How to Guide
SAP Business One Cloud 1.1
Document Version: 1.01 – 2016-05-25

CUSTOMER

How to Deploy SAP Business One Cloud with Browser Access

All Countries

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	2016-04-13	First version.
1.0.1	2016-05-25	Section 4.1: Load balancing mechanism used by the UAP Section 6.5: Troubleshooting logging on to specific Browser Access servers

Table of Contents

1 Introduction

With the Browser Access service, you can work with SAP Business One in a web browser (for supported browsers, please refer to the Administrator's Guide) 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 Cloud.

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 Cloud system.

2 Prepare domains and certificates

Before installing and configuring the Browser Access service, you must make some necessary preparations. These preparations include setting up domains and preparing certificates.

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/PAT, the reverse proxy is more flexible and can filter incoming requests.

> 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 to the reverse proxy server and all machines with SAP Business One services installed.

   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 in the SAP Business One Cloud 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.

   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 domains

As a prerequisite for SAP Business One browser access, set up domains and add relevant servers (all Windows servers, including the presentation servers and Browser Access servers) to the domains.

To enable accessing SAP Business One from outside your corporate network, you must expose relevant SAP Business One services to the Internet (external networks) by assigning an external address to each relevant SAP Business One service. Therefore, prepare a domain for internal use and purchase a domain for external use.

> ➡ Recommendation
>
> 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.
>
> This is also a prerequisite for Google Chrome. If the components are not under the same second-level domain, Google Chrome blocks the cookies and you cannot work with SAP Business One as expected.

Note that if you want to use NAT/PAT to handle client requests, we recommend that you use the same domain name for the internal and external domains. For more information, see Prepare certificates.

2.3 Prepare certificates

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 Cloud

3.1 Install SAP Business One Cloud

For detailed instructions on installing SAP Business One Cloud, please refer to the Administrator's Guide. The following are additional instructions that are required for enabling browser access.

> ⚠ 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 following on the same machine:
>
> - Microsoft SQL server
> - Browser Access service
> - Other SAP Business One components (for example, the SLD)

Security Certificate

When installing the following SAP Business One components, ensure that you import the certificates you have prepared:

- Shared components:
  - System Landscape Directory (SLD)
  - User Access Portal (UAP)
- Service-unit-specific components
  - Browser Access service
  - Integration framework
  - Analytics service

    This is relevant to SAP Business One, version for SAP HANA only.

    For SAP Business One 9.1 PL08 and PL09, version for SAP HANA, during the installation, please also select the license service; otherwise, you cannot import the certificate for the analytics service.
  - Service Layer

    This is relevant to SAP Business One, version for SAP HANA only.

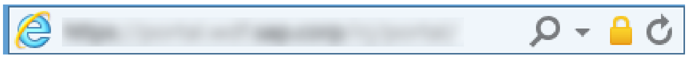
The way you expose your services to the Internet determines which certificates you import for these components:

- Reverse proxy mode: Import the internal certificate.

  Note that the external certificate is for the reverse proxy server.
- NAT/PAT mode: Import the purchased certificate for both internal and external domains.

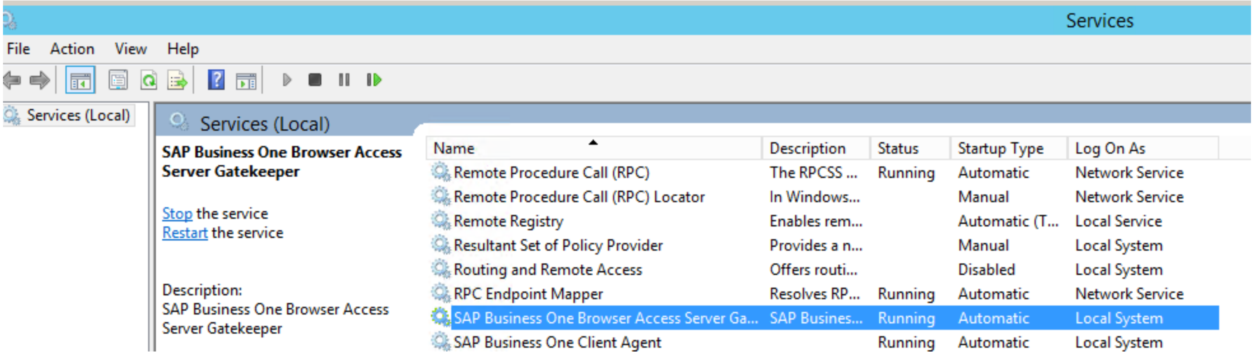
Recommendation

After the installation of each component, check if the certificate has been applied correctly. To do so, open the service URL of each component in a Web browser and click the 🔒 (lock) icon. You can see the details of your certificate.



Service account for SAP Business One Browser Access Gatekeeper service

The Browser Access service is registered as a Windows service SAP Business One Browser Access Gatekeeper. This Windows service must run under the `Local System` account.



SAP Business One Browser Access Server Gatekeeper

Stop the service
Restart the service

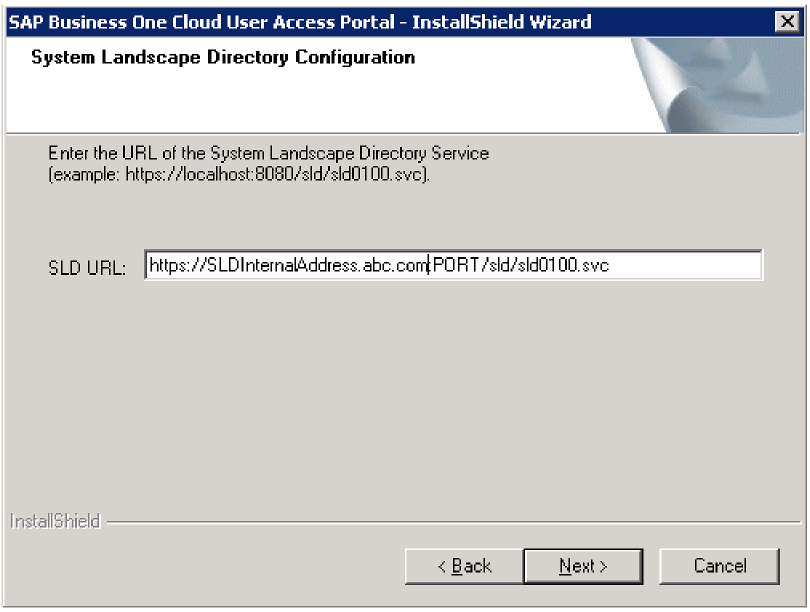
Description:
SAP Business One Browser Access Server Gatekeeper

Name	Description	Status	Startup Type	Log On As
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	Network Service
Remote Procedure Call (RPC) Locator	In Windows...		Manual	Network Service
Remote Registry	Enables rem...		Automatic (T...	Local Service
Resultant Set of Policy Provider	Provides a n...		Manual	Local System
Routing and Remote Access	Offers routi...		Disabled	Local System
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Service
SAP Business One Browser Access Server Ga...	SAP Busines...	Running	Automatic	Local System
SAP Business One Client Agent		Running	Automatic	Local System

SLD agent for SAP Business One Cloud

You must install the SLD agent service on the server before you install the Browser Access service.

During the SLD agent service installation, ensure the domain name (**abc.corp**) is included in the **internal** SLD URL, as follows: https://SLDInternalAddress.abc.corp:Port/sld/sld0100.svc



SAP Business One Cloud User Access Portal - InstallShield Wizard

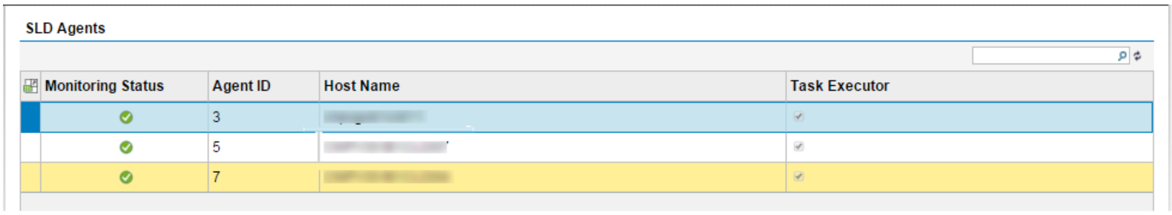
System Landscape Directory Configuration

Enter the URL of the System Landscape Directory Service
(example: https://localhost:8080/sld/sld0100.svc).

SLD URL: https://SLDInternalAddress.abc.com:PORT/sld/sld0100.svc

InstallShield
< Back
Next >
Cancel

After the installation, you can see the SLD agent registered in the SAP Business One Cloud Control Center.

