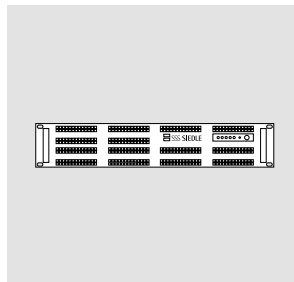
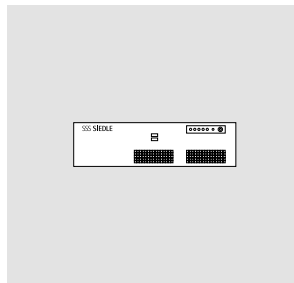


Commissioning instruction  
**Access Professional V 4...**  
**ASH 670-04 S**  
**ASH 670-04 M**



# Contents

This document is used as a guideline for commissioning of Access Professional in an independent network and is designed to provide a brief overview of the most important points to be observed during initial commissioning. Please note that this document cannot cover all possible questions arising from the commissioning of your Access system. This document cannot replace an intensive advanced training course.

This document supplements and is supplemented by the Planning and System Manual Access Professional. In addition to this document, you will find the current valid issue of the entire documentation in the download area under [www.siedle.com](http://www.siedle.com)

## Direct entry point for advanced users

**1** Access Professional – New Installation on customer hardware: from page 18

**2** System update to Access Professional V. 4...: from page 74

**3** System upgrade to Access Professional V. 4...: from page 17

**4** Setting up Access Professional: from page 80

<b>Safety remarks</b>	4	<b>Commissioning</b>	
<b>Important changes</b>	5	Commissioning requirements	13
<b>System overview</b>	6	Connecting and switching on the server hardware	13
Access server variant	7	Recommended commissioning sequence	14
Minimum requirements	8	Commissioning possibilities	16
System conditions	9	Device-specific settings	16
Access Professional	9	System version and network configuration	17
Virtualization	9	<b>Setting up the server operating system</b>	18
Additional requirements imposed on virtualization	9	Assigning the static IP address	20
<b>Licences and test period</b>	10	Setting up and configuring the DHCP server service	22
<b>Maintenance agreements</b>	11	Configuring the DHCP options	50
<b>Apple Push Notification Service (APNS)</b>	12	Changing the server configuration	64
<b>Time synchronisation in the Access system (NTP server)</b>	12	<b>Installing the Access system</b>	66
<b>Connection to telephone systems</b>	12	<b>Optionally: Updating the Access system</b>	74
		<b>Optionally: Uninstalling the Access system</b>	77

<b>Setting up the Access system</b>		<b>Configure devices</b>	124	<b>Final assignments</b>	151
Getting started	80	Device types	124	<b>Optional administration functions</b>	152
Firewall – Necessary ports	81	Virtual device	124	Reboot / shut down	152
Firewall – Video multicast IP addresses	82	ATLC 670-...	125	System version	154
Accessing the Access system	83	AHF/AHFV/AHT/AHTV 870-...	128	System backup	155
Log in	84	AVP 870-...	131	Saving the protocol	158
Licence agreements	84	Button configuration	131	View user status	159
User interface language	85	ASC 170-...	135	System characteristics	160
Changing the password	85	ASHT 170-...	136	<b>Connecting to external networks</b>	161
Safety code	86	ASM 170-...	137	<b>Index</b>	164
Navigation	87	Siedle app for Access Professional	138	<b>As-delivered status / Factory settings</b>	166
Menu structure Access Professional	87	Siedle App for Access Professional for Android panels	139		
Configuring the basic parameters	90	SIP video telephone	140		
Server	90	SIP audio telephone	141		
Configuring the server functions	94	External telephone	142		
Ordering Access licences	96	Virtual device	143		
Configuring the folder and user structure	111	<b>Telephony routes</b>	144		
Differentiation between users and call groups	112	<b>Roles and user accounts</b>	145		
Creating and configuring new folders	113				

We accept no liability for modifications / additions, mistakes or printing errors.

Access Service Center in the  
Furtwangen factory  
Tel. +49 7723 63-540  
access@siedle.de

## Safety remarks

### Observe the safety instructions!

Read and observe the safety instructions and content of the following supplied documents before using the Access server hardware for the first time:

- Product information
- Access Server hardware
- Planning and System Manual Access Professional
- These commissioning instructions

Explain the content of the safety instructions and dangers inherent in using technically complex products to children and those requiring assistance in a way that is easily understandable.

### Electrical voltage



Mounting, installation and servicing work on electrical devices may only be performed by a suitably qualified electrician.

### Devices with 230 V connection

In accordance with DIN VDE 0100 part 410, section 411.1.3 attention must be paid to ensuring a safe separation between system lines and the mains voltage; i.e. system and mains cores must not be permitted to touch! The system line cable (extra-low safety voltage) must be stripped back by the minimum possible.

### System update



During the update process, the power supply to the devices must not be interrupted, as this can result in damage. In this case, a repeat update is no longer possible, and the devices will have to be sent in for repair.

### User access and passwords for the Access system

Siedle Access and the server operating system are delivered with standard passwords. Issue new and secure passwords and keep these in a safe location. Forgotten passwords of the Access server and the server operating system cannot be restored and the server operating system would have to be reinstalled and commissioned.

**All user access codes and passwords are within the sphere of responsibility of the installer/operator/customer.**

### Protect your property!

The Siedle App can be used from any location as a door release! Keep smartphones/tablets on which the Siedle App is activated safe from theft. Protect these devices against unauthorized usage with a code/password/fingerprint. Always use the latest protection mechanisms available for your smartphone/tablet.

### Protect your network!

Only use up-to-date components and terminals in the network in line with the latest state of the art. Regularly update the operating systems of all components and terminals. Exchange obsolete components and terminals for up-to-date models. Use professional protective software (antivirus, firewall, ...) in all terminals. Issue secure passwords. Secure your network with the highest security standards available in the network. Protect your network against unauthorized attack from inside and outside.

### Legal notice

Photographs of individuals taken without their knowledge may not be published or stored in publicly accessible video memory facilities.

Individuals who have been photographed without their knowledge are entitled to request that pictures be deleted based on the right of persons to their own likeness. Never store pictures of persons you do not know in social networks or send them by email to others/public groups. This will infringe their personal rights.

If stored images are used as part of private / criminal law proceedings or in a police investigation, this requires prior clarification with a lawyer or the responsible police authority. Systems with video cameras which are operated within the European Union and are aimed at a publicly accessible area or part of one, and film and record this, are subject to the EU General Data Protection Regulation (EU GDPR) as of May 25, 2018. It is the sole responsibility of the operator to operate such systems in accordance with data protection regulations.

### Servicing

Statutory warranty conditions apply. If the device requires servicing, contact your specialist dealer or electrical installer.

# Important changes

## Access system version

---

since V 4.0.0

- Test period: A 30-day test period begins from initial commissioning, during this time all system functions can be used without any restrictions. In this way, customers can learn about other Access products (e.g. apps or software products). For detailed information, see page 10.
- 

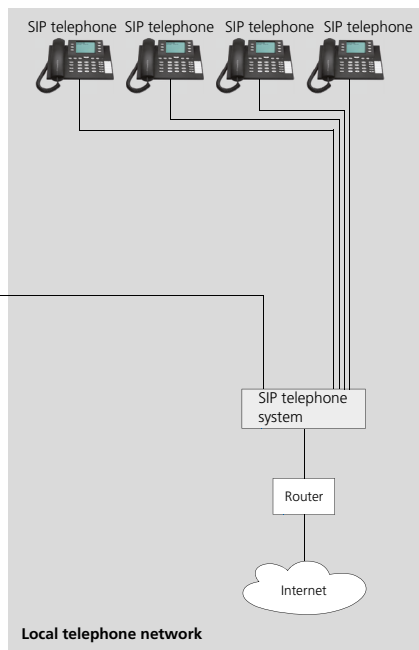
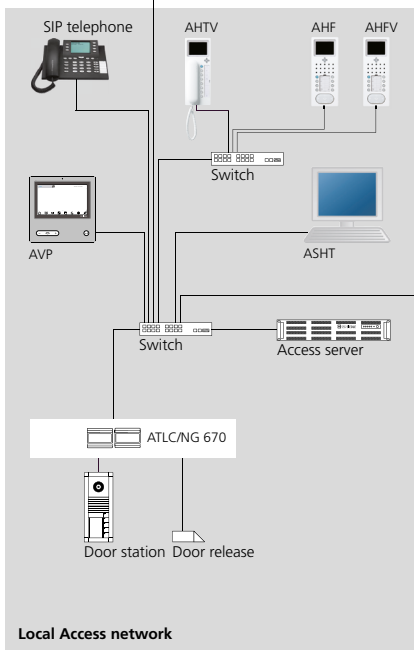
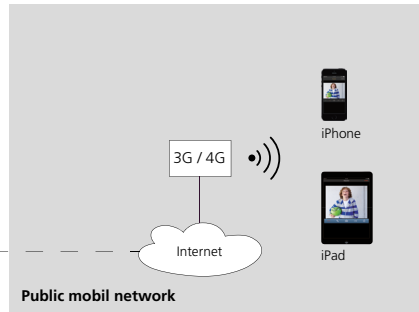
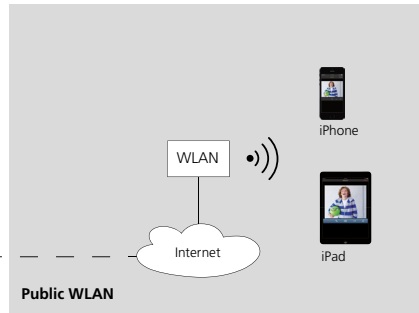
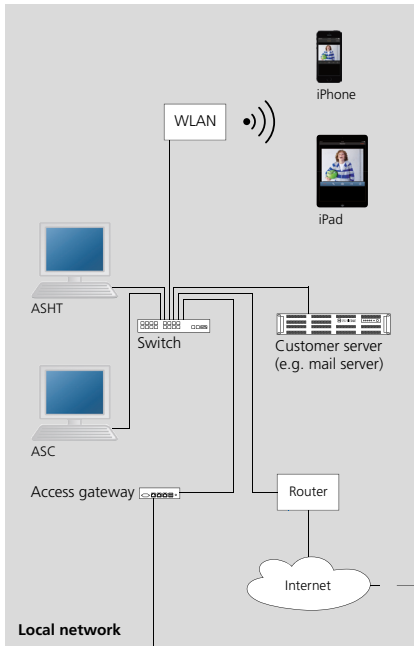
V 4.2.0

- Access Professional V. 4.2.0 includes the following new features:
- With the change to the iOS 11 operating system, apps on mobile iOS end devices can now only be addressed via the “Apple Push Notification Service” (APNS). For the APNS, a permanent internet connection is needed for both the sender (Access Server) and the recipient (Siedle app) of a notification, even if the app is only run in the local WLAN. For this, the DNS server and the standard gateway must be configured in the LAN/WLAN and the Access Server and Siedle app must be known. Local stand-alone operation with apps without connection to the Internet is no longer supported by iOS 11. With the switch to APNS, there is no longer a Siedle app call function (if there is no network connection, no telephone connection is established). From Access Professional V. 4.2.0 and the Siedle app for Access V. 2.2.0, connection to the APNS is included. Access system version 4.2.0 is required for app version 2.2.0 and vice-versa.
  - Siedle App für Access: Quiet mode has been added to the Siedle app. When quiet mode is activated, the Siedle app does not signal incoming push notifications.
  - For JUNG touchpanels (Smart Control...): For connecting and operating touch panels on the Access system. An “ALFP 270-0 Access licence for third-party panel device” is required for each touchpanel that is to be operated on the Access system.
  - The JUNG building automation server (Smart Visu Server) can be integrated and operated via the Access video panel. Please note that the building automation server is not a constituent part of the Siedle Access system. Advisory services and the sale of hardware and licences take place exclusively through ALBRECHT JUNG GmbH & Co. KG.
- 

V 4.0.0

- From Access V 4.0.0, the system is called Access Professional and includes the following new features:
- Access Professional as a pure software solution can now be optionally operated on a server made available by the customer or in a virtual machine (from VMware vSphere 6) in any IT environment which fulfils the Access system specification.
  - An Access user licence is required for the regular use of Access Professional.
  - The Access user licence enables Siedle Access Professional to be enabled and used from V 4.0.0 for up to 320 users/terminals (optionally inclusive of licensed hardware indoor stations/door stations and/or optionally licenced hardware and software terminals).
  - Access user licences can be purchased for 10, 20, 40, 80, 160 or 320 users/terminals and combined for up to 320 users/devices.
  - A flash is no longer required for correct display of the dashboard (start page) of Access Professional.
  - Dedicated symbols have been assigned to the sub-menu points of the administration user interface in order to enhance operating convenience.
  - The switching inputs of the door controller ATLC can now be configured using the storey call button function.
  - The number of users and devices which are being utilized and the maximum number of users and devices are indicated on the dashboard.
-

# System overview



## Access server variant

Access server variant	Access Professional	ASH 670-04 M	ASH 670-04 S
<b>Finish</b>	Software without server operating system/virtualization	Hardware server + pre-installed Access Professional	Hardware server + pre-installed Access Professional
<b>Access system version</b>	Access Professional V 4...	Access Professional V 4...	Access Professional V 4...
<b>Possible number of users (User licences)</b>	10–320	10–320	10–50
<b>Possible number of communication connections (simultaneously)</b>	25	25	10
<b>Conditions</b>	<ul style="list-style-type: none"> <li>• Hardware server</li> <li>• Server operating system (MS Server 2012 R2 Standard)</li> <li>• Microsoft .NET Framework 4.6.1 for Windows Server 2012 R2 (offline installer or web installer if internet connection exists).</li> <li>• Network/VLAN as required</li> <li>• Indoor stations with POE supply</li> <li>• Software clients/apps on terminals with network connection</li> </ul>	<ul style="list-style-type: none"> <li>• Network/VLAN as required</li> <li>• Indoor stations with POE supply</li> <li>• Software clients/apps on terminals with network connection</li> </ul>	<ul style="list-style-type: none"> <li>• Network/VLAN as required</li> <li>• Indoor stations with POE supply</li> <li>• Software clients/apps on terminals with network connection</li> </ul>
<b>As-delivered status</b>	<ul style="list-style-type: none"> <li>• The Access server must be installed and commissioned.</li> <li>• User and application licences are needed for operating the Access system.</li> <li>• A 30-day test period begins from initial commissioning, during this time all system functions can be used without any restrictions.</li> <li>• The server hardware/virtualization and server operating system must be provided by the customer and must be available.</li> <li>• Microsoft licences: Please check whether any Microsoft server access licences (Client Access License – CAL) are required by the customer for operation of the Access users, or whether these already exist. (For detailed information, see Planning and System Manual Access Professional)</li> </ul>	<ul style="list-style-type: none"> <li>• The Access server is installed ready for operation and prepared for commissioning by the customer.</li> <li>• User and application licences are needed for operating the Access system.</li> <li>• A 30-day test period begins from initial commissioning, during this time all system functions can be used without any restrictions.</li> </ul>	
		<p><b>Remark</b></p> <p>The standard password for the server operating system of a Access Server Hardware (from ASH 670-04...) is: <b>SiedleAccessMain2015</b></p>	
			<p><b>Please change the password on initial commissioning, taking note of the security instructions.</b></p>

## System overview

### Minimum requirements

#### Minimum requirements – Server hardware / Virtual machine \*

Possible number of users (User licences)	320	50
Processor output	min. Intel Xeon Quad Core Processor 64 Bit (from launch year 2014 or more recent)	min. Intel Atom D510; 1.6 GHz dual-core *
Random access memory (RAM)	at least 4 GB	at least 2 GB
Storage location (HD)	at least 256 GB	
Network connection (LAN)	at least 1 x 1000 Mbit/s	

#### Server operating system/software

Operating system	Microsoft Server 2012 R2 Standard or Datacenter (installation: Standard full installation -> Server with graphic user interface)
Role of the server operating system	optionally: DHCP server service, if no DHCP server is operated in the existing network.
Other server services	optionally: NTP server
Necessary DHCP options	Time Server, Log Servers, NTP Servers, Boot Server Host Name, Bootfile Name Optionally: Router (Default Gateway), Domain Name and DNS-Server
Access system version	Access Professional – from Version 4.0.0
Access licences	For regular operation of Access Professional, an Access user licence must be purchased against a fee. Optional application licences enable the use of additional performance features.

#### Network connection

Network	Own physical network from CAT-5 and optionally with modified VLAN with Quality of Service (IEEE802.1p)
Transmission speed	100 MBit/sec (End devices) 1000 MBit/sec (Server hardware)
Internet protocol	IPv4
Internet connection	Essential for the use of the "Apple Push Notification Service" when using the Siedle app.
Multicast capability (only if you wish the video signal to be transferred in the network as a multicast stream. As an alternative, the unicast operation mode can be used. With unicast, every video stream is separately generated and can cause very high network capacity utilization where there are high number of users with approx. 1 MBit per user.)	Throughout the entire network
Distribution list	The use of switches is a requirement.
Power over Ethernet (PoE)	Access indoor stations require PoE-capable switches or PoE injectors in compliance with IEEE802.3af



\* For Access systems with up to 50 users, server hardware can be used which corresponds to the performance data of Access server hardware S:

- Processor output: At least Intel Atom D510; 1.6 GHz dual-core
- Random access memory (RAM): at least 2 GB

Important: Please note that in this configuration, no virtualization and no additional system expansion are possible.

### Access Professional

In order to use all the functions of Access Professional correctly as a software variant, the provided server hardware/virtual machine and the network infrastructure must meet the minimum requirements of the Access system.

### Remarks

- In order to work with Access Server Administration, you need an PC with the latest version of the web browser Mozilla Firefox. If you use a different web browser to the Mozilla Firefox, display errors can occur.
- Two network sockets are affixed to the back of the Access server hardware (Extern and Access). For linking the Access devices to the Access network, the Access socket must be used.

### Notice on the scope of supply

The Access server hardware is delivered as standard with the following additional software tools and releases:

- 7-Zip (x64)
- Firefox
- Notepad++
- Putty
- Wireshark
- WinPcap
- Remote desktop release

The listed files and programs are required for configuration and servicing purposes and should only be used by specialist and servicing personnel.

The Access system (software variant) is delivered **without** these additional software tools and releases.

### Additional requirements imposed on virtualization

- For virtualization, from VMware vSphere 6 upwards a virtualization solution configured for server systems must be used.
- The minimum requirements imposed on the virtual machine are the same on principle as server hardware provided by the customer for up to 320 users. With the virtual machine, remember that at least 2 virtual and separate processor units (CPUs) must be made available.
- If virtualization is used, the host (physically present server on which the virtual machine is operated) must have sufficient performance to make available the output needed for the virtual machine.

### Remarks

The size of the hard disk storage capacity which should be selected depends on various factors when using a virtualization solution:

- Number of users, groups and terminals
- Utilization scenario and incidence of communication
- Activated video memory function: If no video memory function is used, we recommend a hard disk storage capacity of at least 30 Gigabytes. When using the video memory function, please contact the Access Service Center to be advised on the minimum capacity required for the hard disk memory.
- For Access systems with up to 50 users, server hardware can be used which corresponds to the performance data of Access server hardware S:
  - Processor output: At least Intel Atom D510; 1.6 GHz dual-core
  - Random access memory (RAM): at least 2 GB
- Important: Please note that in this configuration, no virtualization and no additional system expansion are possible.

## Licences and test period

### Licences

- User and application licences are needed for operating the Access system. The customer determines the required number of users/devices with the licence. The user licence can be purchased for up to 320 users/devices per system – optionally also tiered.
- The customer determines the usable device types/scope of functions with the application licences. User licences for hardware indoor stations and door controllers are contained in the scope of delivery. Additional application licences are needed for software clients, third-party devices and for activating further functionality.
- Each device or client of a user occupies one user licence.

### Licence purchasing

- Customers and sales partners from Germany, please consult one of our Access Certified Partners. \*
  - Customer and sales partners outside Germany please contact your Siedle representative in your country.
- \* Access Certified Partners (ACPs) are authorized to commission Access systems. They have proven their competency as planners and administrators of Siedle Access systems, have passed audits and are certified by Siedle. Contact details are available on the internet at [www.siedle.com/acp](http://www.siedle.com/acp)

### Test period

- A 30-day test period begins from initial commissioning, during this time all system functions can be used without any restrictions.
- After expiry of the 30-day trial period, the Access Professional system is deactivated and cannot be used until the Access licences are imported. The administrator user interface can still be accessed and the relevant notices are displayed on the dashboard.
- The licence can only be successfully imported if at least the number of users/devices contained in the system and the scope of functions are covered by the user/application licences.
- The test period ends when the licence is imported.

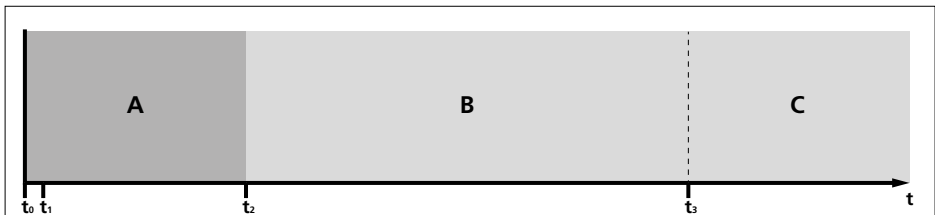
Licence type	Licence	Description	Device type
<b>Fee-based user licences</b>	APR 670-0 10	Access Professional for up to 10, 20, 40, 80, 160, 320 users/end devices per system	–
	APR 670-0 20		
	APR 670-0 40		
	APR 670-0 80		
	APR 670-0 160		
<b>Application licences which contain the scope of supply</b>	APR 670-0 320	Access door loudspeaker controller (ATLC)	Door controller
		Access in-house telephone (AHT)	Internal call station (Audio)
		Access video in-house telephone (AHTV)	Internal call station (Video)
		Access handsfree telephone (AHF)	Internal call station (Audio)
		Access video handsfree telephone (AHFV)	Internal call station (Video)
		Access video panel (AVP)	Internal call station (Video)
<b>Optional application licences</b>	ALFA 270-0	Access licence for external audio device	VoIP audio telephone
	ALFS 270-0	Access licence for external smartphone	iPhone
	ALFT 270-0	Access licence for external tablet	iPad
	ALFP 270-0	Access Lizenz Fremdgerät Panel	Android panel with pre-installed Siedle app (e.g. JUNG Smart Control...)
	ALFV 270-0	Access licence for external video device	VoIP video telephone
	ALKNX 270-0 <50, <300, >300 *	Access licence for KNX connection	KNX gateway
	ALT 270-0 *	Access licence for telephony connection	Telephone system
	ASC 170-0	Access Software Concierge	Windows PC software
	ASHT 170-0	Access Software In-house telephone	Windows PC software
	ASM 170-0	Access software module	Windows touchpanel software

\* does not use a user licence

## Maintenance agreements

- For each Access system, Siedle offers optional maintenance agreements. The maintenance agreements include permanent software updating and regular updates for maintaining security and functionality.
- Maintenance contracts for the Siedle Access system can be purchased both through the Siedle Project Sales and through an Access Certified Partner (ACP).
- The maintenance period is initially 1 year after first commissioning of the Access server for all systems. After this, all customers can decide whether they wish to extend the maintenance period for their system by paying for an extended maintenance contract.
- Alternatively, updates/upgrades must be purchased for a fee in certain circumstances.
- With Access Professional V 4.0.0 and upwards, the field “End maintenance contract” is located on the dashboard of the Access administration user interface. The associated date indicates the date up to which the customer is entitled to install available updates/upgrades for free.

### Maintenance contract recommendation



Periods	Description	Note
A	Free warranty period	30-day test period and 1-year software maintenance
B	Fee-based maintenance period	Maintenance contract with 2-year minimum term
C	Fee-based maintenance period	Annual extension of the maintenance contract with 1-year term

#### Time points

$t_0$	Initial commissioning of the Access system and start of the 30-day unrestricted test period	–
$t_1$	Latest time point for the import of the Access licences and end of the test period	–
$t_2$	Start of the fee-based maintenance period and end of the free warranty period	–
$t_3$	Continuation of the fee-based maintenance period	–

## Apple Push Notification Service (APNS)

With the change to the iOS 11 operating system, apps on mobile iOS end devices can now only be addressed via the "Apple Push Notification Service" (APNS). For the APNS, a permanent internet connection is needed for both the sender (Access Server) and the recipient (Siedle app) of a notification, even if the app is only run in the local WLAN. For this, the DNS server and the standard gateway must be configured in the LAN/WLAN and the Access Server and Siedle app must be known. Local stand-alone operation with apps without connection to the Internet is no longer supported by iOS 11.

With the switch to APNS, there is no longer a Siedle app call function (if there is no network connection, no telephone connection is established). From Access Professional V. 4.2.0 and the Siedle app for Access V. 2.2.0, connection to the APNS is included.

Access system version 4.2.0 is required for app version 2.2.0 and vice-versa.

## Time synchronisation in the Access system (NTP server)

For security reasons, all switching commands are signed and given a time stamp in the Access system. The time deviation between Access end devices and the Access Server must be no more than 59 seconds. Siedle hardware end devices with impermissible time deviations from the Access Server do not execute any switching commands. Switching commands from Siedle software clients (e.g. Siedle app) are always executed, as the time synchronicity of mobile end devices (e.g. smartphones) and the Access system cannot be ensured. Otherwise switching commands would no longer be possible if the time deviation was too great.

Please only use one time server/time server pool with one address for the Access system.

Further information on time synchronisation in the Access system can be found in the planning and system handbook for Access Professional as of the 2018 issue.

## Connection to telephone systems

In order to connect telephone systems (TC system) to the Access system, the following system requirements must be met (from Access system version V. 2.1.x):

- VoIP standard: SIP protocol
- Audio codec: G.711 a-law or  $\mu$ -law
- Length of the audio packets (framing size): 40 ms (can be changed to 20 ms)
- Protocol for DTMF tones: RFC 2833 or SIP info
- A TC system can be connected to the Access system via SIP trunk (SIP gateway) or SIP user/client (SIP provider).

TC systems without VoIP-capable network interface can be connected via analogue or ISDN gateway. Depending on the TC system, it may need to be extended in order to connect to the Access system:

- Hardware: (e.g. retrofitting VoIP assemblies/PCBs)
- Software/software licences: (e.g. system update and additional licences from the TC manufacturer)

These extensions are not part of the scope of supply of the Access system and must not be confused with the user and application licenses which are needed for the operation of the Access system.

For detailed information, see page 102.

# Commissioning

## Commissioning requirements

In order to commission and set up the Access server, you must ensure that the following commissioning requirements are fulfilled:

- The Access system is documented (structures, administration of user rights, devices, correlations, directories, length of telephone numbers (2-5 digits), information on call number plans etc.)
- User and application licences are needed for operating the Access system.
- If the customer performs their own Access installation, Access licences can only be ordered from Siedle at the start of commissioning via Access Certified Partners, as the hardware ID generated by the Access server is required for this.
- The passive network infrastructure has been completely installed and is fully functional. All RJ45 connections are located in the required positions.
- All switches required in the network and for the Access network are ready for operation.
- All door stations are correctly connected to the ATLC and ready for operation, but not yet linked to the network.
- All hardware indoor stations are prepared for installation or installed, but not yet linked to the network.
- POE (Power over Ethernet) is available at all network connections for hardware indoor stations (POE switch or POE injector).
- A permanent internet connection for both the Access Server and the mobile end device on which the Siedle app is to be run is required for the "Apple Push Notification Service" for commissioning and operating the Siedle app for Access.
- The Firefox browser in the latest version is required for commissioning.



### Note!

- In the as-delivered status of the Siedle Access server as a hardware variant, the DHCP and NTP server of the Siedle Access server is active.
- If the IP address of the Access Server has to be changed, first adjust the IP address and then connect the terminals to the server. Otherwise, the terminals will be assigned the wrong IP address and will have to be restarted.
- In large systems, it is advisable following the basic configuration to link the terminals block by block in logically cohesive groups to the server, in order to allow them to be configured in the Access server administration.

### Connecting and switching on the server hardware

Irrespective of whether the server hardware was supplied by Siedle, or whether the customer's own hardware is being used, this must be connected to the power supply and the network.

**Remark:** Operate the Access server hardware exclusively within the admissible ambient temperature of 10 °C to +50 °C.

### Procedure with Siedle server hardware:

- 1 Set up the server hardware or mount the server hardware in the required position in the server cabinet.
- 2 Connect the server hardware to the power supply.
- 3 Connect the server hardware to the Access network.
- 4 Switch on the server hardware.
- 5 Make available a computer for configuration/set-up of the Access server and connect this to the Access network, or provide a possibility of operating the Access server directly using a monitor, keyboard and mouse.

### Remark

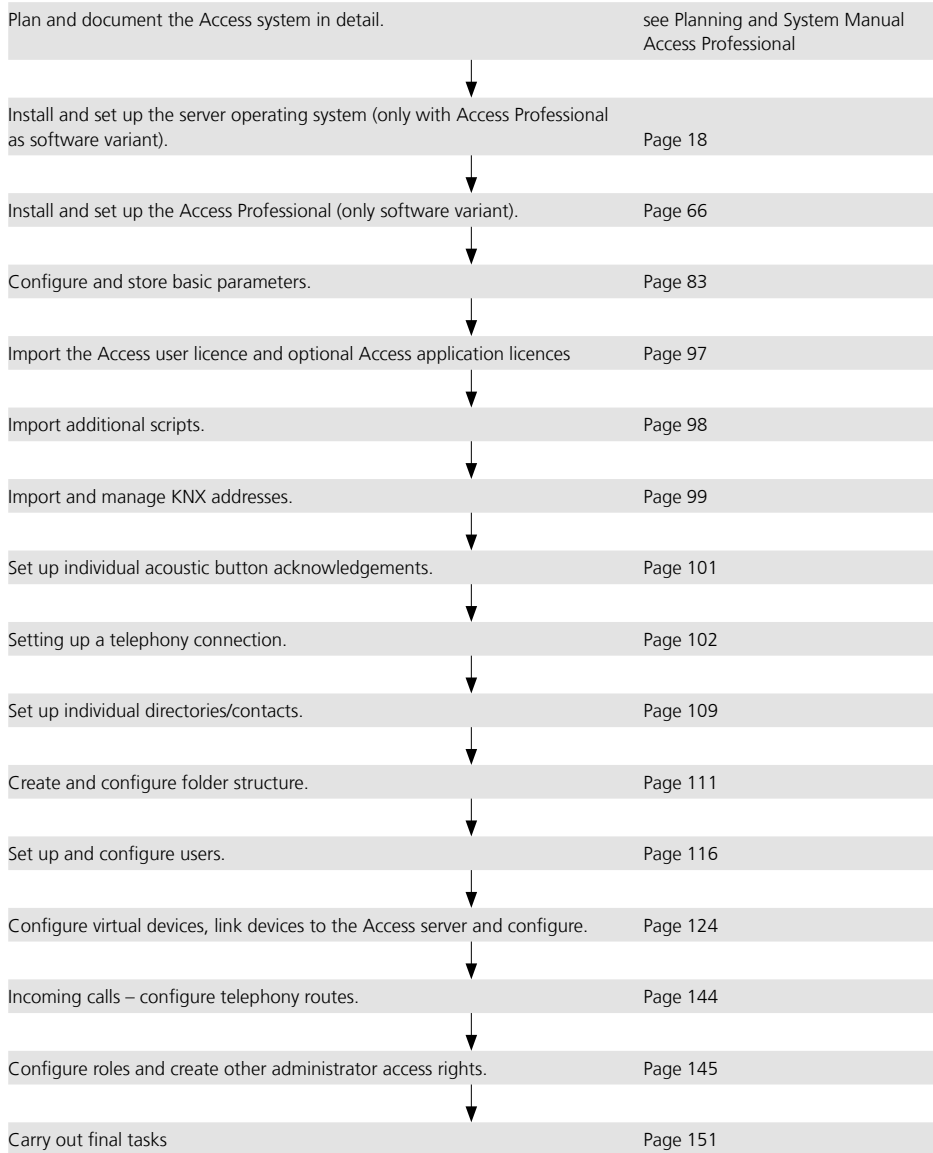
- The Siedle Access servers (hardware variant) are already pre-installed and ready for configuration/set-up. The following steps for installation of the server operating system and the Access server software are omitted. The Access server (hardware variant) can be reached as standard over the IP address 192.168.1.1.

### Procedure with customer's own server hardware:

- 1 Set up the server hardware or mount it in the required position in the server cabinet.
- 2 Connect the server hardware to the power supply.
- 3 Connect the server hardware to the Access network.
- 4 Make available a computer for configuration/set-up of the Access server and connect this to the Access network, or provide a possibility of operating the Access server directly using a monitor, keyboard and mouse.
- 5 Switch on the server hardware.
- 6 Start the installation of the server operating system and the Access server software as instructed over the following pages.

## Commissioning

### Recommended commissioning sequence



**Device commissioning**

Depending on the size (number of devices) of the Access system and the situation on site (e.g. building size on the customer's premises), select the best procedure to use for device commissioning at your own discretion. Possible procedures:

**Using the MAC address label**

With all indoor stations and door controllers, an additional MAC address label for the respective device is included in the scope of supply.

This label should be used for documentation purposes and for commissioning support in the Siedle Access device protocol (e.g. handover protocol for the customer).

The Siedle Access device protocol is located in the Siedle download area at [www.siedle.com](http://www.siedle.com)

Procedure	Description	Commentary
<b>Prepared configuration</b>	Local provisional set-up (workshop) for commissioning and configuration of the Access server and the Access devices prior to actual installation on the customer's premises.	Suitable for all sizes of Access system in buildings in which the final installation is only possible shortly before closure, buildings with a large number of security areas and access restrictions or where communication possibilities are restricted. The preparatory configuration calls for a fully completed detailed plan and a structured and documented work method. In addition, all pre-configured devices must have been logically and traceably inscribed.
<b>Complete configuration</b>	Link all devices to the already set up Access server and configure the devices.	Suitable for small Access systems with a simple structure and few or only few identical Access devices, and buildings with no or minimal internal access restrictions.
<b>Block-by-block configuration</b>	Systematically connect the devices one block at a time to the already set up Access server in order to configure them in blocks.	Suitable for medium and very large Access systems with complex structures which have few or few identical Access devices within one or more users or groups, as well as buildings with no or only minimal internal access restrictions.
<b>Serial configuration</b>	Systematically connect the devices in series to the already set up Access server in order to configure them individually.	Suitable for medium and very large Access systems with complex structures which have few or few identical Access devices within one or more users or groups, as well as buildings with no or only minimal internal access restrictions.

# Commissioning

## Recommended commissioning sequence

### Recommendation

- Only ever commission several devices simultaneously if these can be clearly differentiated by their device type and if assignment to the user is clear.
- Commission devices individually in series if you are dealing with a large quantity of identical device types which need to be commissioned.

### Background

All newly detected devices are located in the **Users** menu in the **Unassigned devices** folder. If there are a large number of identical devices, the identification work increases, as does the effort involved in user-specific configuration and assignment of the individual devices.

### Device-specific settings

In the system, it is possible to select a language for all Access terminals at the Access server. The system language and setting of the bell and voice volume can be centrally configured at the Access server. These settings can be locally individually changed at the terminals.

---

### Commissioning possibilities

### Distribution of tasks

### Remarks

---

#### Commissioning on site with 2 persons

- **Person 1** carries out the final installation, commissioning and function test of the device at the relevant device location.
- **Person 2** carries out the relevant device configuration at the Access server.

Suitable for large Access systems in large buildings or buildings without functioning WIFI. Mobile wireless phones or wireless devices are necessary for communication between the two people.

---

#### Commissioning on site with 1 person

- **Person 1** prepares the Access server for device commissioning.
- The next step is final assembly, commissioning of the device, configuration at the Access server using a mobile computer at the relevant device. Then the device is function tested on site.

Suitable for small to medium Access systems or Access systems in small to medium buildings. WIFI or LTE/UMTS access to the Access server is necessary in order to allow device configuration for the respective devices to be carried out at the Access server.

---

#### Commissioning with 1 person and prepared Access system

- **Person 1** commissions the Access server and starts the network infrastructure.
- In the next step, final assembly, commissioning and function testing of the preconfigured device take place on site.

