PHILIPS Diktieren
OLYMPUS
Dragon
SONIC LABS
EINZIGARTIG IN BERLIN
- IN STUTTGART ZUHAUSE
Danke, dass Sie uns besucht haben !

SpeechExec Enterprise service communication overview

Table of Contents

1 General requirements 4

1.1 Active Directory environment 4

1.2 Service / Web Service ‘run as user’ 4

1.3 File share requirements 4

1.3.1 SEERoot file share 4

1.3.2 Dictations file share 4

1.4 Microsoft SQL Server requirements 4

2 SpeechExec Enterprise License Server 6

2.1 Incoming ports for License Server 6

2.1.1 License Server communication 6

2.2 Outgoing ports for License Server 6

2.2.1 Workflow Manager health scanning (optional) 6

2.2.2 Mobile service and Legacy mobile server health scanning (optional) 6

2.2.3 Email sending (optional) 6

3 SpeechExec Enterprise Mobile Service 7

3.1 Incoming ports for Mobile Service 7

3.1.1 Mobile Service communication 7

3.2 Outgoing ports for Mobile Service 7

3.2.1 License Server communication 7

3.2.2 SpeechLive Service communication (optional) 7

3.3 Active Directory access 7

3.4 SEERoot access 7

3.5 Dictations file share access 7

4 SpeechExec Enterprise SpeechLive Service 8

4.1 Incoming ports for SpeechLive Service 8

4.1.1 SpeechLive Service communication 8

4.2 Outgoing ports for SpeechLive Service 8

4.2.1 License Server communication 8

4.2.2 SpeechLive communication 8

4.3 Microsoft SQL Server access 8

4.4 Active Directory access 8

4.5 SEERoot access 8

4.6 Dictations file share access 8
5 SpeechExec Enterprise WebAccess 9
5.1 Incoming ports for WebAccess 9
5.1.1 WebAccess communication 9
5.2 Outgoing ports for WebAccess 9
5.2.1 License Server communication 9
5.2.2 SpeechLive Service communication (optional) 9
5.3 Active Directory access 9
5.4 SEERoot access 9
5.5 Dictations file share access 9
6 Communication overview diagrams 10
6.1 Full overview 10
6.2 Mobile Service specific (limited) overview 11
7 Appendix 12
7.1 Appendix I - How to configure a firewall for Active Directory domains and trusts 12
7.1.1 Please note that any information stored in this document might have changed since, is provided *as is* without any support.Retrieved content 12

1 General requirements

1.1 Active Directory environment

The SpeechExec Enterprise web service suite components are using Active Directory for authentication / authorization of certain actions. The functionality required to be accessible:

- Group membership (authorization)
- Friendly name lookup (ease of use / personalization)
- Login (authentication)

For reference on Active Directory related port configuration on firewalls, we recommend visiting the official Microsoft configuration guide:
https://support.microsoft.com/en-us/help/179442/how-to-configure-a-firewall-for-domains-and-trusts

For reference purposes, the content of the Microsoft guide linked above retrieved on 2020-04-07 can be found in *Appendix I - How to configure a firewall for Active Directory domains and trusts*. Please note that any information stored in this document might have changed.

1.2 Service / Web Service 'run as user'

Each service / web service (IIS Web Service) requires a 'run as user' (dedicated service user) with access to all of the file shares detailed below and in case of services that require database access, the right to read / write the configured database tables (SEERoot, user dictation folders, database).

1.3 File share requirements

For a reference on file share related port configuration on firewalls, we recommend visiting the official Microsoft configuration guide:
https://support.microsoft.com/en-us/help/298804/internet-firewalls-can-prevent-browsing-and-file-sharing

1.3.1 SEERoot file share

The SpeechExec Enterprise web service suite components also require access to the file share where the SEERoot is located (configurable in every service). Make sure the 'run as user' or 'application pool user' has access and read/write rights to this SEERoot shared folder.

Ideally, this file share is accessible with an UNC path
(e.g.: \\fileserver\SpeechExec\SEERoot)

1.3.2 Dictations file share

The service 'run as user' must also have access to the dictation file share (where user finished folders are located).

