Administration Guide | PUBLIC
Document Version: 1.2 – 2020-06-30

How to Deploy SAP Business One with Browser Access

THE BEST RUN **SAP**

Content

1 Introduction

With the Browser Access service, you can work with SAP Business One in a web browser in the office or from outside the office (your corporate network).

This guide provides instructions on how to make proper preparations and enable browser access for SAP Business One and SAP Business One, version for SAP HANA.

Compared with desktop access, browser access has some behavioral changes and a few limitations. For more information, see SAP Notes 2194215 and 2194233 .

> ⚠ Caution
>
> This guide refers to various third-party solutions (for example, Internet Information Services) on which the Browser Access service is dependent. These solutions may be changed without notification. Please always refer to the documentation of the respective solution provider to ensure a successful deployment of your SAP Business One system.

2 Prepare certificates

Before installing and configuring the Browser Access service, you must make some necessary preparations.

2.1 Choose a method to handle external requests

As the Browser Access service enables you to access SAP Business One from external networks, it is essential that external requests can be sent properly to internal services.

To handle external requests, we recommend deploying a reverse proxy rather than using NAT/PAT (Network Address Translation/Port Address Translation). Compared with NAT/PTA, the reverse proxy is more flexible and can filter incoming requests.

> **i Note**
>
> Regardless of the method, the SAP HANA services are not exposed to external networks; only the SAP Business One services are exposed. However, you must never directly assign an external IP address to any server with SAP Business One components installed.
>
> To improve your landscape security, you can install your SAP HANA database on a machine other than the one holding SAP Business One components.

Reverse Proxy

A reverse proxy works as an interchange between internal SAP Business One services and external clients. All the external clients send requests to the reverse proxy and the reverse proxy forwards their requests to the internal SAP Business One services.

To use a reverse proxy to handle incoming external requests, you need to:

1. Import a trusted root certificate for all SAP Business One services during the installation.
   The certificate can be issued by a third-party certification authority (CA) or a local enterprise CA.
   For instructions on setting up a local certification authority to issue internal certificates, see Microsoft documentation ↗ .
   All the components (including the reverse proxy) in the SAP Business One landscape should trust the root CA which issued the internal certificate for all SAP Business One services.
2. Purchase a certificate from a third-party public CA and import the certificate to the reverse proxy server. Note that this certificate must be different from the first certificate. While the first certificate allows the reverse proxy to trust the CA and, in turn, the SAP Business One services, the second certificate allows the reverse proxy to be trusted by external clients.
   All clients from external networks naturally trust the public CA and, in turn, the reverse proxy. A chain of trust is thus established from the internal SAP Business One services, to the reverse proxy, and to the external clients.

NAT/PAT

If you prefer NAT/PAT to a reverse proxy, be aware that all clients connect directly to the internal SAP Business One services, external clients and internal clients alike.

To use NAT/PAT, you must purchase a certificate from a third-party CA and import the certificate to all machines installed with SAP Business One services. All the clients must trust this third-party public CA.

2.2   Prepare certificates for HTTPS services

Any service listening on HTTPS needs a valid PKCS12 (.pfx) certificate to function properly, especially for external access using the Browser Access service.

How you prepare PKCS12 (.pfx) certificates depends on how you plan to expose your SAP Business One services (including the Browser Access service) to the Internet (external networks).

When preparing the certificates, pay attention to the following points:

- Ensure the **entire certificate chain** is included in the certificates.
- To streamline certificate management, set up a wildcard DNS (*.DomainName).
- The public key must be a 2048-bit RSA key.
  Note that JAVA does not support 4096-bit RSA keys and 1024 bits are no longer secure.
  Alternatively, you can use 256-bit ECDH keys, but RSA-2048 is recommended.
- The signature hash algorithm must be at least SHA-2 (for example, SHA256).

Reverse proxy (recommended)

For a reverse proxy, prepare an internal certificate for the internal domain and import the internal root certificate to all Windows servers. Then purchase for the external domain another external certificate issued by a third-party CA and import this certificate to the reverse proxy server.

NAT/PAT

If you use NAT/PAT to handle external client requests, purchase a certificate issued by a third-party CA for both internal and external domains.

If the internal and external domains have different names, this certificate should list both domains in the *Subject Alternative Name* field. However, we recommend that you use the same domain name for both internal and external domains.

3 Install and configure Browser Access service for SAP Business One

> ⚠ Caution
>
> As the Browser Access service can consume quite a lot of system resources, you must ensure the Browser Access server has been properly sized. To do so, use the system requirement sizing tool for SAP Business One terminal servers and Browser Access🐷.
>
> For SAP Business One, be sure **not** to install the Browser Access service on the Microsoft SQL Server as both are resource-consuming.

3.1 Install the Browser Access service

Prerequisites

You have installed the System Landscape Directory (SLD). In addition, during the installation, you have imported the certificate that you have prepared for the internal domain; for SAP Business One, version for SAP HANA, you have also specified the FQDN (fully-qualified domain name) of the server.

Context

For detailed instructions on installing SAP Business One, please refer to the Administrator's Guide (Microsoft SQL version or SAP HANA version). The following procedure illustrates how to install the Browser Access service.

Procedure

1. Navigate to the root folder of the product package and run the `setup.exe` file (right-click and choose *Run as administrator*).
2. In the welcome window, select your setup language and choose *Next*.
3. In the *Setup Type* window, select *Perform Setup* and choose *Next*.
4. In the *Setup Configuration* window, select *New Configuration* and choose *Next*.
5. In the *System Landscape Directory* window, do the following:
   1. Select *Connect to Remote System Landscape Directory*.

> ⚠ Caution
>
> Select this option even if you are installing the browser access service on the SLD server.