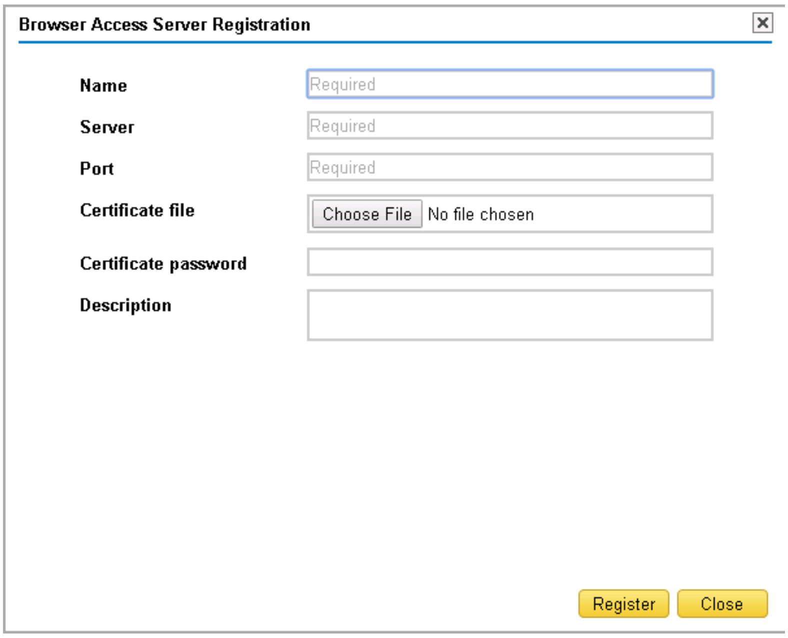


SLD Agents

Monitoring Status	Agent ID	Host Name	Task Executor
✓	3	[redacted]	✓
✓	5	[redacted]	✓
✓	7	[redacted]	✓

3.2 Register Browser Access servers

1. In the Cloud Control Center, choose *Landscape Management* → *Browser Access Servers*, and then choose the *Register* button.



Browser Access Server Registration

Name	Required
Server	Required
Port	Required
Certificate file	Choose File No file chosen
Certificate password	
Description	

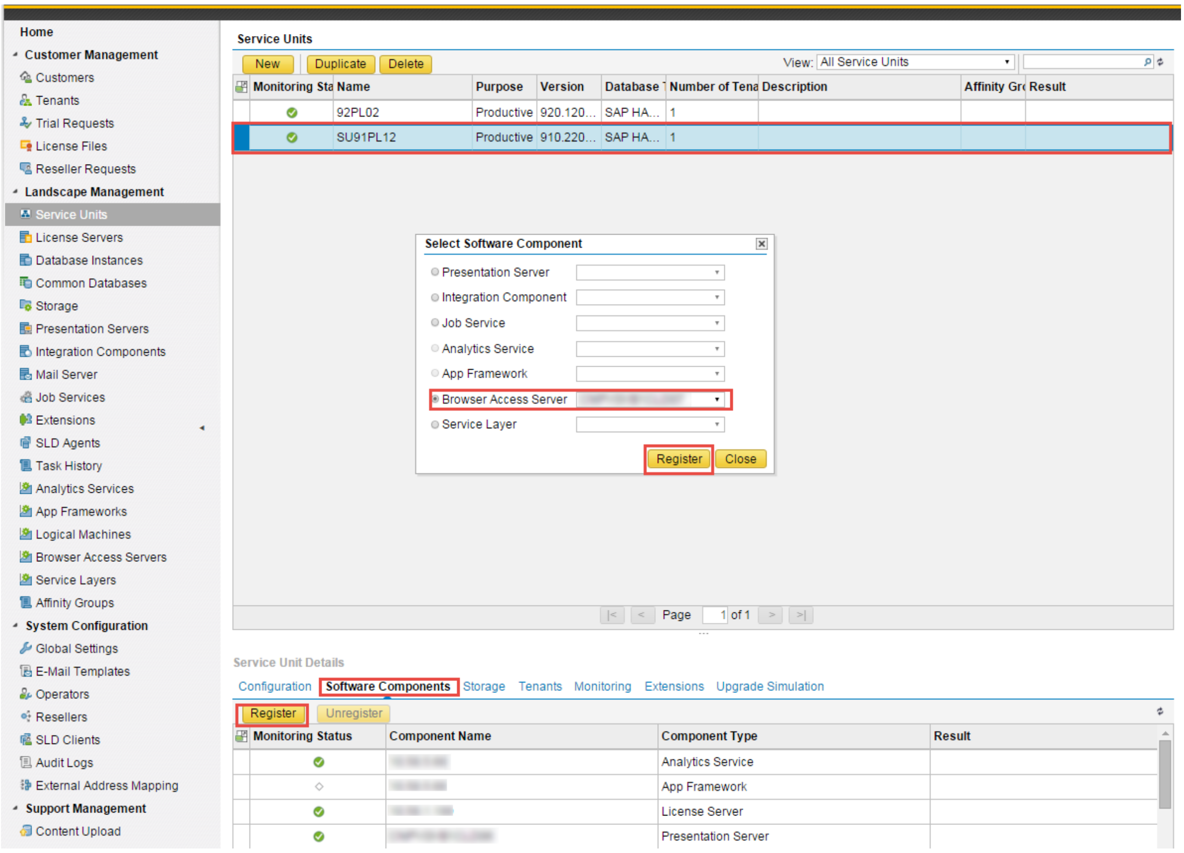
2. In the *Browser Access Server Registration* window, specify the following:
   - *Name* – Enter a name for the Browser Access server.
   - *Server and Port* – Enter the machine name and the port number of the Browser Access server where the *Browser Access Server Gatekeeper* service will listen. This server must have the SLD agent installed. Make sure that the port is not used by other applications.
   - *Certificate File and Certificate Password* – The way you expose your service to the Internet determines the certificates you import :
     - Reverse proxy mode: Import the internal certificate.

       Note that the external certificate is for the reverse proxy server.
     - NAT/PAT mode: Import the purchased certificate for both internal and external domains.
   - *Description* – Enter an optional description for the Browser Access server.
3. To complete the registration process, choose the *Register* button.

3.3 Register Browser Access servers to service units

1. Select a service unit and then in the *Service Unit Details* area, on the *Software Components* tab, choose the *Register* button.

2. In the *Select Software Component* window, select the Browser Access server you want to register, and then choose the *Register* button.



Monitoring Sta	Name	Purpose	Version	Database T	Number of Tena	Description	Affinity Gr	Result
✓	92PL02	Productive	920.120...	SAP HA...	1			
✓	SU91PL12	Productive	910.220...	SAP HA...	1			

Select Software Component

○ Presentation Server

○ Integration Component

○ Job Service

○ Analytics Service

○ App Framework

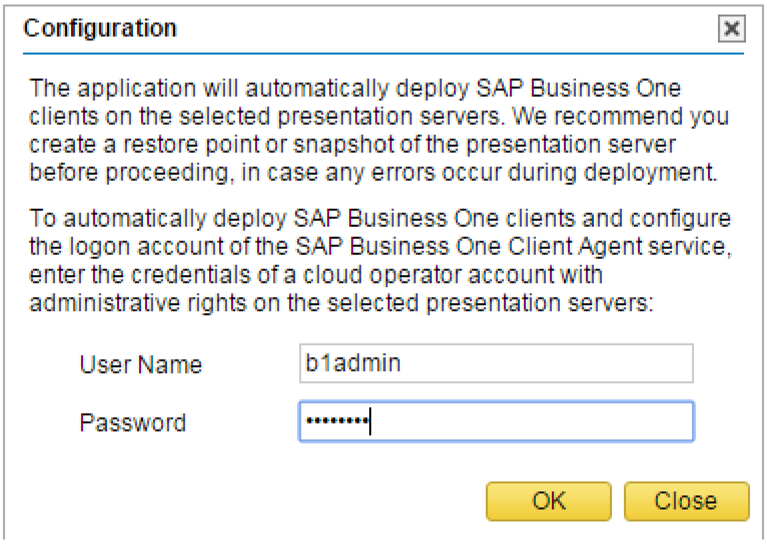
● Browser Access Server [redacted]

○ Service Layer

Register | Close

Monitoring Status	Component Name	Component Type	Result
✓	[redacted]	Analytics Service	
◇	[redacted]	App Framework	
✓	[redacted]	License Server	
✓	[redacted]	Presentation Server	

3. In the *Configuration* window, enter the SLD operator user name and password



Configuration

The application will automatically deploy SAP Business One clients on the selected presentation servers. We recommend you create a restore point or snapshot of the presentation server before proceeding, in case any errors occur during deployment.

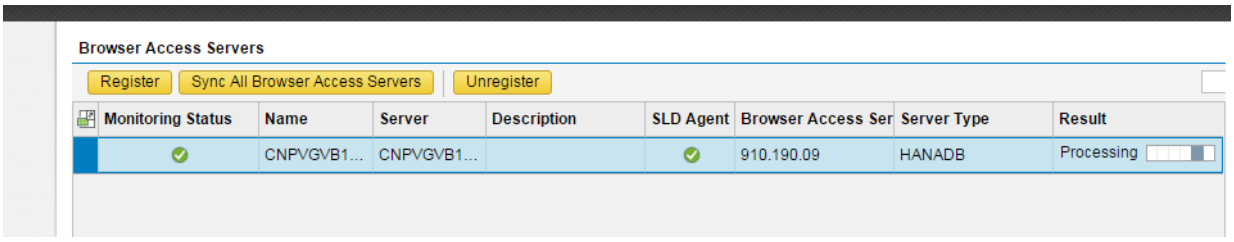
To automatically deploy SAP Business One clients and configure the logon account of the SAP Business One Client Agent service, enter the credentials of a cloud operator account with administrative rights on the selected presentation servers:

User Name: b1admin

Password: ••••••••

4. Wait for several minutes until the configuration is complete.

On the *Browser Access Servers* page, you can see the progress in the *Result* field.



