheless, there are still several ways for a potential attacker to compromise this communication if the communication does not use client and server-side authentication. This is beyond the scope of this guide. You can find more information about server and client-side authentication on the internet and in printed media.

Please assess, if the potential thread of being attacked justifies the increased effort when using identification mechanisms as well as encryption. As a rule of thumb, it is valid to say that the less a network can be trusted and the more open it is, the more it is worth to take extra steps to completely secure the communication. Communication over the internet should always be considered as maximum untrustworthy.

To initiate encrypted communication between an HTTPS client and a server, the server requires a key pair consisting of a public and a private key. As the name implies, the private part of the key pair must always be kept away from anyone but the server. The server must be able to access the private key. The public part is automatically exchanged with connecting client applications, such as browsers.

Usually the key pair is bundled with a so-called certificate. With the public part of the key pair and a valid key chain, the certificate can be used to identify a participant of the HTTPS communication. However, the terms key chain and certificate are relevant for secure server and client identification. This is not the focus of the guide.

For Java applications, such as the integration framework inside Apache Tomcat, the data objects (key pair and certificate) are stored with a keystore-file . The server uses the keystore-file to initiate the encryption of the communication with any connecting client. To encrypt the communication for the integration framework, perform the following tasks:

* Creating the keystore-file
* Configuring Tomcat to use the keystore-file to encrypt communication.

#### Configuring Tomcat to Use HTTPS

Procedure

1. To create a keystore-file, logon to your Raspberry Pi running Raspbian that contains the installation of the integration framework.
2. Open a terminal and do the following:

* Enter cd /etc/tomcat8
* Enter sudo keytool -genkey -alias tomcat -keyalg RSA -keystore ./keystore
* Answer some system questions. The answers are used to create the meta information of new keystore.
* Enter a password, press enter and confirm the password.
* Remember the password for later.
* When a second password is requested, press Enter.
* Enter sudo chown root:tomcat8 keystore
* Enter sudo chmod 640 keystore

The new keystore is owned by the root user and the tomcat8 group. They have read access.

* Enter sudo cp server.xml server.xml.bak
* Enter sudo nano server.xml
* Find the XML tag starting with “<Connector port="8080" protocol="HTTP/1.1"”.
* In a new empty line after the closing bracket of the tag insert the following:

<!-—Business Data Integrator via SSL HTTP/1.1 on port 443 -->

<Connector

protocol="org.apache.coyote.http11.Http11NioProtocol"

port="443" maxThreads="200"

scheme="https" secure="true" SSLEnabled="true"

keystoreFile="/etc/tomcat8/keystore" keystorePass="YOUR PASSWORD"

clientAuth="false" sslProtocol="TLS"/>

* Replace “YOUR PASSWORD” with the password that you created for the keystore file.
* Enter Ctrl-x followed by y, and press ENTER to leave nano by saving the file.
* Enter sudo service tomcat8 restart

Result

You can connect to the integration framework using [https://hostname](https://hostname:8443).

Replace hostname with the Domain Name System (DNS) host name of your Raspberry Pi, either the IP address or localhost if you are connecting from the Raspberry Pi.

Your browser displays a warning about the unsecure connection, because the browser cannot validate the certificate created by issuing the keytool command. This is normal for self-signed certificates. Keep this in mind when connecting to the integration framework with clients. Some clients may refuse to connect to servers offering such self-signed certificates. If you use a self-signed certificate, all clients must be configured not to use host name verification during SSL handshake. Otherwise they reject to connect to the server.

There are several good sources of information available on the internet about how to generate a keystore with an official certificate that browsers and other clients can verify and accept by default. Find further information by searching for Letsancrypt.org and java keystore.

### Disabling HTTP

Once the HTTPS connection is established, we recommend disabling the HTTP support to no longer allow unencrypted access to the integration framework.

Procedure

1. Enter the following statements:

* cd /etc/tomcat8
* sudo cp server.xml server.xml.http
* sudo nano server.xml

1. Find the following tag and comment the tag out by applying valid XML-style comment markers:

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

URIEncoding="UTF-8"

redirectPort="8443" />

**<!--**

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

URIEncoding="UTF-8"

redirectPort="8443" />

**-->**

1. Enter Ctrl-x followed by y and press ENTER to leave nano by saving the file.
2. Enter sudo service tomcat8 restart

## Remote Access Through Secure Shell (SSH)

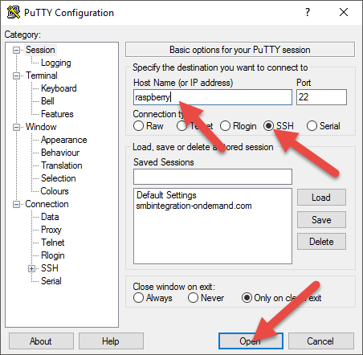
During installation of the integration framework, the access was enabled to the appliance using the SSH protocol. In headless operation, where no display is attached to the system, this is the only way to get administrative access to the operating system and the Web container / Tomcat.