Ideally, this file share is accessible with an UNC path
(e.g.: \\fileserver\SpeechExec\Dictations\%user%\%folderName%)

1.4 Microsoft SQL Server requirements

Enterprise SpeechLive Service requires access to a Microsoft SQL Server installation and appropriate rights to create, read / write data to a pre-configured database (Configuration can be done from Enterprise Manager's SpeechLive Service specific configuration)

For a reference on Microsoft SQL Server related port configuration on firewalls, we recommend visiting the official Microsoft configuration guide: https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15

2 SpeechExec Enterprise License Server

2.1 Incoming ports for License Server

2.1.1 License Server communication

DEFAULT: **13667 TCP**

- The main communication port of license server, required for all licensing operations
- Configurable in Registry under the following key:
  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\
  Philips Speech\SpeechExec\EnterpriseLicenseServer]
  ```
  Editing the “Port” REG_DWORD value
- The License Server must be restarted for the changes to apply

2.2 Outgoing ports for License Server

2.2.1 Workflow Manager health scanning (optional)

DEFAULT: **49256 TCP, 80 HTTP**

- Required for health scanning requests initiated by the License Server towards the Workflow Manager (if configured)
- Configurable in the Enterprise License Manager application (*Email notifications -> Health scanner notifications* tab)

2.2.2 Mobile service and Legacy mobile server health scanning (optional)

DEFAULT: **80 HTTP**

- Required for health scanning requests initiated by the License Server towards the configured service type (usually Mobile service or Legacy MobileServer)
- Configurable in the Enterprise License Manager application (*Email notifications -> Health scanner notifications* tab) by adding a new service health scan item in the list and ticking the ‘Enabled’ checkbox. The configurable URL must contain the desired port.

2.2.3 Email sending (optional)

DEFAULT: **587, 25 SMTP**

- If used, the License Server can send various emails via the SMTP server configured in the Enterprise License Manager application (*Email notifications)*

3 SpeechExec Enterprise Mobile Service

3.1 Incoming ports for Mobile Service

3.1.1 Mobile Service communication

DEFAULT: **80 HTTP, 443 HTTPS**

- Enterprise Mobile Service must be able to accept HTTP/HTTPS requests from the configured mobile applications (PVR for iOS, PVR for Android) or compatible recorder devices (e.g.: SpeechOne).
- The HTTP/HTTPS binding can be configured in the web.config file of the IIS webservice (preferably through the Internet Information Service (IIS) Manager)

3.2 Outgoing ports for Mobile Service

3.2.1 License Server communication

DEFAULT: **13667 TCP**

- Enterprise Mobile Service needs to get licenses from the License Server
- License Server requirements and configuration described in SpeechExec Enterprise License Server