Browser Access Servers

Monitoring Status	Name	Server	Description	SLD Agent	Browser Access Ser	Server Type	Result
✓	CNPVGVB1...	CNPVGVB1...		✓	910.190.09	HANADB	Processing

3.4 Map between internal and external addresses

3.4.1 Prepare external addresses

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

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.
- While the User Access Portal is installed later, we recommend that you prepare an address for it in advance, together with other components. It will save you some configuration efforts.

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 both the System Landscape Directory and the User Access Portal.

  In addition, the internal and external ports must use the same number for the User Access Portal.
- One external address for **each** service unit, which will be shared by the Browser Access service, the analytics service, and the integration framework within the service unit.
- 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

The external URLs are as follows:

- System Landscape Directory: https://servertool.def.com:Port
- UAP: https://servertool.def.com:Port/BrowserAccess
- Browser Access service: https://su01.def.com:Port/dispatcher
- Analytics service: https://su01.def.com:Port/Enablement
- Integration framework: https://su01.def.com:Port/B1iXcellerator

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
  - User Access Portal (UAP)
  - Integration framework (if you use the SAP Business One mobile solution)
- 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

The external URLs are as follows:

- System Landscape Directory: https://SLDExternalAddress.abc.com:Port
- User Access Portal: https://UAPExternalAddress.abc.com:Port/BrowserAccess
- 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

3.4.2 Register external address mapping

You must register in the Cloud Control Center 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

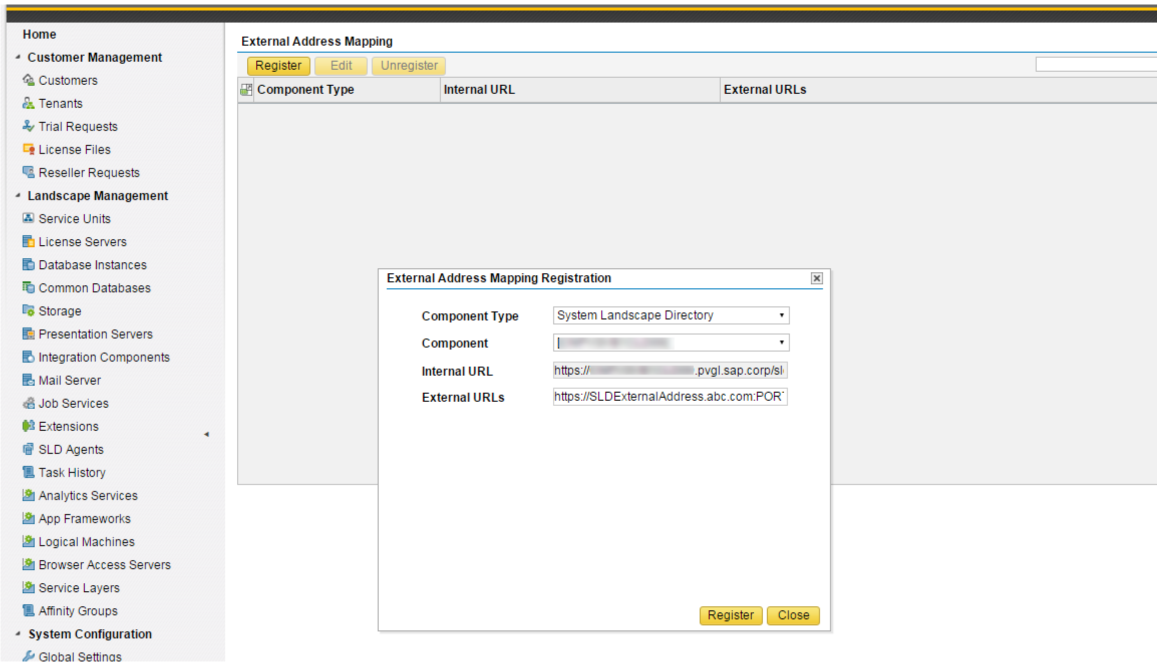
Note that you do not need to register the mapping for the integration framework.

Procedure

To map an external address to an internal address, do the following:

1. In the Cloud Control Center, choose *System Configuration* → *External Address Mapping*.
2. Choose the *Register* button.
3. In the *External Address Mapping Registration* window, select a component type.
4. Specify the component.

   The internal URL is filled automatically.
5. Specify the external URL.



External Address Mapping Registration

Component Type: System Landscape Directory

Component: [redacted]

Internal URL: https://[redacted].pvgl.sap.corp/sl

External URLs: https://SLDExternalAddress.abc.com:POR

6. Choose *Register*.
7. To apply the changes, restart the relevant service.

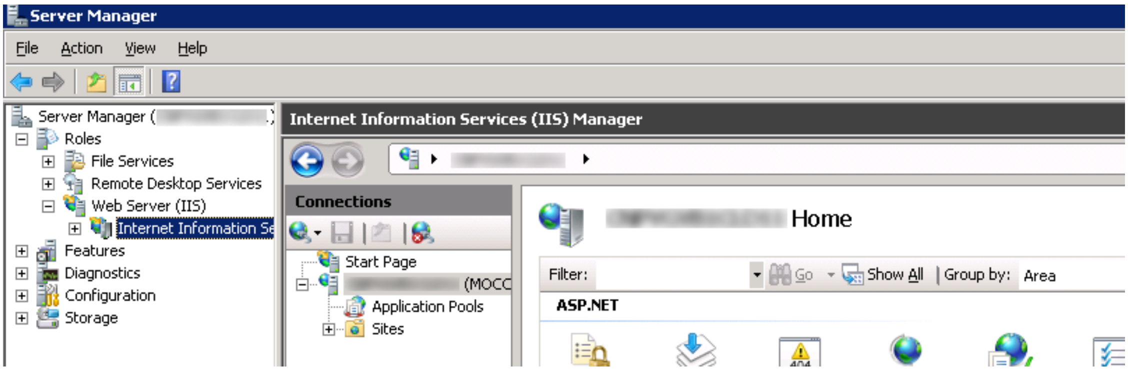
   For example, if you have registered the external address mapping for a Browser Access server, you must restart the SAP Business One Browser Access Server Gatekeeper service.

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

4 Install User Access Portal for Browser Access

Prerequisites

- You have installed and configured Internet Information Services (IIS) on the User Access Portal server.



- For SAP Business One Cloud 1.1 PL05 or lower, ensure that you have imported the PKCS12 (.pfx) certificate.

  The way you expose your services to the Internet determines which certificates you import:

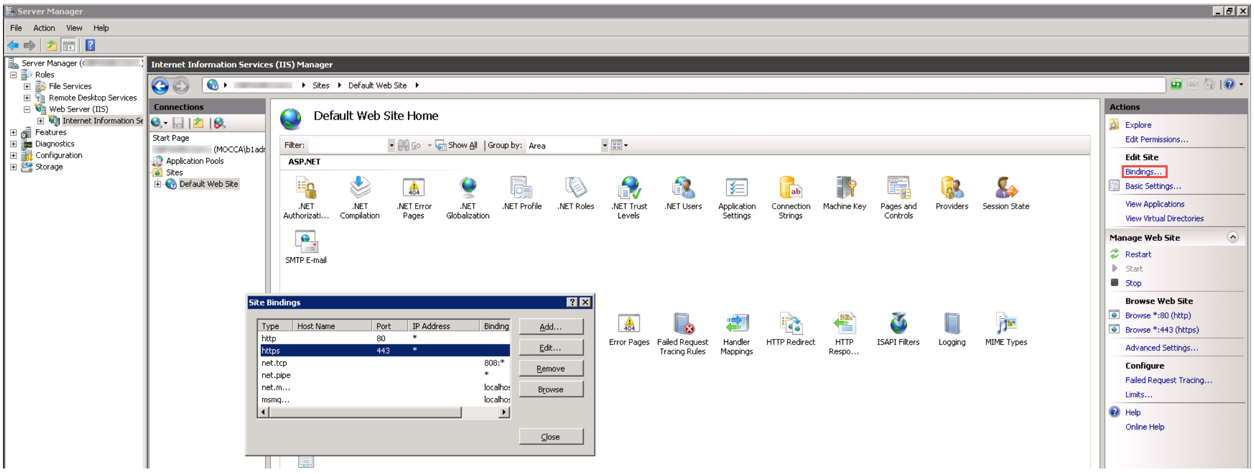
  - Reverse proxy mode: Import the internal certificate.

    Note that the external certificate is for the reverse proxy server.

  - NAT/PAT mode: Import the purchased certificate for both internal and external domains.

  To import the PKCS12 (.pfx) certificate for SSL, perform the following steps:

1. Choose *Start* → *Administrative Tools* → *Server Manager*.
2. In the *Console Tree*, expand *Roles* → *Web Server (IIS)* → *Internet Information Services (IIS) Manager*.
3. In the *Internet Information Services (IIS) Manager* window, choose the host name (domain username) to open the home page and double-click *Server Certificates*.
4. In the *Server Certificates* page, right-click in any blank area and choose *Import*.
5. In the *Import Certificate* window, navigate to and open the certificate, enter the password, and choose *OK*.
6. In the *Internet Information Services (IIS) Manager* window, expand the *computer* → *Sites* → *Default Web Site*.
7. Right-click *Default Web Site* and choose *Edit Bindings*.
8. In the *Site Bindings* window, edit the https port, making sure it is the port you configured in Prepare external addresses for the User Access Portal.