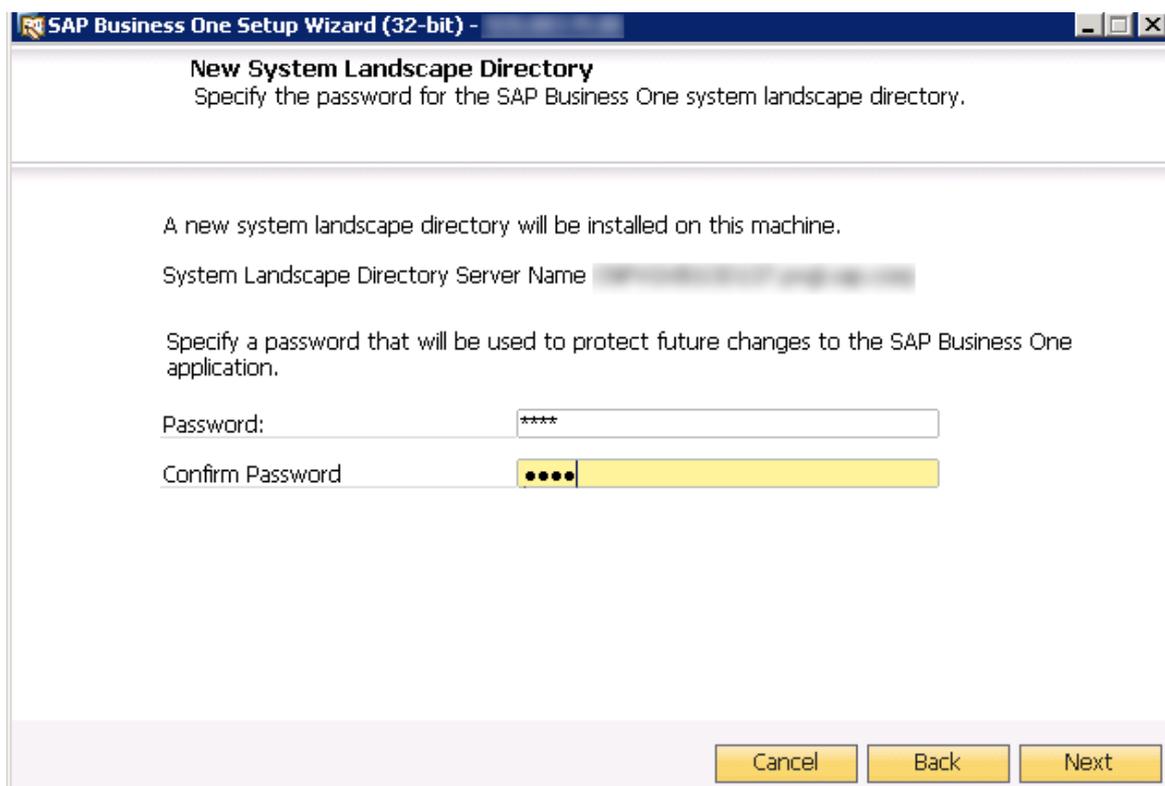2. Enter the FQDN of the SLD server.

   For example: **https://SLDServer.abc.com**
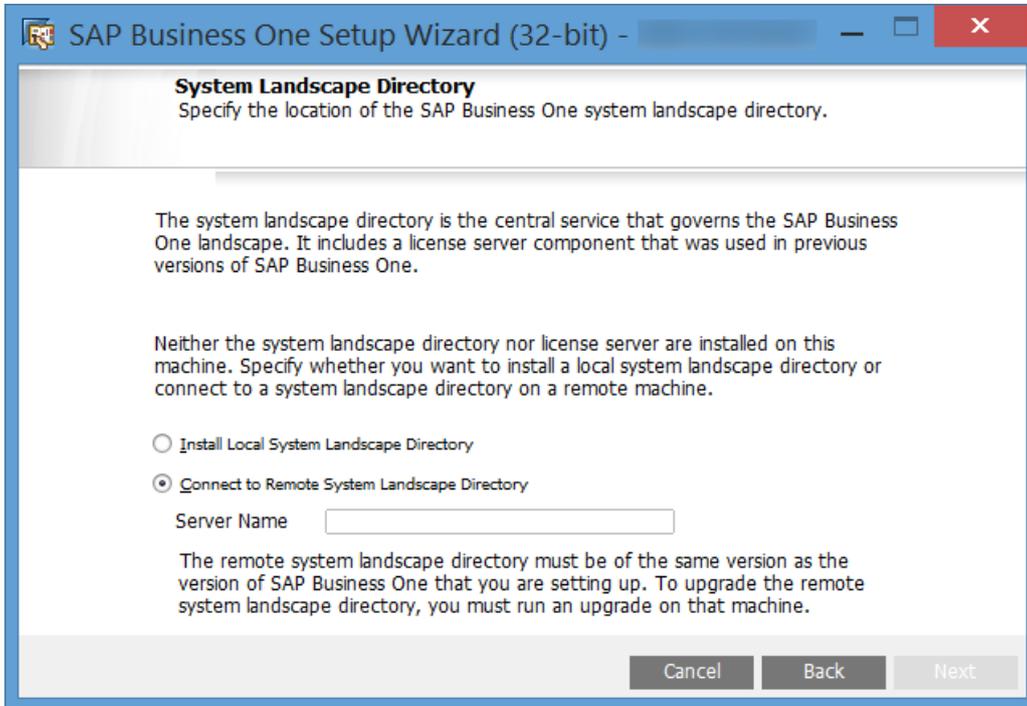
3. Choose *Next*.

6. In the *Site User Logon* window, enter the password for the site super user `B1SiteUser`. This site user was created during the installation of the SLD.