3.2.2 SpeechLive Service communication (optional)

DEFAULT: **80 HTTP, 443 HTTPS**

- Enterprise Mobile Service can send dictations (optionally) to SpeechLive through SpeechLive Service (web service). For this communication the defined SpeechLive Service (web service) port is required to be open. Details in SpeechExec Enterprise SpeechLive Service

3.3 Active Directory access

Detailed in Active Directory environment

3.4 SEERoot access

Detailed in SEERoot file share

3.5 Dictations file share access

Detailed in Dictations file share

4 SpeechExec Enterprise SpeechLive Service

4.1 Incoming ports for SpeechLive Service

4.1.1 SpeechLive Service communication

DEFAULT: **80 HTTP, 443 HTTPS**

- Enterprise SpeechLive Service must be able to accept HTTP/HTTPS requests from the connected services (SpeechExec Enterprise Mobile Service, SpeechExec Enterprise WebAccess, etc.)
- The HTTP/HTTPS binding can be configured in the web.config file of the IIS webservice (preferably through the IIS Manager)

4.2 Outgoing ports for SpeechLive Service

4.2.1 License Server communication

DEFAULT: **13667 TCP**

- Enterprise SpeechLive Service needs to get licenses from the License Server
- License Server requirements and configuration described in SpeechExec Enterprise License Server

4.2.2 SpeechLive communication

DEFAULT: **443 HTTPS**

- Enterprise SpeechLive Service sends dictations to SpeechLive (cloud system). To be able to communicate with SpeechLive, it must have Internet access towards the hardcoded SpeechLive URL (by default through 443 HTTPS): **livebroker.speechexec.com**

4.3 Microsoft SQL Server access

- Enterprise SpeechLive Service stores SpeechLive dictation references in a (pre-configured) database for status updates and upload / download operations. The service 'run as user' must be able to create, read / write to and from this SQL Server's pre-configured database
- The configuration can be done via SpeechExec Enterprise Manager from the 'SpeechLive Service' main node after adding a new SpeechLive service connection. Inside the configuration editor (after pressing connect) on the SQL setup page
- For more details on the SQL Server requirement, refer to Microsoft SQL Server requirements

4.4 Active Directory access

Detailed in Active Directory environment

4.5 SEERoot access

Detailed in SEERoot file share

4.6 Dictations file share access

Detailed in Dictations file share

5 SpeechExec Enterprise WebAccess

5.1 Incoming ports for WebAccess

5.1.1 WebAccess communication

DEFAULT: **80 HTTP, 443 HTTPS**

- Enterprise WebAccess service must be able to accept HTTP/HTTPS requests from the clients (browsers) of the users

The HTTP/HTTPS binding can be configured in the web.config file of the IIS webservice (preferably through the IIS Manager)

5.2 Outgoing ports for WebAccess

5.2.1 License Server communication

DEFAULT: **13667 TCP**

- Enterprise WebAccess needs to get licenses from the License Server
- License Server requirements and configuration described in SpeechExec Enterprise License Server