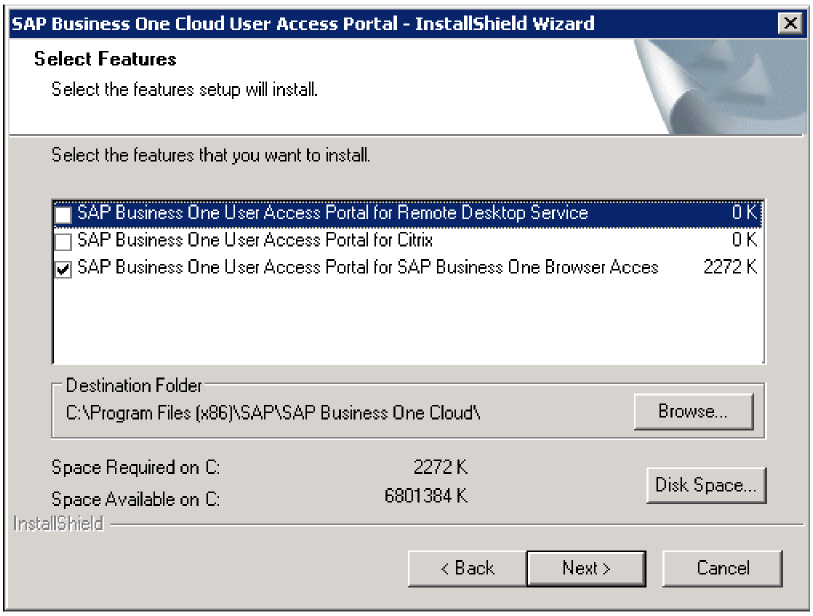
Type	Host Name	Port	IP Address	Binding
http		80	*	
https		443	*	
net.tcp				808:*
net.pipe				*
net.m...				localhos
msmq...				localhos

Procedure

To install the User Access Portal, do the following:

1. Launch the User Access Portal installer.
2. In the *Select Features* window, select *SAP Business One User Access Portal for SAP Business One Browser Access* and its destination folder.

   Note that if you access SAP Business One using Remote Desktop Services or Citrix rather than the SAP Business One Browser Access service, we highly recommend that you use their official Web access portals. Although we provide customized versions (*SAP Business One User Access Portal for Remote Desktop Service* and *SAP Business One User Access Portal for Citrix*) for your reference, we cannot guarantee that they're always compatible with Remote Desktop Services or Citrix. Support for them may be discontinued in future versions.



SAP Business One Cloud User Access Portal - InstallShield Wizard

Select Features

Select the features setup will install.

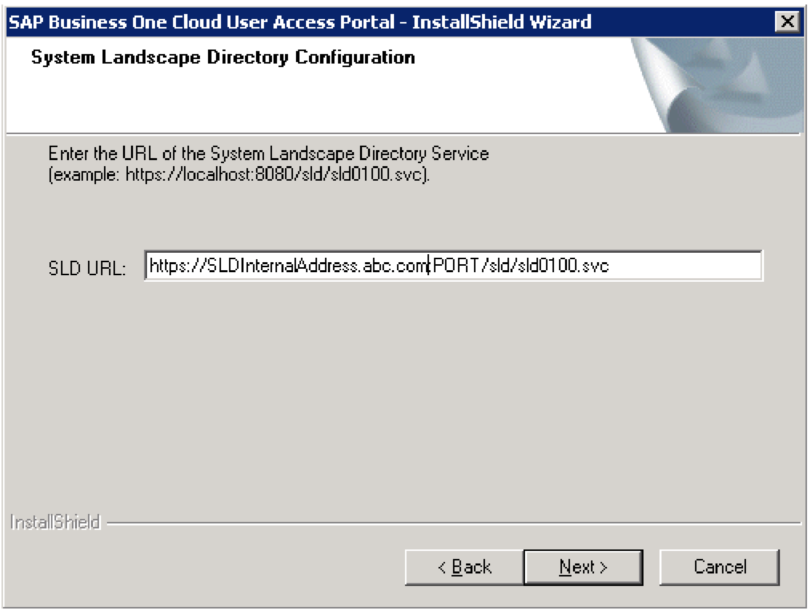
Select the features that you want to install.

□	SAP Business One User Access Portal for Remote Desktop Service	0 K
□	SAP Business One User Access Portal for Citrix	0 K
☑	SAP Business One User Access Portal for SAP Business One Browser Acces	2272 K

Destination Folder
C:\Program Files (x86)\SAP\SAP Business One Cloud\

Space Required on C: 2272 K
Space Available on C: 6801384 K

3. In the *System Landscape Directory Configuration* window, enter the **internal** URL of the SLD service, as follows: https://SLDInternalAddress.abc.com:Port/sld/sld0100.svc

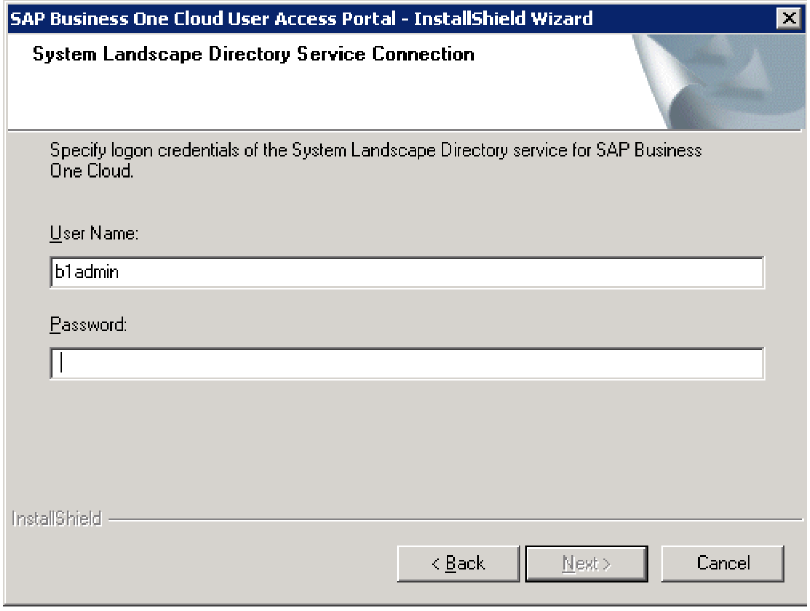

SAP Business One Cloud User Access Portal - InstallShield Wizard
System Landscape Directory Configuration
InstallShield
< Back
Next >
Cancel

Enter the URL of the System Landscape Directory Service (example: https://localhost:8080/sld/sld0100.svc).

SLD URL: https://SLDInternalAddress.abc.com:PORT/sld/sld0100.svc

4. In the *System Landscape Directory Service Configuration* window, specify the following logon credentials:

- *User Name*: Enter the user name which will be used to run the SLD service.
- *Password*: Specify the password for the domain account.


SAP Business One Cloud User Access Portal - InstallShield Wizard
System Landscape Directory Service Connection
InstallShield
< Back
Next >
Cancel

Specify logon credentials of the System Landscape Directory service for SAP Business One Cloud.

User Name: b1admin

Password:

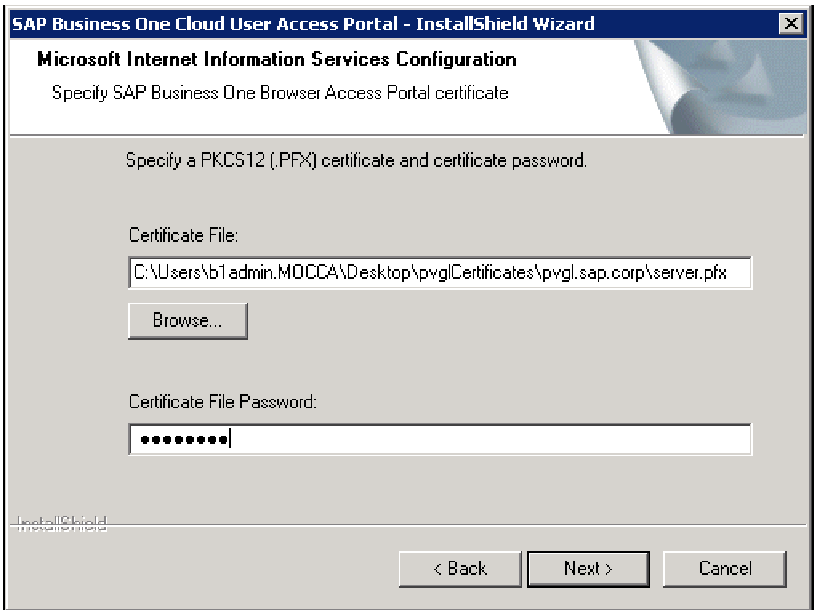
5. In the *Microsoft Internet Information Services Configuration* window, specify the certificate for the Browser Access Portal.

The way you expose your services to the Internet determines which certificates you import:

- Reverse proxy mode: Import the internal certificate.

Note that the external certificate is for the reverse proxy server.

- NAT/PAT mode: Import the purchased certificate for both internal and external domains.



SAP Business One Cloud User Access Portal - InstallShield Wizard

Microsoft Internet Information Services Configuration

Specify SAP Business One Browser Access Portal certificate

Specify a PKCS12 (.PFX) certificate and certificate password.