7. In the *Database Server Connection* window, enter the database server information as follows:

   1. Specify the database server type.

   2. In the *Server Name* field, enter the hostname or the IP address of the database server.

   3. Choose *Next*.
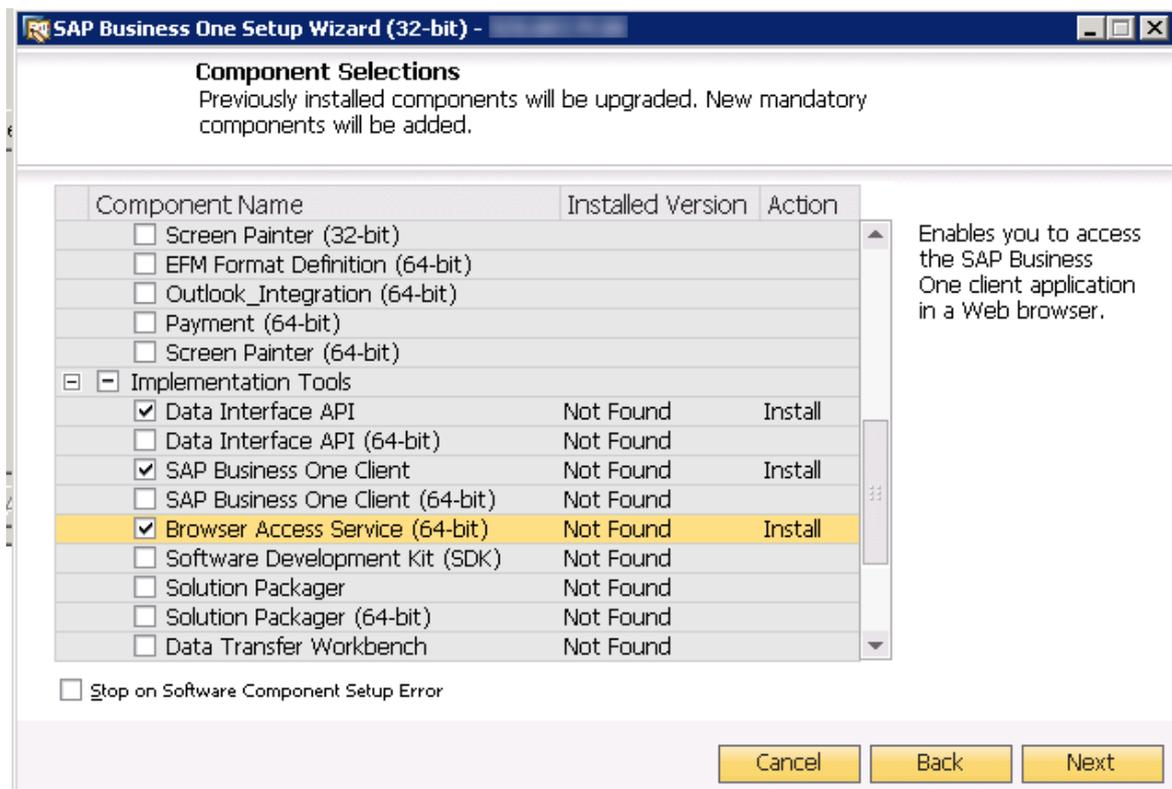
8. In the *Component Selections* window, select the following components and choose *Next*:

- Browser Access service
- SAP Business One client application (32-bit or 64-bit)

Note that the Browser Access service can be selected only if you have selected (or installed) either version of SAP Business One client.

9. In the *Parameters for Browser Access Service* window, specify the following information for the browser access service:

- Internal access URL: For the internal access URL of the service, specify:
    - The network address (hostname, IP address, or FQDN) of the machine
      For example: **`https://BrowserAccess.abc.com`**
    - The port for the service (default: `8100`)
- Security certificate: Import the certificate that you have prepared for the internal domain and enter the certificate password.
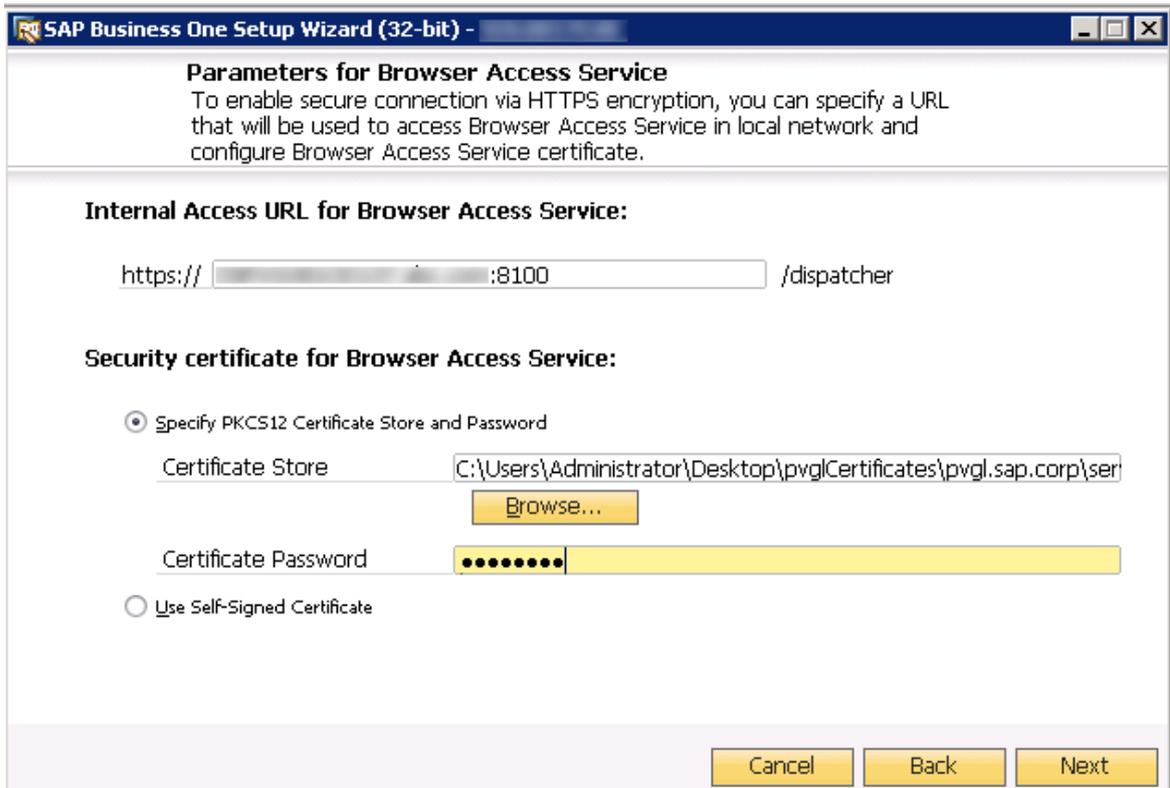
10. In the next *Parameters for Browser Access Service* window, select the version of SAP Business One to be used by the browser access service.