Suitable for small to medium Access systems or Access systems in small to medium buildings. **Requirement:** Completed and released detail planning of the Access system, as well as unambiguous marking and documentation of the pre-configured devices.

---



### Use latest system version

The Access server hardware / Access Professional as a hardware/ software variant are always delivered in the latest Access system version. By the time commissioning takes place on the customer's premises, it is possible that a newer system version exists.

### Remarks

- From Access server 3.0.0 onwards, the updating process of the Access server has been revised. The system updating process will not be launched in future via the Access server, but carried out by the Access server installer (see chapter System update). External access to the new system version is reserved to Access Certified Partners "ACP". More recent system versions can incur a charge.
- Updating Access Professional is optionally possible by an ACP. Using the services of an ACP can also incur a charge.
- If possible, always use the latest system version of the Access server and always keep this version up to date.

### Procedure

- 1** Have an ACP check whether there is a more recent Access Professional system version available.
- 2** If a newer system version exists, where applicable have this delivered, installed or updated by the ACP against a charge.



- In the case of a system version change (upgrade) to Access Professional from V 4.0.0, the hardware ID changes. In addition, the optimum licence package and the right maintenance contract for the customer/operator/end user can be selected from the new user licence model. Before carrying out an upgrade, contact the Access Service Center.
- A system update from **Access V 3...** to **Access Professional V 4...** is possible.
- A system update from **Access Professional V 4.0.0** upwards is only possible if a valid maintenance contract exists. This can be concluded against a fee.

### Changing/adapting the network configuration

Siedle Access server Hardware is delivered with a standard network configuration. DHCP and NTP servers are already preconfigured. Depending on the customer network infrastructure and the already available/set up network services, it can happen that the configuration has to be changed before connecting to the customer's network.

# Setting up the server operating system

## Microsoft Server 2012 R2 Standard

### Installation and operating conditions

In order to allow the Siedle Access server to be correctly operated, you must fulfil the following installation requirements:

- 1** The server hardware or virtual machine (from VMware vSphere 6) you have provided complies at least with the technically specified system requirements for the Access server.
- 2** As a server operating system, you must install **Microsoft Server 2012 R2 Standard** or **Datacenter** as a standard pre-installation (Server with graphic user interface).
- 3** Assign a static IP address for the server operating system.
- 4** **Optionally:** Assign the server operating system the role of the **DHCP server** and where applicable the **NTP server**, if there is no DHCP and NTP server operating in your network.
- 5** Only activate the services necessary for operating the Access server, and where applicable activate the NTP server.
- 6** In the configured server operating system, install only the Siedle Access system. In addition, no other server services may be installed, as this can result in impaired performance of the Siedle Access server. (**Rule:** 1 server service per server operating system installation.)
- 7** The network infrastructure corresponds to the prescribed specification for Siedle Access.
- 8** All network users of the Access server are operated using this network infrastructure.

### Installing the server operating system

You must install the Microsoft server operating system in the **full installation variant – server with graphic user interface** on the server hardware.

#### Procedure

- 1** Start the installation of the server operating system.

**Important: The language of the user interface [app language] must be German or English during installation!**

- 2** As an installation option for the server operating system, select the **full installation – Server with graphic user interface (server graphic shell)** variant.
- 3** Execute the installation of the server operating system.

### Remark

- The values for IP addresses and network entries used in these commissioning instructions are intended as examples only and can deviate from your network environment.

## Log in

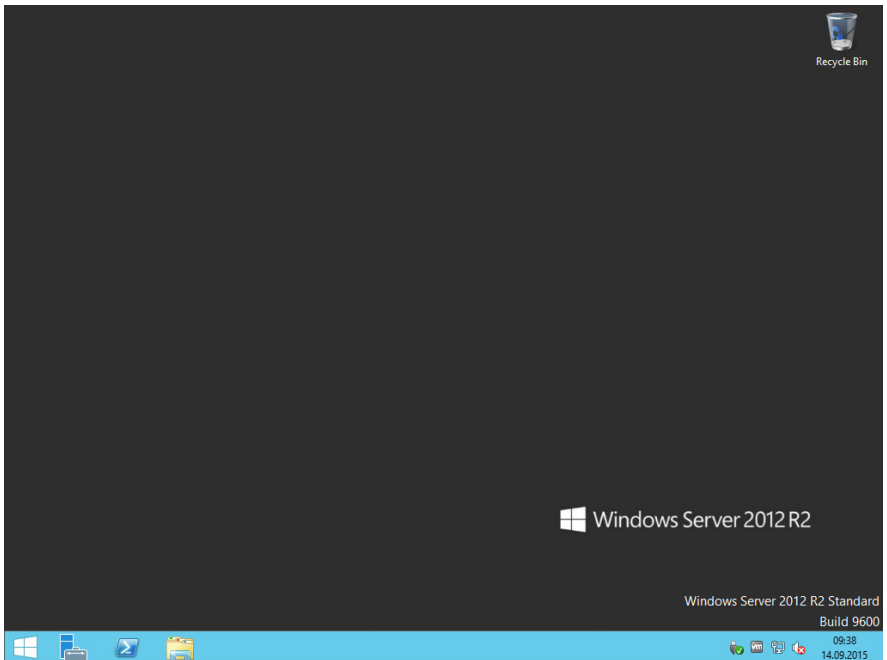
### Procedure

- 1 Log into the Windows server with the administrator access data issued by you during installation.
- 2 The desktop of the Windows server is displayed.

### Remark

- The standard password for the server operating system of a Access Server Hardware (from ASH 670-04...) is: **SiedleAccessMain2015**

**Please change the password on initial commissioning, taking note of the security instructions.**



# Setting up the server operating system

## Assigning the static IP address

### Configuring the static IP address

In order to operate the Access server correctly, you must assign the Server operating system a static IP address. This means that the Access server can always be reached under the same IP address.

A missing static IP address in regular operation results in faults or possible prevention of the Access server being reached.

### Remark

Alternatively, you can also reach the settings using the start menu:

**Start -> Control Panel -> View network status and tasks -> Change adapter settings -> Double click on the used network adapter -> Properties -> Double click on Internet Protocol Version 4 (TCP/IPv4).**

### Procedure

**1** With the right-hand mouse button, click on the network icon in order to open the context menu.

**2** Click on **Open Network and Sharing Center**.

**3** Click on **Change adapter settings**.

**4** Double click on the network adapter you wish to use in order to open the properties of the network adapter.

**5** Click on **Properties** in order to display the properties of the network adapter.

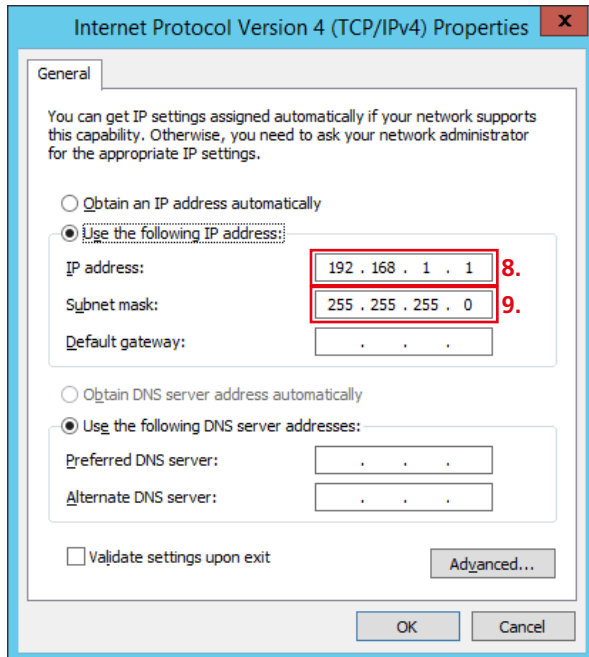
**6** Double click on **Internet Protocol Version 4 (TCP/IPv4)** in order to change the settings.

**7** Click on **Use the following IP address**: in order to assign a static IP address to the server operating system.

**8** In the input field **IP address**, indicate an IP address under which you wish the server operating system to be reachable (e.g. 192.168.1.1).

**9** In the input field **Subnet mask**, enter the subnet mask (e.g. 255.255.255.0).

Continued overleaf...



### Configuring the default gateway and DNS-Server

If you do not use the Access server exclusively in the stand-alone mode, but link it to your existing network (e.g. domain, Access gateway) or if you wish the Access server to be reachable over the internet (e.g. Siedle App for Access), you must enter the correct IP addresses for the **default gateway** and the **preferred DNS server**.

### Procedure

**10** Enter the IP address in the field **Default gateway**.

**11** Enter the IP address in the field **Preferred DNS server**.

**12 Optionally:** If known, enter the IP address in the field **Alternate DNS server**.

**13 Optionally:** Activate the option **Validate settings upon exit** in order to have the entered network settings checked by the Windows server.

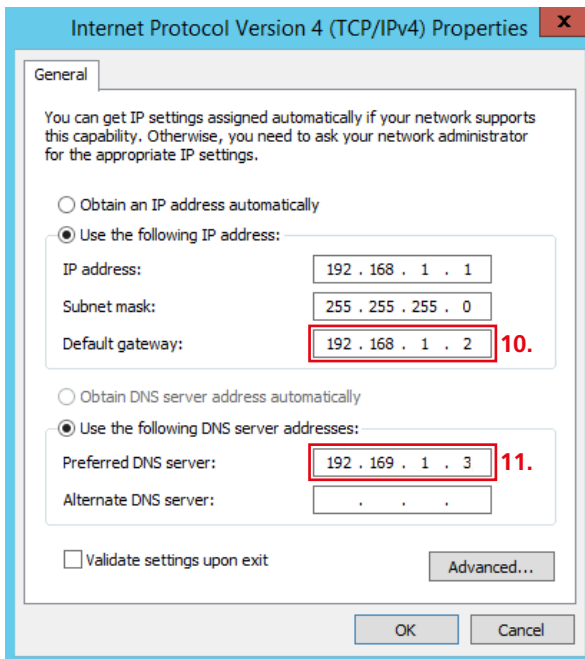
**14** Confirm your entries with **OK**.

**15** Close any remaining open windows which you had opened for this configuration.

**16** You have configured the network settings of the server operating system and are now back on the desktop of the server operating system.

### Remark

- The correct IP addresses are available from your responsible network administrator.



# Setting up the server operating system

Setting up and configuring the DHCP server service

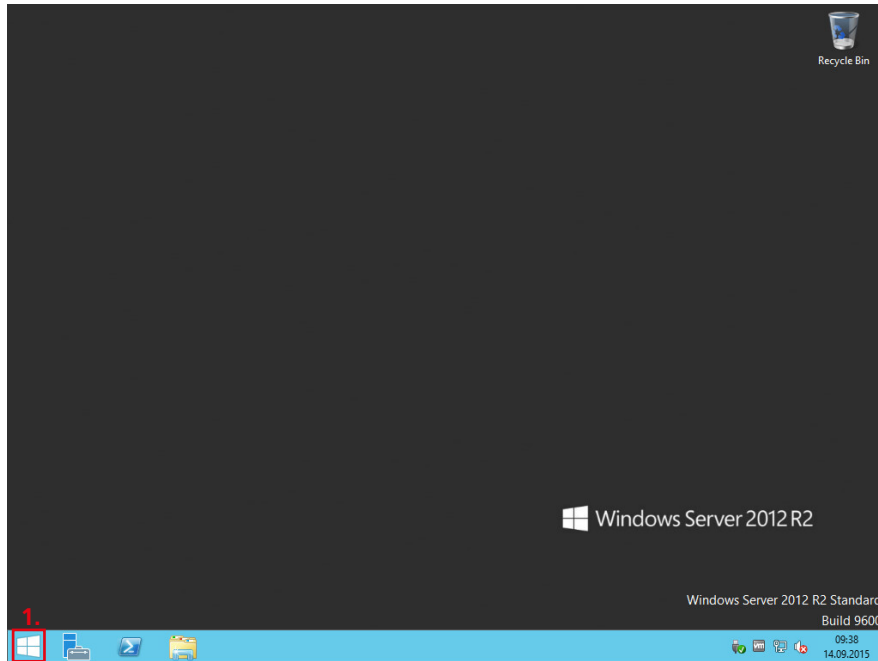
## Starting the server manager

Using the server manager you can add the DHCP server service at the server operating system.

The server manager starts up automatically with each system login.

## Procedure

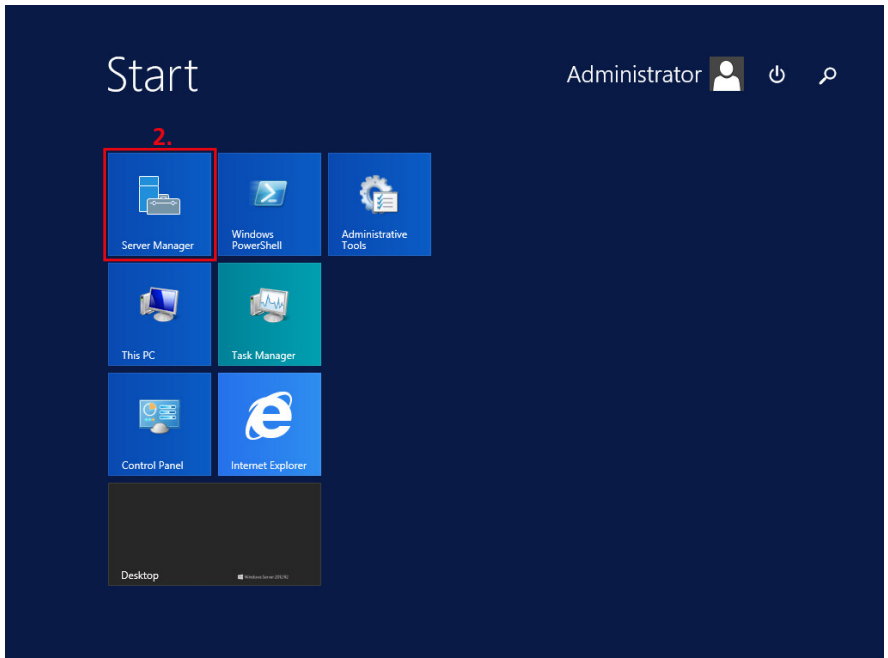
**1** Click on the **Windows start button** (bottom left-hand corner) in order to open the start screen of the Window server.



**Starting the server manager**  
(continued)

**Procedure**

**2** Click on the **Server Manager** tile in order to start the server manager. The **Dashboard** (start page) of the server manager opens up.



# Setting up the server operating system

## Setting up and configuring the DHCP server service

### Starting the server manager

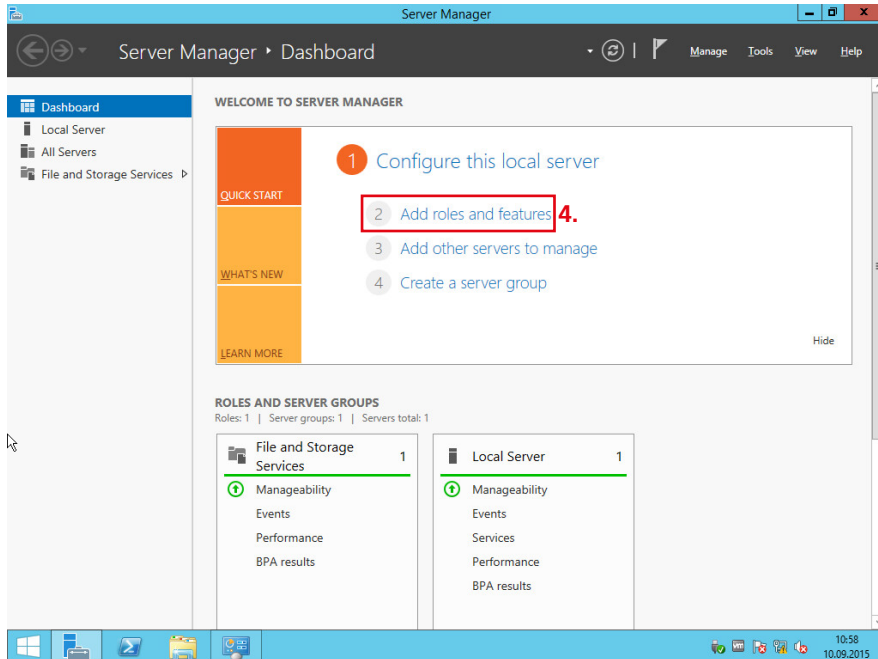
(continued)

### Procedure

Click on **2 Add roles and features**.  
**3** The page **Before you begin** opens up.

### Remarks

- With the Server Manager, you can manage not only your own server but also others.
- In the lower part of the Dashboard under **Roles and Server Groups**, the available servers and the created server services are displayed. After setting up the DHCP server service, this is also shown there.





## Add DHCP server service

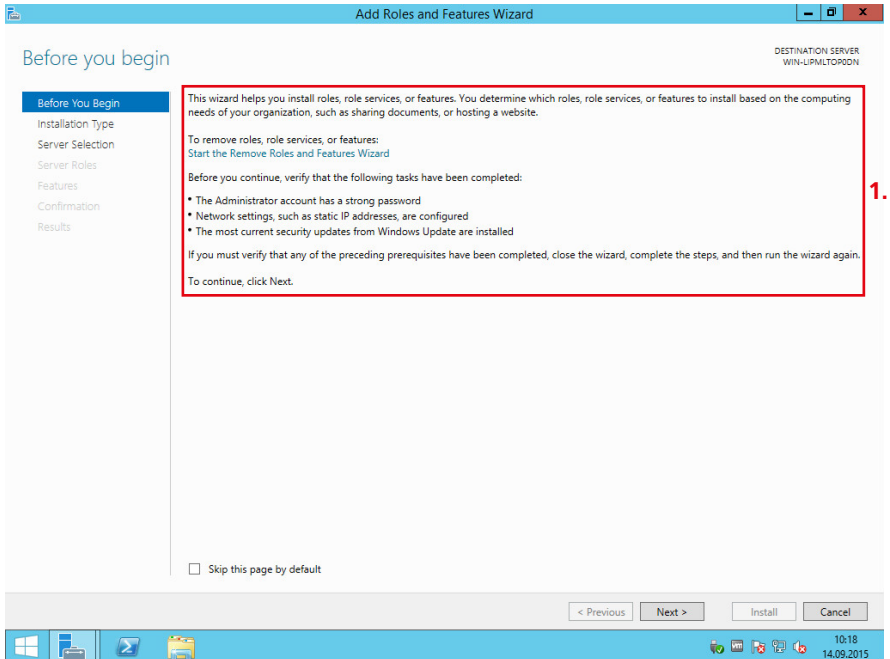
### Procedure

**1** If required, read the instructions on the **Add Roles and Features Wizard**.

**2 Optionally:** If you do not want these instructions to appear in future, click on **Skip this page by default**.

**3** Click on **Next**.

**4** The page **Select Installation Type** opens.



# Setting up the server operating system

## Setting up and configuring the DHCP server service

### Add DHCP server service

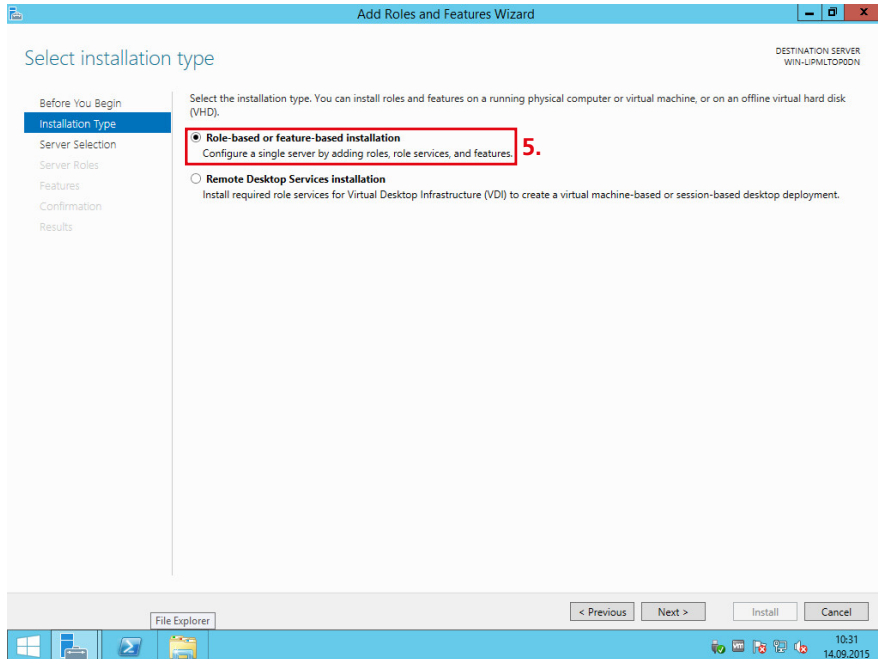
(continued)

### Procedure

**5** If nothing is already preselected, select the option **Role-based or feature-based installation**.

**6** Click on **Next**.

**7** The page **Select destination server** opens up.



## Add DHCP server service (continued)

### Procedure

**8** If not already preselected, select the option **Select a server from the server pool**.

**9** If not already preselected, select your server.

**10** Check whether the displayed IP address agrees with the IP address of your server.

**11** Click on **Next**.

**12** The page **Select server roles** opens up.

### Remark

- In the area **Server Pool**, all servers which can be reached by the Server Manager are displayed. You can identify your server on the basis of the assigned IP address. If you are not able to find out your IP address, check the network settings of your server.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the right, it says 'DESTINATION SERVER WIN-LIPMLTOPDN'. On the left, a navigation pane lists: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text: 'Select a server or a virtual hard disk on which to install roles and features.' Below this are two radio buttons: 'Select a server from the server pool' (selected and highlighted with a red box and the number 8) and 'Select a virtual hard disk'. Below the radio buttons is a 'Server Pool' section with a 'Filter:' input field and a table. The table has columns for 'Name', 'IP Address', and 'Operating System'. One row is visible: 'WIN-LIPMLTOPDN', '10.32.246.10', and 'Microsoft Windows Server 2012 R2 Standard'. Below the table, it says '1 Computer(s) found'. At the bottom, there is a note: 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom of the window, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The Windows taskbar at the bottom shows the time as 10:42 on 14.09.2015.

## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Add DHCP server service

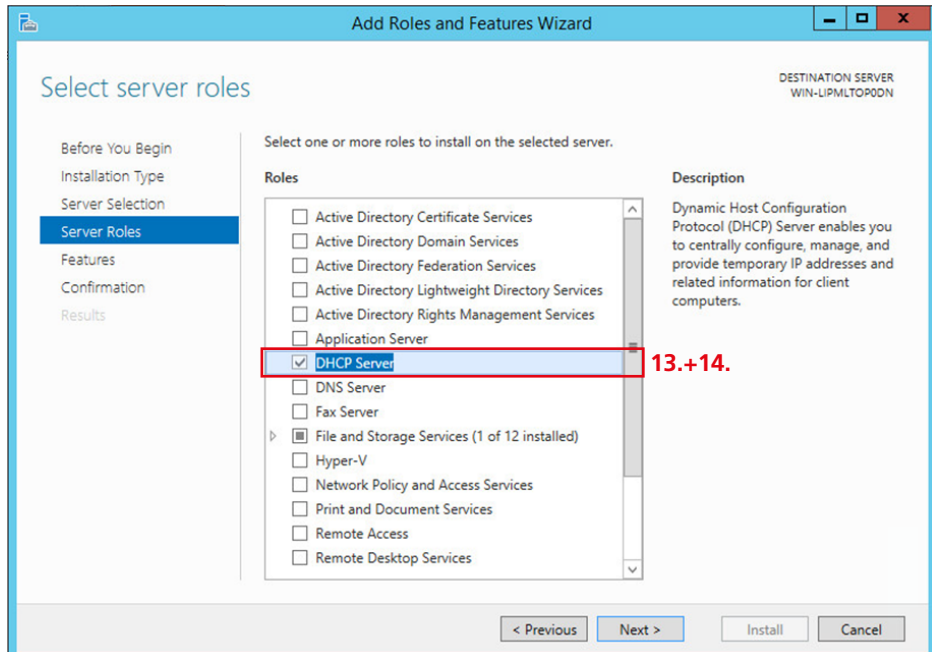
(continued)

#### Procedure

**13** If not already preselected, select the option **DHCP server**.

**14** Click on the checkbox next to the DHCP server in order to activate the role DHCP server.

**15** The sub-page **Add features that are required for DHCP Server?** opens up.



**Add DHCP server service**  
(continued)

**Procedure**

**16** If not already activated, click on the checkbox next to **Include management tools (if applicable)**, in order to also activate the management tools for the DHCP server service.

**17** Click on **Add Features**.

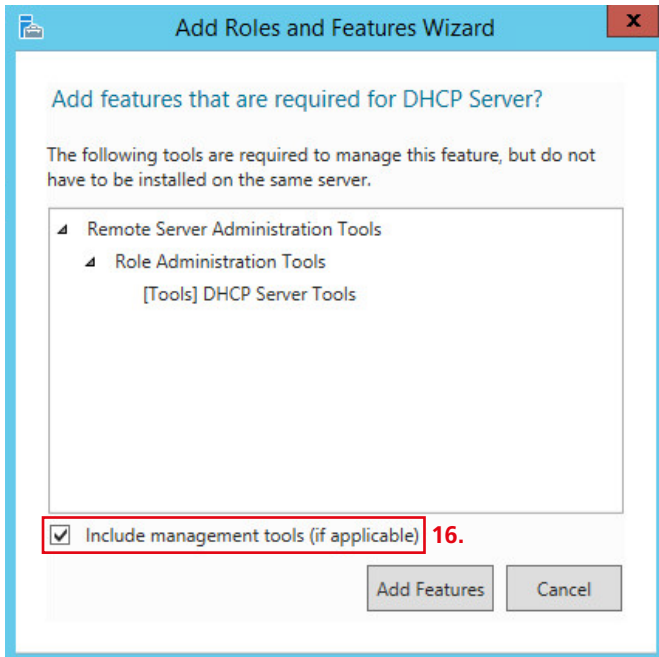
**18** You are then back on the page **Select server roles**.

**19** Click on **Next**.

**20** The page **Select features** opens up.

**Remark**

- All previous steps can be repeated as often as required, for example to extend the existing function scope of the DHCP server service.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Add DHCP server service

(continued)

#### Procedure

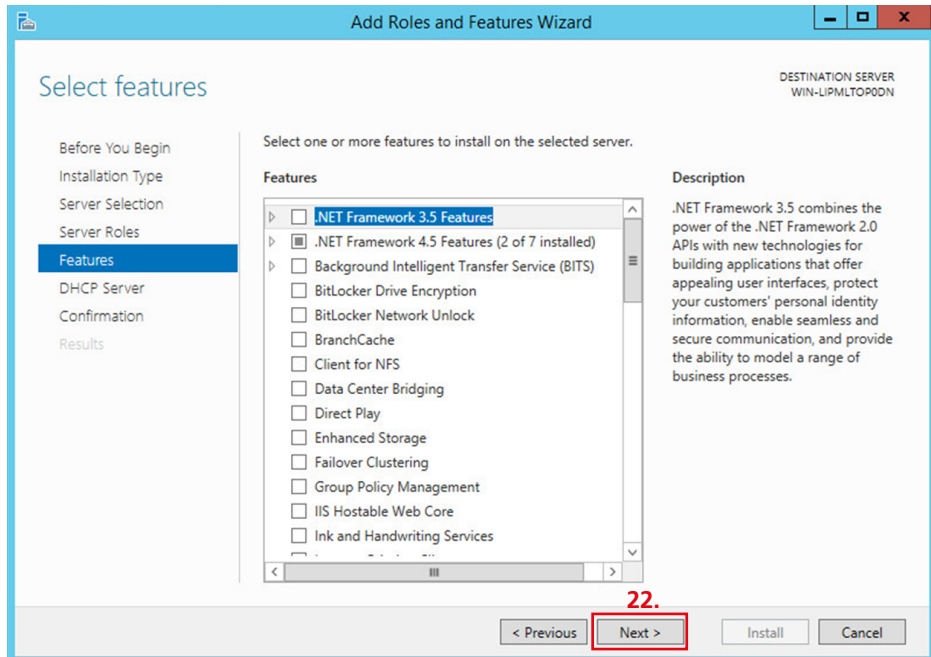
**21** Do not open any other functions/ tools.

**22** Click on **Next**.

**23** The page **DHCP Server** opens up.

#### Remark

- No supplementary functions/tools are required to operate the Access server.



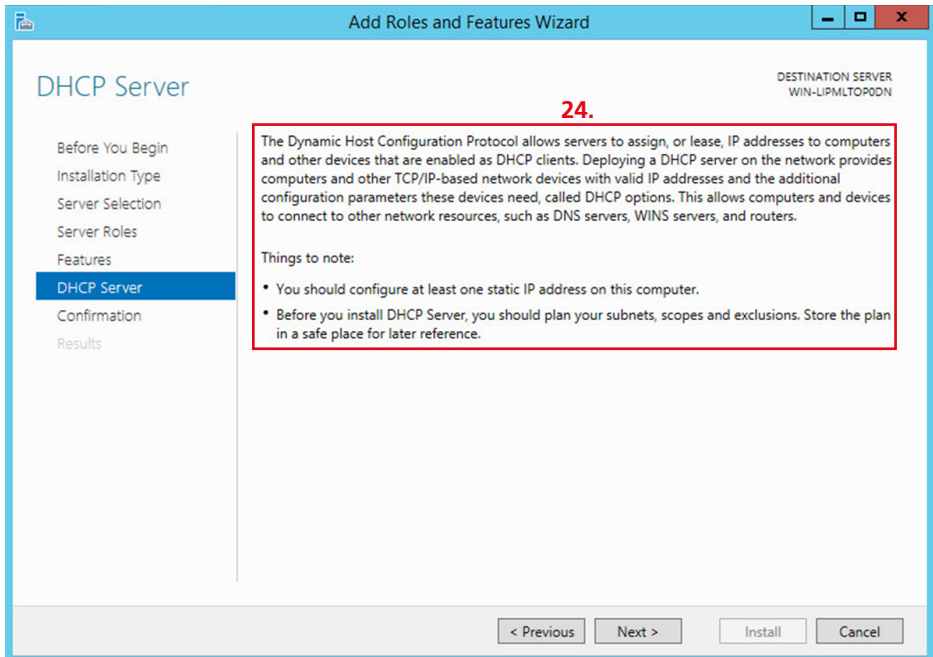
**Add DHCP server service**  
(continued)

**Procedure**

**24** If required, read the instructions on the **DHCP server**.

**25** Click on **Next**.

**26** The page **Confirm installation selections** opens up.



## Setting up the server operating system

Setting up and configuring the DHCP server service

### Add DHCP server service

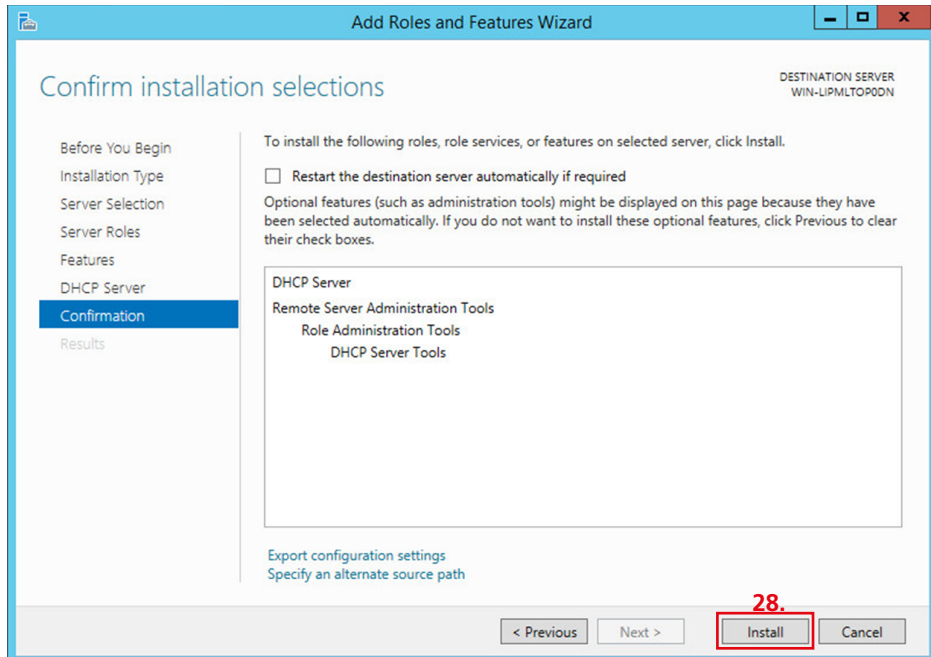
(continued)

#### Procedure

**27** Do not select any additional options.

**28** Click on **install**.

**29** The page **Installation progress** opens up.





**Add DHCP server service**  
(continued)

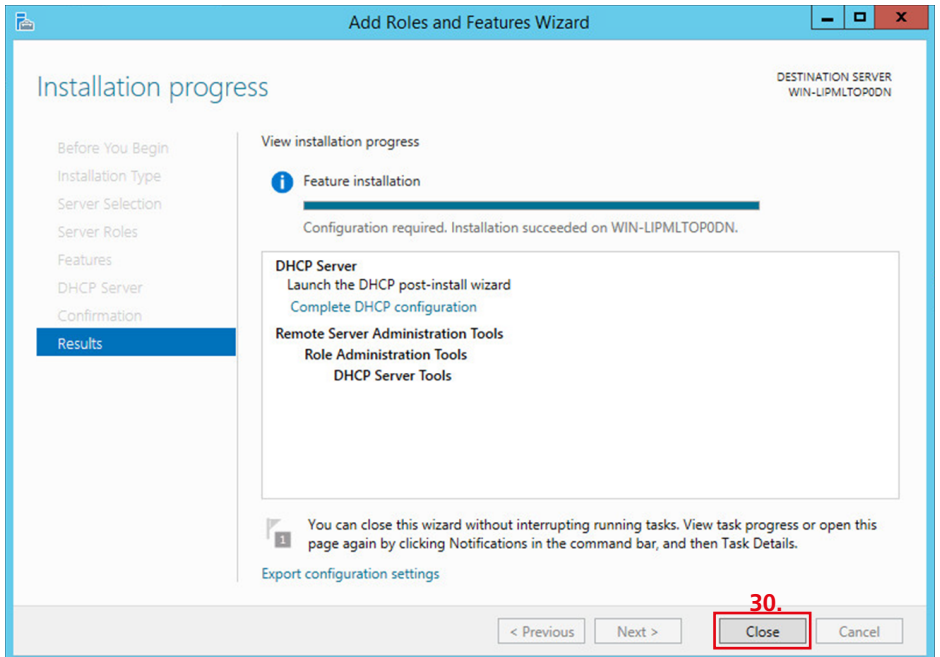
**Procedure**

**30** Click on **Close** to complete the process.

**31** You are back on the page **Dashboard** (start page) of the server manager.

**Remark**

- You have not yet completed the set-up of the DHCP server service. In the Notifications area on the **Dashboard** (start page) of the server manager, a yellow warning triangle is displayed.



# Setting up the server operating system

## Setting up and configuring the DHCP server service

### Add DHCP server service

(continued)

In order to complete the set-up of the DHCP server service, set-up of the DHCP server service still has to be completed in the server operating system.