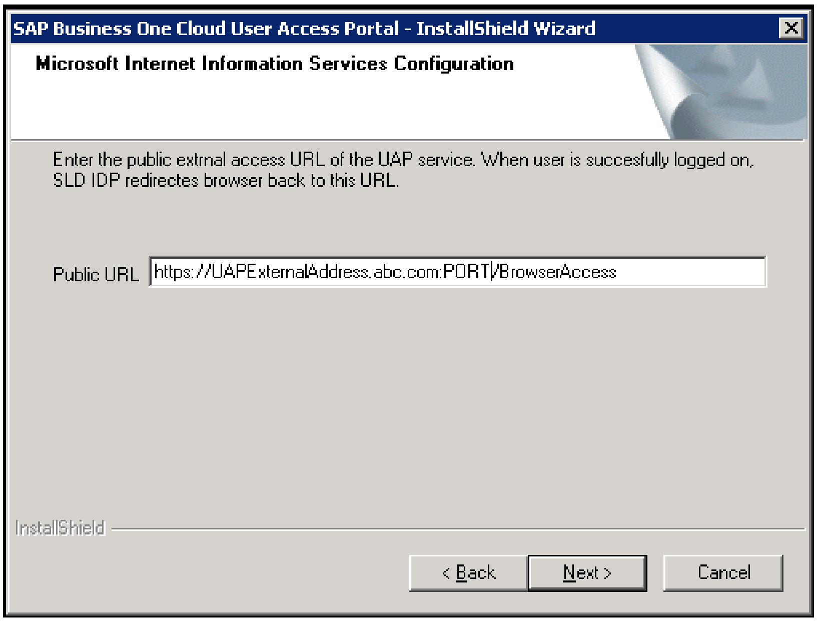
Certificate File:

C:\Users\b1admin.MOCCA\Desktop\pvglCertificates\pvgl.sap.corp\server.pfx

Certificate File Password:

●●●●●●●●●

6. In the *Microsoft Internet Information Services Configuration* window, enter the URL of the User Access Portal, which you have prepared in Prepare external addresses.



SAP Business One Cloud User Access Portal - InstallShield Wizard

Microsoft Internet Information Services Configuration

Enter the public extrnal access URL of the UAP service. When user is succesfully logged on, SLD IDP redirectes browser back to this URL.

Public URL https://UAPExternalAddress.abc.com:PORT/BrowserAccess

7. In the *Complete* window, choose the *Finish* button.

Postrequisites

For instructions on how to edit the configuration details of a Browser Access server, see the Administrator's Guide.

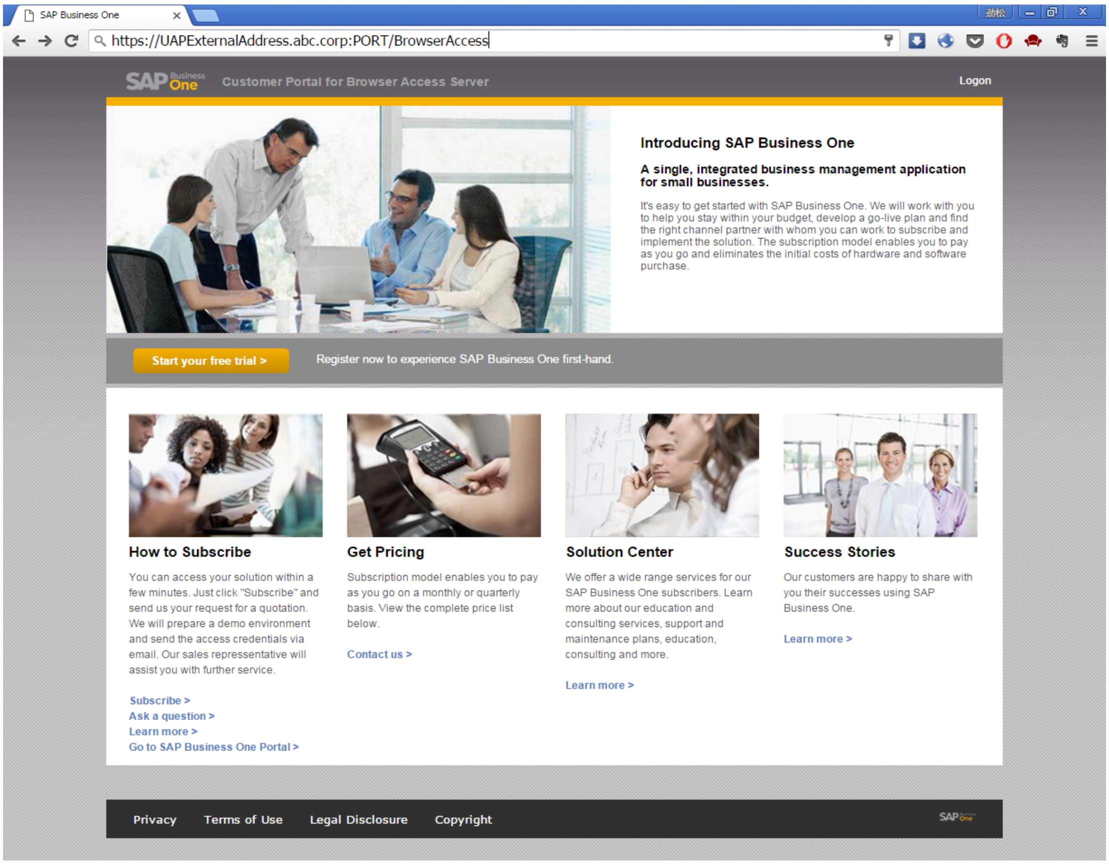
4.1 Access SAP Business One via User Access Portal

Prerequisite

You have ensured that you can log on to the SAP Business One client installed on the Browser Access server.

Procedure

1. In a web browser, navigate to the User Access Portal for Browser Access using its URL (https://servertool.def.com:Port/BrowserAccess or https://UAPExternalAddress.abc.com:Port/BrowserAccess).



Introducing SAP Business One

A single, integrated business management application for small businesses.

It's easy to get started with SAP Business One. We will work with you to help you stay within your budget, develop a go-live plan and find the right channel partner with whom you can work to subscribe and implement the solution. The subscription model enables you to pay as you go and eliminates the initial costs of hardware and software purchase.

Register now to experience SAP Business One first-hand.

How to Subscribe

You can access your solution within a few minutes. Just click "Subscribe" and send us your request for a quotation. We will prepare a demo environment and send the access credentials via email. Our sales repressentative will assist you with further service.

Subscribe >
Ask a question >
Learn more >
Go to SAP Business One Portal >

Get Pricing

Subscription model enables you to pay as you go on a monthly or quarterly basis. View the complete price list below.

Contact us >

Solution Center

We offer a wide range services for our SAP Business One subscribers. Learn more about our education and consulting services, support and maintenance plans, education, consulting and more.

Learn more >

Success Stories

Our customers are happy to share with you their successes using SAP Business One.

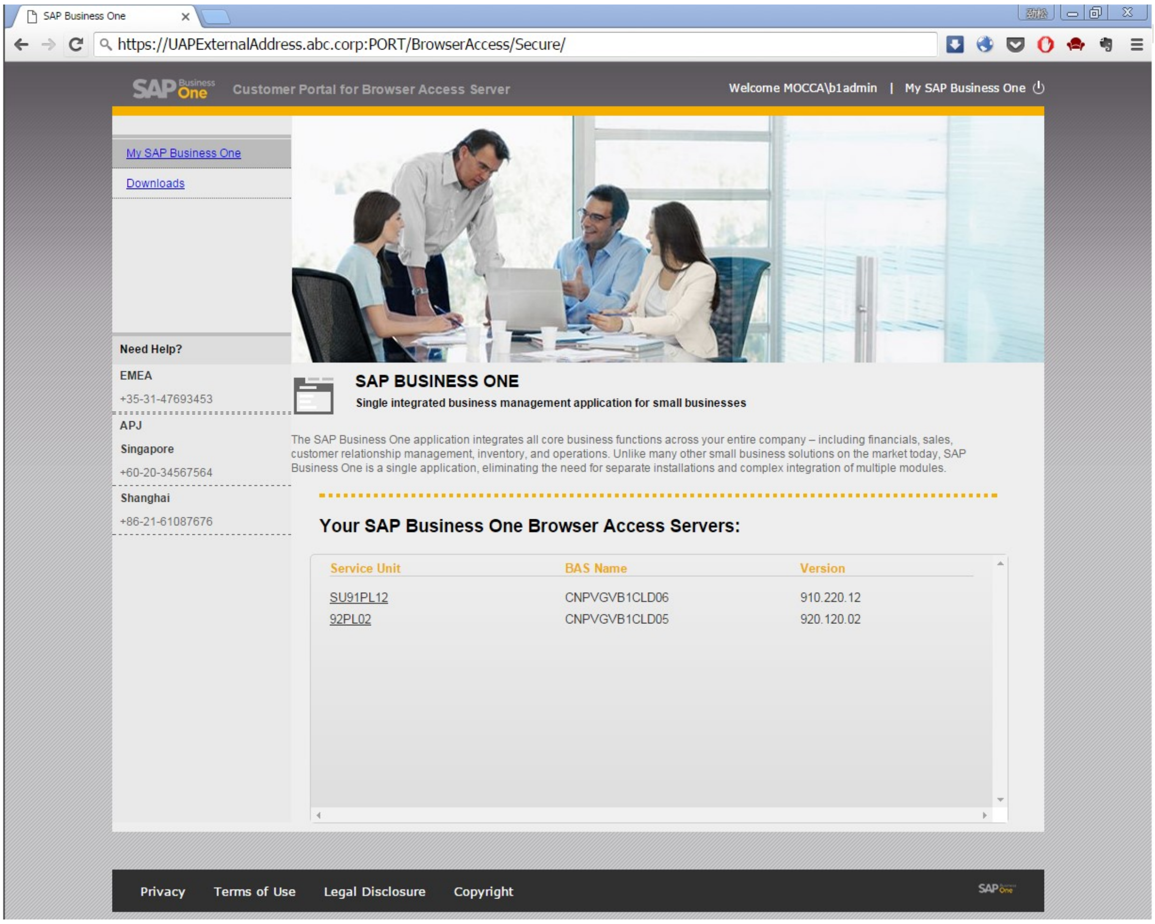
Learn more >

2. Log on to the User Access Portal.

One Browser Access server link is displayed for each service unit.

