Remote Support - Help

What is SAP router?

- SAProuter is a stand-alone program that will establish a secure connection from the customer’s network to the SAP network. It will help to protect your SAP network against unauthorized access, and allow for a much deeper level of technical support by SAP.

- It acts as an intermediate station (proxy) in a network connection between SAP systems, or between SAP systems and external networks. SAProuter controls the access to your network and making it a useful enhancement to an existing firewall system.

- The firewall forms an impenetrable “wall” around your network. However, since particular types of connections need to penetrate this wall, a “gate” has to be made in the firewall. SAProuter assumes control of this gate.

- This gate is only opened for connections you specify.

- SAProuter provides you with the means of controlling access to your SAP system. It is the backbone of establishing a secure connection between SAP Support and a customer. SAP landscape and functions as the cornerstone of many of the remote access technologies and tools utilized by SAP. It needs to be installed and configured by customers on their own network.

- SAProuter can deny or allow a network connection between the SAP network and external customer networks. Again, SAProuter is essentially a proxy that controls incoming and outgoing traffic according to the access list defined by the customer. Communication between SAP software components is based on TCP/IP. SAProuter software enables communication between the customer and SAP using one single IP address. Therefore it is not necessary to enter your entire network; instead it is sufficient to establish one single TCP/IP connection between your SAProuter and the appropriate SAP support server.

- Connections established using SAProuter have the additional advantage that no end-to-end connections between the participating systems are necessary on network level. For example, if accessing a front end PC on an R/3 server with an intermediate SAProuter, it is not necessary to define the complete path between the two systems at TCP/IP level. It is sufficient if both parties can reach the SAProuter. From an SAP communication viewpoint, this represents a point of concentration in your network that serves as a starting point for each sub-connection.

**Complete SAProuter requirements / pre-requisites for configuring Network components (Do this step prior to downloading and Installing SAProuter)**

SAProuter configuration requires SAP Network Support to add a your external IP address to the SAP Network. This creates a secure communication route between SAP and your landscape.
To best facilitate this request it’s vital that you ensure the following items are in place.

<table>
<thead>
<tr>
<th><strong>New Connection Requirements</strong></th>
<th><strong>Existing Connection Requirements</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To register your configuration with SAP, follow the instructions in SAP Note 28976 - Remote connection data sheet to create an incident with the necessary data so that one of SAP’s external partner companies will assist you - for IPSEC you must have two public IP’s</td>
<td></td>
</tr>
<tr>
<td>You must have or be able to provide a contact that has a basic knowledge of the operating system prior to logging a ticket for SAP router network configuration.</td>
<td>You must have an internal contact who is familiar with the SAProuter and the hardware of the physical connection.</td>
</tr>
<tr>
<td>You will not require network experience, but should have an internal network contact that can be called to assist should it become necessary.</td>
<td></td>
</tr>
</tbody>
</table>

If you have any questions after reading the SAP note, log an incident on component XX-SER-NET-NEW and explain what you need help with and one of SAP’s external partner companies will assist you to set up SAProuter.

Once a remote connection is registered by SAP Network Support as requested via the incident created in the previous section, you will get a confirmation message similar to the one shown below in your SAP Support Portal Inbox.

Example:

Dear Customer,

We have registered your connection according to the data provided. You can test it with the following information:

Data at SAP side:

Desitination IP address: xxx.xxx.xxx.xxx

Hostname of this machine: sapservX

Data at customer side:
Choosing your Connection Type

Enter the required logical connections between your SAP systems and SAP.

See also Note 35010 - Service connections: Composite note (overview)

- Vpn gateway
- SNC – [not in itself a prerequisite for saprouter]
- SAP authorised internet provider note SAP note 33953

For more information on connection types, see SAP note 31515

Internet Connections

Access Support

SAP customers can receive services and support from SAP remotely over special connections. Until now these remote connections have been either dial-up connections or leased lines. As of now SAP offers a new cost-effective and more flexible alternative: internet connections which provide a high level of security that is essential for Internet communications. All you need is a connection from your local area network (LAN) to the Internet.

Two Alternatives

Customers can establish Internet connections in two ways:

- Secure network communication (SNC) via SAProuter software to deliver software encryption
- Virtual private networks (VPN), which provide hardware-level encryption

Both options use three types of security measures to protect your systems and data from unauthorized access:

- State-of-the-art encryption
- Server authentication
- Access-control technology

SNC connections are established between two SAProuters. They require no additional hardware, but additional software has to be installed. You can download this software directly from the SAP Support Portal.
A VPN switch is required at the customer site and at SAP. You will find more information on the technical requirements and the mode of operation of both encryption methods in the Technical Specifications.

Your Benefits

Using the latest Internet technology offers clear benefits for the customer:

- Lower costs through lower rates for internet connections
- Access any time, anywhere an internet connection is available
- High security level due to SNC or VPN
- Easy to handle and to maintain
- Low hardware requirements

If you are interested in establishing your internet connection to SAP, set up an internet connection and then contact the relevant network connection consulting company. If you already have an internet connection, you may use this existing connection to establish a secure communication channel to SAP.

**How to run the SAProuter with IPSEC connectivity**

When using IPSEC connectivity, you connect to the SAProuter at SAP called sapserVX depending on your geographical location (SAP note 33135), however no connectivity via IPSEC/VPN to sapserV2 and sapserV9.

For IPSEC connectivity to 'sapserVX' the SAPROUTTAB needs to have the following structure:

Example:

#Connection from sapserVX to local WINDOWS system for WTS

P <sapserVX> 10.0.0.1 3389 [SR password]

#Connection from sapserVX to local UNIX system with SSH

P <sapserV> 10.0.0.2 22 [SR password]

#Deny all other connections

D***

For more information about SAProuter, please read SAP note 30289.

**How to run SAProuter with SNC connectivity**
Please be sure to generate and install the required SNC-certificate exactly as described in the online documentation found [here](#).

The online documentation also describes the structure of the SAPROUTTAB file for SNC connectivity.

For more information on connection types, [click here](#).

**How to Establish an Internet connection to SAP with VPN (pre-requisite network connection)**

Another way to establish an internet connection to SAP is Virtual Private Networks (VPN), which provide hardware-level encryption. VPN is a network that uses tunneling technique to transmit encrypted data from point to point over the public internet. A VPN provides hard data encryption at the hardware level. This approach requires a VPN switch (VPN gateway) at the customer side and at SAP as well as the SAPRouter software.

LAN-to-LAN IPSec VPNs are established between SAP and the customer's network to provide data confidentiality and integrity services. These VPNs complement the leased lines in the current Remote Customer Support Network environment.

Two official IP subnets. These IP subnets are assigned to:

1. The public interface of the VPN box. Additionally, this IP subnet must be routed in the Internet.
2. The customer’s SAProuter.

If the customer is operating any firewall(s) to secure its Internet connection, the firewall(s) must permit the edge VPN equipment to exchange IPsec packets using their respective public interfaces (the VPN gateway may also serve as the firewall). Specifically, the customer’s firewall must allow UDP port 500 (IKE) and IP Protocol 50 (ESP)

Recommended VPN equipment: SAP is using CISCO VPN equipment. Customers may also try to connect using other IPSec compliant VPN equipment. The equipment must support certain IPSec features (see Appendix A) that are mandatory to establish communication with SAP’s VPN equipment. SAP cannot guarantee interoperability between SAP’s CISCO VPN equipment and other types of VPN equipment that the customer elects to use instead. If you wish to use other VPN equipment, contact SAP.

**Mandatory IPSec Features (for the Internet VPN option)**

- Encapsulating Security Protocol (ESP)
- Internet Key Exchange (IKE), with support of Diffie-Hellman Group 2
- (1024 bits keys)
- Encryption Algorithm: Triples DES (3DES)
- Authentication Algorithm: HMAC-MD5 and HMAC-SHA1
- Support for authentication using shared secrets, RSA digital signatures, and X.509 certificates
- Support for Diffie-Hellman Group 2 (keys of 1024 bits)
- Perfect Forward Secrecy
- Key exchanges using Internet PKIs

For more information on connection types, click here.