Procedure

1. To login via SSH from a work station running Linux or the Mac operating system, open a terminal and enter ssh pi@hostname

Replace hostname with the DNS host name or IP address of the Raspberry Pi.

1. On Windows, download and install Putty. Putty is a free SSH client for Windows systems that provides easy access to Unix-based systems using SSH. You can download Putty here: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Run Putty and in the Host Name (or IP address) field, enter your Raspberry Pi, select the SSH connection type and click Open.

  
Putty Configuration

1. If you have not yet changed the default password for the pi user, logon as the pi user with the raspberry password.
2. The password is widely known. Change the password immediately after logon and enter passwd
3. The system requests the current password, the new password and a confirmation for the new password.

Result

The system has secure remote access enabled via SSH.

If you no longer require this access, you can disable SSH on the Raspberry Pi any time by issuing the following command in a terminal:

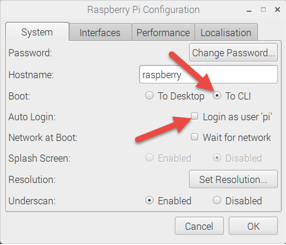
sudo systemctl disable ssh

Only disable the access if you have an alternative, reliable and secure way of accessing the system.

## Securing Console Access

The chosen Raspbian version boots into the graphical desktop environment and automatically logs on the pi user by default. The pi user has generous privileges. The user can, for example, run programs with super user rights by using the sudo command without supplying a password. Anyone who has access to the physical console (connected monitor and keyboard) can run any program with super user rights. For a production system, this is not acceptable and the console access must be secured by a login procedure.

Disabling the automatic login procedure and disabling booting into the graphical desktop, you can additionally save some system resources. This is important for a system with limited resources such as the Raspberry Pi.

  
Raspberry Pi Configuration

Procedure

1. On the Raspberry Pi, open the Start menu.
2. Choose Preferences and run Raspberry Pi Configuration”.
3. In the user interface, click the System tab, in the Boot field, select the To CLI” option and in the Auto Login field, deselect the Login as user ‘pi’ option.

When you reboot the system, it boots into a terminal login.

1. Logon with the pi user and password. If you require the graphical desktop after logon, enter startx.
2. Never leave the console unattended with an active login. If you are in the graphical desktop, leave it by dropping to the command line again, then enter exit.

# Rollout to Further Devices

Once the integration framework is installed and the operating system is configured by following the steps in this guide, you can roll out the installation to further devices. The most efficient way for rollout is to replicate the micro SD Card with the installed Raspbian and integration framework. The following sections describe the tasks.

## Backing Up and Restoring the Installation

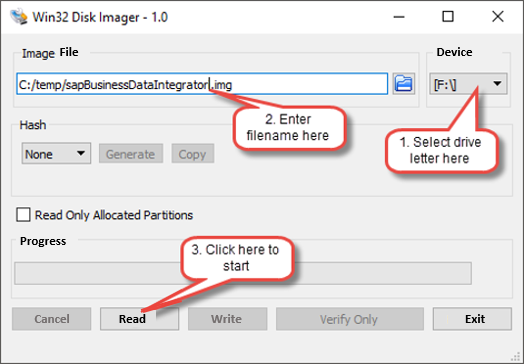
### Backing Up the Installation Using Windows

Procedure

1. Download and install Win32 Disk Imager on your Windows PC.
2. Power off the Raspberry Pi using one of the methods described in the guide.

Do not just disconnect the power supply.

1. Remove the micro SD Card from the Raspberry Pi and connect it to your Windows PC.
2. Start Win32 Disk Imager.
3. If Windows associates, for example, drive F to the SD card, select the F: drive.
4. Enter a file name for the image written to the local disk drive and click Read.
5. Wait until the process is completed.