Note

Even though more than one Browser Access service is registered with a service unit, only one Browser Access service link is displayed. The particular service is picked up randomly to achieve load balancing.


SAP Business One
https://UAPExternalAddress.abc.corp:PORT/BrowserAccess/Secure/
SAP Business One
Customer Portal for Browser Access Server
Welcome MOCCA\b1admin | My SAP Business One
My SAP Business One
Downloads
Privacy
Terms of Use
Legal Disclosure
Copyright

Need Help?

EMEA
+35-31-47693453

APJ
Singapore
+60-20-34567564

Shanghai
+86-21-61087676

SAP BUSINESS ONE

Single integrated business management application for small businesses

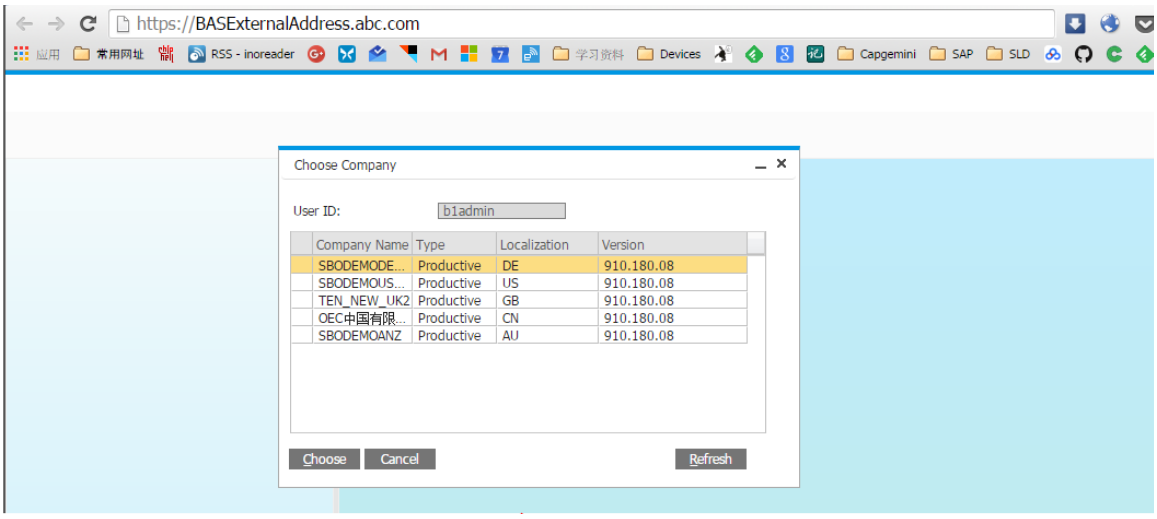
The SAP Business One application integrates all core business functions across your entire company – including financials, sales, customer relationship management, inventory, and operations. Unlike many other small business solutions on the market today, SAP Business One is a single application, eliminating the need for separate installations and complex integration of multiple modules.

Your SAP Business One Browser Access Servers:

Service Unit	BAS Name	Version
SU91PL12	CNPVGVB1CLD06	910.220.12
92PL02	CNPVGVB1CLD05	920.120.02

3. Click one of the Browser Access server links.

The Browser Access page is opened.



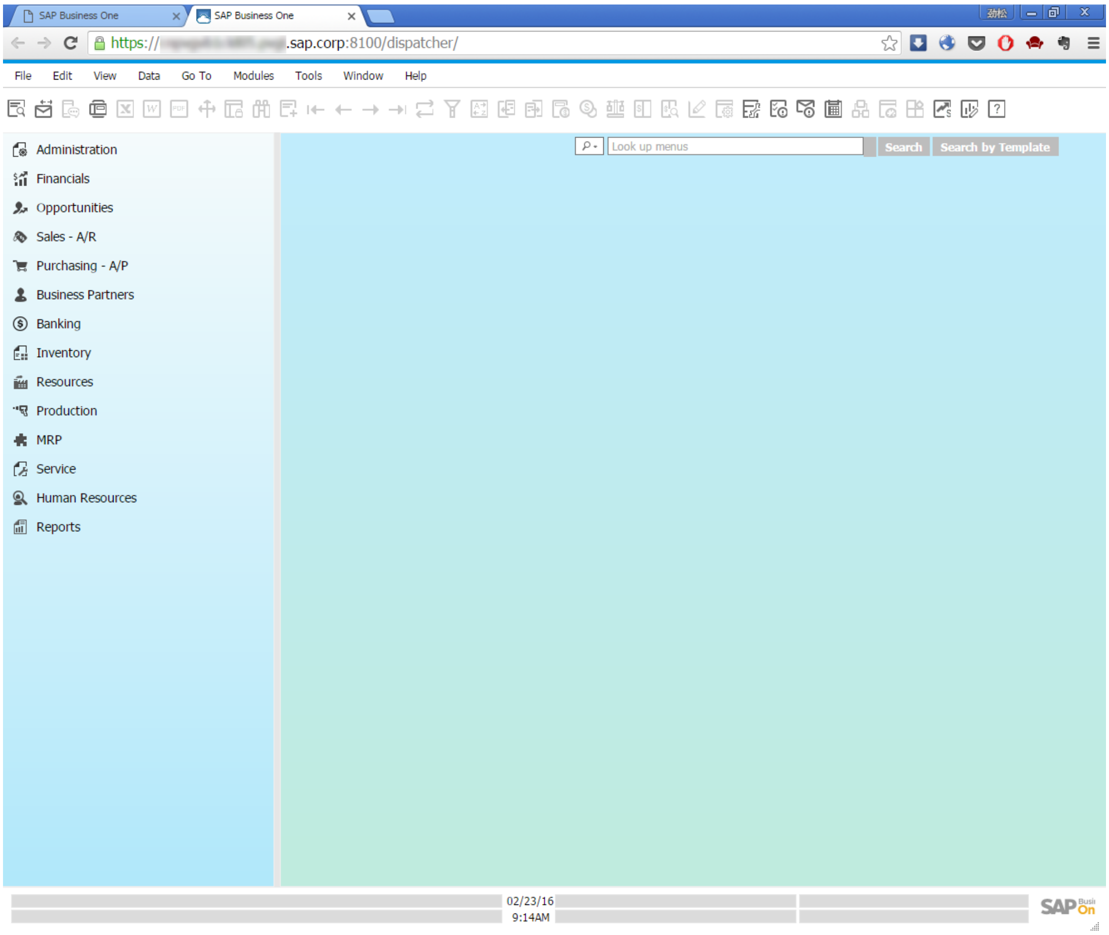
Choose Company

User ID: b1admin

Company Name	Type	Localization	Version
SBODEMODE...	Productive	DE	910.180.08
SBODEMOUS...	Productive	US	910.180.08
TEN_NEW_UK2	Productive	GB	910.180.08
OEC中国有限...	Productive	CN	910.180.08
SBODEMOANZ	Productive	AU	910.180.08

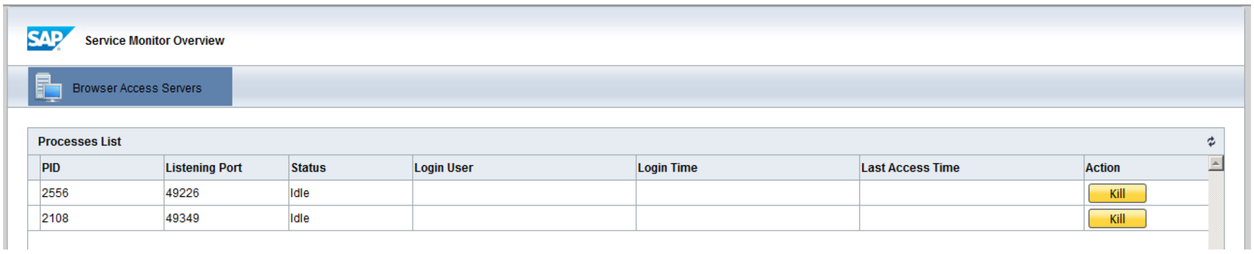
4. Choose the company and log on.