How to setup the router permission table

See SAP Note - 30289 - SAProuter documentation.

How to run the SAProuter

**SAProuter software**

For older releases, you can also use the latest SAProuter (Release 7.20). It is provided on SAP Service Marketplace at http://support.sap.com/swdc under Support Packages and Patches
- Browser our Download Catalog
  - Entry by Application Group
  - Additional Components
    - SAPROUTER

Alternatively, you can click Software Download

**Supported operating systems**

The SAProuter supports all operating systems for which a kernel is also available.

**SAProuter Documentation**

You can find the documentation in the SAP Library, or in the Internet in the Help Portal at http://help.sap.com under:

SAP NetWeaver -> SAP NetWeaver Platform -> Application Help - Function-Oriented View -> Application Server -> Application Server Infrastructure -> Components of the SAP NetWeaver Application Server ABAP/Dual Stack ->
Remote Connection to SAP

A route is defined for SAProuter in the form of a route string, which must observe specific syntax rules. A route string contains an entry, or substring, for each SAProuter and for the target server. Each substring contains the information that SAProuter needs to make a connection in the route: the host name, the port name, and the password, if supplied.

A route string can look like this: `/H/host/S/service/P/pass`

Each substring begins with `/H/`, which indicates the host name. You can optionally specify a service after each host name. The service name is preceded by `/S/`. The substring can then include a password, which is preceded by `/P/`.

By default, route strings are sent without a password. The default value for service is "3299", and the default password is "" (empty).

The diagram below shows a sample connection between SAP and a customer system. In this example, an SAP service engineer working at sappc needs to log on to a customer application server yourapp, which offers or uses the service sapservice.

**Dial-in of an SAP employee into a customer system**

The SAP service engineer logs onto R/3 and connects sappc to yourapp via the SAProuter on saprouter and the customers SAProuter yoursaprouter.

yoursaprouter requires the password pass_to_app for connections to yourapp.

The route string looks like this: `/H/saprouter/H/yoursaprouter/H/yourapp/S/sapservice/P/pass_to_app`
This route string is interpreted by SAProuter as follows:

<table>
<thead>
<tr>
<th>Substring</th>
<th>Host/Address</th>
<th>Service/Port</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Substring 1</td>
<td>/H/saprouter</td>
<td>/S/default</td>
<td></td>
</tr>
<tr>
<td>Substring 2</td>
<td>/H/yoursaprouter</td>
<td>/S/default</td>
<td>&lt;no password&gt;</td>
</tr>
<tr>
<td>Substring 3</td>
<td>/H/yourapp</td>
<td>/S/sapservice</td>
<td>/P/pass_to_app</td>
</tr>
</tbody>
</table>

The connection from **sappc** to the application server is made in the following stages:

- **sappc** (frontend) builds the connection to the SAProuter on **saprouter** according to substring 1, and passes on the remainder of the route information.
- **SAProuter** checks whether the route **sappc** to **yoursaprouter, 3299** is permitted, builds the connection to the SAProuter on **yoursaprouter**, and passes on substring 3.
- **yoursaprouter** (SAProuter) checks whether the route **saprouter to yourapp, sapservice** is permitted. The password **pass_to_app** is also checked. SAProuter then builds the connection to the application server.

SAProuter always checks only the previous host name or IP address and the next substring (/H/.../S/.../P/...) for the host name or IP address, service and password. No password is used in the first substring, since the client is accessing itself.
If the /S/ part is missing, the default SAProuter port number is used.
If the /P/ part is missing, no password is used.

Storing logon data in the Secure Area

The secure area is an area in the SAP Support Portal where customer logon data (user name, password, server name etc.) for remote access is stored. Remote access is sometimes required by SAP Support employees when investigating customer incidents.