11. In the *Review Settings* window, review your settings and proceed as follows:

   - To continue, choose *Next*.
   - To change the settings, choose *Back*.

12. In the *Setup Summary* window, choose *Next*.

13. In the *Setup Status* window, wait for the system to perform the required actions.

14. In the *Complete* window, choose *Finish*.

Next Steps

The Browser Access service is registered as a Windows service SAP Business One Browser Access Gatekeeper. After installation, check if this Windows service runs under the `Local System` account.
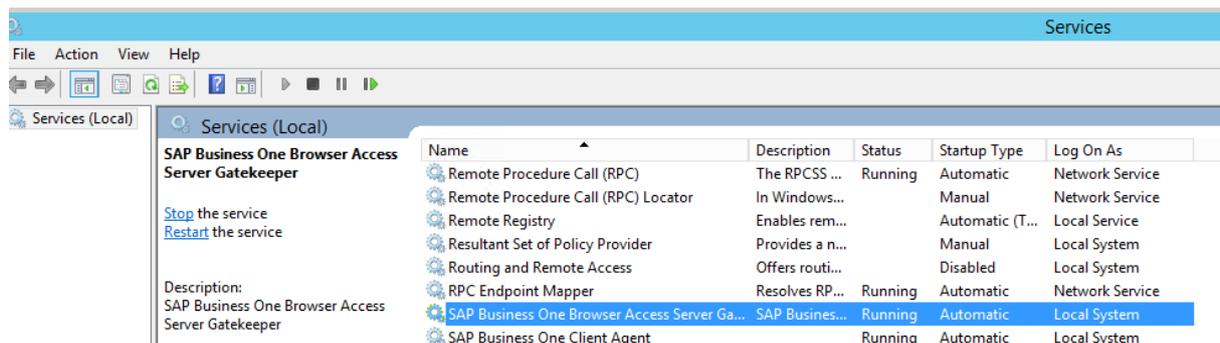
3.2   Configure the Browser Access service

Prerequisites

Ensure that the date and time on the Browser Access server is synchronized with the database server.

Context

The Browser Access service enables remote access to the SAP Business One client in a Web browser. The Windows service name is `SAP Business One Browser Access Server Gatekeeper`.

Procedure

1. In a Web browser, log on to the System Landscape Directory control center using this URL: `https://<Hostname>:<Port>/ControlCenter`.
2. On the *Services* tab, select the *Browser Access* entry for the particular Browser Access server and then choose *Edit*.
3. In the *Edit Service* window, edit the following information:
   - *Service URL*: Edit the URL used to access the service.
     For example, you may want to use the IP address instead of the hostname. Or the hostname, IP address, or the port has changed and you must update the service URL to reflect the changes.
   - *Initial Processes*: Specify the initial number of SAP Business One client processes that the Browser Access service hosts.
   - *Maximum Processes*: Specify the maximum number of SAP Business One client processes that the Browser Access service can host.
   - *Idle Processes*: Specify the number of standby SAP Business One client processes. When a new SAP Business One user attempts to log on, an idle process is ready for use.
   - *Description*: Enter a description for this Browser Access server.

     > **⁙ Example**
     >
     > Specify the following:
     > - Initial processes: 20
     > - Maximum processes: 100
     > - Idle processes: 2
     >
     > Twenty (20) SAP Business One client processes are constantly running on the Browser Access server and allow 20 SAP Business One users to access the SAP Business One client in a Web browser at the same time.

12   PUBLIC

How to Deploy SAP Business One with Browser Access
Install and configure Browser Access service for SAP Business One

> When the 19th SAP Business One user logs on, one (1) more SAP Business One process is started to ensure that two (2) idle processes are always running in the background.
>
> If more SAP Business One users attempt to access the SAP Business One client in a Web browser, more idle processes are started, but at most, 100 users are allowed for concurrent access.

4. To save the changes, choose *OK*.
5. To apply the changes immediately, on the Browser Access server, restart the SAP Business One Browser Access Server Gatekeeper service.

3.3 Map between internal and external addresses

3.3.1 Prepare external addresses

To expose your SAP Business One services to the Internet (external networks), you must prepare external addresses for relevant components.

> **i Note**
>
> The Service Layer is for internal component calls only and you do not need to expose it to the Internet.

Please pay attention to the following points:

- The external address and the internal address of each component must be different; otherwise, the external networks cannot be distinguished from the internal network, making browser access impossible.
- Only one set of external addresses is supported. Communication via the DNS alias of an external address will lead to error.

Reverse Proxy Mode

If you intend to handle client requests using a reverse proxy, we recommend that you use different domain names for internal and external domains. For example, the internal domain is **abc.corp** and the external domain is **def.com**.

Prepare the external addresses as follows:

- Prepare one external address for (hostname or IP address) for each of these components:
  - System Landscape Directory (SLD)
  - Browser Access service
  - [SAP Business One, version for SAP HANA only] Analytics service
  - integration framework (if you use the SAP Business One mobile solution)
  - Mobile service
  - Web Client for SAP Business One

- The internal address of each component must match the common name of the certificate for the internal domain; the external address of each component must match the common name of the purchased certificate for the external domain.

> **⁂ Example**
>
> The internal URLs of the components are as follows:
> - System Landscape Directory: `https://SLDInternalAddress.abc.corp:Port`
> - Browser Access service: `https://BASInternalAddress.abc.corp:Port/dispatcher`
> - Analytics service: `https://B1AInternalAddress.abc.corp:Port/Enablement`
> - Integration framework: `https://B1iInternalAddress.abc.corp:Port/B1iXcellerator`
> - Mobile service: `https://MobileServiceInternalAddress.abc.corp:Port/mobileservice`
> - Web Clients for SAP Business One: `https://WebClientsInternalAddress.abc.corp:Port`
>
> The external URLs are as follows:
> - System Landscape Directory: `https://SLDExternalAddress.def.com:Port`
> - Browser Access service: `https://BASExternalAddress.def.com:Port/dispatcher`
> - Analytics service: `https://B1AExternalAddress.def.com:Port/Enablement`
> - Integration framework: `https://B1iExternalAddress.def.com:Port/B1iXcellerator`
> - Mobile service: `https://MobileServiceExternalAddress.def.com:Port/mobileservice`
> - Web Clients for SAP Business One: `https://WebClientsExternalAddress.def.com:Port`

NAT/PAT

If you intend to handle client requests using NAT/PAT, we recommend that you use the same domain name across internal and external networks. For example, both the internal and external domains are **abc.com**.

Prepare the external addresses as follows:

- Prepare one external address (hostname or IP address) for each of these components:
  - System Landscape Directory (SLD)
  - Browser Access service
  - [SAP Business One, version for SAP HANA only] Analytics service
  - Integration framework (if you use the SAP Business One mobile solution)
  - Mobile service
  - Web Client for SAP Business One
- The combination of external address and port must be different for these components. In other words, if two components have the same external address, the ports they listen on must be different; and vice versa.
- The internal address and external address of each component must match the common name of the certificate purchased for both the internal and external domains.

> **⁂ Example**
>
> The internal URLs of the components are as follows:
> - System Landscape Directory: `https://SLDInternalAddress.abc.com:Port`

- Browser Access service: `https://BASInternalAddress.abc.com:Port/dispatcher`
- Analytics service: `https://B1AInternalAddress.abc.com:Port/Enablement`
- Integration framework: `https://B1iInternalAddress.abc.com:Port/B1iXcellerator`
- Mobile service: `https://MobileServiceInternalAddress.abc.corp:Port/mobileservice`
- Web Client for SAP Business One: `https://WebClientsInternalAddress.abc.corp:Port`

The external URLs are as follows:
- System Landscape Directory: `https://SLDExternalAddress.abc.com:Port`
- Browser Access service: `https://BASExternalAddress.abc.com:Port/dispatcher`
- Analytics service: `https://B1AExternalAddress.abc.com:Port/Enablement`
- Integration framework: `https://B1iExternalAddress.abc.com:Port/B1iXcellerator`
- Mobile service: `https://MobileServiceExternalAddress.abc.com:Port/mobileservice`
- Web Client for SAP Business One: `https://WebClientsExternalAddress.abc.com:Port`

3.3.2 Register external address mapping

Context

You must register in the System Landscape Directory the mapping between the external address of each of the following components and its internal address:

- System Landscape Directory (SLD)
- Browser Access service
- [SAP Business One, version for SAP HANA only] Analytics service
- Mobile service (if you are using SAP Business One Sales app)
- Web Client for SAP Business One

Note that you do not need to register the mapping for the integration framework.
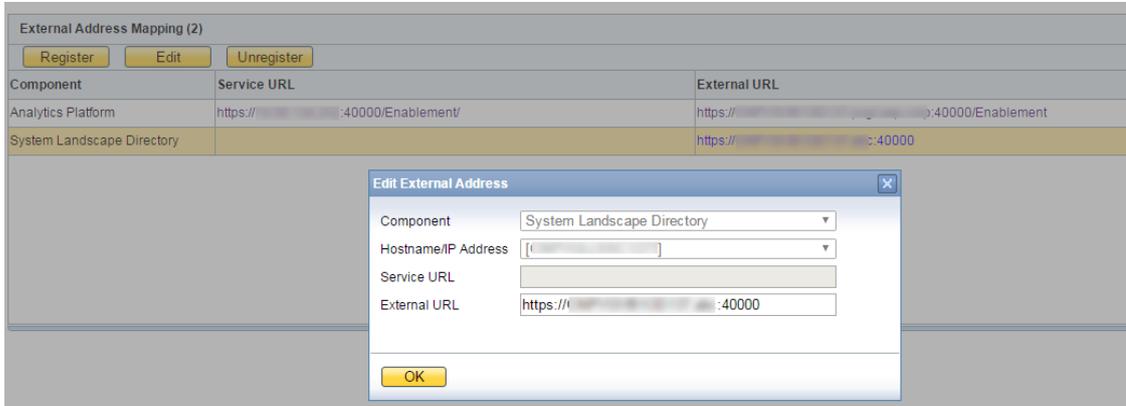
Procedure

1. In a Web browser, log on to the system landscape directory using this URL:
   - Microsoft SQL version: `https://<Hostname>:<Port+10>/ControlCenter`
   - SAP HANA version: `https://<Hostname>:<Port>/ControlCenter`
2. On the *External Address Mapping* tab, choose *Register*.
3. In the *Register External Address* window, specify the following information:
   1. Component
   2. Hostname or IP address of the machine on which the component is installed
   3. External URL
      The external access URL must have the format **`<protocol>://<Path>:<Port>`**.

> **⁂ Example**
>
> http://<IP address>:8080

External Address Mapping (2)		
Register Edit Unregister		
Component	**Service URL**	**External URL**
Analytics Platform	https:// :40000/Enablement/	https:// :40000/Enablement
System Landscape Directory		https:// :40000

Edit External Address

Component	System Landscape Directory ▼
Hostname/IP Address	[ ] ▼
Service URL	
External URL	https:// :40000

OK

The *Hostname/IP Address* field for the SLD may display the hostname rather than the FQDN of the SLD server, or it may be empty; either is fine and can be ignored.

4. Choose *OK*.

Next Steps

After finishing mapping the addresses for all required components, you must restart the services on the machines on which they're installed.

For example, if you have registered the external address mapping for a Browser Access server, you must restart the SAP Business One Browser Access Server Gatekeeper service.

Note that the restart of SAP Business One Browser Access Server Gatekeeper service may take from 5 to 10 minutes.

> **i Note**
>
> For the Web Client, you need to restart the service by performing the following steps:
>
> 1. Log on to the Linux server as root.
> 2. In a command line terminal, navigate to the directory `…/user/sap/SAPBusinessOne/WebClient` where the `startup.sh` script is located.
> 3. Restart the program from the command line by entering the following command:
>   **`sh startup.sh restart`**
>   The restart process begins.
>
> Web Client does not start automatically after a Microsoft Windows server restarts. You need to manually restart the Web Client. For more information, see SAP Note 2875511 .

4 Access SAP Business One

Prerequisites

- You have ensured that you can log on to the SAP Business One client installed on the Browser Access server.
- You are using one of the following Web browsers:
  - Mozilla Firefox
  - Google Chrome
  - Microsoft Edge
    Ensure that you have enabled *Automatically Detect Intranet Network*.
  - Apple Safari (Mac and IPad)
    Ensure that you have enabled Adobe Flash Player. This is a prerequisite for Crystal dashboards.

Context

By default, no load balancing mechanism is applied. You can create a Web access portal and redirect requests to different Browser Access servers using a load balancing mechanism of your own choice, for example, round robin.
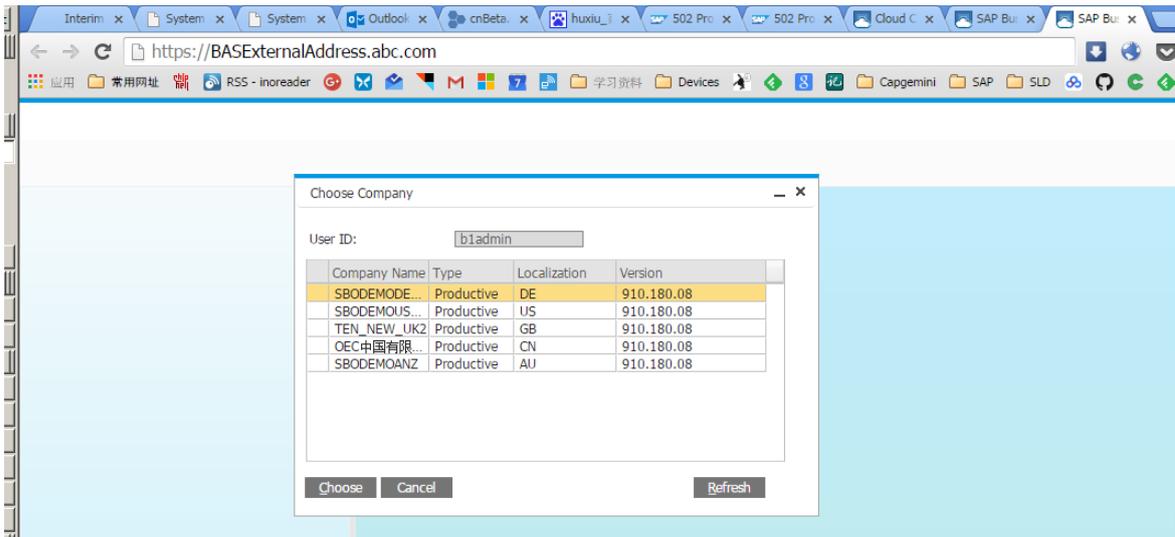
The following procedure illustrates how to access SAP Business One directly in a Web browser.

Procedure

1. In a Web browser, navigate to the external URL of the Browser Access service. For example: `https://BASExternalAddress.abc.com:Port/dispatcher`
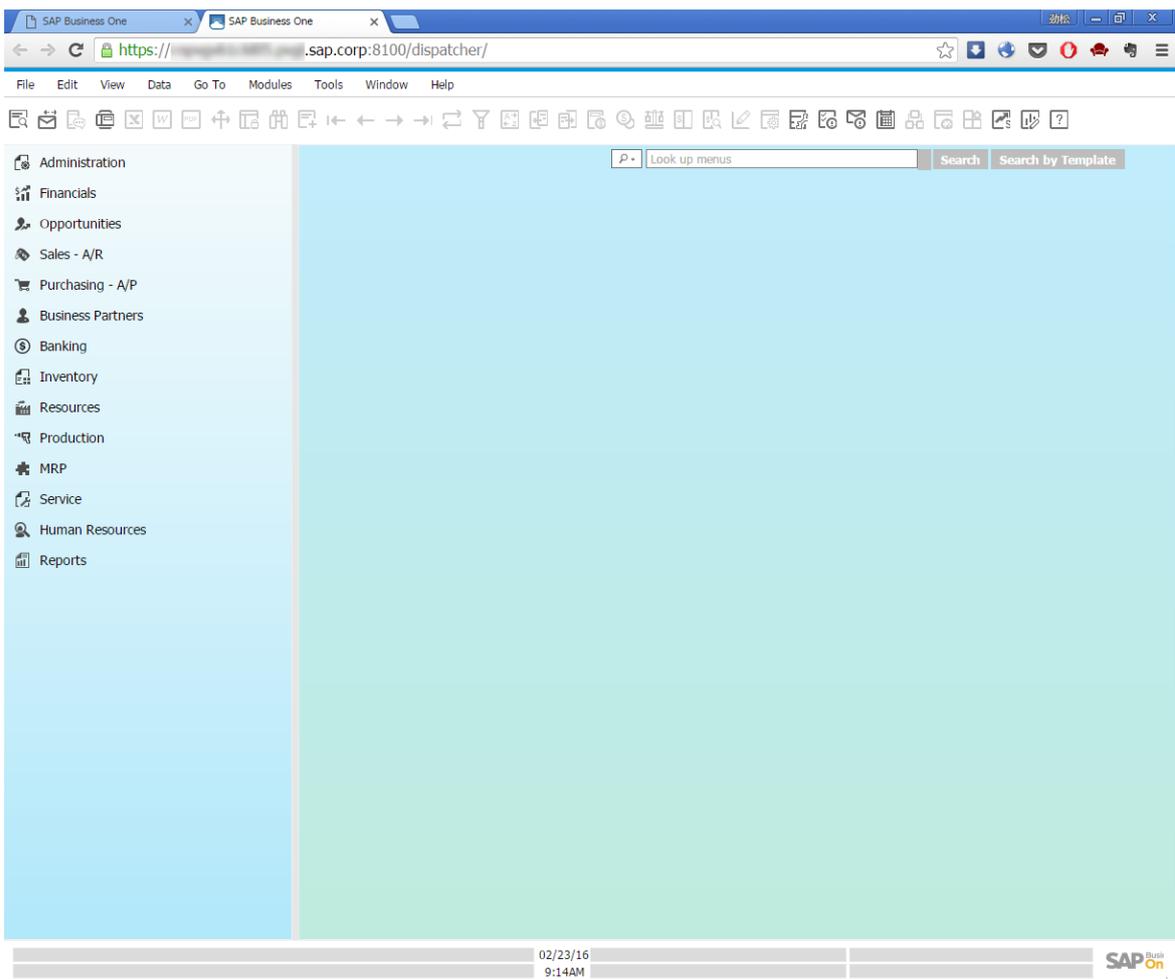
   If you are uncertain about it, you can check the external address mapping in the SLD.
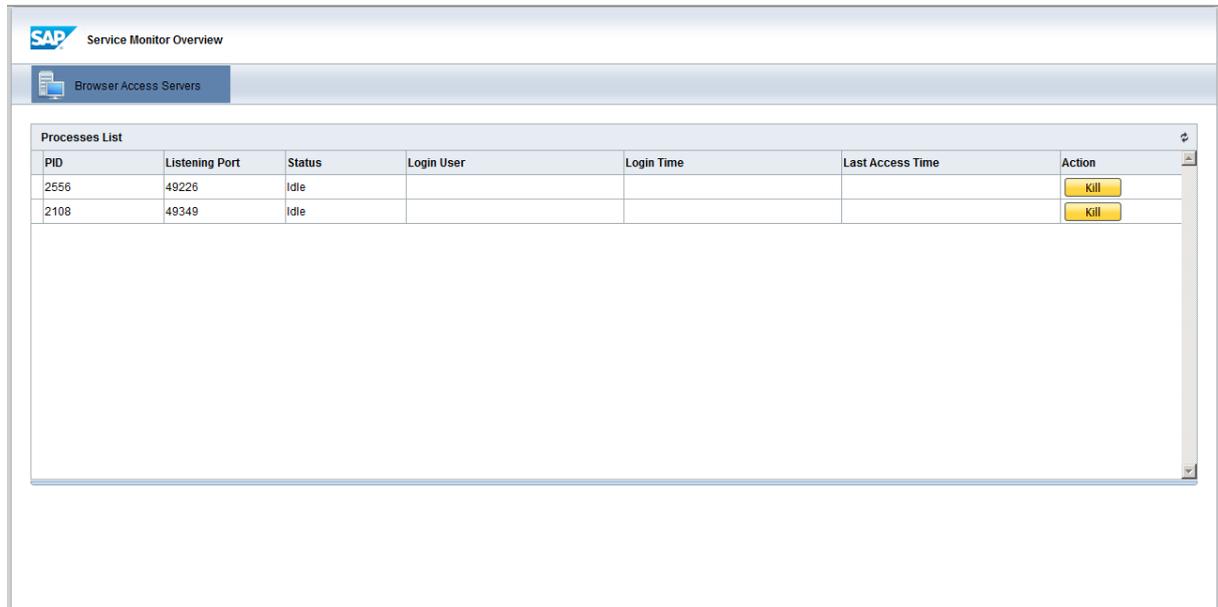
   The Browser Access page is opened.