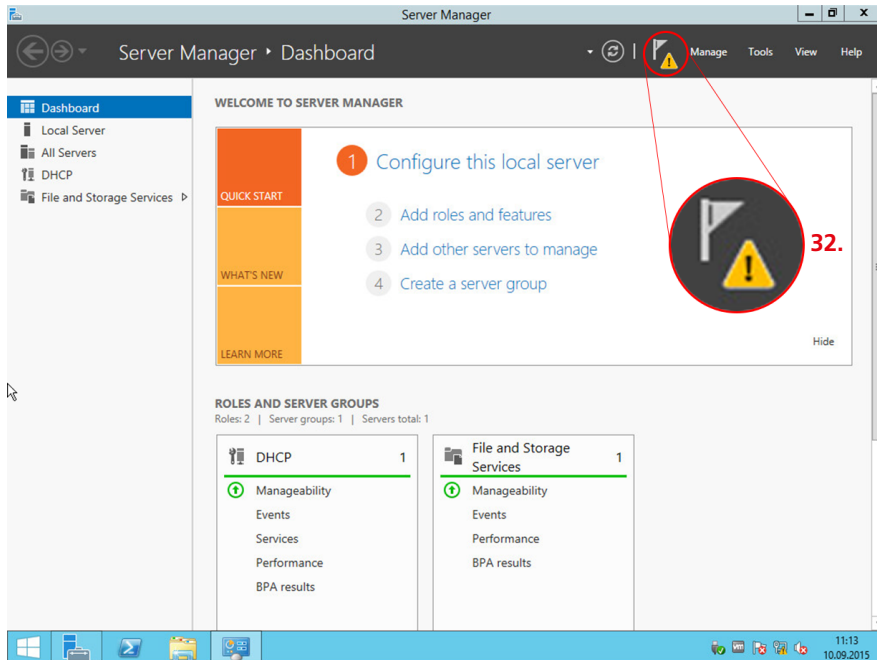
### Procedure

**32** In the header area, click on the **flag symbol with the yellow warning triangle** in order to open the notification area of the server operating system.

**33** The **notification area** is opened with the message indicated by the yellow warning triangle.

### Remark

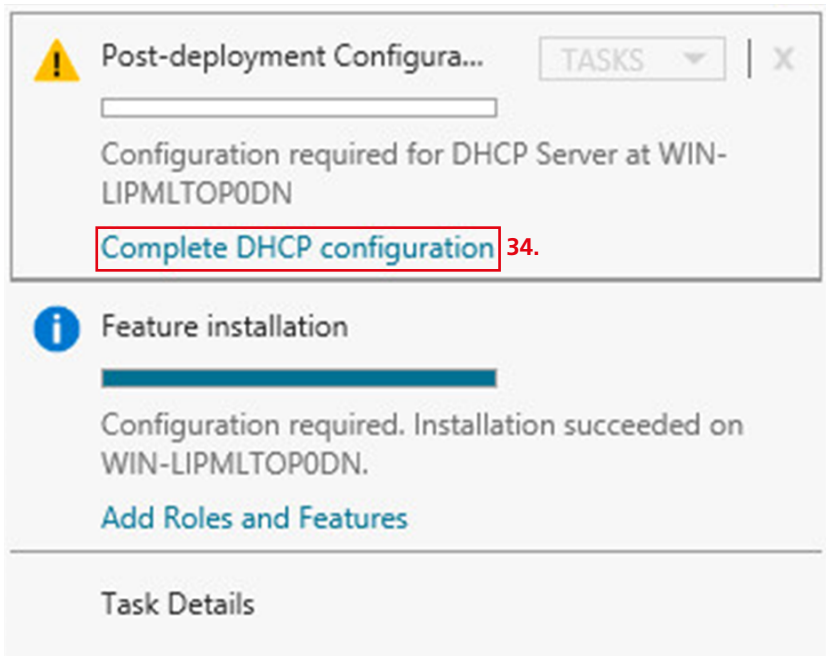
- In the **Roles and Server Groups** area, the DHCP server service you have set up is now displayed as a tile and can be managed directly from here.



**Add DHCP server service**  
(continued)

**Procedure**

**34** Click on **Complete DHCP configuration** in order to complete the set-up of the DHCP server service.



The screenshot shows a Windows task pane with the following content:

- Post-deployment Configura...** (Title bar)
- TASKS** (Dropdown menu)
- Configuration required for DHCP Server at WIN-LIPMLTOP0DN** (Task description)
- Complete DHCP configuration** **34.** (Link, highlighted with a red box)
- Feature installation** (Section header)
- Configuration required. Installation succeeded on WIN-LIPMLTOP0DN.** (Task description)
- Add Roles and Features** (Link)
- Task Details** (Section header)

## Setting up the server operating system

Setting up and configuring the DHCP server service

### Add DHCP server service

(continued)

#### Procedure

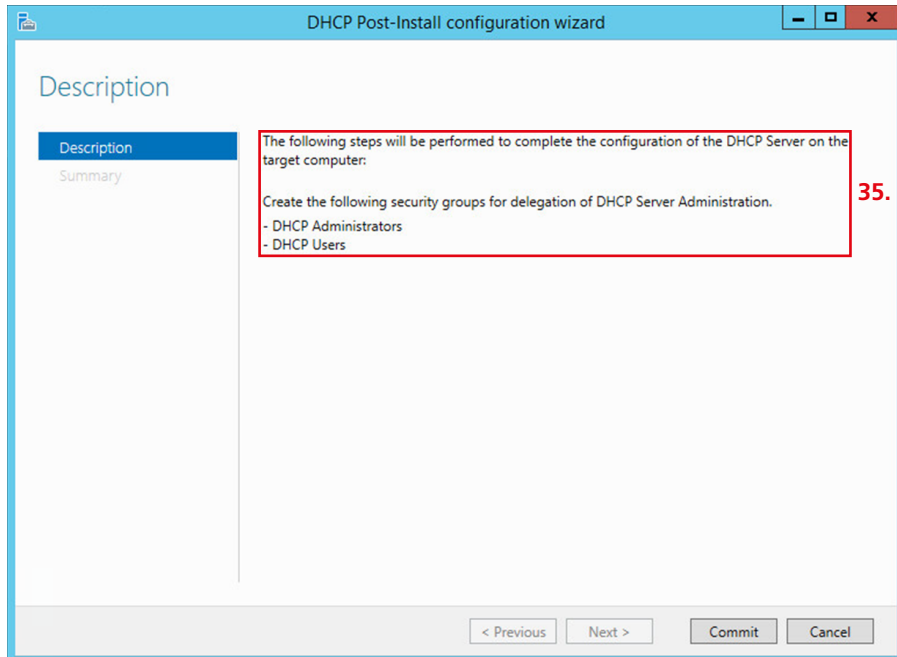
**35** If required, read the instructions on the **DHCP server**.

**36** Click on **Commit**.

**37** The page **Confirm installation selections** opens up.

#### Remark

- In order to complete set-up of the DHCP server service, the system still needs to add group policies for management of the DHCP server service.



**Add DHCP server service**  
(continued)

**Procedure**

**38** If required, read the instructions on the **DHCP server**.

**39** Click on **Close**.

**40** You are back on the page

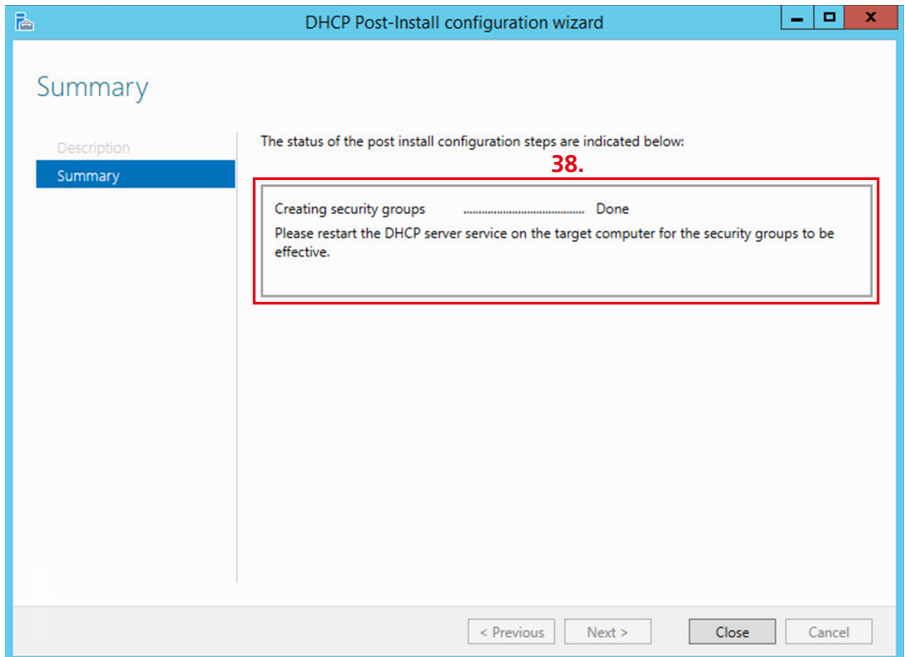
**Dashboard** (start page) of the server manager.

**41** Close the server manager.

**42** You have completed the set-up of the DHCP server service.

**Remark**

- A restart of the DHCP server service on the target devices is not possible/necessary, as in our case these are not yet set up.



# Setting up the server operating system

## Setting up and configuring the DHCP server service

### Configuring necessary services and options

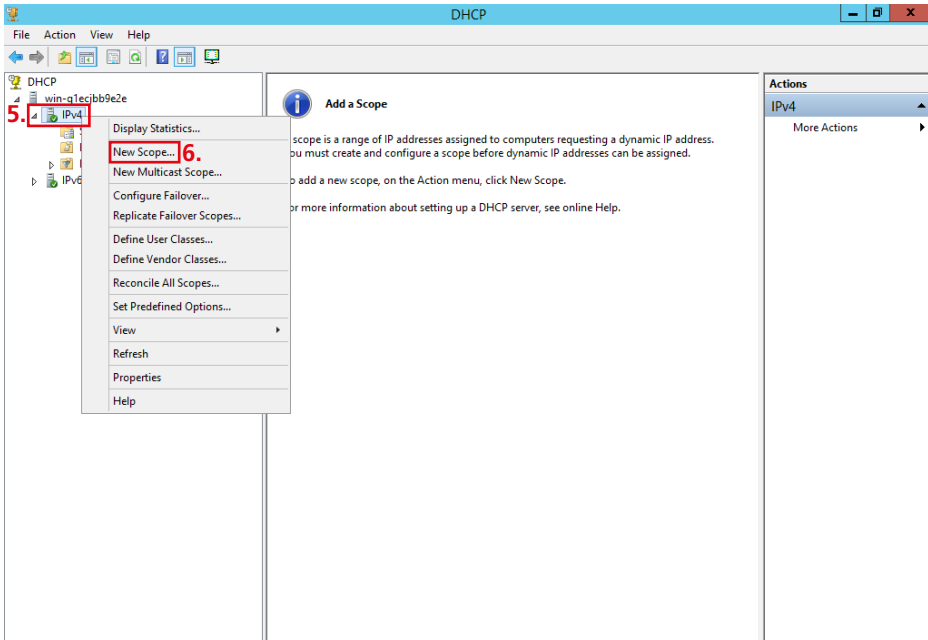
Before installing the Access system, you must configure the DHCP server service with the prescribed and configured IPv4 address pool (Scope) and various DHCP options at the server operating system.

### Procedure

- 1 Click on the **Windows start button** (bottom left-hand corner) in order to open the start screen of the Window server.
- 2 Click on **Administrative Tools > DHCP**.
- 3 The **DHCP** menu opens up.
- 4 Open the menu tree in the navigation area (left-hand column).
- 5 With the right-hand mouse button, click on **IPv4** in order to open the context menu.
- 6 In the open context menu, click on **New Scope...** in order to configure an IPv4 address range for the DHCP server service.
- 7 The Scope Wizard opens up.

### Remarks

- Not all displayed settings are necessary for correct operation of the Access system.
- Optional settings are marked and explained as such.

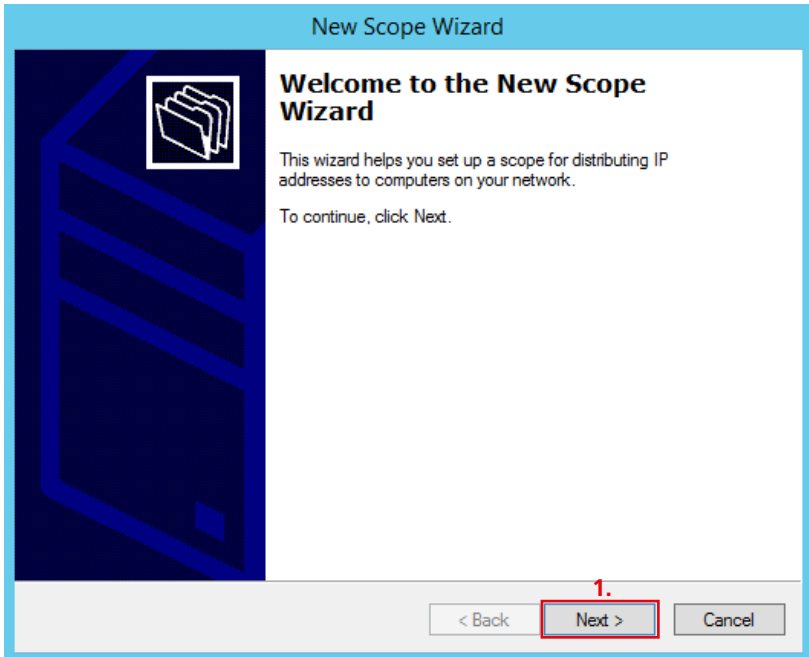


**Scope Wizard – starting the configuration**

**Procedure**

**1** Click on **Next** to start configuration of the IPv4 address range for the DHCP server service.

**2** The **Scope Name** menu opens up.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Enter the name of the server service

To allow the new IPv4 address range for the DHCP server service to be identified, assign a meaningful name in the **Scope Name** menu. You can optionally add a description.

#### Procedure

- 1 Click on the **Name** input field.
- 2 Enter a meaningful name (e.g. Access).
- 3 Click on the **Description** input field.
- 4 Enter an easily understandable description.
- 5 Click on **Next**.
- 6 The **IP Address Range** menu opens up.

### New Scope Wizard

**Scope Name**  
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:  2.

Description:  4.

< Back   Next >   Cancel



### Defining the IP address range

To define the new IPv4 address range for the DHCP server service, assign the start and end IP address and if required change the suffix or the subnet mask.

### Procedure

- 1 Click on the **Start IP address** input field.
- 2 Enter the start IP address of the IPv4 address range.
- 3 Click on the **End IP address** input field.
- 4 Enter the end IP address of the IPv4 address range.
- 5 If required, change the suffix (**length**) or the subnet mask (**subnet mask**).
- 6 Click on **Next**.
- 7 The **Add Exclusions and Delay** menu opens up.

### Remark

- Depending on the start and end IP address, if required you can change the settings for the suffix length or subnet mask accordingly.

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 10 **2.**

End IP address: 192 . 168 . 1 . 199 **4.**

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back    Next >    Cancel

## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Defining exclusions in the IP address range and server time delay

Exclusions in the IP address range can be necessary if you do not wish individual IP addresses or one or more IP address ranges to be made available dynamically over the DHCP server.

To delay the dispatch of a DHCP reply from the server to incoming DHCP enquiries from network users, a server time delay can be used.

#### Procedure

- 1 Click on the **Start IP address** input field.
- 2 Enter the start IP address of the IPv4 address range.
- 3 Click on the **End IP address** input field.
- 4 Enter the end IP address of the IPv4 address range.
- 5 Click on **Add** to adopt the input.
- 6 Enter the **server time delay** in milliseconds.
- 7 Click on **Next**.
- 8 The **Lease Duration** menu opens up.

#### Remark

- For operation of the Access system, you generally require no exclusions in the IP address range or a server time delay. These settings are therefore customer-specific and optional.

### New Scope Wizard

#### Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

2.    5.

Excluded address range:

4.

Subnet delay in milli second:

0   6.

< Back

Next >

Cancel

**Defining the lease duration of assigned IP configurations**

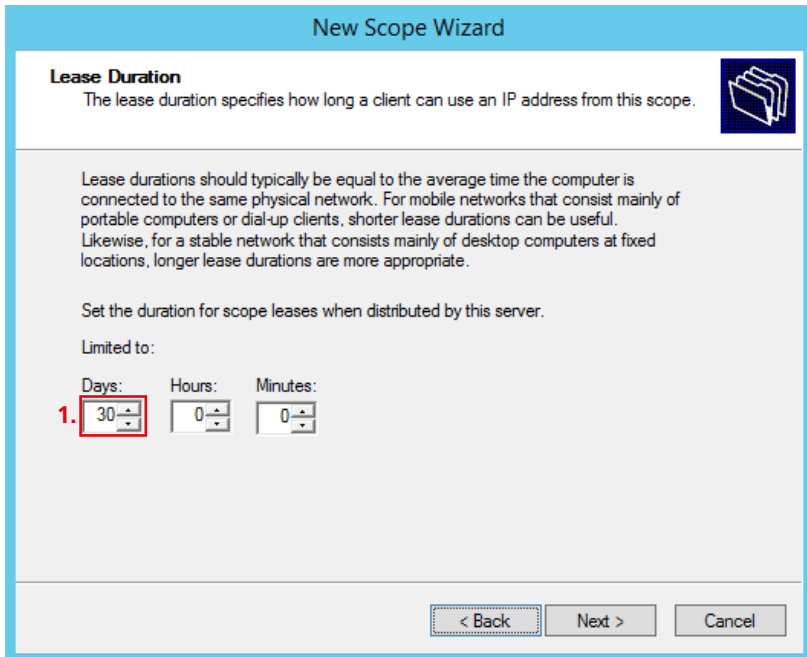
Every IP configuration assigned by the DHCP server to a DHCP client has a limited lease duration. The **lease duration** can be defined for all IP addresses assigned by the DHCP server in the Lease Duration menu.

**Procedure**

- 1 Click on the arrow buttons in the rotary selector field **Days** in order to set the lease duration (Days/Hours/Minutes) to **30 days**.
- 2 Click on **Next**.
- 3 The **Configure DHCP options** menu opens up.

**Remark**

- To operate the Access system, select a lease duration of **30 days**.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Configuring the DHCP options

In order to connect the Access server correctly to the existing network, you can configure the following DHCP options at the server operating system:

- **Router (Default Gateway)**
- **Domain Name and DNS Server**

This permits you to access the existing network or the internet with a computer within the newly configured IPv4 address range.

#### Procedure

- 1** In the option field, click on **Yes, I want to configure these options now** in order to configure the DHCP options.
- 2** Click on **Next**.
- 3** The **Router (Default Gateway)** menu opens up.


#### Remark

- If the Access server is operated in a closed network without connection to the Internet or a different network (stand-alone operation), or if no link to a different network is required, you can leave these DHCP options inactive. In this case, the configuration tasks described on the next three pages are omitted.

### New Scope Wizard

#### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now! **1.**

No, I will configure these options later

< Back    Next >    Cancel

### Specifying IP address for routers/ gateways

To make network users within the assigned IP address range accessible to another network (e.g. the internet), you can specify the IP address of one or more routers/ gateways.

### Procedure

- 1 Click on the **IP address** input field.
- 2 Enter the IP address of the router/ gateway.
- 3 Click on **Add** to adopt the input. If applicable, repeat the process in order to define additional IP addresses of other **routers/gateways**.
- 4 Click on **Next**.
- 5 The **Domain Name and DNS Servers** menu opens up.

### Remark

- If the Access server is operated in a closed network without connection to the internet or a different network (stand-alone operation), no entries are required in this input screen.

**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

2.  . . . 3.

192.168.1.254

Remove  
Up  
Down

< Back    Next >    Cancel

## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Defining the domain name and DNS server

To make network users within the assigned IP address range accessible to another network (e.g. the internet), you can specify the **domain name** and the **DNS server** of the existing network. This allows you to gain access to the Internet via the Access network using a laptop.

#### Important!

Enter only DNS servers which are accessible. DNS servers which are specified but are not accessible prevent the Siedle hardware terminals from operating.

#### Procedure

- 1 Click on the **Parent domain** input field.
- 2 Enter the domain name of the Access network.
- 3 Click on the **IP address** input field.
- 4 Enter the IP address of the DNS server you wish to be assigned to the clients.
- 5 Click on **Add** to adopt the input.
- 6 If applicable, repeat the process in order to define additional IP addresses of other **DNS servers** (redundancy).
- 7 Click on **Next**.
- 8 The **WINS Servers** menu opens up.

#### Remarks

- The **server name** can optionally be assigned; it is not necessary for operation of the Access server.
- If the Access server is operated in a closed network without connection to the internet or a different network (stand-alone operation), no entries are required in this input screen.

### New Scope Wizard

#### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:  2.

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address: 4.

<input type="text"/>	<input type="text" value="192.168.1.5"/>	<input type="button" value="Add"/> 5.
<input type="button" value="Resolve"/>	<input type="button" value="Remove"/>	<input type="button" value="Up"/>
	<input type="button" value="Down"/>	

< Back    Next >    Cancel

**Defining the WINS server**

The WINS server service was required in the past in older server operating systems (such as Windows NT). It has been replaced in current server operating systems, and so is no longer required to operate the Access server.

**Important!**

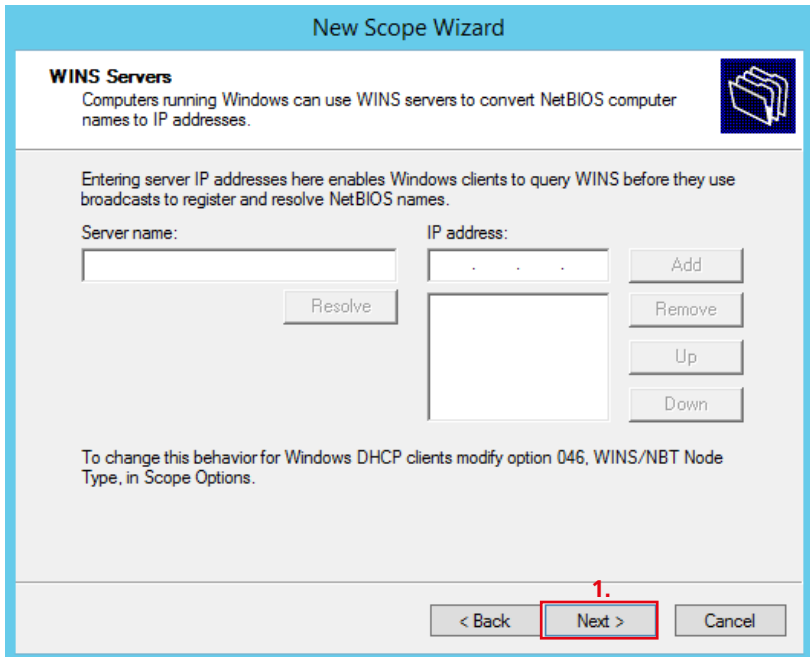
If you already operate one or more WINS servers in your network, enter these here.

**Procedure**

- 1 Click on **Next** to bypass this input.
- 2 The **Activate Scope** menu opens up.

**Remarks**

- To operate the Access server, this service is not required and therefore no entries need to be made.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Activating the IP address range

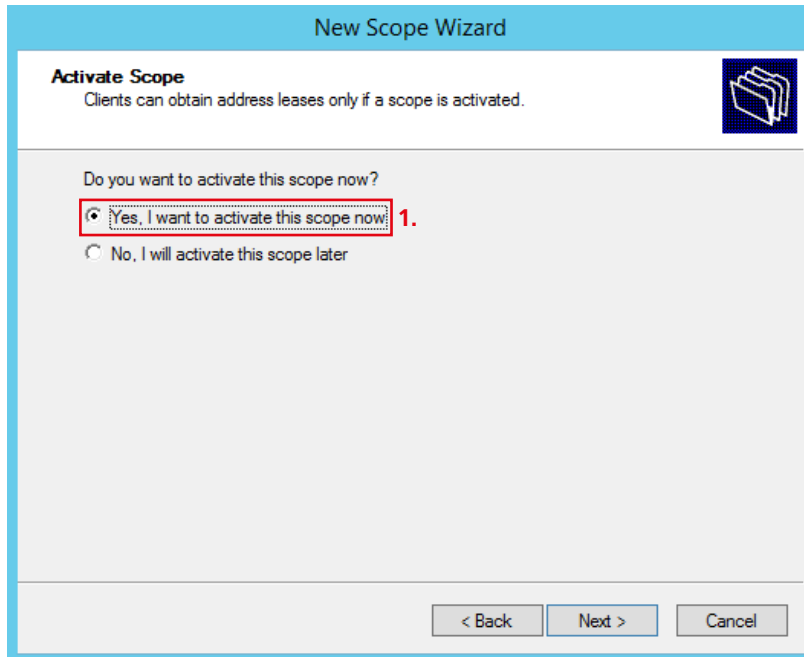
In order to operate the Access server correctly in the network, you must activate the configured IPv4 address range at the server operating system.

#### Procedure

- 1 In the option field, click on **Yes, I want to activate this scope now** in order to configure the IP address range.
- 2 Click on **Next**.
- 3 The **Completing the New Scope Wizard** menu is displayed.

#### Remarks

- If you do not activate the configured IPv4 address range, the Access users will not be able to connect to the Access server.





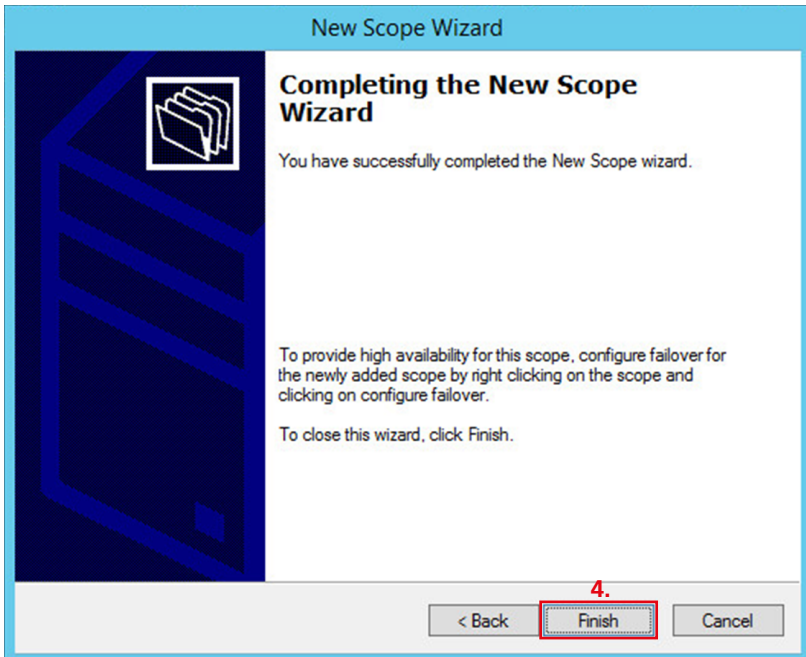
**Activating the IP address range**  
(continued)

**Procedure**

**4** Click on **Finish** to complete the process.

**5** The **DHCP** menu is displayed again.

**6** You have completed the process.



# Setting up the server operating system

## Setting up and configuring the DHCP server service

### Configuring the DHCP options

In order to operate the Access system correctly, you must activate and configure additional DHCP options at the server operating system:

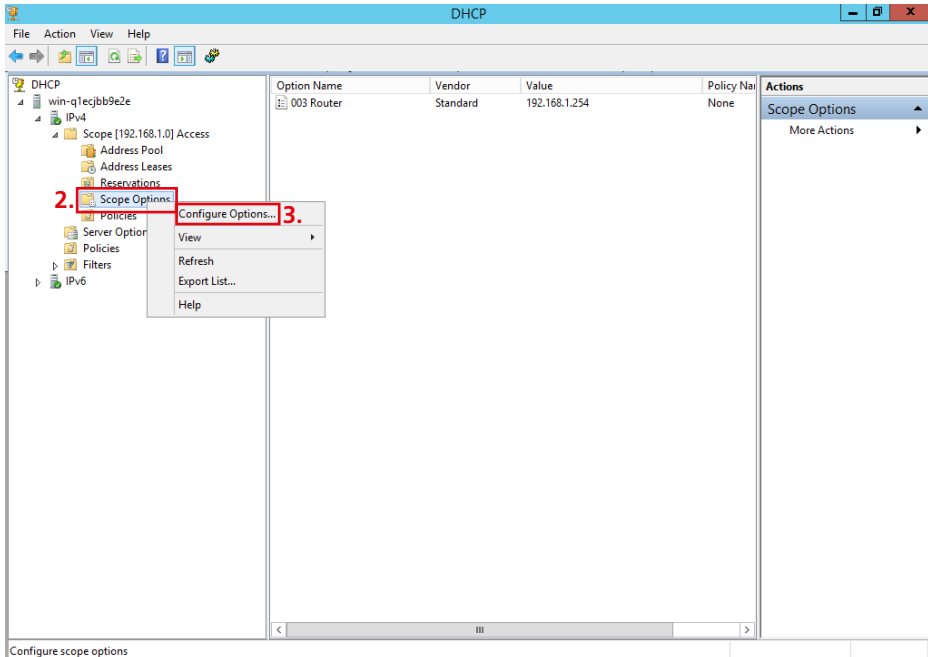
Option	Designation
04	Time Server
07	Log Servers
42	NTP Servers
66	Boot Server Host Name
67	Bootfile Name

### Procedure

- 1 Open the menu tree in the navigation area (left-hand column), until the **Scope Options** folder appears.
- 2 With the right-hand mouse button, click on **Scope Options** in order to open the context menu.
- 3 In the opened context menu, click on **Configure Options...**, in order to configure and activate the defined IPv4 address range.
- 4 The **Scope Options** menu opens up.

### Remarks

- The designations of the listed DHCP options may differ. However, the relevant number of the DHCP option remains unchangeable.



### Activating and configuring the time server

In order to allow the Access system to be correctly operated in the network, you must activate and configure the time server.

### Procedure

- 1** Under the **General** index tab in the list field, activate the entry **Time Server**, in order to activate the time server service.
- 2** Click on the **IP address** input field.
- 3** Enter the IP address of the Microsoft server.
- 4** Click on **Add** to adopt the input.
- 5** Click on **Apply** to adopt the changes.

### Optional procedure

- 6** If you are operating your own time server in the network, additionally enter the IP address of your time server here.

### Remarks

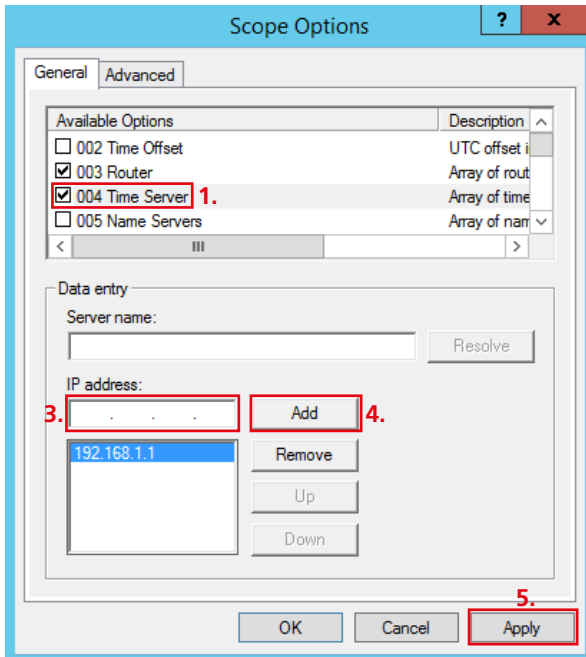
- The server name can be optionally assigned.
- If you do not activate the time server service, a time deviation can occur with the Siedle hardware terminals. The Siedle software clients (e.g. concierge) are not affected by this.

### Important!

Siedle hardware terminals whose time deviates from the Access server (maximum admissible time deviation 59 seconds) **do not** execute any switching or control commands. The Siedle software clients (e.g. concierge) are not affected by this.

### Recommendation

Here, enter only the IP address of the Access server. The Access terminals then always obtain their time setting from the Access server. This ensures that no time differences can occur between the Access server and the Access terminals.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Activating and configuring the Log servers function

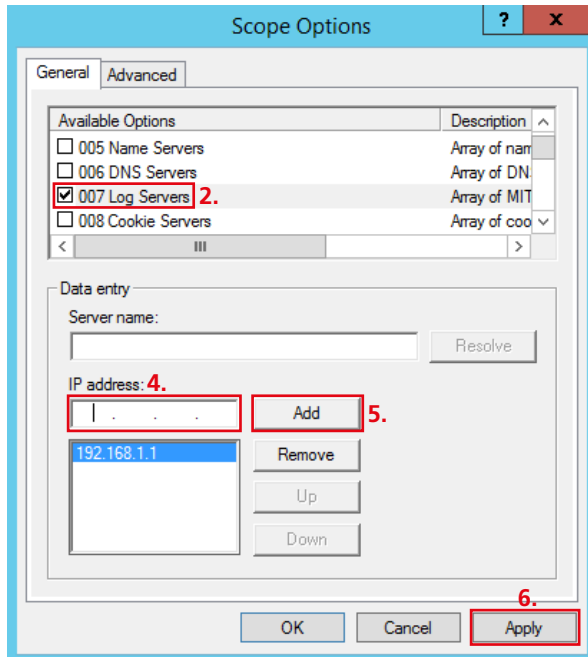
To allow the logs of the Siedle hardware terminals to be viewed at a central location, the Log Servers function must be activated and configured.

#### Procedure

- 1 Under the **General** index tab, scroll through the entries in the list field using the scroll bar until the entry **Log Servers** entry is displayed.
- 2 In the list field, activate the entry **Log Servers** in order to activate the log service.
- 3 Click on the **IP address** input field.
- 4 Enter the IP address of the Microsoft server.
- 5 Click on **Add** to adopt the input.
- 6 Click on **Apply** to adopt the changes.

#### Remarks

- The server name can be optionally assigned.
- If you do not activate the Log Servers function, the logs of Siedle hardware terminals will not be stored and cannot be evaluated if required. The Siedle software clients (e.g. concierge) are not affected by this, as their logs are stored directly on the used terminal.



### Activating and configuring the NTP server

In order to allow the Access system to be correctly operated in the network, you must activate and configure the NTP server or servers.

### Procedure

- 1 Under the **General** index tab, scroll through the entries in the list field using the scroll bar until the entry **NTP Servers** is displayed.
- 2 In the list field, activate the entry **NTP Servers** in order to activate the time server service.
- 3 Click on the **IP address** input field.
- 4 Enter the IP address of the Microsoft server.
- 5 Click on **Add** to adopt the input.
- 6 Click on **Apply** to adopt the changes.

### Optional procedure

- 7 If you are operating your own time server in the network, additionally enter the IP address of your time server here.

### Remarks

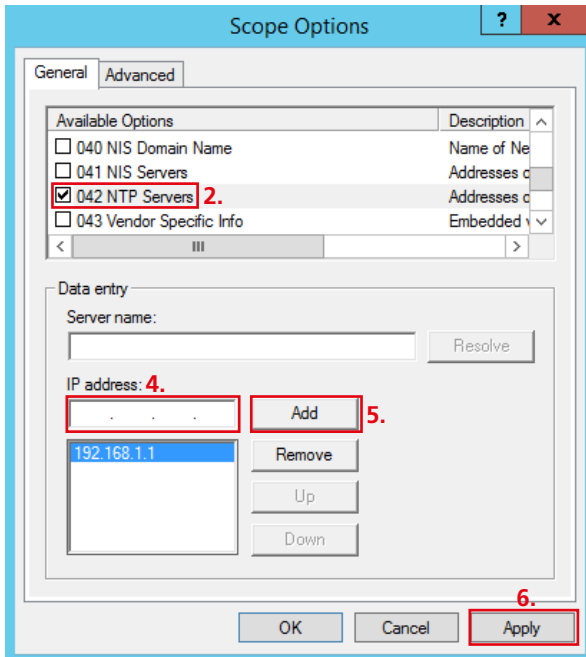
- The server name can be optionally assigned.
- If you do not activate the NTP server service, a time deviation can occur with the Siedle hardware terminals. The Siedle software clients (e.g. concierge) are not affected by this.

### Important!

Siedle hardware terminals whose time deviates from the Access server (maximum admissible time deviation 59 seconds) **do not** execute any switching or control commands. The Siedle software clients (e.g. concierge) are not affected by this.

### Recommendation

Here, enter only the IP address of the Access server. The Access terminals then always obtain their time setting from the Access server. This ensures that no time differences can occur between the Access server and the Access terminals.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Activating and configuring the boot server host name

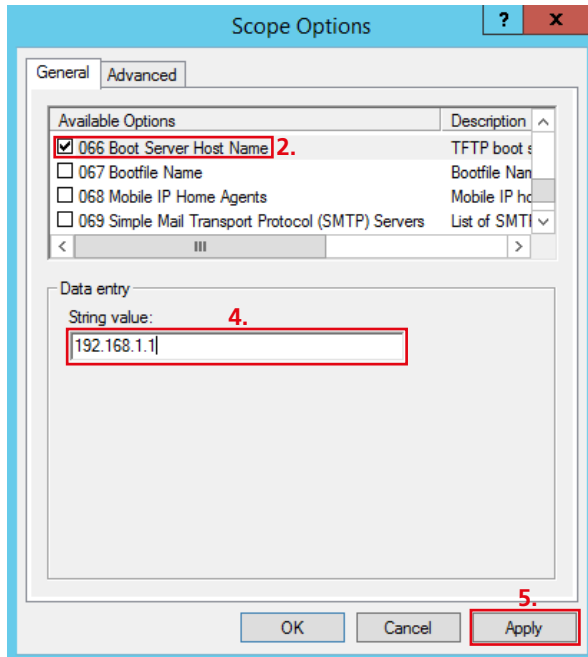
For the Siedle hardware terminals, access to the Access configuration file is required. The network path to the Access configuration file is formed from the entries Boot Server Host Name and Bootfile Name.

#### Procedure

- 1 Under the **General** index tab, scroll through the entries in the list field using the scroll bar until the entry **Boot Server Host name** is displayed.
- 2 In the list field, activate the entry **Boot Server Host Name** in order to activate the network path.
- 3 Click on the input field **String value**.
- 4 Enter the IP address of the Microsoft server.
- 5 Click on **Apply** to adopt the changes.
- 6 Click on **OK** to close the **Scope Options** window.

#### Remarks

- If you do not activate and configure the Boot Server Host Name, the Siedle hardware terminals cannot access the necessary configuration files and cannot be used in the Access network.



### Activating and configuring the Bootfile name

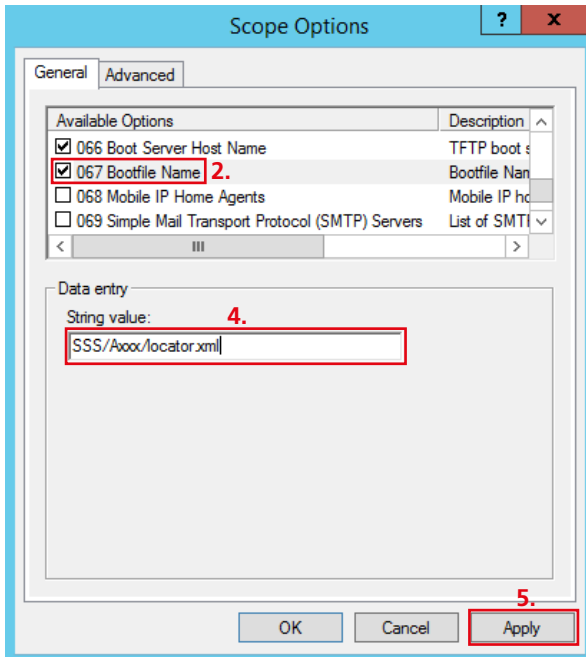
For the Siedle hardware terminals, access to the Access configuration file is required. The network path to the Access configuration file is formed from the entries Boot Server Host Name and Bootfile Name.

### Procedure

- 1 Under the **General** index tab, scroll through the entries in the list field using the scroll bar until the entry **Bootfile Name** is displayed.
- 2 In the list field, activate the entry **Bootfile Name** in order to enter the bootfile path.
- 3 Click on the input field **String value**.
- 4 Enter the complete path of the Access bootfile: **SSS/Axxx/locator.xml**.
- 5 Click on **Apply** to adopt the changes.
- 6 Click on **OK** to close the **Scope Options** window.
- 7 Close any remaining open windows which you had opened for this configuration.
- 8 This concludes the configuration of the newly created IPv4 address range and you are now back on the desktop of the server operating system.

### Remarks

- If you do not activate and configure the Boot Server Host Name, the Siedle hardware terminals cannot access the necessary configuration files and cannot be used in the Access network. The path **SSS/Axxx/locator.xml** is prescribed by the Access server and may not be changed.



## Setting up the server operating system

Setting up and configuring the DHCP server service

### Activating a remote connection

To allow the server operating system / Access server to be configured from another computer, you can allow a remote connection to the server operating system.

### Procedure

- 1 Click on the **Windows start button** (bottom left-hand corner) in order to open the start screen of the Window server.
- 2 Click on the **Server Manager** tile in order to start the server manager.
- 3 The **Dashboard** (start page) of the server manager opens up.
- 4 Click in the Navigation menu on **Local Server** to be allowed to carry out settings.
- 5 In the work area, click on the **Disabled** link which is located on the right of the entry **Remote Desktop**.
- 6 The **System Properties** menu is displayed again.

### Remarks

- This function can be enabled permanently or temporarily for commissioning or maintenance purposes, but is not a vital requirement for correct operation of the Access system. This function can be deactivated again for safety reasons at any time.

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane has 'Local Server' highlighted with a red box and a red '4.' next to it. The main area displays the 'PROPERTIES' for 'WIN-Q1ECJBB9E2E'. The 'Remote Desktop' entry is highlighted with a red box and a red '5.' next to it, showing its status as 'Disabled'.

PROPERTIES For WIN-Q1ECJBB9E2E		
Computer name	WIN-Q1ECJBB9E2E	Last install
Workgroup	WORKGROUP	Windows L
		Last check
Windows Firewall	Public: On	Windows E
Remote management	Enabled	Customer I
Remote Desktop	Disabled 5.	IE Enhance
NIC Teaming	Disabled	Time zone
Ethernet0	192.168.1.1, IPv6 enabled	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors
Hardware information	VMware, Inc. VMware Virtual Platform	Installed m
		Total disk s



**Activating a remote connection**  
(continued)

**Procedure**

**7** Change to the **Remote** index tab if this should not already be displayed.

**8** Click on **Allow remote connections to this computer** in order to enable a remote connection for the server operating system.

**9** Click on **Apply** to adopt the changes.

**10** Carry out a test connection to check whether access to the server operating system / Siedle Access server is working.

**11** Finish the test connection correctly after a successful test.

**12** Click on **OK** to close the **System Properties** window.

**13** Close any remaining open windows which you had opened for this configuration.

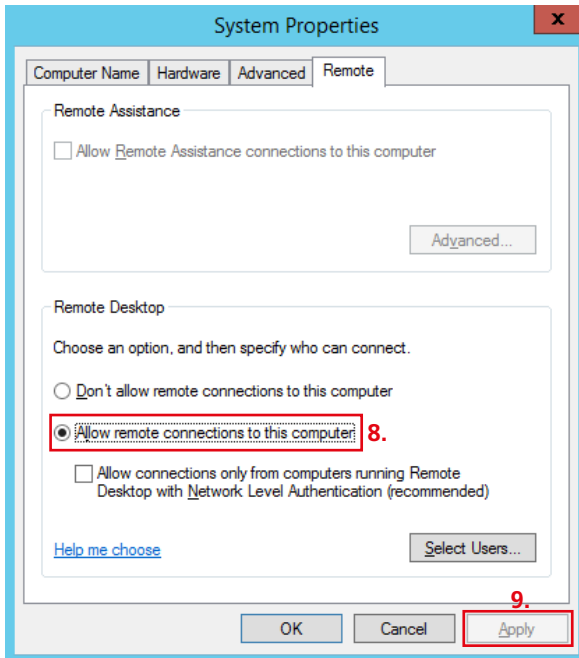
**14** Close the server manager.

**Remarks**

- If the Windows server has been configured as described, all users from the **Local Administrator** user group will be able to access the server operating system using the remote connection, as the group of local administrators has been enabled for access to the remote connection.

- Other users can be added for access over the remote connection by clicking on **Select Users...**

**You have now set up the server operating system as a DHCP server and carried out all necessary configuration steps for operation of the Access server.**



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Modifying the NTP server services configuration

If the NTP server service is made available **not** by an existing server in the customer network but by this server, you may have to adjust the previous configuration of the server operating system.

**The changes described in the following must be implemented for operating the server as a stand-alone system without domain affiliation. If this server is linked into a domain as a member server, these optional changes are not required.**

#### Background

On start-up, the server operating system always checks whether the NTP server should be started or not (domain affiliation or role of the server – e.g. domain controller).

In the previous configuration, the NTP server is not started or is automatically ended again as it is assumed that the NTP server service is provided by an existing customer network. By making these changes, the Windows time server services is set to automatic mode and starts the Windows time server service every time the server operating system is started up.

#### Remarks

To change the configuration of the server operating system, **four steps** have to be carried out.

- **Changing two** registry entries in the Windows server.
- **Entering** a control command to delete service trigger events in the input prompt.
- **Reset and start** the NTP server service **W32Time** to the automatic mode.

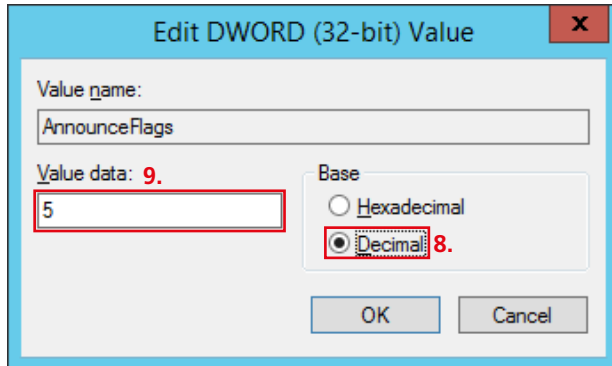
#### Procedure – Step 1:

- 1 Open the **registration editor** (click with the right-hand mouse button on the Windows start button to open the context menu).
- 2 Click in the opened context menu on **Run**.
- 3 The **Run** window opens up.
- 4 Enter **regedit** in the input field.
- 5 Click **OK**.

#### Note!

Incorrect processing of the Registry database can result in serious system disruptions or computer damage. Before making changes to the Registry database, you should back up all important computer data.

- 6 Open the path in the registration editor to change the first registry entry: **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > Config**
- 7 Double click on the registration entry **AnnounceFlags** in order to change its value.
- 8 In the **Basis** area, click on **Decimal**. The hexadecimal value **A** = decimal value **10** is entered here.
- 9 Change the value to **5**.
- 10 Confirm your change by clicking on **OK**.
- 11 You have changed the first registry entry.



**Modifying the NTP server services configuration**  
(continued)

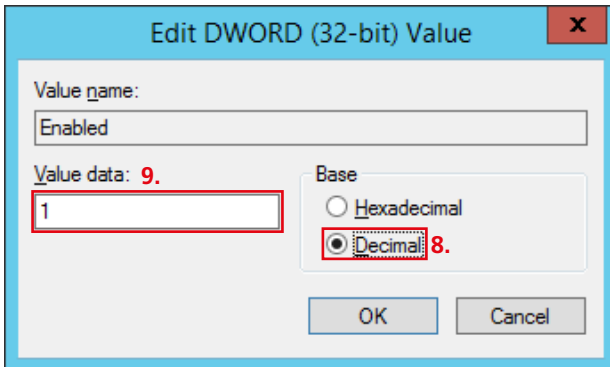
**Procedure – Step 2:**

- 1 Open the **registration editor** (click with the right-hand mouse button on the Windows start button to open the context menu).
- 2 Click in the opened context menu on **Run**.
- 3 The **Run** window opens up.
- 4 Enter **regedit** in the input field.
- 5 Click **OK**.

**Note!**

Incorrect processing of the Registry database can result in serious system disruptions or computer damage. Before making changes to the Registry database, you should back up all important computer data. To process the registration, where possible use other tools or programs than the registration editor.

- 6 Open the path in the registration editor to change the **second** registry entry: **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpServer**
- 7 Double click on the registration entry **Enabled** in order to change its value. The hexadecimal value **0** = decimal value is entered here.
- 8 In the **Basis** area, click on **Decimal**.
- 9 Change the value to **1**.
- 10 Confirm your change by clicking on **OK**.
- 11 Close the registration editor.
- 12 You have changed the second registry entry.
- 13 Close the **Registry editor** window.
- 14 Close any remaining open windows which you had opened for this configuration.



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Modifying the NTP server services configuration

(continued)

#### Procedure – Step 3:

**1** Open the input prompt (click with the right-hand mouse button on the Windows start button to open the context menu).

**2** Click in the opened context menu on **Run**.

**3** The **Run** window opens up.

**4** Enter **cmd** in the input field.

**5** Click **OK**.

**6** The input prompt opens up.

#### Note!

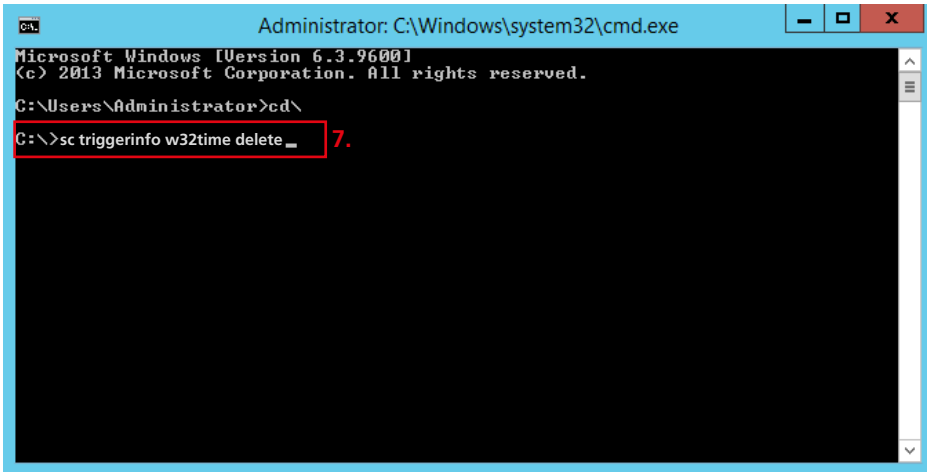
Incorrect inputs in the input prompt can result in serious system disruptions or computer damage. Before making entries in the input prompt, you should back up all important computer data. The command you enter will influence the service control management in the server operating system.

**7** Enter the command **sc triggerinfo w32time delete** in the input prompt and confirm your input with the Enter button. This command will delete the existing service trigger events of the Windows time server service (**w32time**). Originally configured or existing service trigger events affect the service behaviour of the Windows time server service (e.g. service switches off sporadically if previously set framework conditions are no longer met, although the system has been set to automatic).

**8** A confirmation message **[SC] Change-ServiceConfig2 SUCCESS** appears in the input prompt.

**9** Close the **input prompt**.

**10** You have entered the control command in the input prompt and deleted the existing service trigger events.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\
C:\>sc triggerinfo w32time delete _
```

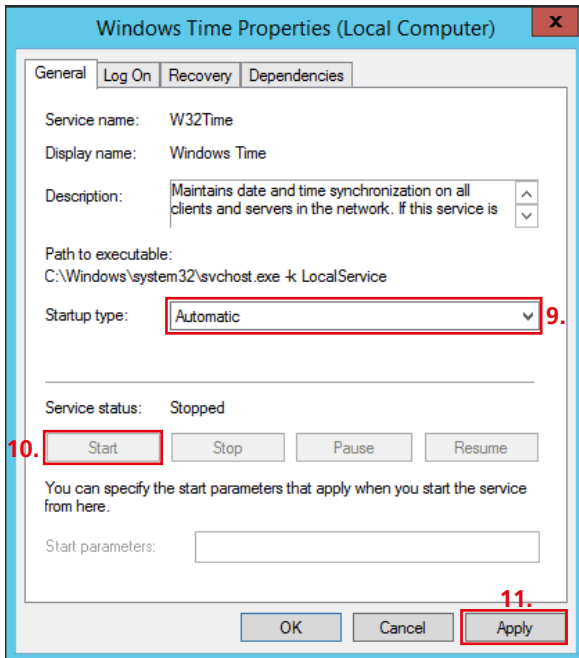
**Modifying the NTP server services configuration**  
(continued)

**Procedure – Step 4:**

- 1 Open **Services** management in the server operating system (click with the right-hand mouse button on the Windows start button to open the context menu).
- 2 Click in the opened context menu on **Run**.
- 3 The **Run** window opens up.
- 4 Enter **services.msc** in the input field.
- 5 Click **OK**.
- 6 The input prompt opens up.
- 7 The Microsoft **Services** management opens up.
- 8 Double click on the service entry **Windows Time** in order to configure the properties of the Windows Time server service.
- 9 Under the index tab **General**, change the entry for **Startup type** to **Automatic** in order to change the service over to the automatic mode.

- 10 Click on the **Start** button to start the server service.
- 11 Click on **Apply** to adopt the changes.
- 12 Click on **OK** to close the **Windows Time Properties** window.
- 13 Close the Service management.
- 14 You have completed the optional configuration of the server operating system, changed the Windows Time server service/NTP server service (Windows Time Service) over to the automatic mode and started it.

**The server operating system is now configured and active for the DHCP and NTP server roles. Now install the Access system.**



## Setting up the server operating system

### Setting up and configuring the DHCP server service

#### Subsequent installation of the missing software platform (Microsoft .NET Framework 3.5) with command line

Some components of the Access server (**Microsoft SQL server**) require the software platform **Microsoft .NET Framework 3.5**, which you must install on the server operating system before installing the Access server.

#### Important!

If you have **not** installed the **Microsoft .Net-Framework 3.5** on the server operating system, you can **not** install the Access system, as this will result in a forced cancellation of the installation process.

#### Remark

- For installation of the software platform **Microsoft .NET Framework 3.5** you require the original installation data carrier of your server operating system.

Subsequent installation of the software platform is carried out using a command line command.

#### Procedure

- 1 Open the input prompt (click with the right-hand mouse button on the Windows start button to open the context menu).
- 2 Click in the opened context menu on **Run**.
- 3 The **Run** window opens up.
- 4 Enter **cmd** in the input field.
- 5 Click **OK**.
- 6 The input prompt opens up.

#### Note!

Incorrect inputs in the input prompt can result in serious system disruptions or computer damage.

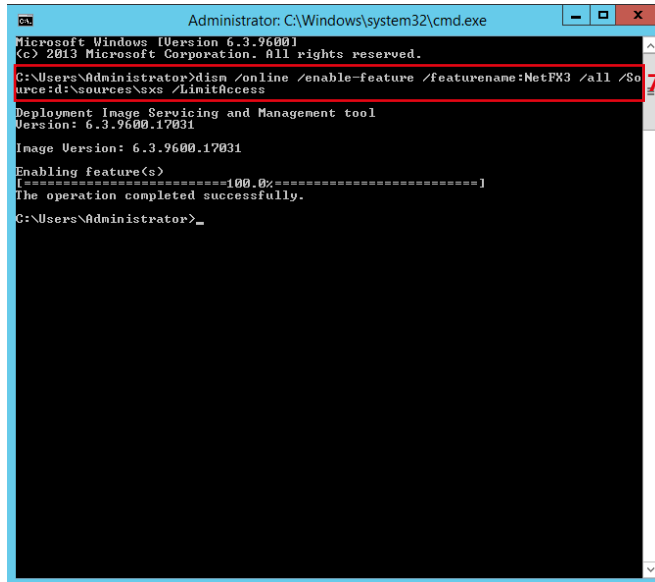
7 Insert the original installation data carrier (**Microsoft Server 2012 R2 Standard**) into the available optical drive. If a window of the Windows configuration should open, shut it.

#### Remark

- In the next command line command, the system assumes the optical drive in question is drive d:; if necessary, change the drive letter.

8 Enter the command-line command (see below) in the input prompt and confirm your input with the Enter button.

9 Close the **input prompt**.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dism /online /enable-feature /featurename:NetFX3 /all /Source:d:\sources\sxs /LimitAccess

Deployment Image Servicing and Management tool
Version: 6.3.9600.17031
Image Version: 6.3.9600.17031

Enabling Feature(s)
[=====100.0%=====]
The operation completed successfully.

C:\Users\Administrator>
```

#### Kommandozeilen-Befehl:

```
dism /online /enable-feature /featurename:NetFX3 /all /Source:d:\sources\sxs /LimitAccess
```

**Installing the missing software platform (Microsoft .NET Framework 4.6.1)**

For operation of the Access system from V 4.0.0, the Microsoft .Net Framework 4.6.1 for Windows Server 2012 R2 is required.

**Important!**

If you have **not** installed the **Microsoft .Net-Framework 4.6.1** on the server operating system, you can **not** install the Access system, as this will result in a forced cancellation of the installation process.

**Remark**

The Microsoft .Net Framework 4.6.1 is available in two variations:

- **Offline installer** for installations without an internet connection
- **Web installer** for installations over the internet

**Procedure**

- 1** Save the **.Net Framework 4.6.1** on the desktop of the server operating system.
- 2** Start the installation with a double click on the program icon.
- 3** Accept the licence terms
- 4** The **.Net Framework 4.6.1** is installed on the server operating system.
- 5** End the installation following completion by clicking on **Finish**.



# Setting up the server operating system

## Changing the server configuration

Roles, services and options which were not installed during commissioning can be set up following preceding commissioning instructions.

If you wish to create a new IP address range in a different subnet for the Access system, we recommend setting up the DHCP server service again (new Scope...).

Configuration change	Value	Path
<b>Server network adapter</b>	IP address	Start > Control Panel > (Network and Internet) > Network and Sharing Center > Change adapter settings > [Right mouse click on Access network adapter] > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties > ...
	Subnet mask	
	Default gateway	
	DNS server (Preferred/Alternate)	
<b>Server services</b>	Add / remove server roles/features	Start > Server Manager > Manage > Add/Remove Roles and Features
<b>DHCP server service</b>	Name of the DHCP server service [Scope name]	Start > Server Manager > Tools > DHCP > [Server name] > IPv4 > Scope... > [right mouse click on <b>Scope...</b> ] > Properties > General > ...
	IP address range [address pool]	
	Validity duration of IP configuration [address leases]	Start > Server Manager > Tools > DHCP > [Server name] > IPv4 > Scope... > [right mouse click on <b>Scope...</b> ] > Properties > Advanced > ...
	Server time delay [subnet delay]	
	IP network class [length/suffix]	
	Subnet mask	The DHCP server service must be set up again: Start > Server Manager > Tools > DHCP > [Server name] > IPv4 > [right mouse click on <b>IPv4</b> ] > New Scope ...
	Exclusions in the IP address area	Start > Server Manager > Tools > DHCP > [Server name] > IPv4 > Scope... > Address Pool > [right mouse click on <b>Address Pool</b> ] > New Exclusion Range... > ...
	Remote connection [remote desktop]	Start > Server Manager > Local Server > Remote Management/Desktop > ...
<b>DHCP options [Scope Options]</b>	003 Router (IP address router/gateway)	Start > Server Manager > Tools > DHCP > [Server name] > IPv4 > Scope... > Scope Options > [right mouse click on <b>Scope Options</b> ] > Configure Options... > ...
	004 Time Server	
	006 DNS Servers (Domain name and DNS server)	
	007 Log Server	
	042 NTP Server	
	044 WINS/NBNS Servers	
	066 Boot Server Host Name	
	067 Bootfile Name	
<b>NTP server</b>	Registration database	See preceding chapter
	Service Trigger Events	
	Service management	



<b>Configuration change</b>	<b>Value</b>	<b>Path</b>
<b>Password options – Administrator</b>	Password validity	Start > Server Manager > Tools > Computer Management > Local Users and Groups > Users > Administrator > General > ...
<b>Windows Update</b>	System updating settings	Start > Server Manager > Local Server > Windows Update > Let me choose my settings > ...
<b>Time zone</b>	Time zone settings as well as date/time	Start > Server Manager > Local Server > Time zone > ...
<b>Computer name</b>	Host name settings	Start > Server Manager > Local Server > Computer name > Change... > ...

## Installing the Access system

### Downloading and installing the Access system

Access Professional can only be downloaded exclusively by certified Siedle partners over the protected Siedle download area.

### Important!

If you have **not** installed the **Microsoft .Net-Framework 3.5 / 4.6.1** on the server operating system, you can **not** install Access Professional, as this will result in a forced cancellation of the installation process.

### Procedure

- 1 Open the link to the protected Siedle download area.
- 2 Carry out the registration process.
- 3 Download Access Professional and save it locally on the server on which you wish to install it.
- 4 Close the protected Siedle download area.
- 5 Start the installation of Access Professional by a double click on the downloaded installation file.
- 6 The installation is prepared and the language selection opens for the installation Wizard.

### Remarks

- For installation of Access Professional, the server operating system Microsoft Server 2012 R2 Standard or Datacenter is required.
- If the Access installer is unable to find an accessible DHCP server service, a notice is generated indicating that a DHCP server must be accessible in or over the Access network in order for Siedle hardware terminals to operate.
- The DHCP Server service does not necessarily have to be installed on this server (Access server).



Please wait while Setup is loading...

verifying installer: 11%



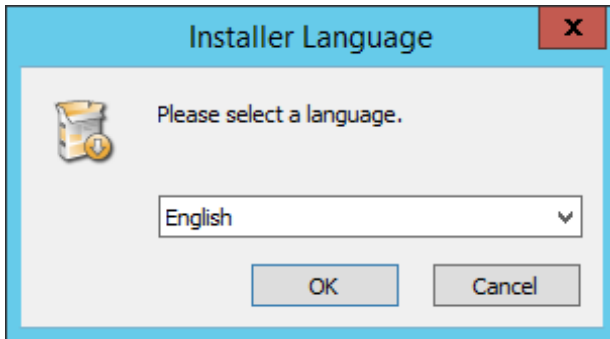
### Installation Wizard – Language selection

#### Procedure

- 1 Select the language you require for the installation Wizard in the dropdown menu.
- 2 Confirm the selection with **OK**.
- 3 The installation Wizard opens up.

#### Remarks

- The installation Wizard can be executed in 2 languages (German or English).
- During a system update, no language selection takes place, and the language selected during initial installation is used.

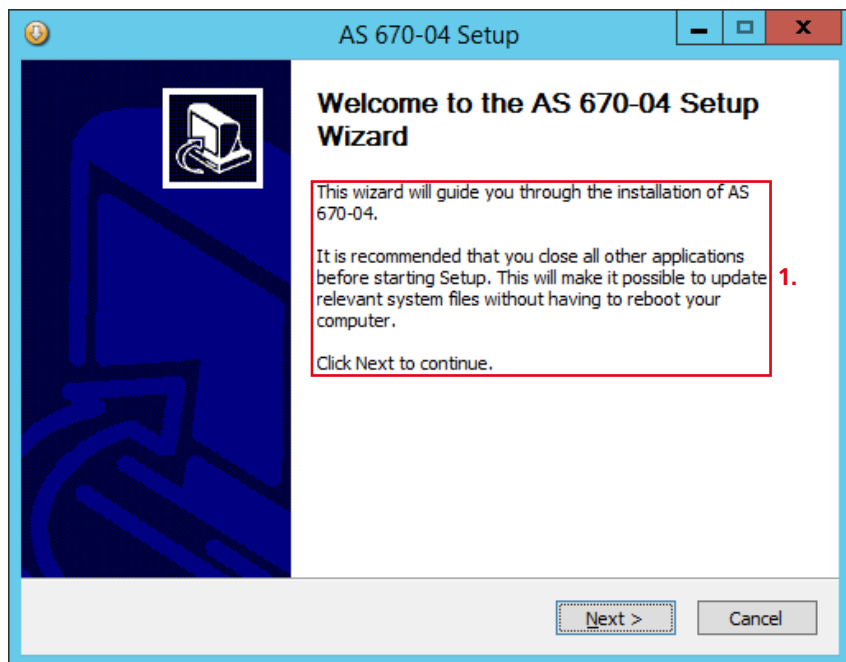


## Installing the Access system

### Starting the installation

#### Procedure

- 1 Observe the instructions and close all other open programs.
- 2 Start the installation process by clicking on **Continue**.



**Checking the safety warning message**

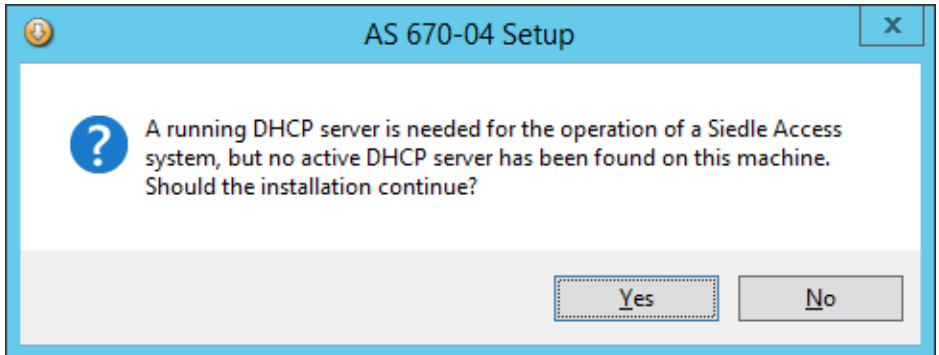
If the Access installer is unable to find an accessible DHCP server service, a notice is generated indicating that a DHCP server must be accessible in or over the Access network in order for Siedle hardware terminals to operate.

**Procedure**

- 1 Interrupt the installation process of Access Professional by clicking on **No**.
- 2 Check that the previously executed configuration of the server operating system was correct and complete.
- 3 Correct any incorrect configurations.
- 4 Restart the installation process of Access Professional.

**Remark**

- This message only appears if the DHCP server service intended for the Access network is **not available**.



# Installing the Access system

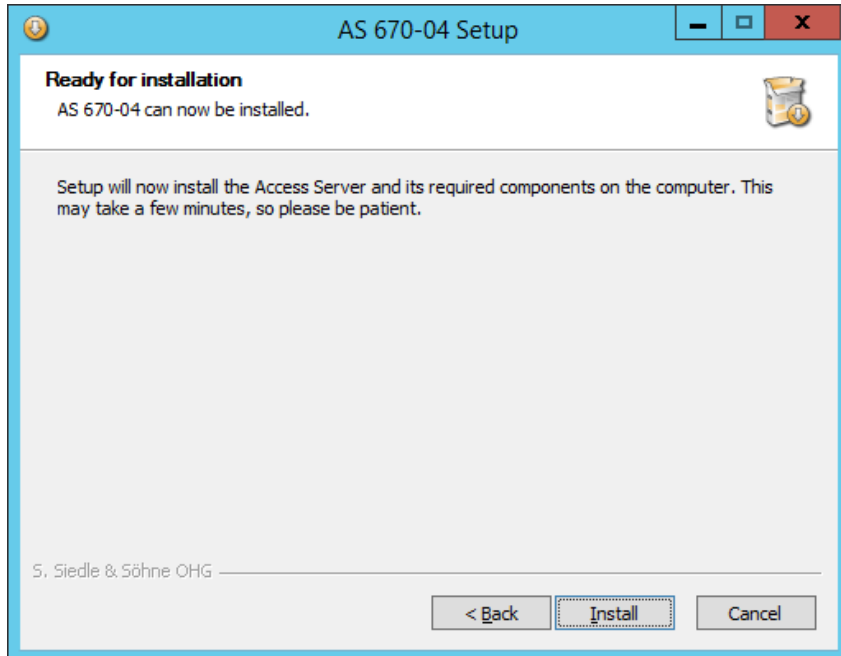
## Starting the installation

### Procedure

- 1 Click on **Install** in order to start the installation of Access Professional.
- 2 Access Professional is installed.
- 3 The installation progress is displayed.

### Remark

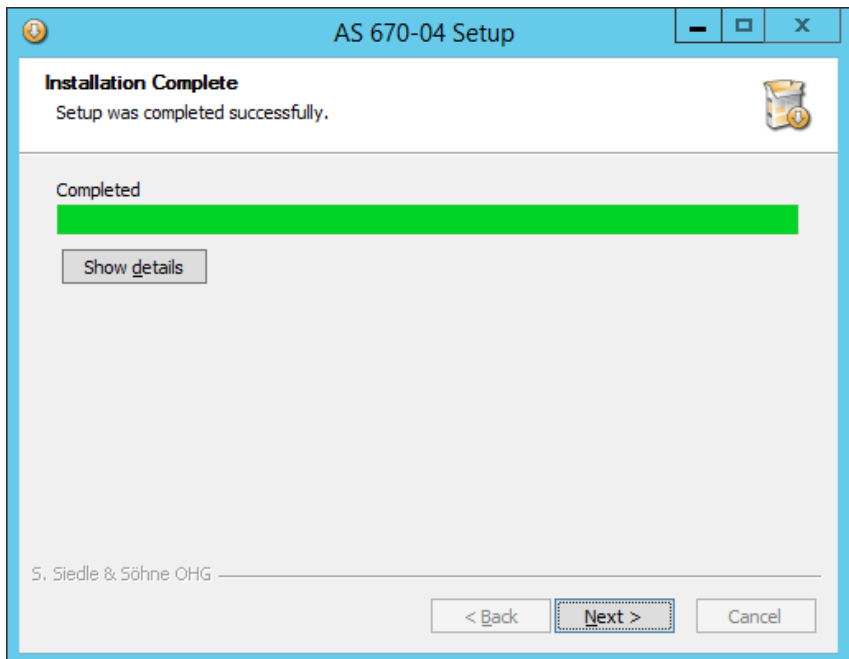
As of Access Professional V. 4.1.0, the Access system is installed in the Windows standard folder for programs.



## Completing the installation

### Procedure

1 Click on **Continue** in order to continue the installation of Access Professional.



## Installing the Access system

### Restart the system

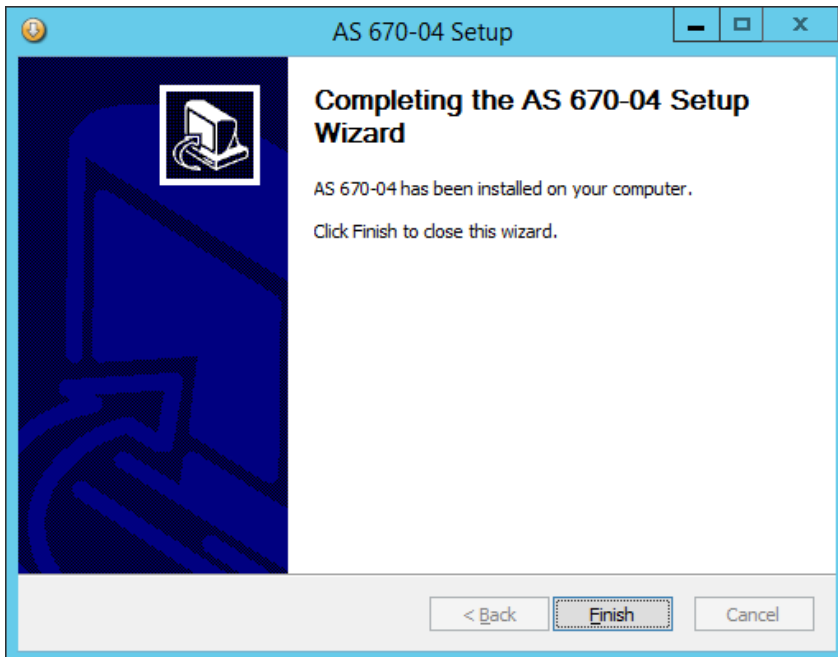
After completed installation of Access professional, the server operating system must be restarted.

### Procedure

1 Click on **Complete** in order to restart the system.

### Remarks

- After completing the installation, new program icons are located on the desktop and in defined folders in the start menu.





**Access Professional –  
File / program icons**

The Access server hardware is delivered as standard with the following additional software tools and releases:

- 7-Zip (x64)
- Firefox
- Notepad++
- Putty
- Wireshark
- WinPcap
- Remote desktop release

**Remarks**

- The listed files and programs are required for configuration and servicing purposes and should only be used by specialist and servicing personnel.
- The Access system (software variant) is delivered **without** these additional software tools and releases.

**On completion of the installation, the Access system can be configured.**

## Optionally: Updating the Access system

### System updating procedure

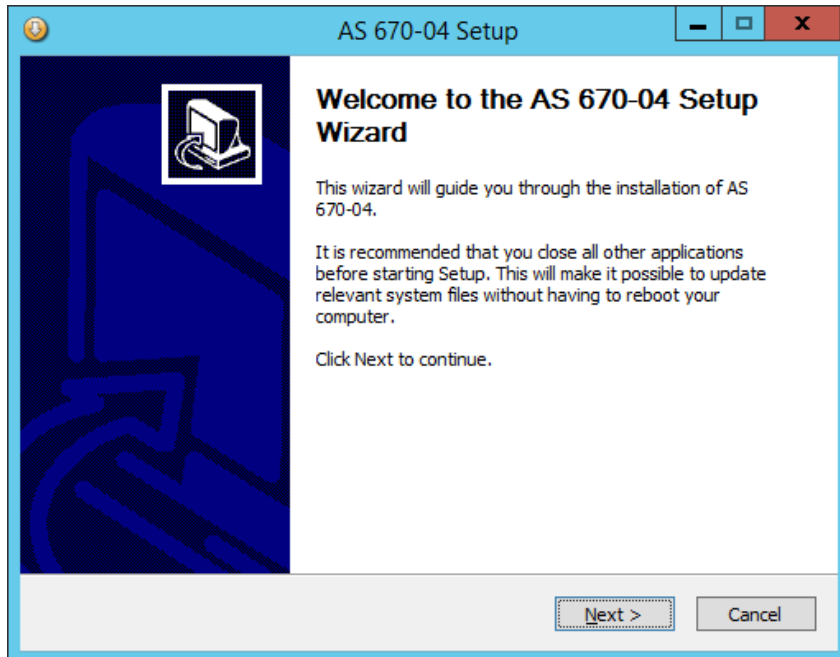
Updating an existing Access system takes place according to the following procedure:

- Shut down all hardware indoor stations linked to the Access server. The software clients and the Siedle app are automatically logged off.
- Shut down all active Access services.
- Backup of the user data (databases, user folders etc.)
- Exchange the previous Access system version and the relevant Client files by the current version.
- Restore the backup.
- Install necessary patches.
- The system update finishes with a restart of the hardware terminals.

### Important!

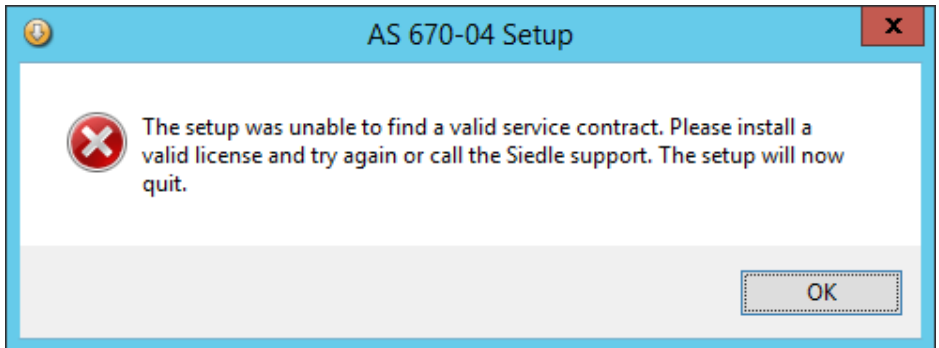
- If new versions of the software client (ASC, ASHT) are available, these must also be updated. For this, administrator rights on the relevant computer are required.
- A system update from **Access V 3...** to **Access Professional V 4...** is possible.
- A system update from **Access Professional V 4.0.0** upwards is only possible if a valid maintenance contract exists. This can be concluded against a fee.
- During the system update, the entire Access communication system is inactive and cannot be used. This means that all communication and any links set up for telephony cannot be used / are not accessible.

**Select a suitable period outside of the customer's business hours and inform all persons and departments affected in good time that the Access server will be down.**



### Checking the safety warning message

This security warning only appears if you attempt to update Access Professional from V 4.0.0 outside the purchased maintenance period. The updating process is completely cancelled after confirming. To be able to carry out a system update, a maintenance contract must be concluded against a fee.



## Optionally: Updating the Access system

### Performing a system update

#### Remarks

Apart from 2 points, the update process is the same as for a new installation of the Access system:

- During the update process, the existing folder structure of the original Access System installation structure is prescribed and can no longer be changed when carrying out a system update.

If you require a new folder, you must carry out a reinstall process.

- Before starting the actual system update, a confirmation prompt is carried out asking you to manually back up the data of your existing Access system.

#### Procedure

**1** Carry out a system backup of the Access system. The system backup is used as a security measure to ensure you can restore the Access system configuration in the event of a fault.

Detailed information on the system backup is available in the chapter **Optional administration functions – Create system backup** on page 155.

**2** Save the new version of the Access system installation file on the desktop of the server operating system.

**3** Start the installation of the Access system by a double click on the downloaded installation file.

**4** The installation Wizard opens up.

**5** Observe the instructions and close all other open programs.

**6** Start the installation process by clicking on **Continue**.

**7** Read and accept the licence agreements.

**8** Carry out the installation process by clicking on **Continue**.

**9** Answer the confirmation prompt with **Yes** or carry out a system backup of the existing Access server as described in point 1.

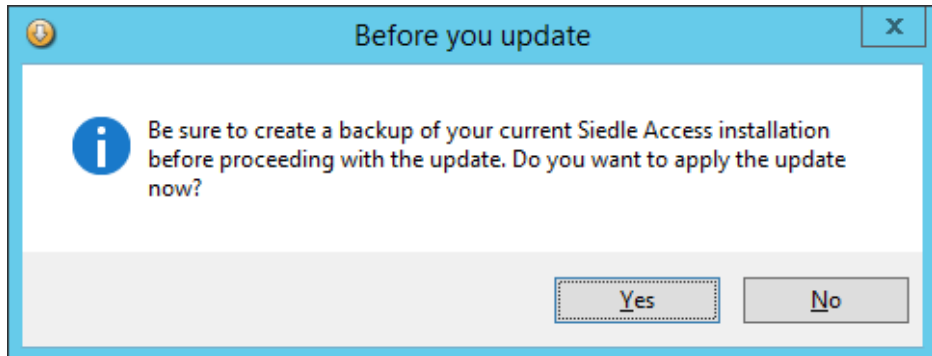
**10** Click on **Install** in order to start the installation of the Access system.

**11** The Access system is installed.

**12** The installation progress is displayed.

**13** Click on **Continue** in order to continue the installation of the Access system.

**14** Click on **Complete** in order to restart the system.



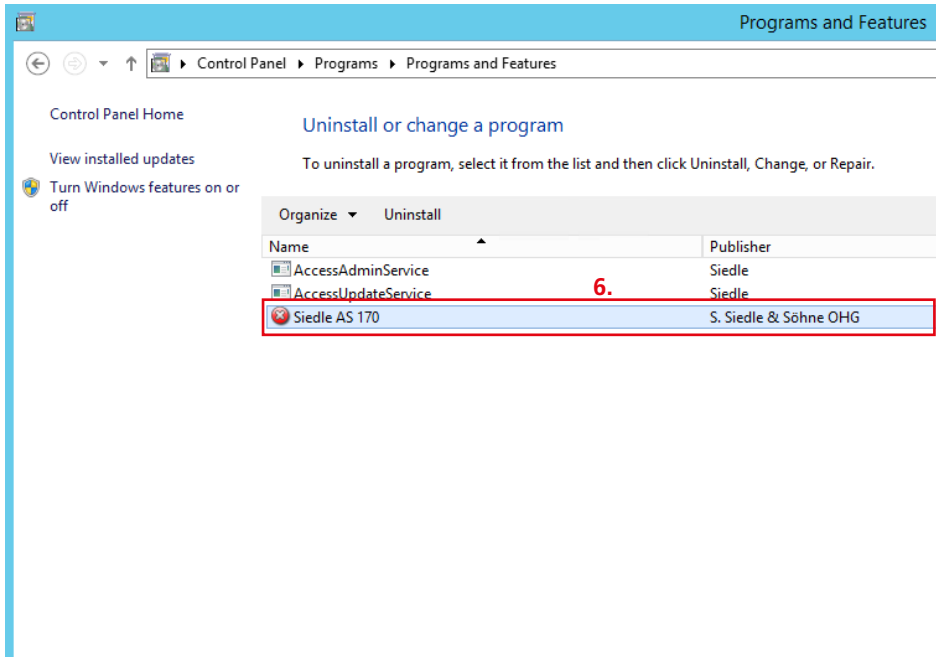
## Optionally: Uninstalling the Access system

### Access the uninstall Wizard

If you need to uninstall the Access system, carry out the uninstall process as described.

### Procedure

- 1 Click on the **Windows start button** (bottom left-hand corner) in order to open the start screen of the Window server.
- 2 Click on the **Control Panel** tile.
- 3 The Control Panel page opens up.
- 4 On the **Control Panel** page, under Programs click on **Uninstall a program**.
- 5 The page **Programs and Features** opens up.
- 6 In the page **Programs and Features**, in the table listing programs, click on **Siedle AS 170**.
- 7 In the header area of the page **Programs and Features**, click on the **Uninstall** button to uninstall the Access server.
- 8 The Uninstall Wizard **AS 170 uninstall** opens up.



## Optionally: Uninstalling the Access system

### Starting the uninstall process

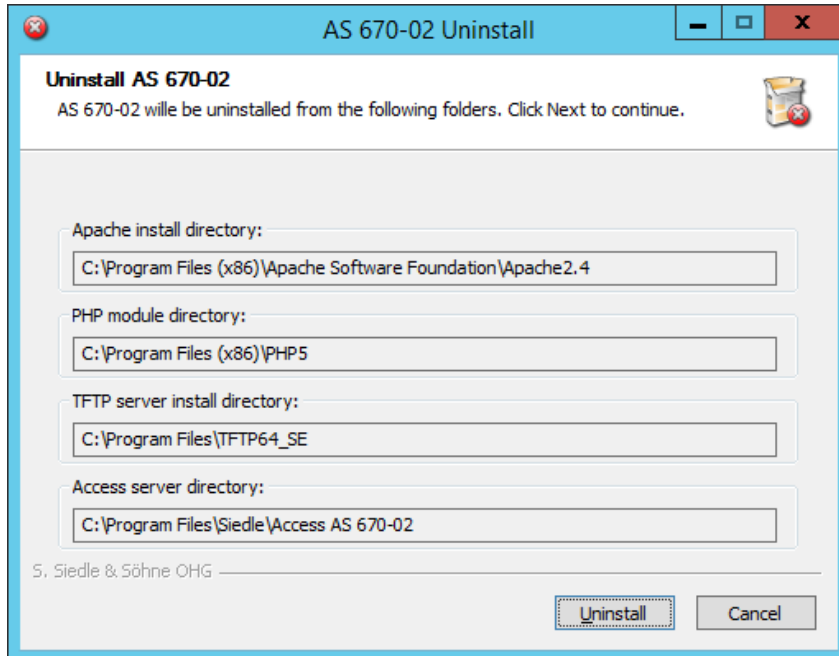
When uninstalling, all program components of the Access system are deleted, and configurations and settings (such as firewall regulations) are removed and/or rescinded.

### Procedure

- 1 Click on **Uninstall** in order to start the Access systems uninstall process.
- 2 The Access system is uninstalled.
- 3 The uninstall progress is displayed.

### Remark

- In the Uninstall Wizard, the standard and individually assigned program paths are displayed.



### Completing the uninstall process

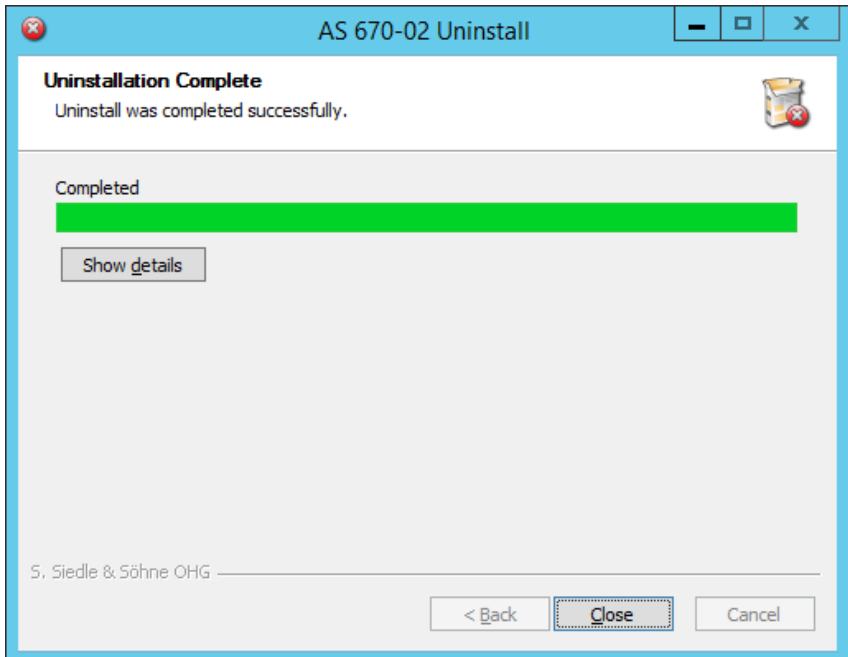
#### Procedure

**1** If required, click on **Show details** in order to see a detailed display of all uninstall steps.

**2** Click on **End** to complete the uninstall process and close the Uninstall Wizard.

#### Status of the Access server

The Siedle Access System has been uninstalled from your server.



# Setting up the Access system

## Getting started

### Installing the Firefox browser

To configure Access Professional you will require the Firefox browser directly on your server or on your commissioning computer. It is possible to directly configure the server operating system on the server or using a remote desktop connection. If you use a different web browser to the Mozilla Firefox, display errors can occur. In addition, an error message will appear, as Access Professional requires the Firefox browser.

### Procedure

**1** Install the latest version of the Mozilla Firefox web browser on your server.

### Remarks

- The Firefox browser is already pre-installed in the Access server hardware with Access Professional from V 4.x.x.
- The optional Mozilla Maintenance Service (silent update) requires a link to the Internet, otherwise it is not possible to update the Firefox browser and this has to be done regularly on a manual basis.

### Important information on the Access user rights system

User rights in the Access System are arranged on the basis of folders. A folder is a logic group combining users, doors and virtual devices in order to depict project circumstances comprising room-based, rights-based or organizationally-based groups and the required Access system topology (e.g. building with several companies or residential units – every company or residential unit is collated as a sub-folder and contains the relevant users and their devices).

Logical separations between users must be carried out using different folders and user rights restrictions. To allow complex circumstances to be depicted, a project structure may be necessary based on folders and subfolders.

### Important!

- All user rights are assigned in folders. Newly created sub-folders initially adopt the rights of the higher-level folder once only when they are created. Subsequent changes must be manually carried out in the folder levels.
- Before generating the folder structure, you ought to have defined the rights of the relevant folders for planning purposes. If the sub-folder is to contain the rights of the higher-level folders, it makes sense to adopt a hierarchical approach. In doing so, each created sub-folder is fully configured according to the plans before you insert further sub-folders. When the folder structure exists, you should create the users and assign the devices to the users. You can then continue with detailed configuration of the individual users and devices in this sequence.

### Planning remarks

- **Plan the project structure you require** (folders, users, hardware and software devices and door stations) **in advance.**
- **Take into account the Access user rights concept without fail** (e.g. door release, calling other users, which devices are visible in the internal directory, which users may release which doors, who is entitled to initiate which switching functions, etc...).
- **Plan your Access system in such a way that both your current and possible future requirements are already taken into consideration.**



## Firewall – Necessary ports

Necessary ports	Protocol / service	Commentary
22	TCP / SSH	AHTV, AHFV and ATLC are restarted by means of SSH. This is why they must also be capable of reaching the ports for SSH and DNS (which are requested by the SSH server of the terminals).
53	UDP / DNS	
67	UDP / DHCP	DHCP requests and assignment of IP addresses and advanced DHCP options
69	UDP / TFTP	Checking/updating the firmware version of the end devices
80	TCP / HTTP	Contact lists are transmitted by HTTP to the AHTV and the AHFV. The administration user interface can also be reached over HTTP.
123	UDP / NTP	The AHTV, AHFV and ATLC receive the time of day from the NTP server.
443	TCP / HTTPS	Communication with the Siedle app via the Apple Push Notification Service (APNS).
514	UDP / SYSLOG	Transfer of log messages for end devices to the Access Server
3121	TCP / CMTP	Signalling and control of the terminals. Remote control / status messages can be freely configured in the Access software module.
5060	UDP / SIP	
8000 - 11998	UDP / RTP	Enabled port range for audio transmission.
8080	TCP / HTTP	From Access system V 3.1...: Only when using the AVP with KNX together with a building automation server (Facility Pilot Server). Port 8080 is required for direct access of the AVP to the building automation server (Facility Pilot Server).
8501	UDP / CMTP-AV	The iPhone and iPad app uses 2 network ports for all communication with the server.
8502	TCP / -	
10000 - 19998	UDP / RAW Video Data	Receive port range of the server for video streams. *
20000 - 29998	UDP / RAW Video Data	Receive port range of the client for video streams. *
33333	UDP / -	Multicast finder communication

\* The Access system manages the port range. The following port ranges are issued:

- Port 10000 to 19998: Is specified by the Access system as the receiving port.

- Port 20000 to 29998: Is specified by the Access client as the receiving port.

## Setting up the Access system

### Firewall – Video multicast IP addresses

Firewall – Video multicast IP addresses	Size	Application
The Access system is limited to a small range of permitted multicast addresses:		
224.3.0.1 - 224.3.0.255	255	H.264 video channels with video calls
224.3.1.1 - 224.3.1.255	255	H.264 video channels with observation requests
224.3.2.1 - 224.3.99.255	255	Reserved for other video standards
224.3.100.1 - 224.3.100.255	255	G.722 – Audio
224.3.101.1 - 224.3.101.255	255	G.711 – Audio
224.3.102.1 - 224.3.255.255	255	Reserved for other audio standards

#### Important remarks

- In the Access system, a single multicast address is used for all video streams.

Setting under:

**Access system: System maintenance > Basic parameters > Server > Video multicast IP**

#### Note!

Input errors are possible in the Admin GUI. Any optional IP address but also invalid character strings can be entered.

# Accessing the Access system

## Accessing the Access system

Depending on how you access the server hardware, access to the Access system takes place as follows:

Access server variant/ Access to the server	ASH 670-04 S/M	Customer's own server with installed Access system
<b>Remote access</b>	<p>The Siedle Access servers can be reached in the network as standard over the IP address <b>192.168.1.1</b>.</p> <p><b>Procedure</b></p> <ol style="list-style-type: none"><li>1 Connect the commissioning computer directly to the Access server by switch.</li><li>2 Start the Firefox browser on the commissioning computer.</li><li>3 Enter the pre-configured IP address <b>192.168.1.1</b> of the Access server.</li><li>4 The login screen of the Access system is accessed and opens in the browser window.</li><li>5 Log into the Access system (account name: admin / password: admin). *</li></ol>	<p>The customer's own server operating system can be reached in the network under the individually assigned static IP address.</p> <p><b>Procedure</b></p> <ol style="list-style-type: none"><li>1 Connect the commissioning computer directly to the Access server by switch.</li><li>2 Start the Firefox browser on the commissioning computer.</li><li>3 Enter the <b>individually assigned IP address</b> of the server operating system.</li><li>4 The login screen of the Access system is accessed and opens in the browser window.</li><li>5 Log into the Access system (account name: admin / password: admin). *</li></ol>
<b>Direct access</b>	<p>When accessing directly using the monitor, keyboard and mouse, after startup of the server hardware the login screen of the server operating system is displayed.</p> <p><b>Procedure</b></p> <ol style="list-style-type: none"><li>1 Log in to the server operating system.</li><li>2 Start the Firefox browser on the server.</li><li>3 Enter the pre-configured IP address <b>192.168.1.1</b>, local host or <b>127.0.0.1</b>.</li><li>4 The login screen of the Access system is accessed and opens in the browser window.</li><li>5 Log into the Access system (account name: admin / password: admin). *</li></ol>	<p>When accessing directly using the monitor, keyboard and mouse, after startup of the server hardware the login screen of the server operating system is displayed.</p> <p><b>Procedure</b></p> <ol style="list-style-type: none"><li>1 Log in to the server operating system.</li><li>2 Start the Firefox browser on the server.</li><li>3 Enter the <b>individually assigned IP address</b> of the server operating system, <b>local host</b> or <b>127.0.0.1</b>.</li><li>4 The login screen of the Access system is accessed and opens in the browser window.</li><li>5 Log into the Access system (account name: admin / password: admin). *</li></ol>

\* Please change the password on initial commissioning, taking note of the security instructions.

# Setting up the Access system

## Log in

## Licence agreements

### Logging in without security code

The login confirmation prompt on the login page is deactivated as standard. When first logging in, you must enter only the account name (admin) and the password (admin).

#### Procedure

- 1 Enter the preset account name **admin**.
- 2 Enter the relevant password (standard: **admin**). \*
- 3 Click on **Log in**.
- 4 The Access System Administration opens.
- 5 You are now on the start page (**Dashboard**) of the Access system.

### Additional functions at the login window

There are two active links provided at the login window:

- **Downloads:** Here, you have dual-language access (DE/EN) to information on system requirements, licence agreements and the Readme file, to the Access software clients (Access Software Concierge and Access Software In-house telephone) and to necessary Windows software components for operation at Windows computers.
- **<https://www.siedle.de>:** Here, you are forwarded to the official Siedle website and can access the latest product documentation.

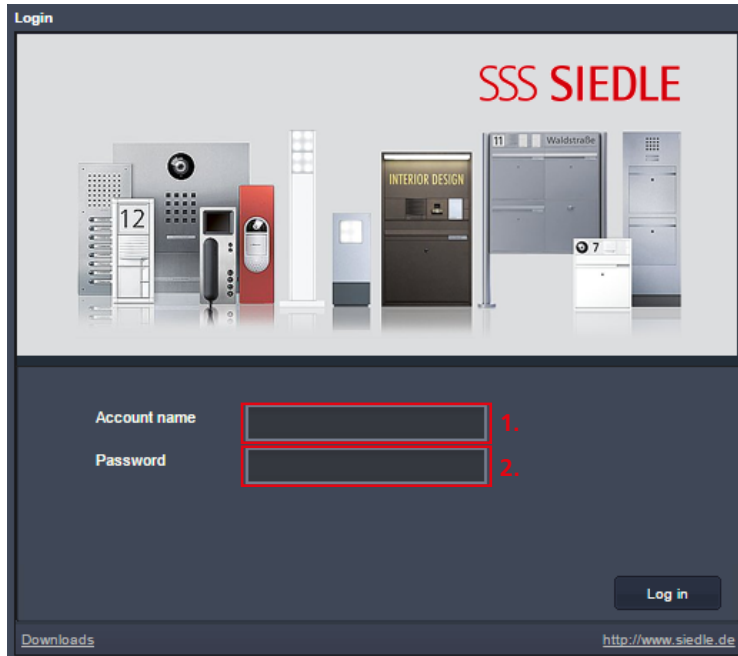
### Accept licensing agreements

When first logging in to the Access system, the page **Siedle Access Licensing Agreements** is displayed once.

On this page, you can access all licensing agreements connected to the Access system.

#### Procedure

- 1 Read all licensing agreements through carefully and save them locally in your management structure.
- 2 Click on **Done** when you have read and accepted the licensing agreements.



**User interface language**

The user interface of the Access system can be individually displayed for the relevant administrator access in two language variants (German or English). **German** is the pre-set default language. In the **Profile** menu, you can adjust the language setting.

**Note:** When you change the language setting, after saving you are automatically logged out by the system.

**Procedure – Change the user interface language**

- 1 Log into the Access system.
- 2 The menu tree **System maintenance** and the menu **Dashboard** are already opened.
- 3 Click in the header area onto **Profile**.
- 4 The **Profile** menu opens in the content area.

5 In the **Language:** line click onto the displayed language (pre-setting: German).

6 A drop-down menu opens up.  
7 Select the required language of the user interface (e.g. English).

8 A confirmation prompt appears.

9 Answer the confirmation prompt by clicking on **Yes** to confirm the change of language.

10 Click on **Save** to take the changes over in the system.

11 You are automatically logged out of the Access system.

12 Log into the Access system again.

13 The user interface of the Access system has been reset to the required language.

**Remark**

You can change the operating language of the Siedle indoor devices in the menu Basic parameters > Server > System language.

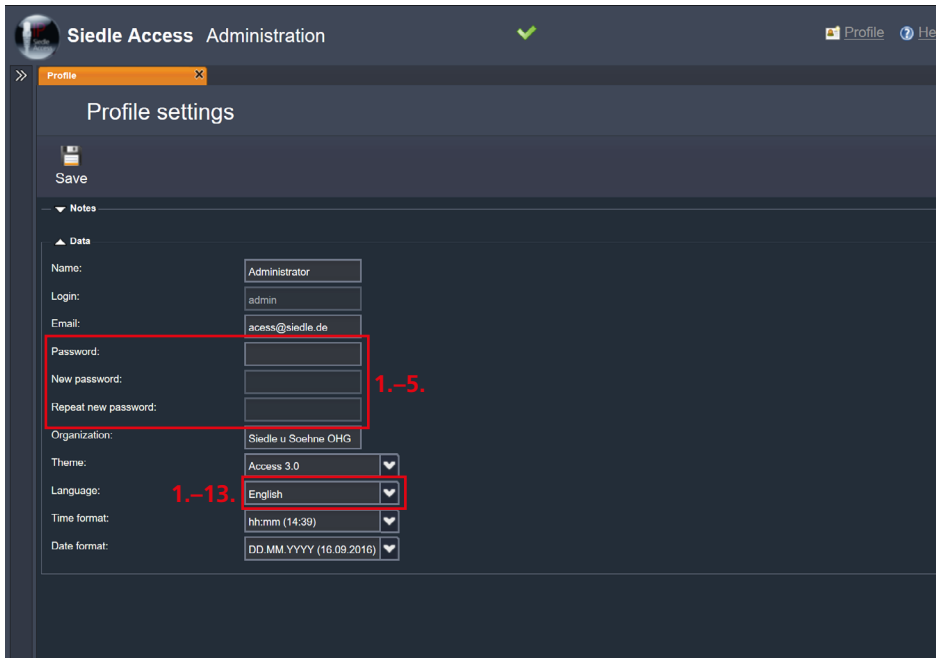
**Changing the password**

The password for user access can be changed in the **Profile** menu.

**Please change the password on initial commissioning, taking note of the security instructions.**

**Procedure**

- 1 Click in the header area onto **Profile**.
- 2 The **Profile** menu opens in the content area.
- 3 Issue a **new password in accordance with the security instructions**.
- 4 Click on **Save** to take the changes over in the system.
- 5 You have now changed the password.



# Setting up the Access system

## Safety code

### Activating the security code request

The security code is used to prevent the (huge number of) automated access attempts/login attempts to the Access system. The security code request (Captcha) is deactivated as standard.

To reactivate the security code request, please carry out the following steps:

- 1 Log into the Access system.
- 2 The menu tree **System maintenance** and the menu **Dashboard** are already opened.
- 3 Open the menu **Basic parameters**.
- 4 In the contents area, click on the **Server** tab.
- 5 Deactivate the checkbox next to **Hide Captcha during login**.
- 6 Confirm your change with **Save**.

7 When the changes to the Access system have been implemented, the system feedback message appears:

**The required operation has been completed.**

8 You have now activated the login with security code request.

### Remark

- For future log-in processes, in addition to the user name and password, the graphically displayed security code must also be entered in order to log into the Access system.

### Logging in with security code

#### Procedure:

9 Enter the preset account name **admin**.

10 Enter the relevant password (standard: **admin**).

11 Enter the dynamically changing security code with letters and numbers exactly as shown (e.g. 32pf).

12 Click on **Log in**.

13 The Access System Administration opens.

14 You are now on the start page (**Dashboard**) of the Access system.

#### Tip:

To change the security code, click on the red graphic with the security code.

Log on

SSS SIEDLE

Account name

Password

Security code

9.

10.

11.

hgXm

Log on

Cancel

Downloads <http://www.siedle.de>

**Menu structure Access Professional**

<b>Menu level 1</b>	<b>Menu level 2</b>	<b>Menu level 3</b>	<b>Page</b>	
<b>System maintenance</b>	Dashboard		88	
	<b>Basic parameter</b>	Server	90	
		Location	91	
		Date and time	92	
		Data management	93	
		Telephony	94	
	Version		154	
	<b>Administrators</b>	Accounts	147	
		Roles	145	
	Licences		97	
	Scripts		98	
	KNX addresses		99	
	Acoustic button acknowledgements		101	
	Logging		158	
	System characteristics		160	
	System backup		155	
	Restarting		152	
	User status		159	
	<b>Users</b>	Unassigned devices		111
		<b>Project</b>	Add folder	111
Add user			116	
Add group			121	
Add door (ATLC)			125	
Adding virtual device			143	
<b>Users</b>		<b>Add device:</b>	124	
		AHF/AHFV	128	
		AHT/AHTV	128	
		ASC	135	
		ASHT	136	
		ASM	137	
		AVP with KNX	131	
		External telephone	142	
		Siedle App iPad	138	
		Siedle App iPhone	138	
		Siedle App Panel (App Android)	139	
		SIP audio telephone	141	
		SIP video telephone	140	
		<b>Telephony link</b>	<b>Gateways</b>	SIP-Gateway
	SIP-Provider			106
Incoming calls	144			
Telephone directories	109			

# Setting up the Access system

## Navigation

### Start page (dashboard)

After every login at the Access system, the start page (**Dashboard**) is displayed.

### Administration graphic user interfaces

The administration graphic user interface is divided into three areas:

**1 Navigation area:** In the left-hand area of the administration graphic user interface is the navigation area with three menu items: **System maintenance**, **Users** and **telephony connection**, in each of which there are a further three menu items. The menu and submenu items are opened by clicking on the relevant button. The navigation area can be permanently opened using the double square brackets, or dynamically with a mouse click on the minimized navigation area. This allows the space for the table of contents to be increased in size.

**2 Header area:** In the upper part of the administration user interface is the header area. Here, the relevant opened menu point is displayed as a tab with heading.

In addition, you can access all tabs which were opened during the current session. The tab of the last actively opened menu is always coloured in **orange**.

On the right-hand side in the header area, you can access the **Profile** of your administration access, the **Help** function and **Logout** function to allow you to log out of the administration graphic user interface.

**Siedle Access Administration** 2. ✓

Profil Hilfe Abmelden

Dashboard

Systemwartung

- Dashboard
- Grundparameter
- Versionen
- Administratoren
- Karten
- Rollen
- Lizenzen
- Skripte
- KNX-Adressen
- Akustische Testlenkqualierungen
- Protokollierung
- Systemmeldungen
- Systemeicherung
- Neustart
- Teilnehmerstatus

1.

Dashboard

Wichtige Systemmeldungen

Nicht zugewiesene Geräte: ■ Nein

Geräte im Anmeldeprozess: ■ Nein

Statistiken anzeigen

Anzahl von Teilnehmern:	9 von 40 (Davon 1 Türen)	Trace-Service:	<span style="color: green;">■</span> Aktiv
Anzahl von Geräten:	16 von 40 (Davon 1 Türen)	DB-Service:	<span style="color: green;">■</span> Aktiv
Systemversion:	V.4.0.0 Build 1051	Base-Service:	<span style="color: green;">■</span> Aktiv
Datum der Erstinbetriebnahme:	06.05.2015	Channel-Service:	<span style="color: green;">■</span> Aktiv
Ende Wartungsvertrag:	30.06.2037	PABX-Service:	<span style="color: green;">■</span> Aktiv
		User-Service:	<span style="color: green;">■</span> Aktiv
		Automation-Service:	<span style="color: green;">■</span> Aktiv
		App-Service:	<span style="color: green;">■</span> Aktiv
		Admin-Service:	<span style="color: green;">■</span> Aktiv
		Webserver:	<span style="color: green;">■</span> Aktiv
		DHCP-Server:	<span style="color: green;">■</span> Aktiv
		TFTP-Server:	<span style="color: green;">■</span> Aktiv
		NTP-Server:	<span style="color: green;">■</span> Aktiv

3.



**3 Content area:** The content area covers the majority of the administration user interface and is located on the right of the navigation area below the header area.

The contents of the menu items are shown in detail in the content area, where they can be configured. The content area is optically grouped according to themes and if required contains user-specific notices relating to configuration of the content area. The notices are always located in the top part of the content area.

### Navigation area

In the **System maintenance** menu are all menu points you will need to manage the Access system:

- **Dashboard:** Show system status of the Access system.
- **Basic parameters:** Configure all necessary parameters for server operation.
- **Version:** View statuses of system/device versions.
- **Administrators:** Folder which contains account and role management for administration of access rights and user roles.
- **Licences:** Export hardware ID and import Access licences.
- **Scripts:** Manage system scripts.
- **KNX addresses:** Manage KNX gateway and switching points.
- **Acoustic button acknowledgements:** Manage, import and delete audio files.
- **Logging:** Manage and export system logs.
- **System messages:** Delete as yet unassigned terminals, enable processes.
- **System backup:** Configure, generate, import and export system backup.
- **Restart:** Execute a system restart and system backup, reset the system.
- **User status:** Display status of Access users.

In the **Users** menu is the structure of the Access network with the folders/groups, the individual users and devices.

Here, you can create, assign, configure and delete folder/group structures, users, virtual devices and devices.

Additional you can form and manage automatically defined and individual call groups and logically group them with the aid of folders. The complete detail configuration of the Access network is set out in this menu by selecting the relevant element (folders, users, devices and virtual devices).

The entries of the internal call numbers in the contact list are dependent on the assignment of **visible** rights for the respective folder.

In the **Telephony connection** menu, you can configure and manage the telephony connection. In addition, here you can set up and manage the assignment of incoming call numbers to internal users. All directory entries and individual directories can be generated and managed here.

With Access Professional V 4.0.0 and upwards, the field "End maintenance contract" is located on the dashboard of the Access administration user interface. The associated date indicates the date up to which the customer is entitled to install available updates/upgrades for free. The maintenance period is initially 1 year after first commissioning of the Access server for all systems. After this, all customers can decide whether they wish to extend the maintenance period for their system by paying for an extended maintenance contract. Alternatively, updates/upgrades must be purchased for a fee in certain circumstances.

# Setting up the Access system

## Configuring the basic parameters

### Basic parameter

In the **Basic Parameters** menu, set up all the operating parameters required for server operation. After saving the basic parameters, the system carries out a **restart of the Access services** (including already connected Access terminals).

Only save your entries at the very end after you have made all of the basic parameter settings.

### Remark

- From Access 3.0.0 onwards, the settings for the DHCP services are no longer configured in the Access system but in the server operating system. In the Access system, only the static IP address of the Access server can be changed. This was defined through the server operating system.

### Procedure

- 1 Open the menu **System maintenance > Basic parameters**.
- 2 The **Basic parameters** menu opens with the index tab **Notices**.
- 3 Change to the index tab **Server**.

### Server

You can carry out the following settings in the **Server** index tab:

- IP address of the Access Server
- Video-Multicast-IP
- System language of the Access indoor stations (10 languages)
- Captcha (security code)

The **server name** and the **hardware ID** are specified by the system. The **hardware ID** is required for ordering Access licences. The selected **system language** can be subsequently changed at the indoor stations.

### Procedure

- 1 Enter the IP address of the Access system assigned in the server operating system, and change the already entered IP address to the required IP address.
- 2 Change the **video multicast IP** within the prescribed ranges (AD-HOC block I – III) only if you are also operating other video multicast servers in your network whose IP address cannot be changed. The standard video multicast IP address used by Siedle is: **224.3.0.59**
- 3 Select the required **system language** of the Access indoor stations (e.g. German).
- 4 Activate or deactivate the security function checkbox **Hide Captcha on login**, in order to deactivate or activate the security code request on login.

The screenshot shows the Siedle Access Administration interface. At the top, there is a navigation bar with the Siedle logo, the text 'Siedle Access Administration', a green checkmark, and links for 'Profile' and 'Help'. Below this is a breadcrumb trail: '>> Base parameters'. The main content area is titled 'Base parameters' with a gear icon. A 'Save' button is visible. Below the title, there are tabs for 'Notes', 'Server', 'Location', 'Date and Time', 'Data management', and 'Telephony'. The 'Server' tab is selected. Under the 'Server' tab, there are several configuration fields: 'Server name' (value: ibx), 'Hardware ID' (value: AAAA-BBBB-CCCC-DDDD-EEEE), 'IP address' (value: 10.32.246.10, highlighted with a red box and labeled '1.'), 'Video Multicast IP' (value: 224.3.0.59), 'System language' (value: English, highlighted with a red box and labeled '2.'), and 'Hide Captcha during login' (checkbox checked).

### Location parameters

The **location parameters** (longitude and latitude) can be determined using search engines / map services in the Internet.

### Procedure

- 1 Change to the index tab **location**.
- 2 Enter your location parameters (**location, post code, street, telephone dialling code, country dialling code, longitude and latitude**).

### Remarks

- If the Access server is in a different time zone than the Access terminals (hardware and software), it makes sense for the location parameters of the time zone in which the Access terminals are located to be stored.
- If terminals of the Access system are operated in several different time zones, you can deactivate the display of the time at the terminals. This change is carried out using the **Users** menu in the general settings (**display the time at the terminal**) of the respective device configuration page.

The screenshot shows the 'Siedle Access Administration' interface. The 'Base parameters' section is active, and the 'Location' tab is selected. The form contains the following data:

Location:	Furtwangen
Postal code:	78120
Street:	Bregstr. 1
Area code:	07723
Country code:	+49
Longitude:	8,2
Latitude:	48,0

A red box highlights the 'Area code' field, which contains the value '+49', with a red '1.' next to it.

# Setting up the Access system

## Configuring the basic parameters

### Date and time

As standard, the Access system uses the time from the server's operating system.

If required, the time can also be assigned via an NTP server (Network Time Protocol server). For this, the Access network must have the relevant access rights for the NTP server. The NTP server is a service for synchronizing the clocks in networks. As an NTP server, either a locally or internet-operated NTP server can be used.

The date, time and time zone can also be manually changed (e.g. Access server is located in a different time zone than the software user).

### Procedure

- 1 Go to the **Date and Time** tab.
- 2 Activate the function **Adjust date and time** to enable changes to be made to the time setting.
- 3 All settings which can be changed are shown highlighted.
- 4 Change the **time zone** if required.
- 5 If you wish the Access system to use an external NTP server, enter the address of the local or public NTP server.

### Remarks

- The **time** and the **date** can only be manually changed in the Access system if nothing is entered in the field **NTP server**. Otherwise, this data is taken from the entered NTP server.
- As standard, the Windows NTP server address **time.windows.com** is entered as the NTP server. If your Access system is operated in stand-alone mode or has no access to the internet, you should enter the address of a local NTP server or delete entries in this field if no NTP server can be reached in the local network.

The screenshot shows the Siedle Access Administration web interface. At the top, there is a header with the Siedle logo, the text 'Siedle Access Administration', a green checkmark, and navigation links for 'Profile' and 'Help'. Below the header is a breadcrumb trail: '>> Base parameters'. The main content area is titled 'Base parameters' and contains a 'Save' button. A tabbed interface is visible with tabs for 'Notes', 'Server', 'Location', 'Date and Time' (which is selected), 'Data management', and 'Telephony'. Under the 'Date and Time' tab, there is a section titled 'Date and Time' with the instruction 'Adjust date and time settings:'. The configuration fields are as follows: 'Time (24 hour format) hh:mm:ss' is set to 19:24:51; 'Date DD/MM/YYYY:' is set to 15/06/2016; 'Time Zone:' is set to '(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna' with a dropdown arrow; and 'NTP server:' is set to 'time.windows.com'.

### Data management

All protocol data is saved in the Access system for an adjustable period of time (5–15 days). In the standard settings, protocol files are deleted after 5 days.

All protocol data older than the prescribed timeframe is automatically deleted. If you wish Access protocols to be permanently retained, these must be saved manually at regular intervals from the Access system.

### Remark

- Manual backup of server and terminal protocols can be carried out in the menu **System maintenance > Logging**.

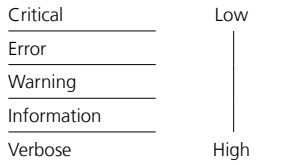
### Procedure

**1** Go to the **Data management** tab.

**2** Using the slider, the period of time (5-15 days) after which you wish the server and terminal protocol data to be deleted can be set.

**3** If necessary, adjust the degree of logging activity.

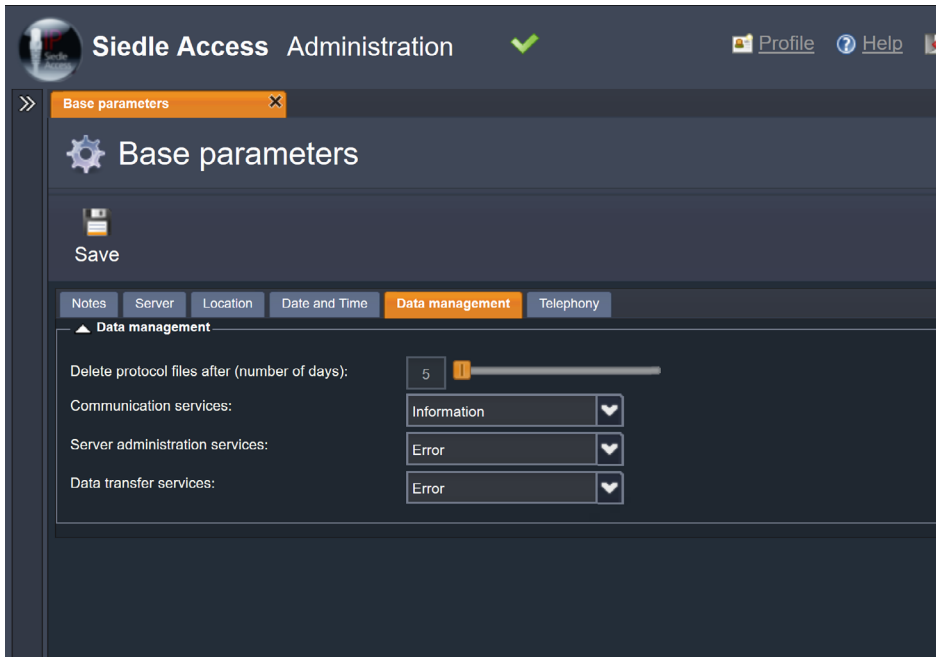
### Level of log activity



### Standard settings – degree of logging activity:

- Communication services: Information
- Server administration services: Error
- Data transfer services: Error

**Please only change the level of log activity if you are asked to do so by the Access Service Center to enable servicing work.**



# Setting up the Access system

## Configuring the server functions

### Telephony

If the Access system is connected to a telephone system, ensure that you observe a homogeneous call number plan. Every call number may only occur once in the whole system (Access system and SIP network).

If applicable, set the length of suggested call numbers to 5 digits and manually adjust the call numbers in the Access system. In the standard settings, the length of the call number suggestions is 3 digits. The length can be changed between 2 and 5 digits.

If, for instance, you wish to use four digit call numbers (such as 4711), set the length of the suggested call numbers to **4**.

### Procedure

- 1 Go to the **Telephony** tab.
- 2 Set the **Length of numbers proposed**. The phone numbers may be between 2 and 5 digits.
- 3 Click on **Save** to take the changes over in the system.

### Remarks

- After saving the basic parameters, the system carries out a restart of the Access services (including already connected Access terminals).
- If you change the length of the suggested call number subsequently, the call numbers in the existing devices/users remain unchanged.
- Only the devices/users subsequently added are assigned the call number with the newly set call number length.

- In this case, the existing devices must be manually changed individually in order to create a uniform call number structure.

**This completes the configuration of basic Parameters.**

The screenshot shows the Siedle Access Administration web interface. At the top, there is a header with the Siedle logo, the text 'Siedle Access Administration', a green checkmark, and links for 'Profile' and 'Help'. Below the header, there is a navigation bar with tabs for 'Base parameters', 'Notes', 'Server', 'Location', 'Date and Time', 'Data management', and 'Telephony'. The 'Base parameters' tab is active, and the 'Telephony' sub-tab is selected. The main content area shows the 'Base parameters' section with a gear icon and a 'Save' button. Below this, there is a section for 'Telephony' with a sub-section for 'Length of numbers proposed'. This section contains a numeric input field with the value '4' and a slider control.

### Start page (dashboard)

After every login at the Access system, the start page (**Dashboard**) is displayed. The Dashboard depicts the entire system status of the Access system. The individual statuses are displayed using a traffic light system with three colours (green, yellow and red). The green status means no faults. The yellow and red status requires investigation.

### Remarks

- From Access Professional V 4.0.0 upwards, a flash is no longer required for correct display of the administration user interface of the Access system.
  - The dashboard updates itself automatically at regular intervals (usually approx. 5 seconds; depending on browser accuracy).
- The dashboard can also be reloaded manually via **System maintenance > Dashboard**.
- Due to the changes to the date processes for the Access system, on the Dashboard, the **System version** is provided as an active link to the menu **System maintenance > Version**.

On the linked page **Version**, the software version statuses of the Access system and all Access terminals (hardware + software) are displayed.

### Procedure

- 1 Check that all statuses are free of faults.

**Siedle Access Administration** Profile Help

**Dashboard**

**Important system messages**

Not assigned devices: <span style="color: green;">■</span> No	Upcoming devices: <span style="color: green;">■</span> No
---	---

**Show statistics**

Number of users:	9 of 40 (including 1 doors)	Trace service:	<span style="color: green;">■</span> Active, No errors
Number of devices:	16 of 40 (including 1 doors)	DB service:	<span style="color: green;">■</span> Active, No errors
System version:	<a href="#">V 4.0.0 Build 1051</a>	Base service:	<span style="color: green;">■</span> Active, No errors
Initial start-up date:	06.05.2015	Channel service:	<span style="color: green;">■</span> Active, No errors
End of support:	30.06.2037	PABX service:	<span style="color: green;">■</span> Active, No errors
		User service:	<span style="color: green;">■</span> Active, No errors
		Automation service:	<span style="color: green;">■</span> Active, No errors
		App service:	<span style="color: green;">■</span> Active, No errors
		Admin service:	<span style="color: green;">■</span> Active, No errors
		Web server:	<span style="color: green;">■</span> Active, No errors
		DHCP server:	<span style="color: green;">■</span> Active, No errors
		TFTP server:	<span style="color: green;">■</span> Active, No errors
		NTP server:	<span style="color: green;">■</span> Active, No errors

# Setting up the Access system

## Configuring the server functions

### Ordering Access licences

The **hardware ID** of the Access server is generated from different hardware and software components of the Access server.

### Remarks

- The licenses are generated for each server. For this, you will need the hardware ID of the server.
  - If you modify significant sections of your hardware sever or exchange the hardware server, the hardware ID of the system changes and the previous licences have to be converted, as they are linked to the previous hardware ID.
- For detailed information on the Access user and application licences, refer to the **Planning and System Manual Access Professional**.

### Procedure – Ordering Access licences

- 1** In the navigation area, click on the **System maintenance** menu.
- 2** The **System maintenance** menu opens up.
- 3** In the opened **System maintenance** menu, click on the **Licences** menu.
- 4** The **Licences** page opens up in the content area.
- 5** Click on **Export hardware ID**.
- 6** In Windows Explorer, select the required storage location on your PC (depends on the browser).
- 7** Use the XML file generated by the Access system with the hardware ID to order an Access user licence or an optional Access user licence.
- 8** Order the Access licences required in your system (these incur a cost) from your Access Certified Partner (ACP), specifying your hardware ID.

### Important!

- A 30-day test period begins from initial commissioning, during this time all system functions can be used without any restrictions.
- After expiry of the 30-day trial period, the Access Professional system is deactivated and cannot be used until the Access licences are imported. The administrator user interface can still be accessed and the relevant notices are displayed on the dashboard.
- For regular operation of Access Professional, an Access user licence must be purchased against a fee.
- User licences for hardware indoor stations and door controllers are contained in the scope of delivery. Additional application licences are needed for software clients, third-party devices and for activating further functionality.

Siedle Access Administration

Licenses

Export hardware ID 5.

License import

Currently available licenses

Name	Description	Count	Usage	Free
AHTV 870...	Access in-house telephone video	—	1	—
AHFV 870...	Access handfree telephone video	—	1	—
AHT 870...	Access in-house telephone	—	0	—
AHF 870...	Access handfree telephone	—	1	—
AVP 870...	Access video panel	—	1	—
ATLCNG 870...	Access door loudspeaker controller	—	1	—
ASHT 170...	Access Software In-house telephone	40	2	38
ASC 170...	Access Software Concierge	40	1	39
ASM 170...	Access software module	40	0	40
ALF-S 270...	Access licence for external smartphone	40	3	37
ALFT 270...	Access licence for external tablet	40	1	39
ALFV 270...	Access licence for external video device	40	1	39
ALFA 270...	Access licence for external audio device	40	2	38
AI KNX 270...	Access licence for KNX connection	40	0	40
ALT 270...	Access licence for telephony connection	40	2	38
APH 170...	Access user	40	—	—



### Importing Access users/ Application licence

In this menu, you can add new licences and see a licence overview.

#### Condition

You were sent the ordered licence file for Access Professional, which you stored on your PC.

#### Procedure

**1** In the navigation area, click on the **System maintenance** menu.

**2** The **System maintenance** menu opens up.

**3** In the opened **System maintenance** menu, click on the **Licences** menu.

**4** The **Licences** page opens up in the content area.

**5** Click in the **License import** area on **Browse**.

**6** In the Windows Explorer, select the licence file you wish to import.

**7** Confirm your input by clicking on **Open**.

**8** The licence file is displayed in the **License import** area.

**9** Click on **Start import**.

**10** The new licences are imported and displayed in the **Available licences** list.

In the area **Current licences** is a display of which and how many devices you can create and how many of the available licences are currently being used.

#### Remark

The application licences for the Siedle hardware end devices...

- Access door loudspeaker controller (ATLC)
  - Access in-house telephone (AHT)
  - Access video in-house telephone (AHTV)
  - Access handsfree telephone (AHF)
  - Access video handsfree telephone (AHFV)
  - Access video panel (AVP)
  - External telephone
- are included in the scope of delivery of Access Professional.

Siedle Access Administration

Licenses

Export hardware id

Notes

License import **5.**

Select license file Browse Start import **9.**

Currently available licenses

Name	Description	Count	Usage	Free
AHTV 870...	Access in-house telephone video	—	1	—
AHFV 870...	Access handsfree telephone video	—	1	—
AHT 870...	Access in-house telephone	—	0	—
AHF 870...	Access handsfree telephone	—	1	—
AVP 870...	Access video panel	—	1	—
ATLCNG 070...	Access door loudspeaker controller	—	1	—
ASHT 170...	Access Software In-house telephoner	40	2	38
ASC 170...	Access Software Concierge	40	1	39
ASM 170...	Access software module	40	0	40
ALF-S 270...	Access licence for external smartphone	40	3	37
ALFT 270...	Access licence for external tablet	40	1	39
ALFV 270...	Access licence for external video device	40	1	39
ALFA 270...	Access licence for external audio device	40	2	38
AI KNX 270...	Access licence for KNX connection	40	0	40
ALT 270...	Access licence for telephony connection	40	2	38
APH 170...	Access user	40	—	—

# Setting up the Access system

## Configuring the server functions

### Additional scripts

When the Access system is delivered, all the scripts required for regular operation are also supplied. Individual control scripts can be integrated in the Access system in order to implement non-standard requests by the customer (e.g. non-standard functions or control sequences which have to be controlled via the Access server). In this menu, you can import additional scripts into the Access system and you can obtain an overview of already imported scripts.

The regular delivery includes the standard script **Standard telephone script** and the non-standard scripts **Camera actuation** and **Secondary signal unit**.

### Important!

To allow an imported script from the Access system to be processed, a system restart must be carried out.

### Procedure

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the opened **System maintenance** menu, click on the **Scripts** menu.
- 4 The **Scripts** page opens in the content area.
- 5 In the **Script import** area, click on **Browse**.
- 6 In the Windows Explorer, select the script you wish to import.
- 7 Confirm your input by clicking on **Open**.
- 8 The selected script is displayed in the display field in the **Script import** area.
- 9 Click on **Start import**.
- 10 After a successful import, a message box appears.
- 11 Confirm the message box with **OK**.
- 12 The new script is shown in the list **Current scripts**.
- 13 Carry out a system restart of the Access server.

### Remarks

- Imported scripts cannot be deleted but overwritten with the same name, for instance in order to allow changes to be carried out in already imported scripts.
- When configuring terminals, individual scripts can be integrated. These scripts are only displayed if these have previously been imported in the **Scripts** menu.
- **Standard telephone script:** Standard script used to allow communication and standard functions to be carried out.
- **Secondary signal unit:** Extended standard script to allow the additional connection of a secondary signal unit (e.g. visual signal unit in loud environments).
- **Camera actuation:** Extended standard script to allow the additional connection of a camera actuating device (e.g. video surveillance system covers the door area if a door call is initiated by a person).

**Siedle Access Administration** Profile Help

**Scripts**

Notes

Script import

5.    9.

Current scripts

Name	Version	Provider	Activated	Type of license
Camera actuation	1.1.1	Siedle	18.01.2012 11:37	SSS-BASE-3
Secondary signal unit	1.1.3	Siedle	18.01.2012 11:37	SSS-BASE-3
Default phone script	1.0.8.4	Siedle	18.01.2012 11:37	SSS-BASE-3

## KNX addresses

In this menu, you can create and manage a KNX gateway and import and manage KNX addresses (ESF file).

### Conditions

- The IP address for the KNX gateway is known.
- The number of the KNX communication port is known.
- The KNX programming is completed.
- The ESF export file (KNX address configuration) is available.

### Procedure

#### Step 1 – Create KNX gateway(s):

**1** In the navigation area, click on the **System maintenance** menu.

**2** The **System maintenance** menu opens up.

**3** In the opened **System maintenance** menu, click on the **KNX addresses** menu.

**4** The **KNX addresses** page opens in the content area.

**5** In the **Edit KNX gateway** area, click on **Add**.

**6** A new line has been entered for the KNX gateway in the overview table.

**7** In the **Names** column, click onto the empty field in order to assign a name for the KNX gateway.

**8** In the **IP address** column, click onto the empty field in order to assign the IP address for the KNX gateway.

**9** If necessary, change the entered value in the column **Port**, if a different port is required.

**10** If required, change the status in the **NAT** column to **On** if there is a router between the Access server and the KNX gateway.

**11** Check the correctness of all entered data.

**12** In the **Edit KNX gateways** area, click on **Save** in order to adopt the changes.

**13** Carry out **Step 2** on the following page.

Siedle Access Administration

KNX addresses

Notes

Edit KNX gateways

5. Add Delete Save

Name Type IP address Port NAT 6.-11.

Address import

Gateway: [dropdown]

File selection: [text input] Browse

Run

Existing KNX addresses

Delete Save

Address	Gateway	Name	Label	Data type	Data value	Usage 21.
---------	---------	------	-------	-----------	------------	-----------

# Setting up the Access system

## Configuring the server functions

### KNX addresses (continued)

#### Procedure

#### Step 2 – Add KNX address(es):

**14** In the **Address import** area, select the KNX gateway.

**15** In the **Address import** area, click on **Browse**.

**16** In the Windows Explorer, select the ESF export file (KNX address configuration) you wish to import.

**17** Confirm your input by clicking on **Open**.

**18** The ESF export file is displayed in the **File selection** field.

**19** Click on **Execute**.

**20** After completed import, all imported KNX addresses are shown in an overview table.

**21** In the **Existing KNX addresses** area, in the **Use** column, activate the checkboxes of the KNX addresses which may be used for Access device configuration.

**22** If required, carry out **Step 3**.

#### Step 3 (optional) – Manage KNX address(es):

**23** In the **Existing KNX addresses** area, carry out the necessary changes in the relevant column (e.g. **Use**).

**24** In the **Existing KNX addresses** area, click on **Save** in order to adopt the changes.

#### Note

- To allow the newly added KNX gateway to be used, you must restart the Access server services.

**25** Carry out a restart of the Access system (menu: **System maintenance > Restart**).

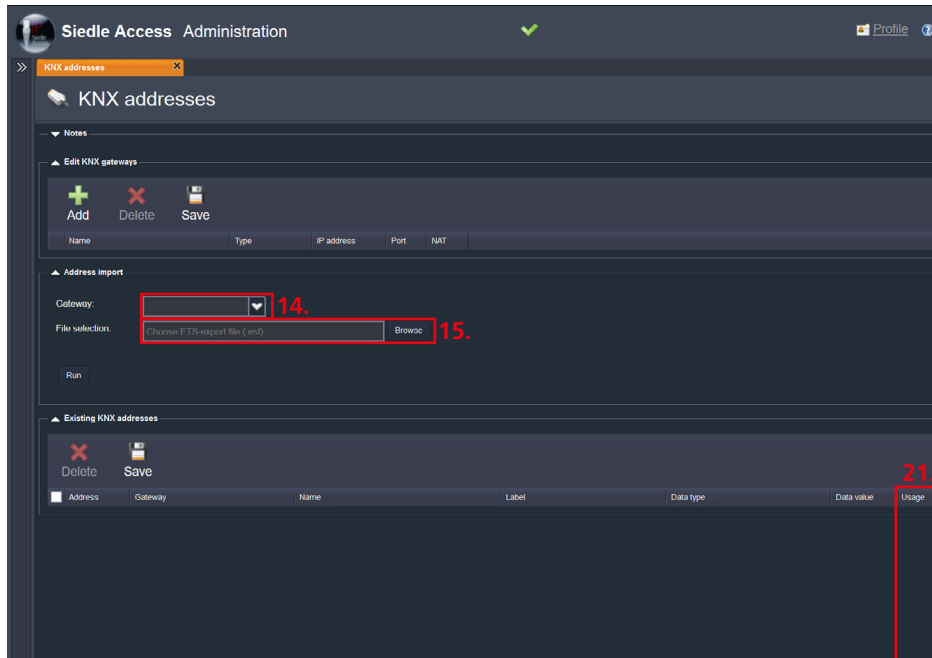
#### Remarks

- Only one KNX gateway per Access system can be created.

- In the Existing KNX addresses area, the imported KNX addresses are shown in an overview table, from where they can be individually deleted.

- In the Use column, you can determine which of the imported KNX addresses are available in the device configuration for switching and control tasks.

- The possible number of usable KNX addresses is dependent on the purchased Access application licence package for the KNX connection.



### Acoustic button acknowledgements

In this menu, you can add (your own) new acoustic button acknowledgements and see an overview of acoustic button acknowledgements already existing in the Access system. The audio file for the acoustic button acknowledgements must be created using the **pulse code modulation method** or converted into this and then stored as raw data in the uncompressed audio file format **PCM**. For this, you will require a suitable audio editor or audio recorder.

#### Technical requirements for the audio file

- Audio file format: PCM (\*.pcm)
- Metadata (Header): Raw format (RAW)
- Sampling rate: 8000 Hz
- Coding type: Signed 16 Bit PCM
- Bits: 16 Bit
- Recommended maximum length of audio content: 5 seconds

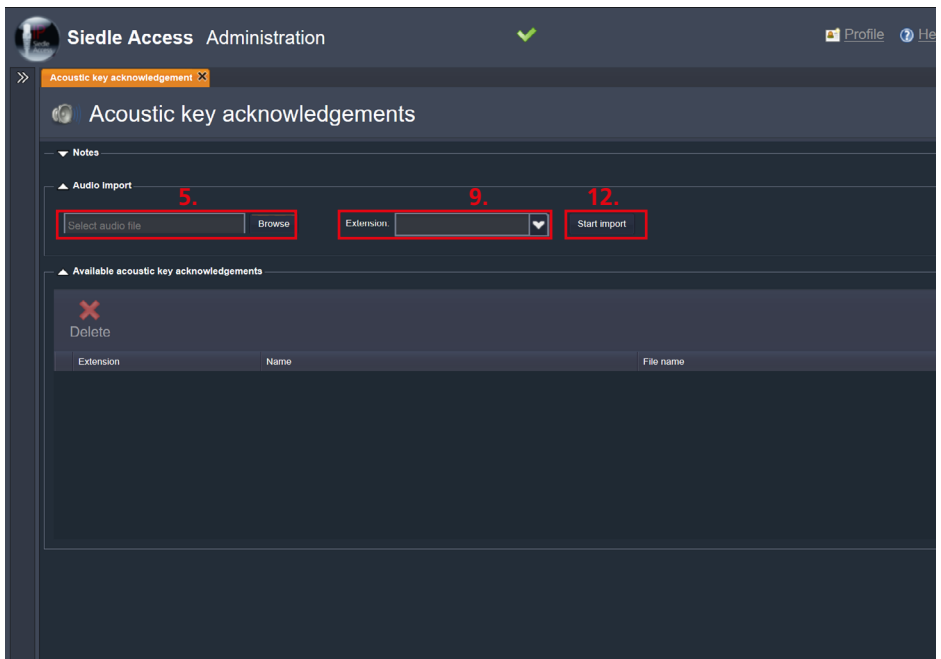
#### Procedure

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the opened **System maintenance** menu, click on the **Acoustic button acknowledgement** menu.
- 4 The **Acoustic button acknowledgement** page opens in the content area.
- 5 In the **Audio import** area, click on **Browse**.
- 6 Navigate in your Windows Explorer to the storage location of the audio file.
- 7 Click on **Open**.
- 8 The audio file is displayed in the **Audio import** area.
- 9 Click on the input field next to **Direct dial**.
- 10 A dropdown menu opens.
- 11 Select an optional call destination (**device/user/group**) to which you wish to assign the acoustic button acknowledgement.
- 12 Click on **Start import**.

13 The new acoustic button acknowledgement is displayed in the **Available acoustic button acknowledgements** list.

#### Important!

- To ensure that an assigned acoustic button acknowledgement can be played at the door station, in the **Users** menu next to the door station in question (e.g. door controller ATLC 670-0) in the **General** area, activate the function **TLC button acknowledgement**.
- The acoustic button acknowledgement is only signalled at the door station once the content of the audio file has been completely transmitted from the Access server to the door station. The call to the called user (device) is not actually established until completed signalling of the button acknowledgement at the door station. In the case of long audio files, this means that call signalling is delayed.



# Setting up the Access system

## Configuring the server functions

### Connection to telephone systems

A TC system can be connected to the Access system via SIP trunk (SIP gateway) or SIP user/client (SIP provider).

There are 2 operating modes (SIP provider and SIP gateway) for connecting a TC system to the Access system:

- Single channel connection (SIP provider)
- Bundle channel connection (SIP gateway)

### Information about SIP provider (single channel connection)

Connecting the Access system to the TC system as a PBX extension:

- One connection channel per configured SIP provider connection in the Access system (max. 50 SIP providers can be configured per Access system, including via the same prefix), one ALT 270-0 telephony connection Access licence is required per connection channel (optional).

- A PBX extension/user for connection of the Access system is also created in the TC system. This connection may vary depending on the TC system.
- Each call from the Access system to the TC system is shown with the same PBX extension call number in the TC system (call differentiation is not possible).

### Notes on the SIP gateway (bundle channel connection)

Network-side connection of the Access system to a TC system via SIP trunk:

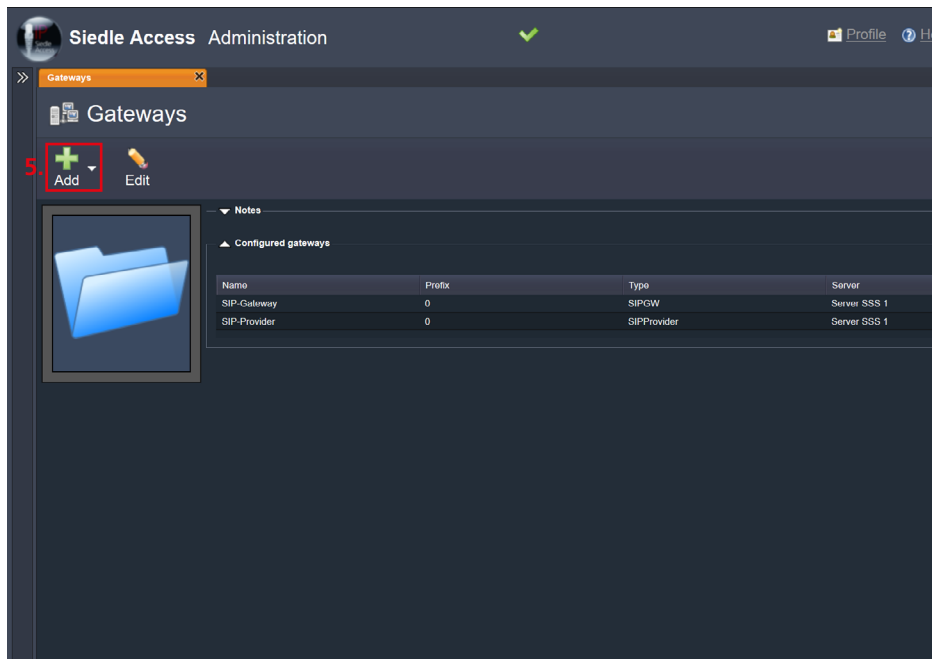
- Up to 50 connection channels in the Access system (without authentication), one ALT 270-0 telephony connection Access licence is required per connection channel (optional).
- A uniform call number plan is recommended (each assigned call number in the common Access and TC system group is unique).

- A gateway for connection to the Access system is also created in the TC system. This connection may vary depending on the TC system.

- Each call from the Access system to the TC system is shown with the relevant Access user call number (call differentiation is possible).

- As of Access system V. 2.3.0, both the call number and the user name is transmitted to the TC system.

Many TC systems include display of transmitted user names as a configurable performance feature, which must be activated and configured in the TC system if necessary. Please ask the manufacturer of the TC system whether it includes this performance feature.



### Telephony link

In this menu, you can assign an external telephone number integrated using a configured SIP gateway or an SIP provider account to any optional internal Access user or an optional door station as a call destination. The overview shows the most important information on the created telephony routes (gateway, incoming call number and destination in the Access system).

### Remarks

- Please note that any changes are only applied after restarting the Access system and the Siedle terminals.
- Details on configuration of the telephony connection are provided on the following pages.

### Procedure – Creating a SIP gateway or SIP provider account:

- 1** In the navigation area, click on the **Telephony connection** menu.
- 2** The **Telephony connection** menu opens up.
- 3** In the opened **Telephony connection** menu, click on the **Gateways** menu.
- 4** The **Gateways** page opens up in the content area.
- 5** Click on **Add**.
- 6** Select a **SIP gateway** or **SIP provider**.
- 7** Enter the necessary data.
- 8** Click on **Save** to take the changes over in the system.

### Procedure – Editing a SIP gateway or SIP provider account:

- 1** In the navigation area, click on the **Telephony connection** menu.
- 2** The **Telephony connection** menu opens up.
- 3** In the opened **Telephony connection** menu, click on the **Gateways** menu.
- 4** The **Gateways** page opens up in the content area.
- 5** Select a **SIP gateway** or **SIP provider**.
- 6** Click on **Edit**.
- 7** Carry out the changes or click on **Delete**, if you wish to delete the **SIP gateway** or the **SIP provider**.
- 8** Click on **Save** to take the changes over in the system.

### Configure SIP gateways

In this menu, you can configure and delete SIP gateways (VoIP telephony). In addition, you are given a central overview of the configured SIP gateways. SIP gateways enable connection of the Siedle Access server on the network side to an SIP-capable telephone system via a SIP trunk. A SIP trunk is a technology which allows IP-based telephone systems to manage and operate many call numbers via an access point.

### Configuration – Access System General parameters

- **Name:** Displayed device name in the system (e.g. SIP gateway)
- **Description:** Short description (e.g. Public telephone network connection ISDN). Always assign meaningful names and descriptions.

### Connection

- **Prefix:** Preceding number to obtain a public telephone network link (external line digit). One (e.g. **0**) or more digits (e.g. **99**). Using these indicates to the Access system that you wish to make a call into the external telephone network which can then be initiated.

**Note:** A prefix must be assigned to each SIP gateway. A prefix should be a number or number combination which is not used for internal calls in the Access system. A prefix for SIP gateways can be assigned any number of times in the Access system (e.g. connection of different telecommunication systems with the same prefix).

- **IP address:** IP address of the SIP gateways in the local network
- **Channels:** Maximum number of SIP speech channels available to the SIP gateway in parallel.

## Setting up the Access system

### Configuring the server functions

- **Size of audio frame [ms]:** Length of the audio content, i.e. the transmitted RTP data packages (audio frame) in milliseconds. The value to be set depends on the remote station. The values which can be set are prescribed (**20ms** and **40 ms**). Only Audio-Codec **G.711** is used.
- **External connection:** This option must be set if a telephony gateway is used for external telephony (public telephone network).

#### Linked devices

In the **Linked devices** area, the devices configured in the Access system are displayed with an assigned incoming call number. A link can be configured in two ways depending on the device:

- Assignment of an assigned incoming call number for the call function of the device **Siedle App iPhone** (field: Call number).
- Assignment of an assigned incoming call number for the device **External telephone** (field: Call number).

#### Important!

- A gateway can only be deleted if there are no linked devices within it.
- If you remove a device with the Delete device function, this device is completely deleted from the system. If you wish the device to be retained, in the **Users** menu at the relevant device, the call number of a different gateway has to be entered. Without a call number, the Siedle iPhone app for instance could only be reached over the network and no longer over the telephony connection if the network were down or otherwise not available.

#### Incoming call numbers

In the **Incoming call numbers** area, you can allocate the call numbers or call number block (e.g. 123-40 to 123-49) assigned to the SIP gateway from the public telephone network. (**Example:** The SIP gateway is linked to an external ISDN system connection with a consecutive 10 call number block (e.g. 123-40 to 123-49).).

You can assign the entries to the individual Access call destinations in the **Telephony connection > Incoming calls** menu.

#### Configuration – Access System – Incoming calls

- **Number:** Individual complete call numbers (e.g. 123456) or call number block without extension (e.g. 123-40 to 123-49 -> 123).
- **Start of the range:** Starting range of the extension range of a cohesive call number block (e.g. 12340 to 12349) – lowest numbers (e.g. 40)
- **End of the range:** End range of the extension range of a cohesive call number block (e.g. 123-40 to 123-49) – highest numbers (e.g. 49)

#### Remarks

- Depending on the telephony system used, you can enter the dialling code/country dialling code in all customary formats (e.g. The country dialling code for Germany: **49, 0049, +49**)
- If you have several non-cohesive call numbers, you must enter these individually in the **Number** field. To allow an external call to be held over the public telephone network using a device, in the **Users** menu, in the higher-level folder of this device, you must have configured a number plan and an **External call** with entered **Prefix** of the SIP gateway. A prefix should be a number or number combination which is not used for internal calls in the Access system.

#### Procedure – Configure SIP gateways

- 1** The telephony gateway (e.g. your telephone system) is already configured.
- 2** In the navigation area, click on the **Telephony connection** menu.
- 3** The **Telephony connection** menu opens up.
- 4** In the opened **Telephony connection** menu, click on the **Gateways** menu.
- 5** The **Gateways** page opens up in the content area.
- 6** Click on **Add**.
- 7** A **drop-down menu** opens up.
- 8** Select **SIP gateway** in this drop-down menu.
- 9** The **Create gateway** page opens up in the content area.
- 10** Carry out all inputs in the **General** area.
- 11** Assign a meaningful **Name** and **Description** to the SIP gateway to ensure that this is clearly identifiable.

- 12** Change to the area **Connection**.
- 13** Enter a **Prefix** (e.g. **0**).
- 14** Enter the **IP address** of the SIP gateway (e.g. 192.168.1.2).
- 15** Under **Channels**, select the maximum number of available speech channels available in the SIP gateway.
- 16** Under **Audio frame size [ms]** enter the value (**20** or **40**) which is supported by your SIP gateway.
- 17** If you wish the gateway to be used for external telephony (public telephone network), the option **External connection** must be activated.

**Note:** If a homogeneous call number plan is used (each assigned call number is unique in the joint Access and TC system network), when calling an **incoming call number**, this is called directly in the Access System, even if the optional configuration steps **18-22** have not been carried out.



**Optional steps (18-22):**

**Note:** The configuration steps 18-22 are optional and only necessary if the user also wishes to call to the Access system internally from the connected SIP telecommunication system. This results in mapping being carried out between the SIP telecommunication system PBX extension and a call number from the Access system.

**18** Change to the area **Incoming call numbers**.

**19** Click in the area **Incoming call numbers** on **Add** in order to configure a newly incoming call number.

**20** Enter the **country dialling code** into the relevant field.

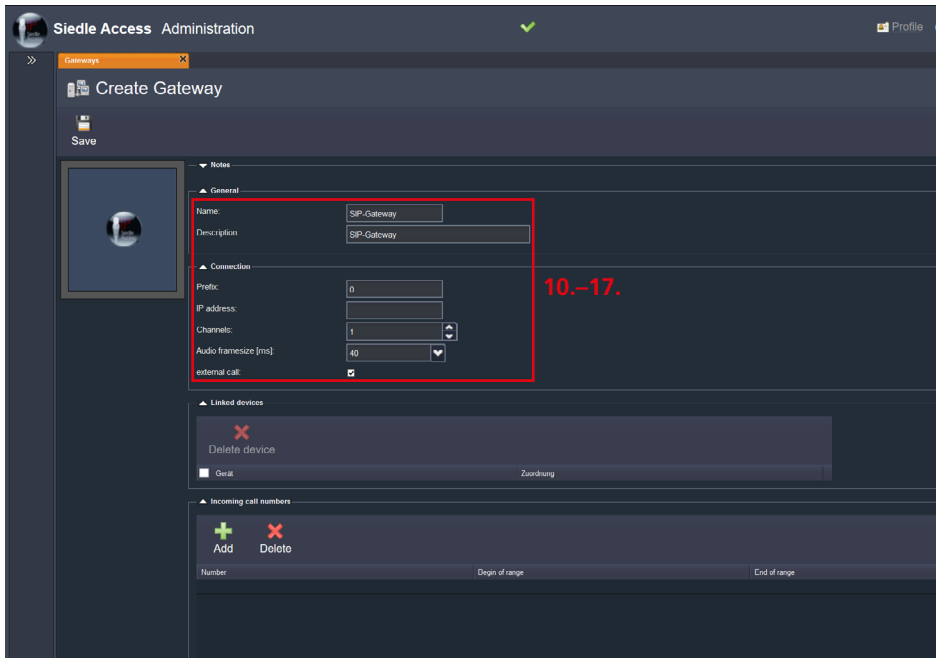
**21** Enter the **dialling code** into the relevant field.

**22** Enter an individual telephone number in the **Number** field, but with a consecutive call number block (e.g. 123-40 to 123-49 -> 123), enter the lowest Extension (e.g. 40) at the **beginning of the range** and the highest Extension (e.g. 49) at the **end of the range**.

**Note:** Configure all incoming call numbers which can come in over the connected provider / which were assigned to this gateway (e.g. PBX extensions from a central telephone system).

Click on **Save** to take the changes over in the system.  
Carry out a restart of the Access system (menu: **System maintenance > Restart**).

**Note:** After creating an SIP trunk, you must restart the Access server services in order to use them.



# Setting up the Access system

## Configuring the server functions

### Configuring SIP provider accounts

In this menu, you can configure SIP provider accounts and add or delete incoming call numbers. Log on as SIP user at a SIP provider with 1 speech channel (TC system, Cloud,...). In addition, you are given a central overview for configuration of the SIP provider account. SIP provider accounts link the Access system over the Internet to the VoIP telephony connection of a VoIP provider by means of the Session Initiation Protocol (SIP).

**Note:** After creating an SIP provider account, you must restart the Access server services in order to use them.

### Configuration – Access System General parameters

- **Name:** Displayed device name in the system (e.g. SIP provider [provider name]).
- **Description:** Short description (e.g. external VoIP connection). Always assign meaningful names and descriptions.

### Connection

- **Prefix:** Preceding number to obtain a public telephone network link (external line digit). One (e.g. **0**) or more digits (e.g. **99**). Using these indicates to the Access system that you wish to make a call into the external telephone network which can then be initiated.

**Note:** A prefix must be assigned to each SIP provider. A prefix should be a number or number combination which is not used for internal calls in the Access system. A prefix for SIP providers can be assigned any number of times in the Access system (e.g. grouping of several SIP providers).

- **IP address:** IP address or DNS name of the SIP server of the SIP provider in the Internet (e.g. 11.22.33.44 or voipgate.de).

- **Account name:** Account or user name issued by the SIP provider or call number of the SIP provider account.

- **Digest:** Access key issued by the SIP provider comprising the user name and hash tag made up of the password, random number and other variables in the form of digits, letters and/or a combination sequence with **@** from both (e.g. 111111A2B3C4D5E6F7G8H9I@voipgate.de or 508b93a5167b-342ba055164ef10aa610d35efb78).

- **Realm:** Domain (URL) of the SIP server / directory service (Realm => Domain e.g. voipgate.de).

- **Password:** Password provided by the SIP provider (SIP password) of the SIP provider account.

- **Size of audio frame [ms]:** Length of the audio content, i.e. the transmitted RTP data packages (audio frame) in milliseconds. The value to be set depends on the remote station. The values which can be set are prescribed (**20ms** and **40 ms**). Only Audio-Codec **G.711** is used.

- **External connection:** This option must be set if a telephony gateway is used for external telephony (public telephone network).

### Linked devices

In the **Linked devices** area, the devices configured in the Access system are displayed with an assigned incoming call number. A link can be configured in two ways depending on the device:

- Assignment of an assigned incoming call number for the call function of the device **Siedle App iPhone** (field: Call number).
- Assignment of an assigned incoming call number for the device **External telephone** (field: Call number).

### Incoming call numbers

In the **Incoming call numbers** area, you can allocate the call numbers or call number block (e.g. 123-40 to 123-49) assigned to the SIP gateway from the public telephone network.

**(Example:** The SIP gateway is linked to an external ISDN system connection with a consecutive 10 call number block (e.g. 123-40 to 123-49).). You can assign the entries to the individual Access call destinations in the **Telephony connection > Incoming calls** menu.

### Configuration – Access System – Incoming call numbers

- **Number:** Individual complete call numbers (e.g. 123456) or call number block without extension (e.g. 123-40 to 123-49 -> 123).
- **Start of the range:** Starting range of the extension range of a cohesive call number block (e.g. 12340 to 12349) – lowest numbers (e.g. 40)
- **End of the range:** End range of the extension range of a cohesive call number block (e.g. 123-40 to 123-49) – highest numbers (e.g. 49)

### Remarks

- Depending on the telephony system used, you can enter the dialling code/country dialling code in all customary formats (e.g. The country dialling code for Germany: **49, 0049, +49**)
- If you have several non-cohesive call numbers, you must enter these individually in the **Number** field. To allow an external call to be held over the public telephone network using a device, in the **Users** menu, in the higher-level folder of this device, you must have configured a number plan and an **External call** with entered **Prefix** of the SIP provider account.

### Procedure – Configuring SIP provider accounts

- 1 The login data of the provider access of your VoIP provider are known and an open connection exists for VoIP telephone calls to the internet / VoIP server.
- 2 In the navigation area, click on the **Telephony connection** menu.
- 3 The **Telephony connection** menu opens up.
- 4 In the opened **Telephony connection** menu, click on the **Gateways** menu.
- 5 The **Gateways** page opens up in the content area.
- 6 Click on **Add**.
- 7 A **drop-down menu** opens up.
- 8 Select **SIP provider** in this drop-down menu.
- 9 The **Create gateway** page opens up in the content area.
- 10 Carry out all inputs in the **General** area.

**11** Assign a meaningful **Name** and **Description** to the SIP provider to ensure that this is clearly identifiable.

**12** Change to the area **Connection**.

**13** Enter a **Prefix** (e.g. 0).

**14** Enter the **IP address** of the SIP provider (e.g. 11.22.33.44).

**15** Enter the **Account names** for the SIP provider account you wish to use (e.g. [your VoIP telephone number]).

**16** Enter the **Digest** allocated by the SIP provider.

**17** Enter the **Realm** allocated by the SIP provider.

**18** Enter the **password** allocated by the SIP provider.

**19** Under **Audio frame size [ms]** enter the value (**20** or **40**) which is supported by your SIP provider.

**20** If you wish the SIP provider account to be used for external telephony (public telephone network), the option **External connection** must be activated.

**Note:** If a homogeneous call number plan is used (each assigned call number is unique in the joint Access and TC system network), when calling an **incoming call number**, this is called directly in the Access System, even if the optional configuration steps **21–25** have not been carried out.

Siedle Access Administration

Profile

Gateways

Create Gateway

Save

Notes

General

Name: SIP-Provider

Description: Extremor SIP-Provider

Connection

Prefix: 0

IP address:

Account name:

Digest:

Realm:

Password:

Audio frame size [ms]: 40

external call:

9.–19.

I linked devices

Delete device

Geist Zuordnung

Incoming call numbers

Add Delete

Number Beginn of range End of range

## Setting up the Access system

### Configuring the server functions

#### Optional steps (21-25)

**Note:** The configuration steps 21–25 are optional and only necessary if the user also wishes to call to the Access system via the SIP provider account itself. This results in mapping being carried out between the SIP provider connection and a call number from the Access system.

**21** Change to the area **Incoming call numbers**.

**22** Click in the area **Incoming call numbers** on **Add** in order to configure a newly incoming call number.

**23** Enter the **country dialling code** into the relevant field.

**24** Enter the **dialling code** into the relevant field.

**25** Enter an individual telephone number in the **Number** field, but with a consecutive call number block (e.g. 123-40 to 123-49 -> 123), enter the lowest Extension (e.g. 40) at the **beginning of the range** and the highest Extension (e.g. 49) at the **end of the range**.

**Note:** Configure all incoming call numbers which can come in over the connected provider / which were assigned to this gateway (e.g. PBX extensions from a central telephone system).

**26** Click on **Save** to take the changes over in the system.

**27** Carry out a restart of the Access system (menu: **System maintenance > Restart**).

### Telephone directories

In this menu, you can create new and individual directories for external call destinations, edit them and fill them with contact addresses and telephone numbers.

The overview shows the directories available in the system to which you can assign the relevant user or users in the **Users** menu.

There are **three** types of phonebook in the Access system:

- **System directory (internal)** with the internal call numbers of the Access system (administered and issued by the system through the allocation of user rights).
- **Individual directory (external)** with manually generated external contacts which can be assigned to one or more users (updated and managed by the administrator).

- **Local directory of software clients** (concerge), which exists only locally on the used computer and is not synchronized with the Access system (updated and managed by the user).

**Note:** New contacts which are created for instance in the Concierge software are not adopted in the system or individual telephone directory.

The **contact list** of an Access device contains entries from the:

- **System directory**
- **Individual directory**
- **Local directory** (only with software client **ASC**).

### Procedure – Creating an individual directory

- 1 Click on **Add**.
- 2 Enter all data (**Name** and **Description**).

- 3 Create **Contacts** with telephone numbers (details on the next page).
- 4 Click on **Save** to take the changes over in the system.

### Procedure – Editing an individual directory

- 1 Select the relevant telephone directory.
- 2 Click on **Edit**.
- 3 Carry out the required inputs/ changes.
- 4 Click on **Save** to take the changes over in the system.

### Procedure – Delete directory

- 1 Select the relevant telephone directory.
- 2 Click on **Delete**.
- 3 Confirm the confirmation prompt with **Yes**.

Name	Description
Telefonbuch	Standard-Telefonbuch

# Setting up the Access system

## Configuring the server functions

### Creating contacts

In this menu, you can fill the selected directory with external contacts (name, telephone number, address and remarks).

The overview shows the existing contacts in the selected directory.

### Configuration – Access System General parameters

- **Name:** Displayed name of the telephone directory in the system (e.g. Directory – Mr Maier)
- **Description:** Short description (e.g. all external and internal contacts). Create new contacts and edit existing contacts.

### Procedure – Creating contacts

- 1 You have the contact data to hand.
- 2 You are in an opened directory (create directory or edit directory).
- 3 Click on **Add** to create a new contact.
- 4 In the **Name** column, double click on the new line and enter the complete name of the contact (e.g. Maier Peter).
- 5 In the **Telephone number** column, double click on the new line and enter the complete telephone number with all necessary dialling codes and the prefix to obtain an external telephone line (e.g. B. 0, 0049, 7723 and 123456 => 000497723123456).
- 6 In the **Location** column, double click on the new line and enter the postcode and location name of the contact (e.g. 78120 Furtwangen).

7 In the **Remarks** column, double click on the new line and enter any optional comment about this contact (e.g. Sales).

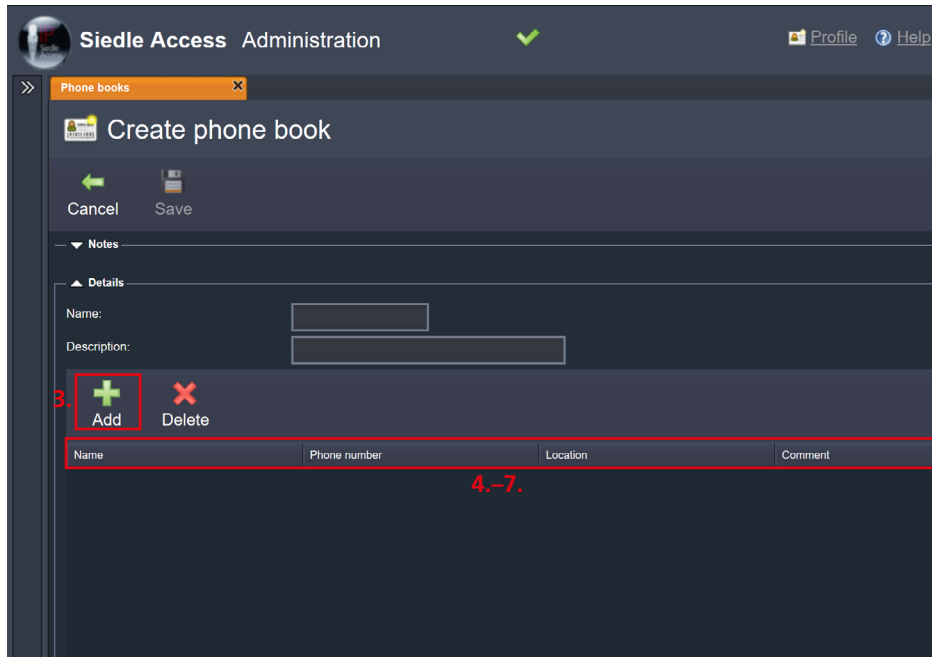
8 Click on **Save** to take the changes over in the system.

### Procedure – Edit contacts

- 1 Select the relevant telephone directory.
- 2 Click on **Edit**.
- 3 Carry out the required inputs/changes.
- 4 Click on **Save** to take the changes over in the system.

### Procedure – Delete contact

- 1 Select the relevant contact.
- 2 Click on **Delete**.
- 3 Click on **Save** to take the changes over in the system.



## Configuring the folder and user structure

### Creating a project

The **Project** folder forms the complete project structure of the Access system and is the central location for user, device and group configuration. In the project structure, create sub-folders, users, groups, door stations, devices and virtual devices and configure them. The **Project** folder itself cannot be configured, edited or deleted.

### Recommendation

Create a central folder for your project (e.g. building 1) in the Project folder, in which you map out the entire project structure.

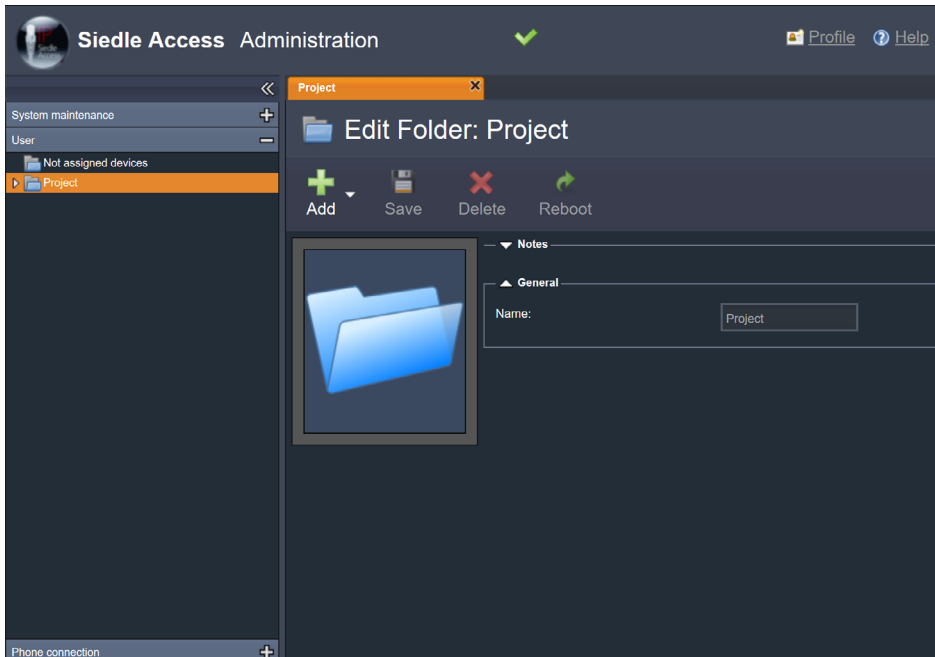
### Remarks

- Before assigning and manually creating Access terminals, you must have created the necessary Access project structure comprising sub-folders and users in the **Project** folder.

- You can create sub-folders, users, groups, door stations and virtual devices (binary switching devices) manually in the **Project** folder.
- Users located in the **Project** folder have unrestricted access to all switching and call authorisations of the Access system.
- Devices can only be created under a user or assigned to a user from the **Unassigned devices** folder.
- **Door stations** can only be assigned (subordinated) to the previously created sub-folders in the project tree or to the project folder itself.
- When selecting the position of the door stations within the project structure, take into consideration which users may be entitled to access this door station.
- In the project folder structure of the **Project** folder, the Access terminals can be assigned by means of Drag & Drop to the respective users.

**Exception:** Manually created Access terminals are already located in the project structure position in which you created them.

- Access terminals whose higher-level users or folders have been deleted are moved by the Access system back to the **Not assigned devices** folder. In doing so, the device configuration is lost and the device is treated as a device that is being connected for the first time.
- Users are deleted when the higher-level folder is deleted.
- Access terminals of a user which have been assigned to a particular folder (subordinated) are subject to the same **settings and user rights** as the folder.
- Several devices assigned to one user (subordinated) form a user-based device call group.



## Setting up the Access system

### Configuring the folder and user structure

- **Folder:** Logic group combining users, doors and virtual devices in order to depict project circumstances comprising room-based, rights-based or organizationally-based groups (e.g. building with several companies or residential units – every company or residential unit is collated as a sub-folder and contains the relevant users and their devices). **User rights in the Access System are arranged on the basis of folders.** Logical separations between users must be carried out using different folders and user rights restrictions. **Important:** No matter which position it assumes in the project folder structure, **every folder** must be viewed as independent and in isolation from the others and can be assigned the access rights **Visible** and **Switchable** for any other folder and subfolder, irrespective of how higher-level folders and subfolders have been configured and the position assumed by the folder in the project structure. However, already performed user rights settings from a higher-level folder are copied once only from a higher-level folder to the subfolder if this is created as a direct subfolder of this higher-level folder. When moving a folder, the configuration always remains unchanged.

- **Users:** Logic group combining devices in order to summarize and depict the availability of a person (e.g. 1 employee can be reached by video panel, app for iPhone and SIP video telephone) and in order to maintain synchronicity of important functions. However, a user without assigned **Devices** can **not** be called, even though a user call number exists in the Access system.

**Please note:** Maximum only one software client (Access in-house telephone or Access concierge) and one app (app for iPhone or app for iPad) can be assigned to each user. If a user requires two apps, for example, you must create a separate user for each app and form a call group from these users.

- **Door:** Door station located at an access or passageway of a property which has a door (e.g. door station at the entrance door). Every door station requires an Access door loudspeaker controller (ATLC) which is automatically recognized by the Access system.
- **Device:** Hardware and/or software-based communication unit which can be used in conjunction with the Access server for communication inside and outside the Access system (e.g. Access in-house telephone video, Siedle app for the iPhone or iPad).
- **Virtual Device:** Switching and control device connected via a gateway to the Access server which can be remotely activated using a configured device (e.g. binary KNX switching device).

#### Differentiation between users and call groups

A user can comprise one or more devices. A call group comprises one or more users which in turn can contain one or more devices. As central functions of the Access system fall within the jurisdiction of the users and the devices can only access these, the following characteristics (e.g. different behaviour patterns) must be observed:

- **Video memory:** All users have their own central video memory. All devices assigned to a user may access it. If an image is deleted by one device, the image is deleted for the user and is no longer available for this user's other devices.
- **Call group:** In the case of a call group, several users exist and therefore several video memories. If there is a door call to a call group, an image is saved in the video memory of all users with an activated automatic video memory. The door call image is thus stored on several video memories. If such an image is then deleted by a device, this image is only deleted for its users and it remains available in the video memories of the other users.
- **Call log:** The same behaviour as for the video memory, as the call list lies within the jurisdiction of the user/users -> Call groups therefore have several decentral call logs which are not synchronized.
- **Rejected calls:** If a user with several assigned devices is called and if the call is rejected by one of this user's devices, the calls to the remaining devices of this user are terminated. If a call group with several assigned users is called and the call is rejected by one of the user's devices, the calls to the remaining devices of this user are terminated, but the call to other users of this call group is retained and can be accepted by any optional device.



• **Background calls / several simultaneous calls:**

**User:** If a user is called several times (e.g. door calls and internal calls), the incoming calls for the devices assigned to the user are displayed as follows:

**AHT/AHTV, AHF/AHFV:** A maximum of one foreground call and one background call can be displayed at the same time. The first incoming call is shown in the foreground, all subsequent incoming calls are queued as background calls and prioritised (first all door calls, then the other calls). The calls can be processed in the specified order.

**ASC:** Incoming calls are displayed in order. The calls can be processed in any order.

**ASHT:** Door calls are displayed in order before all other calls. The calls can be processed in any order.

**Siedle app:** After the first incoming call, the connection is engaged for further calls. Only one call can be displayed and accepted at any time.

**Call group:** If a group is called several times from several doors or users (e.g. door calls and internal calls), then the first incoming calls are displayed as foreground call and subsequent calls as background call (not with the Siedle app). If a device of a called user accepts the first incoming call, then the second, still pending call, is shown as a background call on this device, on the other devices the first call is terminated again and the second call appears as an incoming call in the foreground.

**Creating and configuring new folders**

In the **Users** menu, folders are used to facilitate logical grouping of users and to depict the required Access system topology. User rights in the Access System are arranged on the basis of folders (see below). Folders must be considered as organizational aids and should not be confused with call groups. However, it is possible to have several users grouped in a folder automatically created as a call group.

**Configuration – Access System General parameters**

**Name:** Designation of the folder (e.g. 2nd floor).

**Description:** Description of the folder content (e.g. all users from the 2nd floor).

**Use as an automatically defined call group:** If this option is selected, the folder is created as a call group. In other words, you can call the users assigned directly to this folder in parallel as a group (**Note:** This does not apply to doors or sub-folders).

**Note**

A folder which has been configured as an automatically defined call group can be recognized by the changed folder symbol (folder symbol with person symbol). The function **Use as automatically defined call group** is only executed after saving and the call group of all the users is generated in this folder. The call number for this call group can be changed if required. In order to delete the automatically generated call group again, deactivate the option **Use as automatically defined call group**. The call group is only deleted after repeated saving.

**Authorizations**

**Important:** No matter which position it assumes in the project folder structure, **every folder** must be viewed as independent and in isolation from the others and can be assigned the access rights **Visible** and **Switchable** for any other folder and subfolder, irrespective of how higher-level folders and subfolders have been configured and the position assumed by the folder in the project structure.

**Exception:** Newly created sub-folders initially adopt the rights of the higher-level folder once only when they are created. Subsequent changes must be manually carried out in the folder levels. In the case of deep folder structures, this can take up a lot of valuable time.

**Example:** If a configured folder A is moved into a configured folder B, the rights of both folders remain unchanged. If the user rights are subsequently changed in a higher-level folder, the user rights of the sub-folders it already contains remain unchanged.

**Important!**

Before generating the project structure, you must have defined the user rights of the respective folders for the whole project structure and must also configure the user rights of the folders immediately when creating them, before inserting additional sub-folders. When the folder structure exists, you should create the users and assign the devices to the users. You can then continue with detailed configuration of the individual users and devices in this sequence.

**Subsequently changed user rights for a folder must be manually updated in all subfolders.**

## Setting up the Access system

### Configuring the folder and user structure

#### Option Visible

If for a folder A the option **Visible** is selected for folder B, then all the participants in folder A can see the participants of folder B. These are then shown, for example, in the contact lists of the Siedle terminal devices.

**Note:** Each folder contains the folder itself with the option **Visible**. If this option is deleted again, the users contained in this folder are separated from each other and not visible in the contact lists. This behaviour can be used in order to implement changes in the property (e.g. an apartment with several devices is turned into a shared apartment and each room with a device is separate from the other rooms. However, the owner does not wish to change the folder structure of the complete apartment).

#### Option Switchable

If the **Switchable** option is selected in folder B for folder A, then it is possible for all users in folder A to initiate switching functions for devices assigned to folder B. This can be a door release, a door light or a KNX actuator, for example.

**Note:** Each folder also contains the folder itself with the option **Switchable**. If this option is deleted again, the users contained in this folder are no longer able to initiate a switching function in their own property and mutually in the property of another user within this folder. This behaviour can be used in order to implement changes in the property (e.g. an apartment with several devices is turned into a shared apartment and each room with a device is separate from the other rooms. However, the owner does not wish to change the folder structure of the complete apartment).

#### Groups

If the option **Visible** has been activated for **Individually defined groups** or other subfolders they contain, then these call groups are displayed in the contact list of the users of a folder which have been activated in this option.

#### Call number plan

Using the call number plan, you can authorize or block the users of a folder for certain call or telephone numbers.

If the option **Allowed** for a call number plan entry is not activated, call and telephone numbers conforming to the specified pattern are disabled.

Call number plan entries can be individually generated by using wild cards and have to be saved before they become functional.

#### Possible place holders for map of call numbers:

\* place holder for any number of ciphers

? place holder for one cipher

x external calls (first cipher)

Possible digits: **0–9**

Possible characters: + as a replacement for **00**

#### Example of call number plan entries – call destinations with wild card:

##### Internal calls

\* relates to all internal call numbers  
-> If the option **allowed** is set, these users may dial these call numbers from their devices. Otherwise these call numbers would be blocked.

**09\*** relates to all internal call numbers which start with 09 – e.g. 09156 or 09874 -> If the option **allowed** is set, these users may dial these call numbers from their devices. Otherwise these call numbers would be blocked.

**44??** relates to all internal call numbers which start with 44 followed by two optional numbers, such as 4455 or 4412 -> If the option **allowed** is set, these users may dial these call numbers from their devices. Otherwise these call numbers would be blocked.

#### External calls – Important!

Call number plans for external calls require an established gateway to at least one telephone system or a telephony gateway. Without the existence of this type of connection, no external calls are possible. A prefix must be assigned to each SIP gateway. A prefix should be a number or number combination which is not used for internal calls in the Access system. It is also possible to enter individual complete external call numbers in the call number plan which you wish to explicitly allow or block.

**x55\*** applies to all external call numbers with a prefix required for external telephony e.g. **55** for a telephone gateway intended for external telephony e.g. 55+497723123456789. If the **allowed** option is set, these users may dial all external call numbers from their devices if the relevant prefix is entered. Otherwise, all external call numbers with this prefix are blocked.

### Procedure – Creating and configuring folders/subfolders

- 1 In the navigation area, click on the **Users** menu.
- 2 The **Users** menu opens up.
- 3 In the navigation area in the opened menu **Users**, click on the **Project** folder or into the position of the existing folder structure in which you wish to create a new folder/subfolder.
- 4 The page **Edit folder: Project / Edit folder: [folder name]** opens in the content area.
- 5 Click on **Add**.
- 6 A drop-down menu opens up.
- 7 Select **Folder** in this drop-down menu.
- 8 The **Create folder** page opens up in the content area.

**Note:** The configuration of the higher-level folder is adopted (copied) once only by its subfolders.

**Exception:** Folders which have been subordinated to the **Project** folder must be individually configured when managing the user rights.

- 9 Always assign meaningful names and descriptions.
- 10 Activate the option **Use as automatically defined call group** if you wish all users of this folder/subfolder to be collated as a call group with its own group call number.
- 11 Configure the user rights for the folder/subfolder in accordance with your planning and the information provided above.
- 12 Supplement, edit or delete the call number plan in accordance with your planning and the information provided above.
- 13 Click on **Save** to take the changes over in the system.
- 14 Create all the required folders and subfolders in order to create a map of the required/planned Access project structure.

### Preparing door stations (ATLC)

A **Door** is a door station located at an access or passageway of a property which has a door, barrier or similar (e.g. door station at the entrance door).

Every door station requires an Access door loudspeaker controller (ATLC) which is automatically recognized by the Access server. A door station is both a device but also a user, and therefore cannot be assigned (subordinated) to a user, but only to a folder or sub-folder.

Every door/door station offers facility for setting up the Doormatic function. The Doormatic function is generally activated for the last access area of a building if the previous access areas are freely accessible due to opening hours (e.g. entrance door of a doctor's surgery in a publicly accessible practice building).

The Doormatic function must be configured as **can be activated** at the door/door station, and can be activated on the user level for the subordinated devices. The Doormatic function can be activated at one user for all or selected doors/door stations which **can be activated**.

### Important!

If the users in your Access system are allowed to use the Doormatic function at selected door stations, all the affected doors/door stations (e.g. main entrance, underground car park entrance, storey entrance, office entrance) should be connected to the Access server and correctly positioned in the project/folder structure.

### Procedure – Preparing the door stations

#### Note

You can omit this step **if** the users in your network

- Are **not** allowed to use the Doormatic function.
- Are allowed to use the Doormatic function from **all** doors/door stations.

- 1 Connect the door station required for the user configuration to the Access network.

#### Note

All door stations which are recognized by the Access system are located in the **Users** menu in the folder **Not assigned devices**.

- 2 In the navigation area, click on the **Users** menu.
- 3 The **Users** menu opens up.
- 4 Click in the navigation area in the opened **Users** menu on the folder **Not assigned devices**, in order to open it.
- 5 The folder **Not assigned devices** is opened in the navigation area.
- 6 All unassigned devices are displayed.
- 7 Drag&Drop the still unassigned door/door station using the mouse from the folder **Not assigned devices** to the required position of the **Project/folder structure**.
- 8 Click on the required door station (**ATLC...**).
- 9 The page **Edit user: [previously set device name – MAC address]** opens in the content area.
- 10 Always assign meaningful names and descriptions.
- 11 Click on **Save** to take the changes over in the system.
- 12 Continue using the same procedure for additional doors/door stations.

## Setting up the Access system

### Configuring the folder and user structure

#### Remarks

- For subsequent configuration of the Doormatic function at the users, the door station must be recognizable with a unique name to eliminate any possible confusion.
- The complete configuration of a door station which has been given a new name is carried out at a **later juncture**.
- In large Access networks, it is advisable to proceed one block at a time (e.g. door stations, users and devices for storey 1, then door stations, users and devices for storey 2).

#### Creating and configuring users

A user is a logic group combining devices in order to summarize and depict the availability of a person (e.g. 1 employee can be reached by video panel, app for iPhone and SIP video telephone) and in order to maintain synchronicity of important functions. A user therefore forms the central communication interface in the Access system administration. A user has a variable number of permanently assignable devices which can be called in parallel and with equal rights under the assigned user call number. A user without assigned devices cannot be called. Devices which have been assigned to a user can be called direct.

**Please note:** Maximum only one software client (Access in-house telephone or Access concierge) and one app (app for iPhone or app for iPad) can be assigned to each user. If a user requires two apps, for example, you must create a separate user for each app and form a call group from these users. The voicemail, video memory and call lists are directly assigned to the user. This means that all devices assigned to the user have **equal rights** and can access it in parallel.

#### Differentiation between user calls and group calls

- The user call calls all the devices of a user in parallel.
- The group call calls all the devices of the users that belong to a group in parallel.

#### Differentiation between users and call groups

A user can comprise one or more devices. A call group comprises one or more users which in turn can contain one or more devices. As central functions of the Access system fall within the jurisdiction of the users and the devices can only access these, the following characteristics (e.g. different behaviour patterns) must be observed:

- **Video memory:** All users have their own central video memory. All devices assigned to a user may access it. If an image is deleted by one device, the image is deleted for the user and is no longer available for this user's other devices.
- **Call group:** In the case of a call group, several users exist and therefore several video memories. If there is a door call to a call group, an image is saved in the video memory of all users with an activated automatic video memory. The door call image is thus stored on several video memories. If such an image is then deleted by a device, this image is only deleted for its users and it remains available in the video memories of the other users.
- **Call log:** The same behaviour as for the video memory, as the call list lies within the jurisdiction of the user/users -> Call groups therefore have several decentral call logs which are not synchronized.
- **Rejected calls:** If a user with several assigned devices is called and if the call is rejected by one of this user's devices, the calls to the remaining devices of this user are terminated. If a call group with several assigned users is called and the call is rejected by one of the user's devices, the calls to the remaining devices of this user are terminated, but the call to other users of this call group is retained and can be accepted by any optional device.

- **Background calls / several simultaneous calls:**

**User:** If a user is called several times (e.g. door calls and internal calls), the incoming calls for the devices assigned to the user are displayed as follows:

**AHT/AHTV, AHF/AHFV:** A maximum of one foreground call and one background call can be displayed at the same time. The first incoming call is shown in the foreground, all subsequent incoming calls are queued as background calls and prioritised (first all door calls, then the other calls). The calls can be processed in the specified order.

**ASC:** Incoming calls are displayed in order. The calls can be processed in any order.

**ASHT:** Door calls are displayed in order before all other calls. The calls can be processed in any order.

**Siedle app:** After the first incoming call, the connection is engaged for further calls. Only one call can be displayed and accepted at any time.

**Call group:** If a group is called several times from several doors or users (e.g. door calls and internal calls), then the first incoming calls are displayed as foreground call and subsequent calls as background call (not with the Siedle app). If a device of a called user accepts the first incoming call, then the second, still pending call, is shown as a background call on this device, on the other devices the first call is terminated again and the second call appears as an incoming call in the foreground.

## Configuration – Access System General parameters

- **Name:** Displayed user name in the Access system (e.g. Mr. Maier)

- **Description:** Short description of the user (e.g. employee – engineering)

- **Call number:** Direct dial, internally assigned call number (e.g. 222)

- **Telephone directory:** Assigned telephone directory (see menu **Telephony connection**).

Individually created directories can also be assigned.

- **Assignment:** The standard entry is the designation of a higher-level folder. The designation can be changed at any time.

- **Video mode:** Mode which determines how the video data should be sent from the server over the Access network (for a video stream, a network bandwidth of 1 MBit/s is required.):

**UNICAST (1-to-1 connection):** A video stream is only sent to one user.

- **Benefit:** Standard network hardware is sufficient. Simple configuration in the network.

- **Drawback:** With large call groups, the video stream for each user must be separately generated and sent by the Access server.

**MULTICAST (multi-point connection):** A video stream is sent simultaneously to several users.

- **Benefit:** The video stream only needs to be generated once in the Access server and is then forwarded duplicated to the users in the multicast-capable network. Uses less capacity of the Access server.

- **Drawback:** In some cases complex network configuration. All network components (switches etc.) in the Access network must be completely multicast capable or must be exchanged for multicast-capable network components.

- **Account name:** Unchangeable information field. Each account name is unique in the Access system. The account name is generated by the Access system.

- **Password:** Central password for all subordinate devices (hardware and software). The central password is automatically assigned by the Access system and can be changed at any time.

- **Automatic video memory active:** If this option is activated, a door call image of the calling door station is stored for each door call to this user. In the video memory, the automatically generated door call images are filed and can be viewed and managed here via all the devices. All users have their own video memory. The video memories are not mutually synchronized (e.g. call group formation with several users). If the option is deactivated, a door call image can be stored using the manual video memory function.

**Important:** If the option **Automatic video memory active** is activated for a user, it is possible to access this from all devices which are assigned (subordinated) to this user.

### Note

The Access server automatically issues a free call number when a user is created, which depends on the **call number suggestion length** set in the **basic parameters**. This call number can be changed at any time. Each call number may only appear once in the Access system.