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



4.2 Monitor Browser Access processes

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



PID	Listening Port	Status	Login User	Login Time	Last Access Time	Action
2556	49226	Idle				Kill
2108	49349	Idle				Kill

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

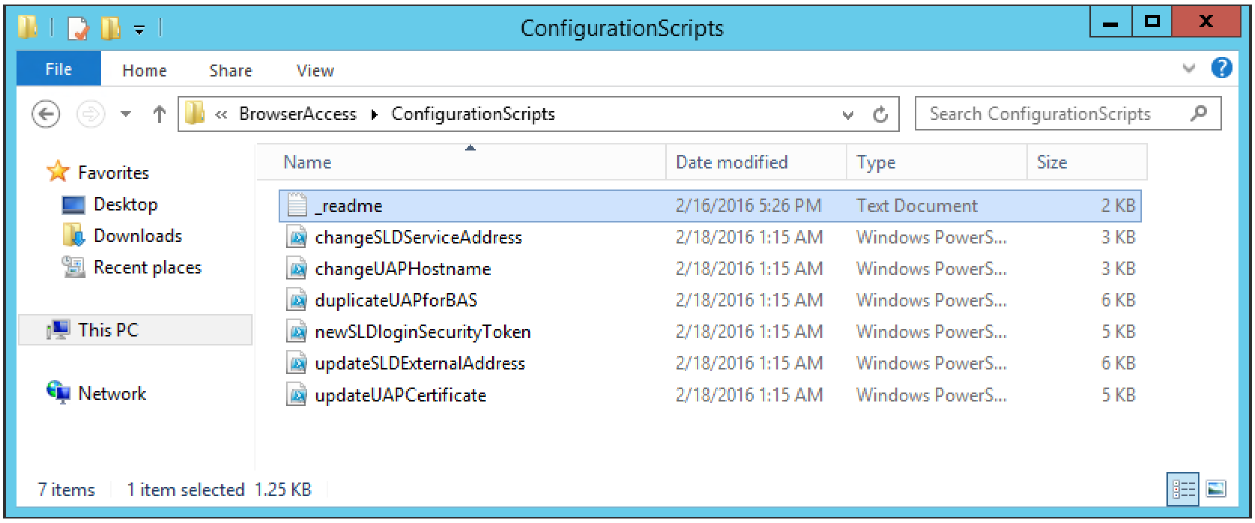
4.3 Reconfigure User Access Portal web app

You need to reconfigure the User Access Portal web app in the following cases:

- The SLD service address (**internal** address) has changed.
- The configured SLD external address has changed.
- The SLD has been reinstalled, which means the security token has changed.
- You want to change the address of the User Access Portal server (for example, use the fully qualified domain name instead of a simple hostname or the IP address).
- You want to change the certificate for the User Access Portal server.

To reconfigure the User Access Portal web app, use the PowerShell scripts located at *<BrowserAccessInstallationFolder>\BrowserAccess\ConfigurationScripts*. The default directory is *C:\Program Files (x86)\SAP\SAP Business One Cloud\BrowserAccess\ConfigurationScripts*.

> Note
>
> These scripts are available only for SAP Business One Cloud 1.1 PL06 and higher. For previous versions, you must reinstall the User Access Portal to achieve the desired reconfigurations.



Name	Date modified	Type	Size
_readme	2/16/2016 5:26 PM	Text Document	2 KB
changeSLDServiceAddress	2/18/2016 1:15 AM	Windows PowerS...	3 KB
changeUAPHostname	2/18/2016 1:15 AM	Windows PowerS...	3 KB
duplicateUAPforBAS	2/18/2016 1:15 AM	Windows PowerS...	6 KB
newSLDloginSecurityToken	2/18/2016 1:15 AM	Windows PowerS...	5 KB
updateSLDExternalAddress	2/18/2016 1:15 AM	Windows PowerS...	6 KB
updateUAPCertificate	2/18/2016 1:15 AM	Windows PowerS...	5 KB

7 items 1 item selected 1.25 KB

Duplicate existing User Access Portal web app for browser access

If you have installed and configured the User Access Portal for internal use, and now want to use it also for external access, you can execute the *duplicateUAPforBAS* script. With this script, you can duplicate the web app, utilizing the same IIS, and reconfigure it with the new certificate and the SLD external address.

5 Workarounds for limitations

Update IP address to FQDN for the analytics service

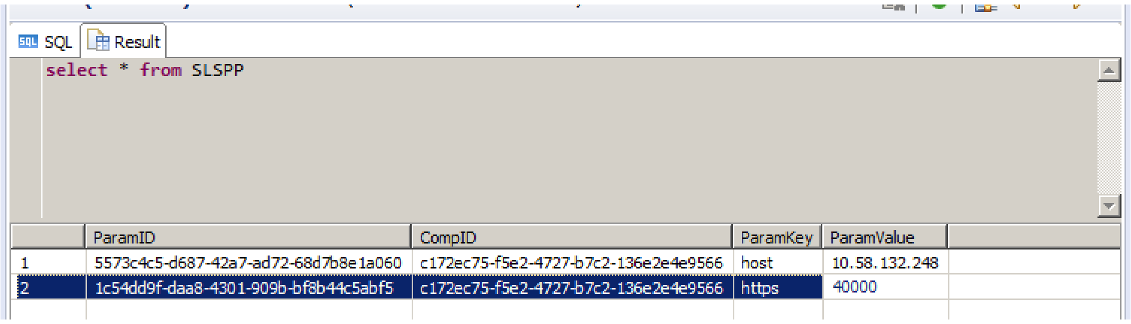
In some 9.1 versions, the analytics service is always registered in the SLD with its IP address even though you have specified its hostname during the installation. To update the IP address to the fully qualified domain name (FQDN), do the following:

1. Log on to the Cloud Control Center.
2. In the left panel, click *Analytics Services*.
3. On the *Analytics Services* page, select the row for the affected service.
4. In the *Analytics Service Details* section, on the *Configuration* tab, choose the *Edit* button, and in the *Access URL* field, replace the IP address with the hostname.

   Example

   https://${B1AHostName}.abc.corp:${port}/sld/sld0100.svc
5. To save the changes, choose the *Save* button.
6. Update the `slspp` table in the `COMMON` schema, as follows:.

```
update sbocommon.slspp set "ParamValue"='${B1AHostName}.abc.corp' where
"ParamKey"='host'
```



```
select * from SLSPP
```

	ParamID	CompID	ParamKey	ParamValue
1	5573c4c5-d687-42a7-ad72-68d7b8e1a060	c172ec75-f5e2-4727-b7c2-136e2e4e9566	host	10.58.132.248
2	1c54dd9f-daa8-4301-909b-bf8b44c5abf5	c172ec75-f5e2-4727-b7c2-136e2e4e9566	https	40000

Update User Access Portal index.html

If you have set up an nginx reverse proxy and your SAP Business One Cloud version is 1.1 PL05, a slash (/) is missing in the *index.html* file (default location: *C:\Program Files (x86)\SAP\SAP Business One Cloud\BrowserAccess*) after you install the User Access Portal. To set up an external address for the User Access Portal in your reverse proxy server, you must first fix this issue: Open the file for editing and, in line 33, change `href` to **`Secure/`**. For example:

```
<a id="Btn_Login" href="Secure/">Logon</a>
```

6 Troubleshooting

6.1 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.

<table>
<tr><th>Service</th><th>Microsoft SQL Version</th><th>SAP HANA Version</th></tr>
<tr><td>System Landscape Directory</td><td>Restart the Windows service with the <i>SAP Business One SLD Service</i> identifier.</td><td rowspan="2">Run this command on the Linux server:
<code>/etc/init.d/sapb1servertools restart</code></td></tr>
<tr><td>Analytics service</td><td>/</td></tr>
<tr><td>Browser Access service</td><td colspan="2">Restart the Windows service with the <i>SAP Business One Browser Access Server Gatekeeper</i> identifier.</td></tr>
<tr><td>Integration Framework</td><td colspan="2">Restart the Windows service with the <i>SAP Business One Integration Service</i> identifier.</td></tr>
</table>

6.2 "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.

6.3 Fiori-style cockpit cannot be displayed

Symptom

You have logged on to 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

7. 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.
8. 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.

9. 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.

6.4 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.

6.5 Cannot log on to a specific Browser Access server

Symptom

More than one Browser Access server is registered with your service unit. In the User Access Portal, however, only one Browser Access server link is displayed at one time and the display is random.

When troubleshooting issues on a particular Browser Access server, the IT administrator or the operator needs to have all Browser Access server displayed and log on to the required Browser Access server.

Solution

Append `/?allservers=1` to the UAP URL. For example,
https://servertool.def.com:Port/BrowserAccess/?allservers=1 or
https://UAPExternalAddress.abc.com:Port/BrowserAccess/?allservers=1.

All registered Browser Access servers are displayed in the UAP.

Appendix: Configure an nginx reverse proxy

Prerequisites

- You have predefined an external domain name for the following:
  - The server tools (SLD and UAP), for example, servertool.def.com
  - Each service unit, for example, su01.def.com, su02.def.com
- You have obtained the *nginx_conf ServerTool.zip* and *nginx_conf SU.zip* files delivered along with this guide.

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 one or more servers.

   We recommend that you use Linux servers rather than Windows servers for nginx. For instructions on installing nginx on Linux, see http://nginx.org/en/docs/install.html.

   We also recommend that you install nginx on **at least two** Linux servers. Use one nginx server for configuring the external addresses of the SLD and the UAP, and use the other nginx servers for configuring the external addresses of the components (for example, the analytics service, the integration framework, and so on) within each service unit.

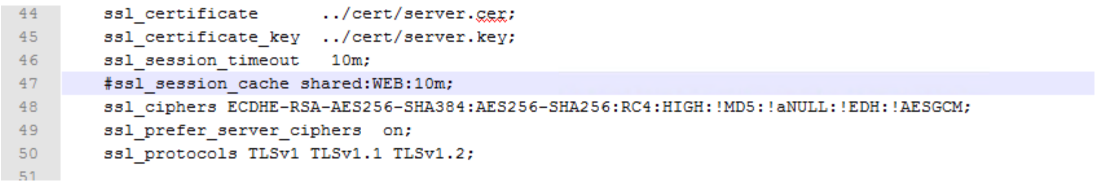
3. Copy the *ccc.war* file (located at *${SLDInstallationFolder}\tomcat\webapps*) from the SLD server to the nginx server, and unzip all contents to *${nginx}\html\ccc*.