5.2.2 SpeechLive Service communication (optional)

DEFAULT: **80 HTTP, 443 HTTPS**

- Enterprise WebAccess can send dictations (optionally) to SpeechLive through SpeechLive Service (web service). For this communication the defined SpeechLive Service (web service) port is required to be open. Details in SpeechExec Enterprise SpeechLive Service

5.3 Active Directory access

Detailed in Active Directory environment

5.4 SEERoot access

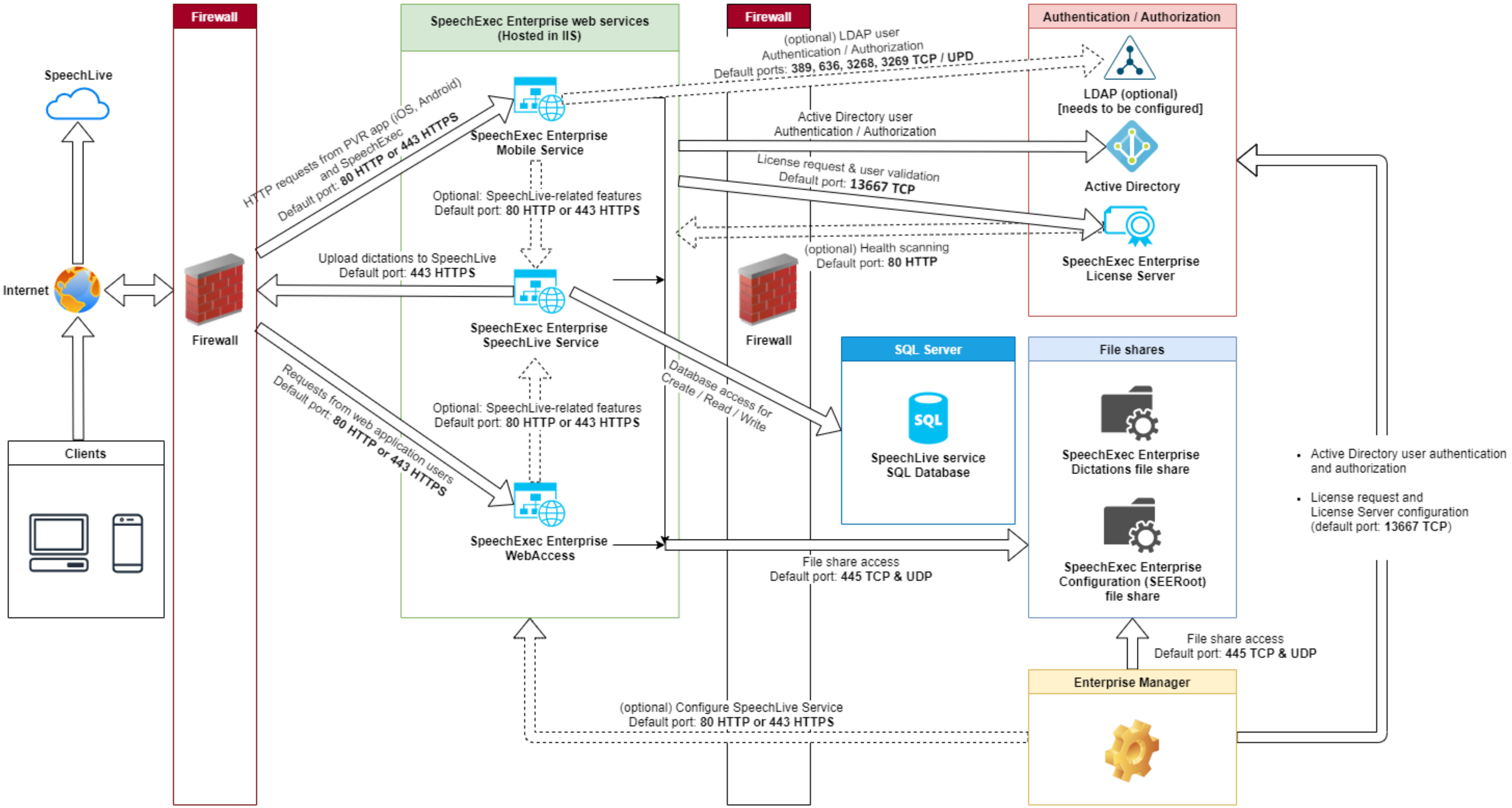
Detailed in SEERoot file share

5.5 Dictations file share access

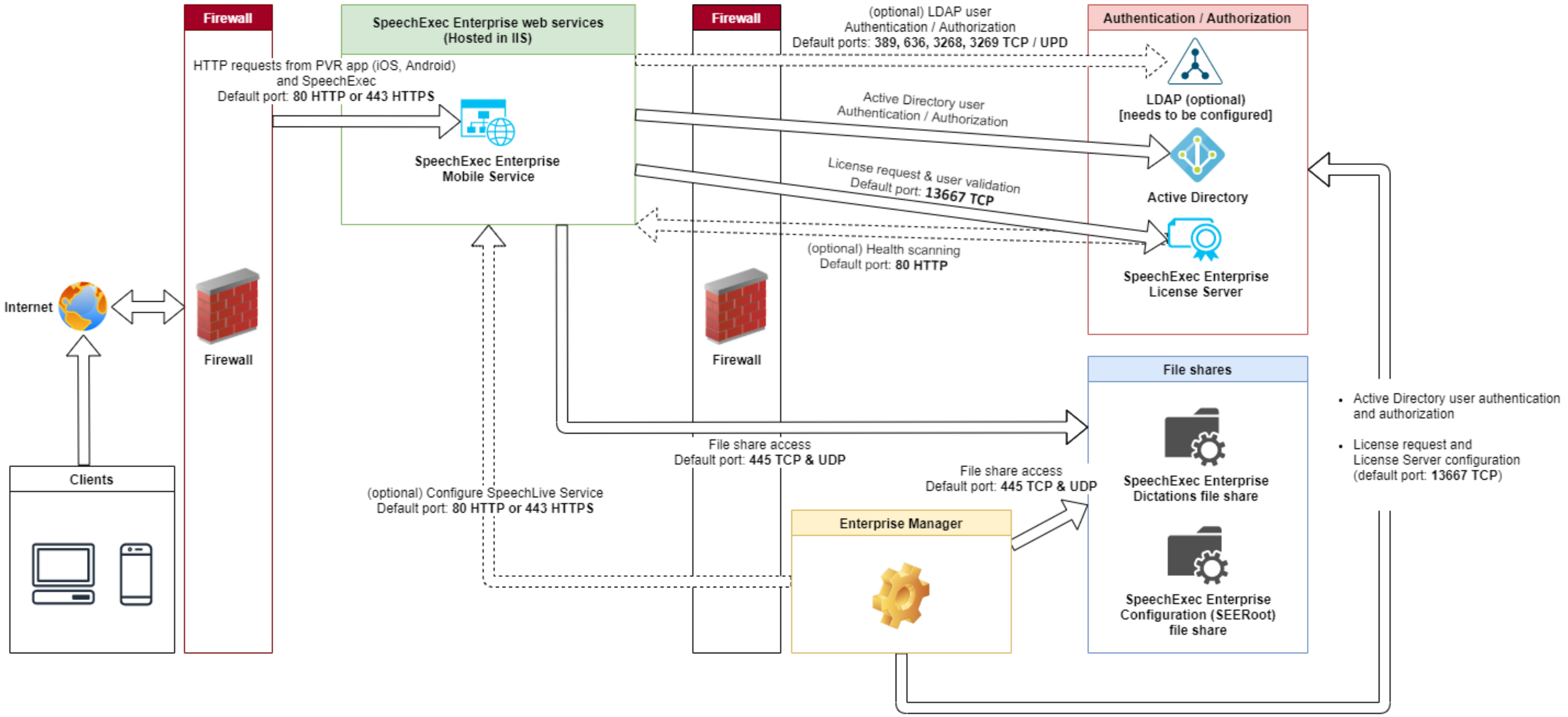
Detailed in Dictations file share

6 Communication overview diagrams

6.1 Full overview


SpeechLive
Internet
Clients
Firewall
Firewall
SpeechExec Enterprise web services
(Hosted in IIS)
HTTP requests from PVR app (iOS, Android)
and SpeechExec
Default port: 80 HTTP or 443 HTTPS
SpeechExec Enterprise
Mobile Service
Optional: SpeechLive-related features
Default port: 80 HTTP or 443 HTTPS
Upload dictations to SpeechLive
Default port: 443 HTTPS
SpeechExec Enterprise
SpeechLive Service
Optional: SpeechLive-related features
Default port: 80 HTTP or 443 HTTPS
Requests from web application users
Default port: 80 HTTP or 443 HTTPS
SpeechExec Enterprise
WebAccess
Firewall
Firewall
(optional) LDAP user
Authentication / Authorization
Default ports: 389, 636, 3268, 3269 TCP / UPD
Active Directory user
Authentication / Authorization
License request & user validation
Default port: 13667 TCP
(optional) Health scanning
Default port: 80 HTTP
Database access for
Create / Read / Write
File share access
Default port: 445 TCP & UDP
Authentication / Authorization
LDAP (optional)
[needs to be configured]
Active Directory
SpeechExec Enterprise
License Server
SQL Server
SQL
SpeechLive service
SQL Database
File shares
SpeechExec Enterprise
Dictations file share
SpeechExec Enterprise
Configuration (SEERoot)
file share
File share access
Default port: 445 TCP & UDP
Enterprise Manager
(optional) Configure SpeechLive Service
Default port: 80 HTTP or 443 HTTPS
• Active Directory user authentication
and authorization
• License request and
License Server configuration
(default port: 13667 TCP)

6.2 Mobile Service specific (limited) overview


Firewall
SpeechExec Enterprise web services
(Hosted in IIS)
Firewall
(optional) LDAP user
Authentication / Authorization
Default ports: 389, 636, 3268, 3269 TCP / UPD
Authentication / Authorization
HTTP requests from PVR app (iOS, Android)
and SpeechExec
Default port: 80 HTTP or 443 HTTPS
LDAP (optional)
[needs to be configured]
Active Directory user
Authentication / Authorization
SpeechExec Enterprise
Mobile Service
Active Directory
License request & user validation
Default port: 13667 TCP
SpeechExec Enterprise
License Server
(optional) Health scanning
Default port: 80 HTTP
Internet
Firewall
Firewall
File shares
Active Directory user authentication and authorization
License request and License Server configuration (default port: 13667 TCP)
File share access
Default port: 445 TCP & UDP
Clients
SpeechExec Enterprise
Dictations file share
File share access
Default port: 445 TCP & UDP
(optional) Configure SpeechLive Service
Default port: 80 HTTP or 443 HTTPS
Enterprise Manager
SpeechExec Enterprise
Configuration (SEERoot)
file share

7 Appendix

7.1 Appendix I - How to configure a firewall for Active Directory domains and trusts

For reference purposes, this appendix contains the content of the following Microsoft guide, retrieved on 2020-04-07: https://support.microsoft.com/en-us/help/179442/how-to-configure-a-firewall-for-domains-and-trusts

7.1.1 Please note that any information stored in this document might have changed since, is provided *as is* without any support.Retrieved content

** * * START OF RETRIEVED CONTENT * * **

Applies to: Windows Server 2008 Standard, Windows Server 2008 R2 Standard, Microsoft Windows Server 2003 Standard Edition (32-bit x86), Windows Server 2012 R2 Standard, Windows Server 2012 Standard, Windows Server 2016, Windows Server 2019

7.1.1.1 Summary

This article describes how to configure a firewall for Active Directory domains and trusts.

Note:

Not all the ports that are listed in the tables here are required in all scenarios. For example, if the firewall separates members and DCs, you don't have to open the FRS or DFSR ports. Also, if you know that no clients use LDAP with SSL/TLS, you don't have to open ports 636 and 3269.

7.1.1.2 More Information

Note:

The two domain controllers are both in the same forest, or the two domain controllers are both in a separate forest. Also, the trusts in the forest are Windows Server 2003 trusts or later version trusts.

Client Port(s)	Server Port	Service
1024-65535/TCP	135/TCP	RPC Endpoint Mapper
1024-65535/TCP	1024-65535/TCP	RPC for LSA, SAM, Netlogon (*)
1024-65535/TCP/UDP	389/TCP/UDP	LDAP
1024-65535/TCP	636/TCP	LDAP SSL
1024-65535/TCP	3268/TCP	LDAP GC
1024-65535/TCP	3269/TCP	LDAP GC SSL
53,1024-65535/TCP/UDP	53/TCP/UDP	DNS
1024-65535/TCP/UDP	88/TCP/UDP	Kerberos
1024-65535/TCP	445/TCP	SMB
1024-65535/TCP	1024-65535/TCP	FRS RPC (*)

NETBIOS ports as listed for Windows NT are also required for Windows 2000 and Windows Server 2003 when trusts to domains are configured that support only

NETBIOS-based communication. Examples are Windows NT-based operating systems or third-party Domain Controllers that are based on Samba.

(*) For information about how to define RPC server ports that are used by the LSA RPC services, see the following Microsoft Knowledge Base articles:

- 224196: Restricting Active Directory replication traffic and client RPC traffic to a specific port
- "Domain controllers and Active Directory" section in 832017: Service overview and network port requirements for the Windows Server system

7.1.1.2.1 Windows Server 2008 and later versions

Windows Server 2008 newer versions of Windows Server have increased the dynamic client port range for outgoing connections. The new default start port is 49152, and the default end port is 65535. Therefore, you must increase the RPC port range in your firewalls. This change was made to comply with Internet Assigned Numbers Authority (IANA) recommendations. This differs from a mixed-mode domain that consists of Windows Server 2003 domain controllers, Windows 2000 Server-based domain controllers, or legacy clients, where the default dynamic port range is 1025 through 5000.

For more information about the dynamic port range change in Windows Server 2008, Windows Server 2012 and Windows Server 2012 R2, see the following resources:

- Microsoft Knowledge Base article 929851: The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008
- Ask the Directory Services Team blog article Dynamic Client Ports in Windows Server 2008 and Windows Vista

Client Port(s)	Server Port	Service
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	RPC Endpoint Mapper
49152 -65535/TCP	464/TCP/UDP	Kerberos password change
49152 -65535/TCP	49152-65535/TCP	RPC for LSA, SAM, Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	636/TCP	LDAP SSL
49152 -65535/TCP	3268/TCP	LDAP GC

49152 -65535/TCP	3269/TCP	LDAP GC SSL
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB (**)
49152 -65535/TCP	49152-65535/TCP	DFSR RPC (*)

NETBIOS ports as listed for Windows NT are also required for Windows 2000 and Server 2003 when trusts to domains are configured that support only NETBIOS-based communication. Examples are Windows NT-based operating systems or third-party Domain Controllers that are based on Samba.

(*) For information about how to define RPC server ports that are used by the LSA RPC services, see the following Microsoft Knowledge Base articles:

- 224196: Restricting Active Directory replication traffic and client RPC traffic to a specific port
- "Domain controllers and Active Directory" section in 832017: Service overview and network port requirements for the Windows Server system

(**) For the operation of the trust this port is not required, it is used for trust creation only.

Note

External trust 123/UDP is only needed if you have manually configured the Windows Time Service to Sync with a server across the external trust.

7.1.1.2.2 Active Directory

In Windows 2000 and Windows XP, the Internet Control Message Protocol (ICMP) must be allowed through the firewall from the clients to the domain controllers so that the Active Directory Group Policy client can function correctly through a firewall. ICMP is used to determine whether the link is a slow link or a fast link.

In Windows Server 2008 and later versions, the Network Location Awareness Service provides the bandwidth estimate based on traffic with other stations on the network. There is no traffic generated for the estimate.

The Windows Redirector also uses ICMP Ping messages to verify that a server IP is resolved by the DNS service before a connection is made, and when a server is located by using DFS.

If you want to minimize ICMP traffic, you can use the following sample firewall rule:

```
<any> ICMP -> DC IP addr = allow
```

Unlike the TCP protocol layer and the UDP protocol layer, ICMP does not have a port number. This is because ICMP is directly hosted by the IP layer.

By default, Windows Server 2003 and Windows 2000 Server DNS servers use ephemeral client-side ports when they query other DNS servers. However, this behavior may be changed by a specific registry setting. For more information, see Microsoft Knowledge Base article 260186: SendPort DNS registry key does not work as expected

For more information about Active Directory and firewall configuration, see the Active Directory in Networks Segmented by Firewalls Microsoft white paper.

Or, you can establish a trust through the Point-to-Point Tunneling Protocol (PPTP) compulsory tunnel. This limits the number of ports that the firewall has to open. For PPTP, the following ports must be enabled.

Client Ports	Server Port	Protocol
1024-65535/TCP	1723/TCP	PPTP

In addition, you would have to enable IP PROTOCOL 47 (GRE).

Note

When you add permissions to a resource on a trusting domain for users in a trusted domain, there are some differences between the Windows 2000 and Windows NT 4.0 behavior. If the computer cannot display a list of the remote domain's users, consider the following behavior:

- Windows NT 4.0 tries to resolve manually-typed names by contacting the PDC for the remote user's domain (UDP 138). If that communication fails, a Windows NT 4.0-based computer contacts its own PDC, and then asks for resolution of the name.
- Windows 2000 and Windows Server 2003 also try to contact the remote user's PDC for resolution over UDP 138. However, they do not rely on using their own PDC. Make sure that all Windows 2000-based member servers and Windows Server 2003-based member servers that will be granting access to resources have UDP 138 connectivity to the remote PDC.

7.1.1.2.3 Reference

832017: Service overview and network port requirements for the Windows Server system is a valuable resource outlining the required network ports, protocols, and services that are used by Microsoft client and server operating systems, server-based programs, and their subcomponents in the Microsoft Windows Server system. Administrators and support professionals may use this Microsoft Knowledge Base article

as a roadmap to determine which ports and protocols Microsoft operating systems and programs require for network connectivity in a segmented network.
You should not use the port information in KB article 832017 to configure Windows Firewall. For information about how to configure Windows Firewall, see the following Microsoft website:

Networking and Access Technologies: Windows Firewall

Last Updated: Apr 16, 2019

** * * END OF RETRIEVED CONTENT * * **

DIKTAT - STUTTGART
ppm-stuttgart Diktiersysteme

www.DIKTAT-STUTTGART.de Telefon: 0711 / 34 16 93-60

Dieses Dokument wurde heruntergeladen
bei www.DIKTAT-STUTTGART.de

Für die Richtigkeit der im Dokument angegebenen Daten, haftet ausschließlich der angegebene Hersteller.

Gerne dürfen Sie uns jederzeit wieder besuchen oder bei Fragen auch telefonisch kontaktieren.

Mit freundlichen Grüßen
Ihr Team von
DIKTAT-STUTTGART
ppm-stuttgart ● Diktiersysteme
Friedrichstraße 18 – 22, 70736 Fellbach

Tel.: 0711 / 34 16 93- 60
Fax: 0711 / 34 16 93- 66
e-mail: ppm@ppm-stuttgart.de

Sie haben Fragen ?

Sprechen Sie uns einfach an.
Wir stehen Ihnen jederzeit
gerne zur Verfügung.

Büro Stuttgart
Andreas Ester
GF & Kundenbetreuung
Telefon 0711 - 34 16 93 60

Büro Berlin
Alexander Schnell
Key-Account Manager Diktierlösungen
Telefon 0711 - 34 16 93 63