1. Authorization to create/change/display access data.

   - Maintain all Logon Data: You have full read and write access to all logon data of all your customers and you can store new logon data.
   - Maintain my Logon Data: If you have this authorization, you can store, view and change access data if you have stored it yourself. You cannot read passwords stored by others, but you can overwrite them.

2. How is the access data created?

   The management of access data for the remote logon to an SAP system has been system-based (and no longer incident-based) since the middle of March. Therefore you only have to store the access data once for each system, instead of once for each message.

   You can change the access data in the new Secure Area whenever you want. The system logs all data changes and access to the Secure Area in an action log. The SAP incident wizard shows you whether access data has been stored. In addition, you can use the system data application to manage the access data centrally.

   To create the access data, proceed as follows:

   You have two options:

   - Use the quick link or message to call the SAP incident assistant.
   - Select the system for which you want to create an incident.
   - Choose 'Maintain Access Data'.
   - In the new window that opens, select the system and then choose 'Change'. Enter all of the required logon data and then save the data.

OR
Use the quick link or system data to call the system data.

Important: To execute this function, you require the following authorization: Maintain System Data.

Pre-requisites to store logon data in the secure area

S-users with authorization *Maintain my Logon Data* can store logon data and display or change logon data they have stored previously. However, they cannot see the passwords entered by other users (but they can still change them).

S-users with authorization *Maintain all Logon Data* (e.g. supers-administrators) have full access to create/change/display all stored logon data of all S-users.

The processor at SAP who is investigating your message can also access and update the logon data. If the customer message is in process at SAP, your employees (those that have the Authorization object: *Maintain all Logon Data* or *Maintain my Logon Data*) can access the logon data.

How to access the Secure Area

- Click the *Change Access Data* button in the incident
- Centrally via the system data application by clicking *Access Data* button.

*Note:* The option to limit the view of SAP employees for certain incidents is only offered when the secure area has been accessed via a customer incident.

How to enter logon data in the Secure Area

Four buttons are provided on the entry page of the secure area for a selected system (called via customer message):

- **Modify**: Click to enter or change access data.
- **History Log**: All data changes and access to the secure area are tracked in the history log.
- **Close Window**: Close the Secure Area window.
- **Maintain User Restricted View**: Option to limit the user information seen by SAP employees for a certain message.

To maintain access data click **Modify** and enter all required access data for remote logon to an SAP system by using the tabs.

*Note: Save entries of each tab separately!*

Click *Display Logon Data* after having entered logon data: All entered logon data is shown at a glance in display mode. Only users that have maintained these data and users with *Maintain all Logon Data* authorization can see the stored passwords. For users with *Maintain my Logon Data* authorization the stored passwords of other colleagues are not visible, but can be changed.
How to limit what logon data SAP employees can see - Customer Message Restricted View

When creating or working on a customer incident, you are able to assign specific users stored in the secure area to a certain customer incident.

Therefore you can restrict the number of users visible to this specific incident for SAP incident processors. When creating a customer incident you have to save the incident in order to get access to the restricted view by clicking the button *Maintain User Restricted View*:

- This restriction refers to SAP system users only and will not affect any other users like SAPRouter user or user for additional servers.
- Also users from other systems or installations are selectable.
- If users are explicitly assigned to the incident, SAP will be able to see only those users that are part of this restricted list. All other users are not displayed.
- If no user is explicitly assigned to the message, there is no restriction regarding the visibility of the login information. All users and passwords are then visible by SAP.

**Note:** With this modification it is possible that customers can create a user for a system that is only valid for a specific customer incident. If the restricted view is created this will be indicated (after refresh) by an icon under the corresponding system by the incident number this view is built for.

You can delete a view which is valid for a specific customer incident by selecting all users in the view and clicking the *Delete View* button.

**IPv6**

SAP is currently in the process of changing the remote support infrastructure to support the IPv6 protocol. IPv6 is short for 'Internet Protocol Version 6'. IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4. One of the key features of IPv6 is its extra address space — from the IPv4’s 32 bits to 128 bits — which increases the number of available IP addresses from $4.0 \times 10^9$ to over $3.4 \times 10^{38}$ unique IP addresses. The current IPv4 address pool is almost completely exhausted. Very soon new users and devices will only be able to use unique IPv6 addresses on the internet. More information can be found at Wikipedia.

The remote support infrastructure of SAP will continue to support the IPv4 protocol for many years. No action is required for our current customers on IPv4 and we strongly recommend they continue to use IPv4 protocol to remotely connect to SAP.

The infrastructure to support the IPv6 protocol at SAP is currently being developed. Detailed instructions of how to set up an IPv6 remote connection to SAP will be provided when the functionality is available for customers to use. In the future, the option ‘Use IPv6’ in the System Data Maintenance section of the SAP Support Portal will control which
protocol version will be used in establishing a remote connection. Please do not set this option to “YES” until further notice.

Getting Help

If you have any questions or problems installing, running or setting up SAProuter or problems with the connectivity, please open an incident in the SAP Support Portal using component XX-SER-NET-NEW and describe the problem at hand with as much background as possible and one of SAP’s external partner companies will assist you. If you have any questions about maintaining your system data in the SAP Support Portal, log an incident using component XX-SER-SAPSMP-SYS to get help.

Internet Connections

Access Support

SAP customers can receive services and support from SAP remotely over special connections. Until now these remote connections have been either dial-up connections or leased lines. As of now SAP offers a new cost-effective and more flexible alternative: Internet connections which provide the high level of security that is essential for Internet communications. All you need is a connection from your local area network (LAN) to the Internet.

Two Alternatives

Customers can establish Internet connections in two ways:

- Secure network communication (SNC) via SAProuter software to deliver software encryption
- Virtual private networks (VPN), which provide hardware-level encryption

Both options use three types of security measures to protect your systems and data from unauthorized access:

- State-of-the-art encryption
- Server authentication
- Access-control technology

SNC connections are established between two SAProuters. They require no additional hardware, but additional software has to be installed. You can download this software directly from the SAP Service Marketplace.

For the VPN approach a VPN switch is required at the customer site and at SAP. You will find more information on the technical requirements and the mode of operation of both encryption methods in the Technical Specifications (Adobe PDF).

Your Benefits

Using the latest Internet technology offers clear benefits for the customer:
Lower costs through lower rates for Internet connections
Access any time, anywhere an Internet connection is available
High security level due to SNC or VPN
Easy to handle and to maintain
Low hardware requirements

If you are interested in establishing your Internet connection to SAP, set up an Internet connection and then contact the relevant network connection consulting company. If you already have an Internet connection, you may use this existing connection to establish a secure communication channel to SAP.

How to Install SAProuter (Please see Register your SAProuter with SAP first)

Ensure that you have completed the perquisites prior installing and the SAProuter. If you have done so and have an established connection please continue to install and configure SAProuter. You have a choice of following either a video of the steps for downloading and installing SAProuter, or a technical brief.

To install SAProuter you need both the SAProuter software and the SAPCAR software that is used to unpack the software bundle. The SAProuter and SAPCAR software are available to download on Service Marketplace.

2. Click on ‘Support Packages and Patches’.
3. Click on ‘Browse our Download Catalog’.
4. Click on ‘Technology Components’.
5. Click on ‘SAPROUTER’ to download it or add to your download basket.
6. Click on ‘SAPCAR’ to download it or add to your download basket.
7. Choose your operating system. It is recommended that you always download the newest SAProuter version for your operating system.
8. Create a subfolder called saprouter on your local drive in the location <drive>\usr\sap.
9. Save both the downloaded .SAR file for SAProuter and the executable for SAPCAR in the new folder.
10. To extract the SAProuter software, open a command line prompt and run the command:

```
SAPCAR -xvf "<path of xxxxxxx.SAR>"
```

Ensure double quotes are placed before and after the .SAR file. The following files should populate the saprouter folder after extraction.

Niping.exe, saprouter.exe

Download and Install SAProuter