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 ServerTool.zip* file or the *nginx_conf SU.zip* file to the *${nginx}/conf* folder and extract the content. Override any existing content, if necessary.

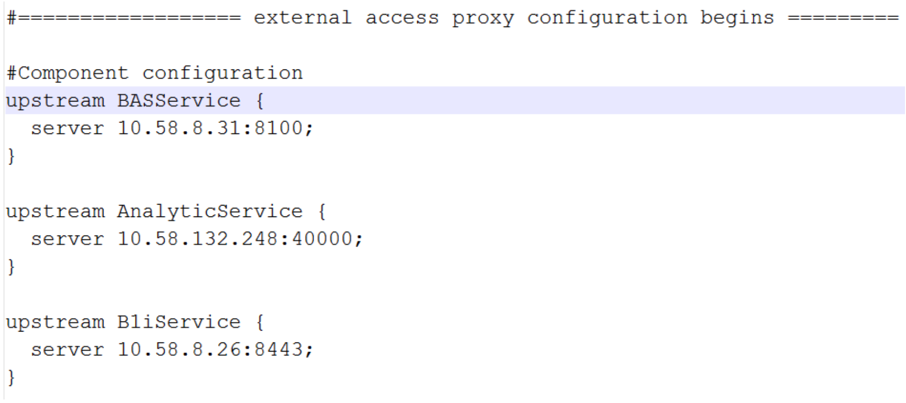
   If you use Windows servers for nginx, please comment out *ssl_session_cache shared:WEB:10m*; in the *nginx.conf* file.



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

6. On an nginx server for service unit 01, configure the service addresses:
   1. Open the *b1c_extAddress_su_01.conf* file for editing.

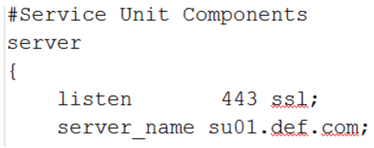
    2. To specify the internal address and port of each component within service unit 01 (for example, the analytics service, the integration framework, and so on), modify the *Component Configuration* section.



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

#Component configuration
upstream BASService {
  server 10.58.8.31:8100;
}

upstream AnalyticService {
  server 10.58.132.248:40000;
}

upstream B1iService {
  server 10.58.8.26:8443;
}
```

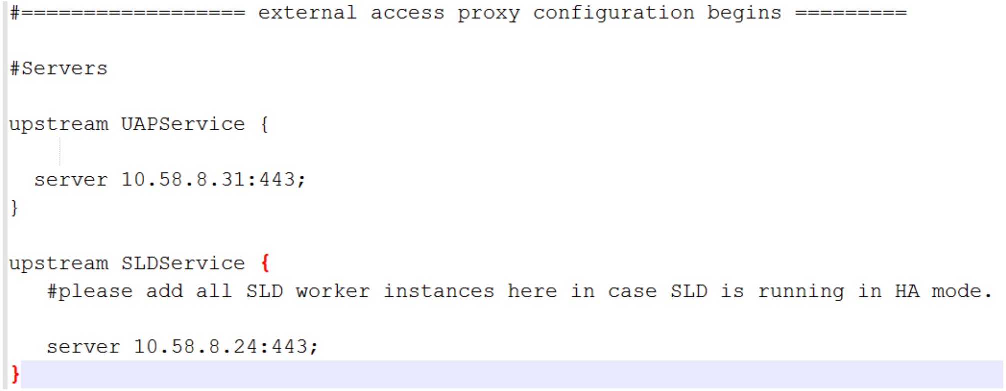
    3. To configure an external domain name for the components within service unit 01, modify the *Server* information in the *Service Unit Components* section.

       Note that you must ensure the domain name is bound to the public IP address of this nginx server.



```
#Service Unit Components
server
{
    listen       443 ssl;
    server_name su01.def.com;
```

7. On the nginx server for the SLD and the UAP, do the following:
    1. Open the *b1c_extAddress_serverTool.conf* file for editing.
    2. To specify the internal addresses and port of the SLD and the UAP, modify the *Servers* section.



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

#Servers

upstream UAPService {

  server 10.58.8.31:443;
}

upstream SLDService {
   #please add all SLD worker instances here in case SLD is running in HA mode.

   server 10.58.8.24:443;
}
```

    3. To configure an external domain name for the SLD and the UAP, specify the *Server* information in the *Service* section.

       Note that you must ensure the domain name is bound to the public IP address of this nginx server.

8. For each of the other service units, do the following:
    1. Make a copy of the *b1c_extAddress_serviceUnit.conf* file and rename it to *b1c_extAddress_xxxx.conf* (for example, *b1c_extAddress_su_02.conf*).
    2. Copy the *b1c_extAddress_xxxx.conf* file to the nginx server for the respective service unit.

3. Reference the new configuration file at the end of the *nginx.conf* file by appending this statement: "**`include b1c_extAddress_xxxx.conf;`** ",

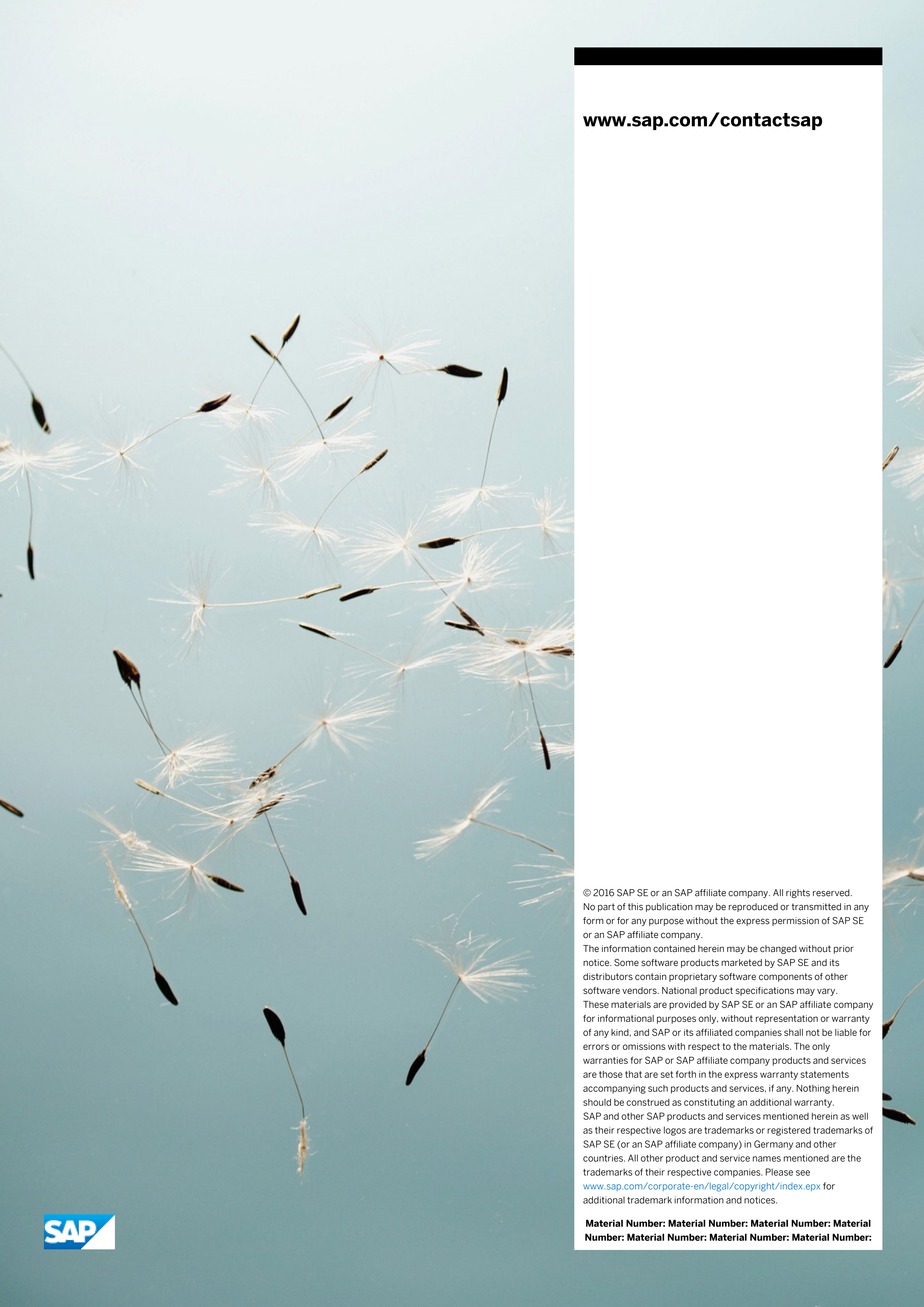
Results

The external addresses of the SLD and the UAP are as follows:

- SLD: https://servertool.def.com:443
- User Access Portal: https://servertool.def.com:443/BrowserAccess

The external addresses of the components within service unit xx are as follows:

- Browser Access service: https://su01.def.com:443/dispatcher
- Analytics service: https://su01.def.com:443/Enablement
- B1iService: https://su01.def.com:443/B1iService



www.sap.com/contactsap

Material Number: Material Number: Material Number: Material Number: Material Number: Material Number: Material Number: