



Administration Guide | PUBLIC
Document Version: 1.0 – 2022-11-25

How to Enable External Access to SAP Business One Services

Content

- 1 Introduction. 3
- 2 Choose a method to handle external requests. 4
- 3 Prepare certificates for HTTPS services. 6
- 4 Prepare external addresses. 7
- 5 Register external address mapping. 10
- 6 Appendix: Configure an nginx reverse proxy. 12

1 Introduction

The SAP Business One Browser Access service, integration framework, mobile service, analytics service and Web Client help you to use SAP Business One outside your corporate networks. For secure access, you must be sure to do the following:

1. Use an appropriate method to handle external requests.
2. Use valid certificates to install relevant SAP Business One services.
3. Assign an external address to each relevant SAP Business One service.
4. Build proper mapping between the external addresses and the internal addresses.

Alternatively, you can use Citrix or similar solutions for external access. These third-party solutions are not covered in this guide.

2 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.

3 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.

4 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://SLDEternalAddress.def.com:Port`
- Browser Access service: `https://BASEternalAddress.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://SLDEternalAddress.abc.com:Port`
- Browser Access service: `https://BASEternalAddress.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`

5 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

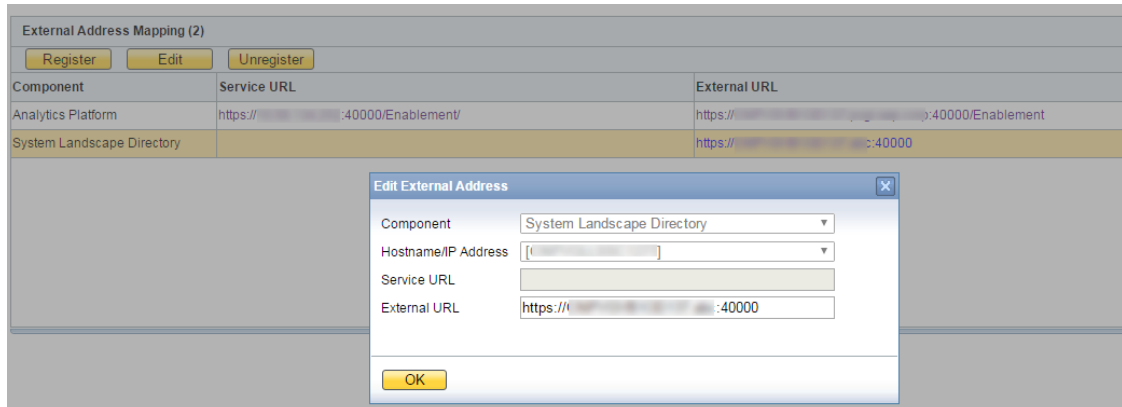
Note that you do not need to register the mapping for the integration framework.

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 URLThe external access URL must have the format `<protocol>://<Path>:<Port>`.

❁ Example

`http://<IP address>:8080`



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](#).

6 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 `${nginx}\html\ControlCenter`.
4. Prepare certificates:
 1. Generate the `server.cert` and `server.key` files from your PKCS12 (.pfx) file using the OpenSSL library.
 2. Copy both files to the `${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;
endy 46     ssl_session_timeout 10m;
47     #ssl_session_cache shared:WEB:10m;
pvglis 48     ssl_ciphers ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!aNULL:!EDH:!AESGCM;
5     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`
- BliService: `https://ExternalAddress.def.com:443/BliService`
- 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.

© 2023 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 <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.