   
Win32 Disk Imager

Result

On the internet, several reports are available stating that the procedure does not work reliably depending on the Win32 Disk Imager and the Windows versions. This is not a matter of the integration framework nor SAP. Try again with a different Windows version or try to run Win32DiskImager as administrator. If it still does not work, consider using Linux instead.

### Backing Up the Installation Using Linux

If you do not have a Linux PC available, boot your Raspberry Pi from a different SD card than the one you want to back up.

Prerequisites

Before inserting the SD card into the reader on your Linux PC or Raspberry Pi, make sure you have sufficient free disk space available to store the image. The image becomes much smaller than the size of the original SD card but you should still expect between a quarter and half the size of the original SD card.

Procedure

1. Open a terminal and run the following command to find out, which devices are currently available:

df -h

The system returns something like:

Filesystem Size Used Avail Use% Mounted on

udev 3,0G 12K 3,0G 1% /dev

tmpfs 603M 1,8M 602M 1% /run

/dev/sda1 28G 20G 6,3G 77% /

none 4,0K 0 4,0K 0% /sys/fs/cgroup

none 5,0M 0 5,0M 0% /run/lock

none 3,0G 676K 3,0G 1% /run/shm

none 100M 40K 100M 1% /run/user

1. Insert the SD card into a card reader and connect it to your Linux PC or Raspberry Pi and run the df -h command to display the available disk space.

The system returns something like:

Filesystem Size Used Avail Use% Mounted on

udev 3,0G 12K 3,0G 1% /dev

tmpfs 603M 1,8M 602M 1% /run

/dev/sda1 28G 20G 6,3G 77% /

none 4,0K 0 4,0K 0% /sys/fs/cgroup

none 5,0M 0 5,0M 0% /run/lock

none 3,0G 676K 3,0G 1% /run/shm

none 100M 40K 100M 1% /run/user  
**/dev/sda5 100M 50M 50% /media/boot  
/dev/sda6 28G 14G 50% /media/b5afbc64-ced4-4fb7-83fe-f51640219258**

The new device that was not available before is your SD card.

1. Before you continue, enter the following to unmount any mounted partitions

umount /dev/sda5

Replace /dev/sda5 with the device listed for you as first partition of your SD Card and repeat the step for all other listed partitions of the SD card.

The left column contains the device name of your SD card, for example, /dev/mmcblk0p1 or /dev/sdb1. The last part is the partition number.

1. Since you want to back up the complete SD card, re**move** the last part of the device name, for example, /dev/mmcblk0 or /dev/sdb to have the disk available for reading.

sudo su

dd if=/dev/sdb | pv | gzip -9 > ~/sapBusinessDataIntegrator\_backup.img.gz

Replace /dev/sdb with the correct device name.

1. Wait until the process is completed.
2. Enterexit

Result

Depending on the size of your SD card and the speed of your card reader and system, this can take up to one hour or longer. The procedure leaves you with a compressed backup of the SD card that can be deployed to any number of SD cards of at least the same size.

### Restoring the Backup Using Windows

If the backup procedure using Windows and Win32DiskImager works, follow the steps described in the Preparing the Installation section of this guide.

Proceed as if the image you created was the already unzipped version from the internet.

### Restoring the Backup Using Linux

You can restore the backup created on Linux to a different SD card. Follow the steps described in the Preparing the Installation section of this guide.

The only prerequisite is, that the backup must be unzipped before. Depending on the system use 7-zip (in Windows), gzip -d (in Linux) or The Unarchiver (in Mac).

Under Linux, enter:

sudo su

gzip -d -c /path/to/image | pv | dd of=/dev/[device] conv=fsync

exit

For details about how to determine the correct device, refer to the Preparing the Installation section of this guide.

## Using SD Cards on Further Devices

Following the procedures above, you obtain a second bootable SD card. You can use the card to instantly run the integration framework on a second Raspberry Pi. Use the backed-up image to create any number of SD cards containing the integration framework.

Depending on how you configure the host name in your environment, repeat the client-side host name configuration for each new device you are setting up to keep host names in your network unique. If you use the server-side host name management, no further configuration is required on each cloned device.

Keep in mind that further configuration steps may be required on your network DHCP server. However, such steps are out of scope for the configuration described in this guide. Ask your IT department for further assistance.

|  |
| --- |
|  |
| www.sap.com/contactsap |
| .  © 2019 SAP SE or an SAP affiliate company. All rights reserved. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary. These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty. SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Please see http://www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices. |

SAPLogo.gif