2. Choose the company and log on.

   Now you can work with SAP Business One in your web browser.

5 Monitor Browser Access processes

As of release 9.2 PL02, you can monitor the Browser Access processes in a Web page using this URL:
`https://dispatcherHostname:port/dispatcher/serviceMonitor/`.

If a process hangs for a long time, you can kill it directly.

6 Logging

The log files for the browser access service are stored at `<Installation Folder>\SAP Business One BAS GateKeeper\tomcat\logs`.

If you need to troubleshoot problems, edit the file `<Installation Folder>\SAP Business One BAS GateKeeper\tomcat\webapps\dispatcher\WEB-INF\classes\logback.xml`, and change the logging level from the default `WARN` to `DEBUG`.

> i Note
>
> You must change the logging level back to the default value after the investigation.

7 Troubleshooting

7.1 Cannot use SAP Business One in a web browser

Symptom

You have configured the external address mapping for all relevant components (System Landscape Directory, Browser Access service, analytics service, integration framework). However, you still cannot access SAP Business One in a web browser.

Cause

After the configuration, you did not restart the relevant services.

Solution

Restart the relevant services after configuring the external address mapping.

Service	Microsoft SQL Version	SAP HANA Version
System Landscape Directory	Restart the Windows service with the *SAP Business One SLD Service* identifier.	Run this command on the Linux server: `/etc/init.d/ sapb1servertools restart`
Analytics service	/	
Browser Access service	Restart the Windows service with the *SAP Business One Browser Access Server Gatekeeper* identifier.	
Integration Framework	Restart the Windows service with the *SAP Business One Browser Access Server Gatekeeper* identifier.	

7.2 "Internal Error"

Symptom

Navigate to the external URL of a service (for example, the analytics service). An "Internal Error" message is displayed.

Cause

You did not configure the external address mapping for the System Landscape Directory.

Solution

In the System Landscape Directory, configure the external address mapping for the System Landscape Directory.

7.3 Fiori-style cockpit cannot be displayed

Symptom

You have logged onto SAP Business One but cannot use the Fiori-style cockpit. The Fiori-style cockpit is blank.

Cause 1

The analytics service doesn't have a valid certificate or you haven't accepted to trust the self-signed certificate.

Solution 1

Install the analytics service using a valid certificate.

If you have installed the analytics service using a self-signed certificate, open the external URL of the analytics service and accept to trust the certificate.

Cause 2

You have used different SLD addresses to install the Browser Access service and the analytics service. For example, you used the FQDN of the SLD server to install the Browser Access service and used the IP address of the SLD server to install the analytics service. Service single sign-on fails as a result.

Solution 2

1. To identify the SLD address used for installing the Browser Access service, open the external URL of the Browser Access service.
   You're redirected to the System Landscape Directory logon page. Check the URL, which contains the SLD address you're looking for.
2. To identify the SLD address used for installing the analytics service, open the external URL of the analytics service.
   You're redirected to the System Landscape Directory logon page. Check the URL, which contains the SLD address you're looking for.
3. If the two SLD addresses are different, reinstall the analytics service using the SLD address used for installing the Browser Access service.

Cause 3

The machine where you install the analytics service is blocked from external networks.

Solution 3

For SAP Business One 9.2 PL02 and lower, version for SAP HANA, after the configuration, make sure that the SLD **external** address can be reached by the Browser Access service and the analytics service from the **external** network.

To make the verification, on the Browser Access server or the analytics service machine, try connecting to `https://<SLDExternalAddress>:<Port>/sld/saml2/idp/metadata` in a Web browser. If the connection cannot be established, expose the Browser Access service and the analytics service to external networks.

For more information about this limitation, please refer to SAP Note 2299536 .

7.4 Fiori-style cockpit cannot be displayed in Google Chrome

Symptom

The Fiori-style cockpit cannot be displayed in Google Chrome but can be displayed in other supported web browsers (for example, Microsoft Internet Explorer).

Cause

Google Chrome version 45 and higher blocks cookies by default.

Solution

If you access SAP Business One in external networks, ensure that all SAP Business One components share the same second-level external domain; and likewise if you access SAP Business One in internal networks. For example, **ServerTools.example1.example.corp** and **B1A.example2.example.corp** are under the same second-level domain.

8 Appendix: Configure an nginx reverse proxy

Prerequisites

- You have predefined an external domain name for the SLD (System Landscape Directory) and other components. For example, ExternalAddress.def.com.
- You have obtained the `nginx_conf OP.zip` file (download it from here).

Procedure

1. From http://nginx.org/ ⬈ , download the nginx binary file according to your target operating system, and extract the binary file to a local folder.

   The recommended nginx version is 1.8.0 or higher.

2. Install nginx on a Windows server or a Linux server.

   Note that only version 9.2 PL03 and above support nginx installed on Linux servers. In addition, you must ensure that OpenSSL is enabled.

3. Copy to the nginx server some SLD files:
   - Microsoft SQL version: Copy the `ControlCenter` folder (located at `${SLDInstallationFolder}\tomcat\webapps\ControlCenter`) from the SLD server to the nginx server: `${nginx}\html\`.
   - SAP HANA version:
     1. On the nginx server, under the `${nginx}\html\` folder, create a folder named as `ControlCenter`.
     2. On the SLD server, go to `${SLDInstallationFolder}/ServerTools/SLD/webapps`, get the `SLDControlCenter.war` file.
     3. Copy and unzip the `SLDControlCenter.war` file to `${nginx}\html\ControlCenter`.

4. Prepare certificates:
   1. Generate the `server.cer` and `server.key` files from your PKCS12 (.pfx) file using the OpenSSL library.
   2. Copy both files to the `${nginx}/cert` folder.
      If the `cert` folder does not already exist, create it manually.

5. Copy the `nginx_conf OP.zip` file to the `${nginx}/conf` folder and extract the content. Override any existing content, if necessary.

   If you use Windows servers for nginx, please comment out `ssl_session_cache shared:WEB:10m;` in the `nginx.conf` file.

```
44    ssl_certificate       ../cert/server.cer;
45    ssl_certificate_key  ../cert/server.key;
46    ssl_session_timeout    10m;
47    #ssl_session_cache shared:WEB:10m;
48    ssl_ciphers ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH:!AESGCM;
49    ssl_prefer_server_ciphers  on;
50    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
51
```

6. Configure the service addresses:

   1. Open the `b1c_extAddress.conf` file for editing.
   2. To specify the internal address and port of each component, modify the *Component Configuration* section.

```
#==================== external access proxy configuration begins ==========

#Component configuration
upstream SLDService{
  server 10.58.112.232:40000;
}


upstream BASService {
  server 10.58.115.45:8100;
}

upstream AnalyticService {
  server 10.58.112.232:40000;
}

upstream BliService {
  server 10.58.8.26:8443;
}

upstream MobileService{
  server 10.58.112.232:40000;
}


upstream WebClient{
  server 10.58.112.232:443;
}
```

   3. To configure an external domain name for the components, modify the *Server* information in the `b1c_extAddress.conf` file.
      Note that you must ensure the domain name is bound to the public IP address of this nginx server.

```
#Service
server
{
    listen        443 default ssl;
    server_name ExternalAddress.def.com;

    #root html/ControlCenter;

    #if (-d $request_filename){
    #    rewrite ^/(.*)([^/])$ $schema://$host/$1$2/ permanent;
    #  }

    #Control Center
    location /ControlCenter {

     #root html/ControlCenter;

    }
```

4. For Web Client, use the same server name in step 3, and give a different port to be listened.

```
#webclient
server
        {
        listen 8443 ssl;
        server_name ExternalAddress.def.com;



        location  ~* ^(/|/.*)
                {
        set $pass_access_scheme  $scheme;
        set $pass_server_port    $server_port;
        set $best_http_host      $http_host;
        set $pass_port           $pass_server_port;

                    include b1c_proxy_common.conf;

            # proxy_set_header HOST $server_name:$server_port;
                proxy_pass https://WebClient;
            include b1c_proxy_common.conf;
                    include b1c_proxy_common_ext.conf;

            proxy_set_header HOST $host:$server_port;
        proxy_set_header X-Forwarded-Host        $best_http_host;
        proxy_set_header X-Forwarded-Port        $pass_port;
        proxy_set_header X-Forwarded-Proto       $pass_access_scheme;
        proxy_set_header X-Forwarded-Scheme      $pass_access_scheme;
                }

        }




#=================== external access proxy configuration ends ==========
```

7. Go to `${nginx}/sbin` and start the nginx server.

Results

The external addresses of the SLD and the other components are as follows:

- SLD: `https://ExternalAddress.def.com:443`
- Browser Access service: `https://ExternalAddress.def.com:443/dispatcher`
- Analytics service: `https:// ExternalAddress.def.com:443/Enablement`
- B1iService: `https://ExternalAddress.def.com:443/B1iService`
- Mobile service: `https://ExternalAddress.def.com:443/mobileservice`
- Web Clients for SAP Business One: `https://WebClientsExternalAddress.def.com:8443`

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon 　 : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.

  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

- Links with the icon 　: You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN **SAP**