# Setting up the Access system

## Configuring the folder and user structure

### • Assignment of ringtones

In the **Ringtone assignment** area, you can define which call type (e.g. door call) is signalled with which ringtone at the respective terminal. In addition, you can define a different ringtone for incoming calls with the newly generated user-specific call types, or delete individually created call types. In the Access system, standard call types are pre-configured for which only the ringtone can be changed. If you wish to assign a dedicated ringtone to a selected user or door station, you must **Add a User-specific** caller type, and in the Caller column select the relevant user or door station and assign a ringtone to it.

### • Doormatic

In the **Doormatic** area, define whether a user may use the doormatic function or not. If doormatic is active, the door release of the assigned door station is automatically triggered if a door call is received by this user (e.g. automatic opening of the entrance door in a doctor's practice).

### Configuration – Doormatic

**Time in seconds:** Time period after ringing before which the door is automatically released.

- **Door:** Selection of whether a certain door or all doors should be automatically opened. It is only possible to select all or one of the prepared door stations if these are within the scope of user rights assigned to this user.
- **Doormatic function can be activated:** If this option is activated, the Doormatic function can be switched using the Access terminals of the user. If this option is deactivated, the Doormatic function cannot be activated at a door/door station.

### Procedure – Creating and configuring users

- 1 In the navigation area, click on the **Users** menu.
- 2 The **Users** menu opens up.
- 3 In the navigation area in the opened menu **Users**, click on the **Project** folder or into the position of the existing folder structure in which you wish to create a new user.

#### Note

- Users can be created exclusively in folders and subfolders.

4 The page **Edit folder: Project / Edit folder: [folder name]** opens in the content area.

5 Click in the content area onto **Add** at the top left.

6 A drop-down menu opens up.

7 Select **User** in this drop-down menu.

8 Carry out all inputs in the **General** area.

9 The **Create user** page opens up in the content area. Always assign meaningful names and descriptions.

#### Note

- The fields **Call number**, **Phonebook** and **Assignment** are automatically issued by the Access system and can be edited at any time.

10 Check the **Call number** and change it if required, for example to implement your call number system.

11 If you have created individual directories, select the **Phonebook** created for this user.

12 Check the **Assignment** and change/supplement it if required. When creating the user, the name of the higher-level folder is entered. This can be supplemented/changed at any time.

13 Select the **Video mode**, i.e. the type of video transmission in the Access network (unicast or multicast). Detailed information about video transmission is provided in the previous pages under **Video mode**.

**Note:** The account name and password of a user are automatically issued by the Access system when saving. The account name cannot be changed, but the password can. The account name and password are required for login of the subordinate devices (hardware and software).

14 If required, issue your own **Password** in order to implement your password policy.

15 If required, activate the **automatic video memory** for this user.

16 Change to the area **Ringtone assignment**.

17 In the **Ringtone assignment** area, in the **Category** column, select the caller type whose ringtone you may wish to modify.

18 In the same line, change to the column **Ringtone**.

19 Double click on the field with the entered ringtone and select the required ringtone in the drop-down menu.

20 Carry out all the ringtone adjustments according to your requirements.

21 If you wish to assign a selected device, user or call group with its own ringtone, implement the following procedure.

**Procedure – Creating an individual call type with ringtone (only Siedle hardware terminals)**

**22** In the **Ringtone assignment** area, click on **Add**.

**23** In the table view, the entry **User-specific** is inserted.

**24** In the **Ringtone assignment** area, in the **Category** column, select the call type or caller for which you would like to assign a different ringtone.

**25** In the same line, change to the **Caller** column and double click on the field to select a caller (device, user or call group) using the drop-down menu.

**26** In the **Caller** column, double-click and select a caller for the newly created entry (e.g. user Mr Maier) from the drop-down menu.

**27** In the same line, change to the **Ringtone** column and double click on the field to select a ringtone using the drop-down menu.

**28** Select a **Ringtone**.

**29** Click on **Save** to take the changes over in the system. For all the devices of a user, in future all calls from Mr Maier, for instance, will be signalled with a defined ringtone.

**Remarks**

- With the Siedle app and the software clients, these settings are carried out in their respective menus. A common ringtone can be selected using the app.
- All unsaved changes are displayed in the affected fields with a **small triangle**.

**Procedure – Configuring the Doormatic function**

**30** In the **Doormatic** area, activate the option **Doormatic can be activated**, if this user is entitled to use the Doormatic function.

**31** Select one or all doors/door stations at which the user may actuate the Doormatic function.

**32** Select a time span after which the door release should be automatically actuated if a door call is initiated. When making your selection, take into account the distances between the door and bell buttons on site.

**33** Click on **Save** to take the changes over in the system.

**34** Create all required users according to **this** procedure.

# Setting up the Access system

## Configuring the folder and user structure

### Editing already defined call groups

In this menu, you are given an overview of the management possibilities for the automatically defined call groups.

If in the **Users** menu the option **Use as automatically defined call group** is activated in a folder/sub-folder, all the users located within it (and their assigned devices) are grouped together as a call group made up of users with its own call number and shown in the Users menu with a changed symbol. If this group call number is called, all users in the call group (and their subordinated devices) are called simultaneously.

### Remarks

- The Access system automatically issues a call number when this call group is created, which depends on the call number suggestion length set in the basic parameters.
- This call number can be changed at any time.

### Procedure – Changing the call number of an automatically defined call group

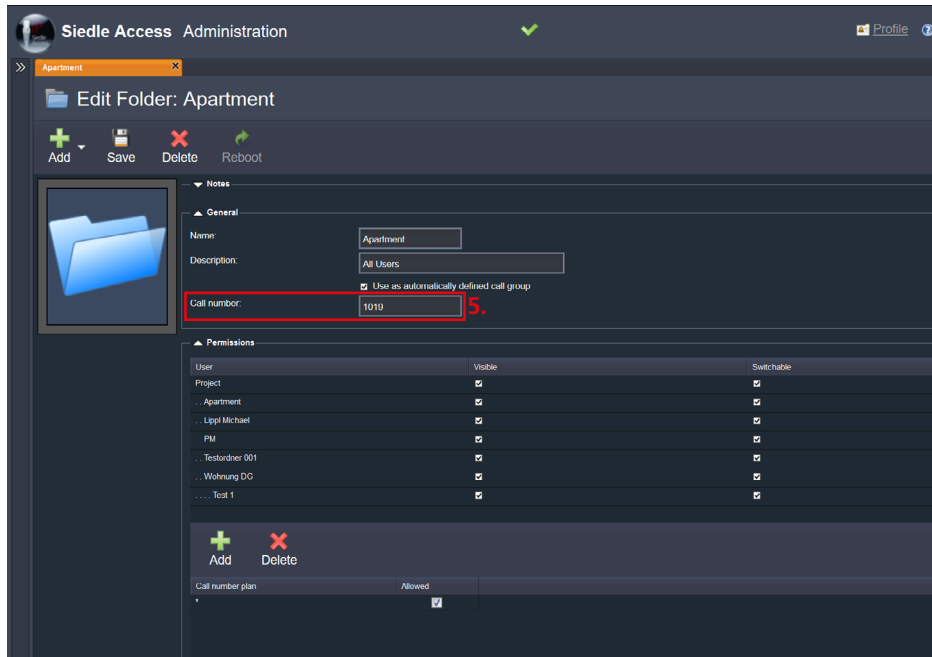
- 1 In the navigation area, click on the **Users** menu.
- 2 The **Users** menu opens up.
- 3 In the navigation area, in the opened **Users** menu, click on the required folder within the existing folder structure.
- 4 The page **Edit folder: [Folder name]** opens in the content area.
- 5 Check the **Call number** and change it if required, for example to implement your call number system.

6 Check the **Authorizations** and change them if required.

7 Click on **Save** to take the changes over in the system.

### Procedure – Deleting an automatically defined call group

- 1 Change to the **Users** menu.
- 2 Click on the folder of the affected automatically defined call group in order to open it.
- 3 The page **Edit folder: [Folder name]** opens in the content area.
- 4 Deactivate the option **Use as automatically defined call group**.
- 5 Click on **Save** to take the changes over in the system.
- 6 This **Automatically defined call group** has been deleted.





### Creating and editing individually defined call groups and folders

In the **Users** menu, you can create and edit individual call groups, and structure them using folders. Individually defined call groups can be compiled from any configured users (e.g. each receptionist on each storey). If you want to add all users in a folder to a group, use the option “use as automatically defined call group” in the required folder. An individually defined call group is assigned its own internal group call number by the Access system. Calling the group call number of this individually defined group will cause every assigned user (and all their sub-ordinated devices) to be called simultaneously.

### Creating a folder

A **Folder** is used to group together different groups within the same user rights system or to separate them by using different folders and different user rights systems. All additionally generated folders are displayed in the user rights administration of every folder, where they can be assigned the right **Visible**.

### Configuration – Access System General parameters

- **Name:** Name of the folder (e.g. receptions)
- **Description:** Short description

### Procedure – Creating a folder

- 1 In the navigation area, click on the **Users** menu.
- 2 The **Users** menu opens up.

3 In the navigation area in the opened menu **Users**, click on the **Project** folder or into the position of the existing folder structure in which you wish to create a new folder/ subfolder.

4 The page **Edit folder: Project / Edit folder: [folder name]** opens in the content area.

5 Click on **Add**.

6 A drop-down menu opens up.

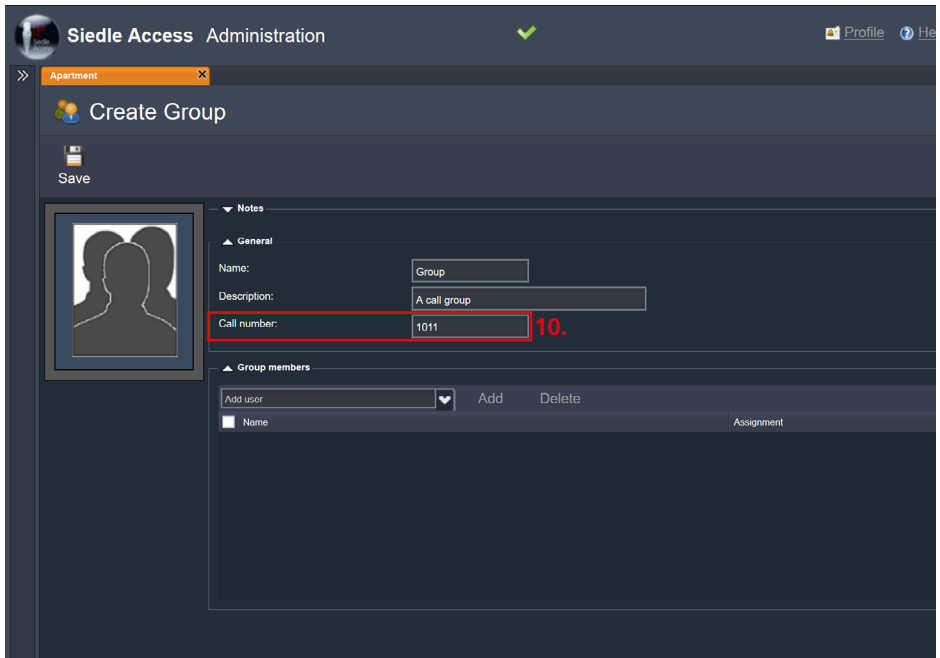
7 Select **Folder** in this drop-down menu.

8 The **Create folder** page opens up in the content area.

9 Carry out all inputs in the **General** area. Always assign meaningful names and descriptions.

10 Click on **Save** to take the changes over in the system.

11 Create all required folders for the individually defined call groups according to this procedure.



# Setting up the Access system

## Configuring the folder and user structure

### Creating and editing individually defined call groups

#### Configuration – Access System General parameters

**Name:** Displayed call group name in the system (e.g. Sales Department)

**Description:** Short description (e.g. all in-house sales team members)

**Call number:** Direct dial, internally assigned call number (e.g. 222)

#### Note

- The Access system automatically issues a call number when this call group is created, which depends on the call number suggestion length set in the basic parameters. This group call number can be changed at any time.

#### Procedure – Creating individually defined group

**1** In the navigation area, click on the **Users** menu.

**2** The **Users** menu opens up.

**3** In the navigation area in the opened **Users** menu, click on the **Project** folder or on a folder into the position of the existing folder structure in which you wish to create an individual call group.

**4** The page **Edit folder: Project / Edit folder: [folder name]** opens in the content area.

**5** Click on **Add**.

**6** A drop-down menu opens up.

**7** Select **Group** in this drop-down menu.

**8** The **Create group** page opens up in the content area.

**9** Carry out all inputs in the **General** area. Always assign meaningful names and descriptions.

#### Note

- The **Call number** field is automatically assigned by the Access system and can be changed at any time.

**10** Check the **Call number** and change it if required, for example to implement your call number system.

#### Note

- In the **Group members** area, you can add users to the call group or remove existing users. In addition, you will be shown an overview of already assigned users.

**11** In the group members area, click on the drop-down menu **Add user**.

**12** A drop-down menu opens up.

**13** In the opened drop-down menu, click on the required user to select it.

**14** The selected user is displayed in the field of the closed drop-down menu.

**15** Click on the **Add** button to adopt the selected users as group members in the call group.

**16** Add additional users in accordance with the previous points.

**17** Click on **Save** to take the changes over in the system.

**18** Create all required individually defined call groups according to this procedure.

#### Procedure – Deleting users from an individually defined call group

**1** In the navigation area, click on the **Users** menu.

**2** The **Users** menu opens up.

**3** In the navigation area, in the opened **Users** menu, click on the required folder within the existing folder structure.

**4** Click on the individually defined call group you wish to change.

**5** The page **Edit group: [Group name]** opens in the content area.

#### Note

- In the **Group members** area, you can add users to the call group or remove existing users. In addition, you will be shown an overview of already assigned users.

**6** In the Group members area, click on the **Check box** of the required user(s) in order to select it/them.

**7** The **Delete** button in the Group members area becomes active.

**8** Click on **Delete**, to delete all marked users from the selected call group.

**9** Click on **Save** to take the changes over in the system.

**10** Carry out adjustments to the group members (users) of a call group according to the following procedure.

### **Differentiation between user calls and group calls**

- The user call calls all the devices of a user in parallel.
- The group call calls all the devices of the users that belong to a group in parallel.

### **Differentiation between users and call groups**

A user can comprise one or more devices. A call group comprises one or more users which in turn can contain one or more devices. As central functions of the Access system fall within the jurisdiction of the users and the devices can only access these, the following characteristics (e.g. different behaviour patterns) must be observed:

- **Video memory:** All users have their own central video memory. All devices assigned to a user may access it. If an image is deleted by one device, the image is deleted for the user and is no longer available for this user's other devices.
- **Call group:** In the case of a call group, several users exist and therefore several video memories. If there is a door call to a call group, an image is saved in the video memory of all users with an activated automatic video memory. The door call image is thus stored on several video memories. If such an image is then deleted by a device, this image is only deleted for its users and it remains available in the video memories of the other users.
- **Call log:** The same behaviour as for the video memory, as the call list lies within the jurisdiction of the user/users -> Call groups therefore have several decentral call logs which are not synchronized.

- **Rejected calls:** If a user with several assigned devices is called and if the call is rejected by one of this user's devices, the calls to the remaining devices of this user are terminated. If a call group with several assigned users is called and the call is rejected by one of the user's devices, the calls to the remaining devices of this user are terminated, but the call to other users of this call group is retained and can be accepted by any optional device.

### **Background calls / several simultaneous calls:**

**User:** If a user is called several times (e.g. door calls and internal calls), the incoming calls for the devices assigned to the user are displayed as follows:

**AHT/AHTV, AHF/AHFV:** A maximum of one foreground call and one background call can be displayed at the same time. The first incoming call is shown in the foreground, all subsequent incoming calls are queued as background calls and prioritised (first all door calls, then the other calls). The calls can be processed in the specified order.

**ASC:** Incoming calls are displayed in order. The calls can be processed in any order.

**ASHT:** Door calls are displayed in order before all other calls. The calls can be processed in any order.

**Siedle app:** After the first incoming call, the connection is engaged for further calls. Only one call can be displayed and accepted at any time.

**Call group:** If a group is called several times from several doors or users (e.g. door calls and internal calls), then the first incoming calls are displayed as foreground call and subsequent calls as background call (not with the Siedle app). If a device of a called user accepts the first incoming call, then the second, still pending call, is shown as a background call on this device, on the other devices the first call is terminated again and the second call appears as an incoming call in the foreground.

## Configure devices

### Door (Door controller to door station)

A door is a door station located at an access or passageway of a property which has a door (e.g. door station at the entrance door). Every door station requires an Access door loudspeaker controller (ATLC) which is automatically recognized by the Access server. A door station is both a device but also a user, and therefore cannot be assigned (subordinated) to a user, but only to a folder or sub-folder.

### Model

A device is a hardware or software device which can be used by the end user, and forms the lowest level in the project/folder structure in the Access system.

In contrast to a folder or a user, nothing can be subordinated to a device. A device can only be assigned (subordinated) to a user.

**Exceptions:** The **Door** and the **Virtual device** can only be assigned (subordinated) to a folder, as these are central components which must be capable of being accessed by several or all users.

### Virtual device

A virtual device is a switching or control facility (e.g. binary KNX switching device) which is linked over a gateway to the Access server and can be remotely actuated using a configured device (e.g. Access video panel). A virtual device is a central non-standard device and cannot be assigned (subordinated) to a user, but only to a folder or sub-folder.

### Device types

Door (Door controller to door station)	Description
Access door loudspeaker controller (Siedle ATLC 670-...)	Hardware switch panel device for linking a door station to the Access server.
Model	Description
Access handsfree telephone (Siedle AHF 870-...)	Hardware terminal: Audio indoor station for wall or table-top operation.
Access video handsfree telephone (Siedle AHFV 870-...)	Hardware terminal: Video indoor station for wall or table-top operation.
Access in-house telephone (Siedle AHT 870-...)	Hardware terminal: Audio indoor station for wall operation.
Access video in-house telephone (Siedle AHTV 870-...)	Hardware terminal: Video indoor station for wall operation.
Access video panel (Siedle AVP 870-...)	Hardware terminal: Touch panel-based video indoor station for wall or table-top operation.
Access Software Concierge (Siedle ASC 170-...)	Software client: Central door management system and video indoor station for operation on any optional Windows-based computer.
Access Software In-house telephone (Siedle ASHT 170-...)	Software client: Video indoor station for operation on any optional Windows-based mobile or stationary operated computer.
Access software module (Siedle ASM 170-...)	Software module to integrate the functionality of an Access indoor station into third-party software.
Siedle App iPad	Software client: Video indoor station for operation on a mobile tablet (iOS).
Siedle app iPhone	Software client: Video indoor station for operation on a mobile smartphone (iOS).
Siedle App Panel (App Android)	Software client: Video indoor station for operation on a Android touch-panel (e.g. JUNG Smart Control...).
SIP video telephone	SIP telephone linked over the network at the Access server.
SIP audio telephone	SIP telephone linked over the network at the Access server.
External telephone	Any optional telephone linked over the telephony gateway at the Access server.
Virtual device	Description
Binary switching device	Binary KNX switching device which can be controlled over a KNX gateway.

### Configuring the door station (ATLC)

In this menu, you can create a door/door station and/or configure a recognized door/door station. A door station is always assigned directly to a folder or a sub-folder.

#### Remarks

- The door loudspeaker controller (ATLC) of the door station must be restarted after initial installation or in the event of changes (e.g. extension to include call button modules). After a successful restart, the configuration page of the ATLC must be called up again so that the changes made are displayed in the browser.

- During run-up, the Access door loudspeaker controller of the door station logs the connected modules and if applicable the door camera into the system.

**Tip:** If you replace this Access door loudspeaker controller, for instance due to a service, then save the new MAC address in this screen before carrying out the replacement. This means that the previous ATLC is replaced by the new ATLC with the existing configuration and there is no need to carry out a new configuration.

### Procedure – Restart of the Access door loudspeaker controller

- 1** In the **Users** menu, click on the door/door station you wish to reboot.
- 2** The page **Edit user: [door name]** opens in the content area.
- 3** Click in the header area onto **Restart**.
- 4** Confirm the confirmation prompt to reboot with **Yes**.
- 5** In the event of a visible hardware change, the displayed picture of the door station is adjusted by the Access server.

### Button configuration

In the **Button configuration** area, assign the individual buttons of the door station to an executive function. The number of configurable buttons depends on the connected call button modules.

#### Note

- If other parameters have to be configured stored for a particular button assignment (e.g. with one switching point), the button **Setting** becomes active. After clicking on **Setting**, a dialogue is displayed in which the relevant required data can be selected or entered.

### Procedure – Button configuration with switching point

- 1** In the **Users** menu, click on the door/door station you wish to configure.
- 2** The page **Edit user: [door name]** opens in the content area.
- 3** In the **Button configuration** area, click on a **button** (e.g. button 1).
- 4** In the drop-down menu of the selected button, select the function **Scripts and switching functions**.
- 5** A drop-down menu opens up.
- 6** Select the required function (e.g. **Switching point**).
- 7** The **Setting** button becomes active.
- 8** Click on **Setting**.
- 9** In the **Setting** dialogue, select the switching output (e.g. Mr. Maier: Output 1).
- 10** Click on **Save** to adopt the selected switching point.

### Switching outputs/inputs

At **output 23,24** a door release, an interfacing relay with equivalent consumption or similar consumers can be directly connected. The **output 23,24** is **not** a potential-free switching contact but, independently of its configuration, a **voltage emitting terminal**, to which no other external voltages may be connected or can be switched.

The remaining switching outputs can be freely used, paying due attention to the admissible electrical load data, as potential-free configurable switching outputs for wide-ranging functions. Due to the use of potential-free signalling contacts, the switching inputs can be used for wide-ranging functions.

## Configure devices

ATLC 670-...

### Voltage mode output 23,24 (AC/DC)

At the **output terminals 23,24**, it is possible to configure direct current operation (DC) or alternating current operation (AC) for the door release during the programmed door release time. In this case, synchronous or alternating voltage is applied. The door releases must be operated depending on their type with either direct current (DC) or alternating current (AC). When using a different switching output with the door release function, an external voltage supply is required, as only a potential-free switching contact is available.

### Doormatic

In the Doormatic area, define whether the Doormatic function should be capable of being activated at this door/door station or not. If the option **Doormatic can be activated** is active, devices will be able to activate the Doormatic function at this door/door station. If a device can be called from this door/door station with the Doormatic function activated, the contact (door release) configured as the door release is actuated.

### Storey call

With Access Professional V. 4.2.0 and above, each switching input can be configured for the storey call function.

### Procedure – Configuring the door station (ATLC)

- 1 Connect the ready wired Access door loudspeaker controller (ATLC) of the door/door station to the Access network.
- 2 In the navigation area, click on the **Users** menu.
- 3 The **Users** menu opens up.
- 4 Click in the navigation area in the opened **Users** menu on the folder **Not assigned devices**, in order to open it.
- 5 The folder **Not assigned devices** is opened in the navigation area.
- 6 The door/door station is displayed following detection by the Access server in the menu **Users > Not assigned devices**.
- 7 Drag&Drop the still unassigned door/door station using the mouse from the folder **Not assigned devices** to the required position of the **Project/folder structure**.
- 8 Click on the required door station (ATLC...).
- 9 The page **Edit user: [door name]** opens in the content area.
- 10 Carry out all inputs in the **General** area.
- 11 Always assign meaningful names and descriptions.

### Note

- The fields Call number and Assignment are automatically issued by the Access system and can be edited at any time.
- 12 Check the **Call number** and change it if required, for example to implement your call number system.
  - 13 Check the **Assignment** and change/supplement it if required.
  - 14 Leave the entered **MAC address** unchanged and change to the next field.
  - 15 The **hardware revision** is an information field and cannot be edited.
  - 16 Set the **voice volume** in accordance with the assumed ambient volume using the slide controller at the door station (high volume for loud environments).

- 17 Set the **microphone sensitivity** in accordance with the assumed ambient volume using the slide controller at the door station (high microphone sensitivity with a large gap between the speaker and the door station).

### Note

- For optimum setting of the voice volume and the microphone sensitivity, you may have to carry out several tests during function testing.

- 18 Under **Camera available**, check whether the information agrees with this door/door station.

- 19 Leave the selection **Default telephone script** unchanged under **Telephone script** if you do not wish a secondary signal unit or a surveillance camera to be operated at this door/door station. Otherwise select the required telephone script.

- 20 Activate the option **Acoustic button acknowledgement**, if you wish every actuation of call button at this door station to be audibly signalled with a standard or individually designed confirmation tone at the loudspeaker of the door station.

- 21 Change to the area **Button configuration**.

- 22 Configure the button **Door light** and the buttons of the call button module(s) with one of the offered functions in accordance with the configuration parameters described on the previous pages. The following functions are offered for selection: **No action**, **Device call**, **User call**, **Group call**, **External call** or **Scripts and switching functions**.

- 23 Change to the area **Switching outputs/inputs**.

- 24 At **Output 23,24** configure its application (**No action**, **Free switching time**, **Door release** or **Door light**).

- 25** In the **Voltage mode output 23,24** area, activate the option **AC** if the door release operated at the door has to be operated using alternating voltage. Activate the option **DC** if the door release operated at the door has to be operated using direct voltage.
- 26** At the remaining outputs, define the required applications (**No action, Free switching time, Door release** or **Door light**) and configure them in accordance with the configuration parameters described in the previous pages.
- 27** At the inputs, define the required applications (**No action, Switching point** or **Signal status**) and configure them in accordance with the configuration parameters described in the previous pages.
- 28** Change to the area **Doormatic**.
- 29** Activate the **Doormatic can be activated** option, if the Doormatic function is /has to be used at this door/door station.
- 30** Under **Time in seconds**, set the value at which you wish the door release to be actuated after pressing the call button (bell button).
- 31** Click on **Save** to take the changes over in the system.
- 32** Configure additional doors/door stations using the same procedure.

## Configure devices

AHF/AHFV/AHT/AHTV 870-...

### Configuring the Siedle indoor stations AHF, AHFV, AHT, AHTV

In these menus, you can create and configure a Siedle indoor station (AHF, AHFV, AHT, AHTV).

- The **Access handsfree telephone**

(**AHF**) is an audio indoor station with handsfree functionality.

- The **Access handsfree video telephone (AHFV)** is an indoor station with handsfree and video functionality.

- The **Access receiver telephone (AHT)** is an Audio indoor station with receiver functionality.

- The **Access handsfree video telephone (AHFV)** is an indoor station with receiver and video functionality.

### Button configuration

The button configuration is assigned as standard with the **single click** and **double click** modes and can be upgraded by activating the **expert mode** to include the **press button** and **release button** modes.

### Important!

- A button can either be configured for the “single/double-click” modes or the “press/release button” modes. If the mode is changed for a button, the previous button configuration is lost once this is confirmed.

If a status indicator is needed for a mode, only one status indicator can be configured for each button.

- If a function with status feedback (e.g. LED button lights up when doormatic is activated) is set to single or double-click mode, then no other switching or status function can be set for the other mode. Status feedback can be configured for all functions that do not trigger any calls (call rerouting, scripts and switching functions).

- A status is signalled by all functions which do not initiate a call, i.e. everything which is configured using scripts and switching functions, and the setting of call rerouting functions.

- If you wish to reroute a group, it is essential for this to be selected as the rerouting origin.

- The devices or users to which calls can be rerouted depends on the logical grouping in the user tree and the relevant user rights settings.

- If other parameters have to be configured for a particular button assignment (e.g. with one switching point), the **Set** button becomes active.

- After clicking on **Set**, a dialogue is displayed in which the relevant required data can be selected or entered.

- Using **Scripts and switching functions > Switching point**, the Doormatic function can be assigned to one of the buttons – provided the Doormatic function is activated for the user to which the device assigned.

### Procedure – Configuring call rerouting to any optional button

**1** In the navigation area, click on the **Users** menu.

**2** The **Users** menu opens up.

**3** In the folder/project structure, click into the required Access indoor station.

**4** The page **Edit device: [device name]** opens in the content area.

**5** In the **Button configuration** area, define the rerouting to the required selection (device, user, group, external) for one of the buttons.

**6** Depending on the selection (device, user, group, external), select the destination to which all calls should be rerouted.

**7** Click on **Setting**.

**8** In the **Parameterization** dialogue, select:

**9** The time in seconds after which you wish the waiting call to be rerouted (if you define a time of e.g. 5 seconds, you can still accept the call in this time).

**10** the routing source, i.e. a user or group for which you want to set the rerouting (depending on your rights).

**11** Click on **Save** to save your selection.

**12** Click on **Save** to take the changes over in the system.

**13** Carry out a function test.



### Switching outputs/inputs

Each of the Access indoor stations (AHF, AHFV, AHT, AHTV, AVP) is assigned a switching input and a switching output. Optionally, an Access indoor station can be upgraded with the Access Input/Output accessory **AZIO 870-0** to include an additional input and output. A connected AZIO is also shown here and can be configured via this user interface.

### Procedure – Button configuration with switching point

**1** In the navigation area, click on the **Users** menu.

**2** The **Users** menu opens up.

**3** In the folder/project structure, click into the required Access indoor station.

**4** The page **Edit device: [device name]** opens in the content area.

**5** In the **Button configuration** area, select the function **Scripts and switching functions** for one of the buttons.

**6** Select **Switching point**.

**Note:** If other parameters have to be configured for a particular button assignment (e.g. with one switching point), the **Set** button becomes active.

After clicking on **Set**, a dialogue is displayed in which the relevant required data can be selected or entered.

**7** Click on **Setting**.

**8** In the **Setting** dialogue, select the switching output (e.g. Mr. Maier: Output 1).

**9** Click on **Save** to save your selection.

**10** Click on **Save** to take the changes over in the system.

**11** Carry out a function test.

### Procedure – Configuring the Siedle indoor stations AHF, AHFV, AHT, AHTV

**1** Connect the server hardware to the Access network.

**2** In the navigation area, click on the **Users** menu.

**3** The **Users** menu opens up.

**4** Click in the navigation area in the opened **Users** menu on the folder **Not assigned devices**, in order to open it.

**5** The folder **Not assigned devices** is opened in the navigation area.

**6** The hardware terminal is displayed following detection by the Access system in the menu **Users > Not assigned devices**.

**7** Drag&Drop the still unassigned hardware terminals using the mouse from the folder **Not assigned devices** to the required position of the **Project/folder structure**.

**8** Click on the hardware terminal.

**9** The page **Edit device: [name of the hardware terminal]** opens up in the content area.

**10** Carry out all inputs in the **General** area.

**11** Always assign meaningful names and descriptions.

### Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

**12** Check the **Call number** and change it if required, for example to implement your call number system.

**13** Check the **Assignment** and change/supplement it if required.

**14** Leave the entered **MAC address** unchanged and change to the next field.

**15 Only with AHF/AHFV:** Define the mounting method, **Wall** or **Table**.

**16** The **hardware revision** is an information field and cannot be edited.

**17** Set the **ringtone volume** in accordance with the assumed ambient volume using the slide controller at the hardware terminal (high volume for loud environments).

**18** Set the **voice volume** in accordance with the assumed ambient volume using the slide controller at the door station (high volume for loud environments).

### Note

- For optimum setting of the ringtone volume and the voice volume, you may have to carry out several tests during function testing.

**19** Activate/deactivate the option **Show time at terminal**, if you wish the system time at the Access server to be displayed (**Yes**) nor not (**No**) (default setting: **Yes**).

**20** Leave the selection **Default telephone script** unchanged under **Telephone script** if you do not wish a secondary signal unit or a surveillance camera to be operated at this door/door station. Otherwise select the required telephone script.

## Configure devices

AHF/AHFV/AHT/AHTV 870-...

**21** Change to the area **Button configuration**.

### Remarks

- The button configuration is assigned as standard with the **single click** and **double click** modes and can be upgraded by activating the **expert mode** to include the **press button** and **release button** modes.
- **Observe the configuration parameters, instructions on button configuration and if applicable on call rerouting described in detail on the previous pages.**

**22** Activate the **Expert mode** option if you wish to expand the existing configuration scope of the buttons provided at the hardware terminal.

**23** Configure each of the **door releases** and the other device buttons of the hardware terminal with one of the offered functions (No action, Device call, User call, Group call, External call, Rerouting to device/User/Group/External or Scripts and switching functions), in accordance with the configuration parameters and instructions on the previous pages.

**24** Change to the area **Switching outputs/inputs**.

**25** At the output, define the required application (**No action**, **Free switching time**) and configure it in accordance with the configuration parameters described in the previous pages.

**26** At the input, define the required application (**No action**, **Switching point** or **Signal status**) and configure it in accordance with the configuration parameters described in the previous pages.

**27** Click on **Save** to take the changes over in the system.

**28** Configure each **AHF**, **AHFV**, **AHT**, **AHTV** using the same procedure.

### Configuring the Access video panel (AVP with KNX)

In this menu, you can create the Access video panel (AVP) and/or configure a recognised AVP. The AVP is an indoor station with touch screen, audio, video and control functionality. The AVP has a flat surface mount housing for wall and table-top mounting. For table-top mounting, you need a table-top accessory.

### Button configuration

Up to 44 tiles can be configured. The designation and the symbols for the tiles must be configured. The designation can be individually assigned. 26 different symbols (e.g. light, group call) are available for selection. If no symbol is selected, one is automatically stored when it is saved.

### Remarks

- The inscription as well as the selected symbol for a tile have **no** influence on the assigned function. This means that you can assign a function which does not match the inscription or symbol to an inscribed or symbolized tile (e.g. tile with **mail notification system** symbol with the assigned function **Group call**).
- If other parameters have to be configured for a particular button assignment (e.g. with one switching point), the **Set** button becomes active. After clicking on **Set**, a dialogue is displayed in which the relevant required data can be selected or entered.
- The devices or users to which calls can be rerouted depends on the logical grouping in the user tree and the relevant user rights settings.
- Using **Scripts and switching functions > Switching point**, the Doormatic function can be assigned to one of the buttons – provided the Doormatic function is activated for the user to which the device assigned.

### Procedure – Configuring call rerouting to any optional tile

- 1** In the **Button configuration** area, define the rerouting to the required selection (device, user, group, external) for one of the tiles.
- 2** Depending on the selection (device, user, group, external), select the destination to which all calls should be rerouted.
- 3** Click on **Setting**.
- 4** In the **Parameterization** dialogue, select:
  - The time in seconds after which you wish the waiting call to be rerouted (if you define a time of e.g. 5 seconds, you can still accept the call in this time).
  - the routing source, i.e. a user or group for which you want to set the rerouting (depending on your rights).
- 5** Click on **Save** to save your selection.
- 6** Click on **Save** to take the changes over in the system.
- 7** Carry out a function test.

### Switching outputs/inputs

Every Access video panel is equipped with one switching input and one switching output. The AVP can be extended to include an additional switching output/input using the Access input/output accessory AZIO 870-...

### Remarks

- The designation of the switching output/input is displayed in the switching lists of the Access terminals and in the button configuration area on the administration interface. You should consequently choose meaningful designations.
- The function **Free switching time** can additionally be statically switched (**Toggle 0s**).
- Before you can assign a group to the storey call, a group must be configured.
- If other parameters have to be configured for a particular tile assignment (e.g. with one switching point), the button **Setting** becomes active.
- After clicking on **Setting**, a dialogue is displayed in which the relevant required data can be selected or entered.

### Procedure – Tile configuration with switching point

- 1** In the **Button configuration** area, select the function **scripts and switching functions** for one of the tiles.
- 2** Select **Switching point**.
- 3** The **Set** button is displayed.
- 4** Click on **Setting**.
- 5** In the **Setting** dialogue, select the switching output (e.g. Mr. Maier: Output 1).
- 6** Click on **Save** to save your selection.
- 7** Click on **Save** to take the changes over in the system.

# Configure devices

AVP 870-...

## Procedure – Configuring the Access video panel (AVP with KNX)

- 1 Connect the server hardware to the Access network.
- 2 In the navigation area, click on the **Users** menu.
- 3 The **Users** menu opens up.
- 4 Click in the navigation area in the opened **Users** menu on the folder **Not assigned devices**, in order to open it.
- 5 The folder **Not assigned devices** is opened in the navigation area.
- 6 The hardware terminal is displayed following detection by the Access system in the menu **Users > Not assigned devices**.
- 7 Drag&Drop the still unassigned hardware terminals using the mouse from the folder **Not assigned devices** to the required position of the **Project/folder structure**.

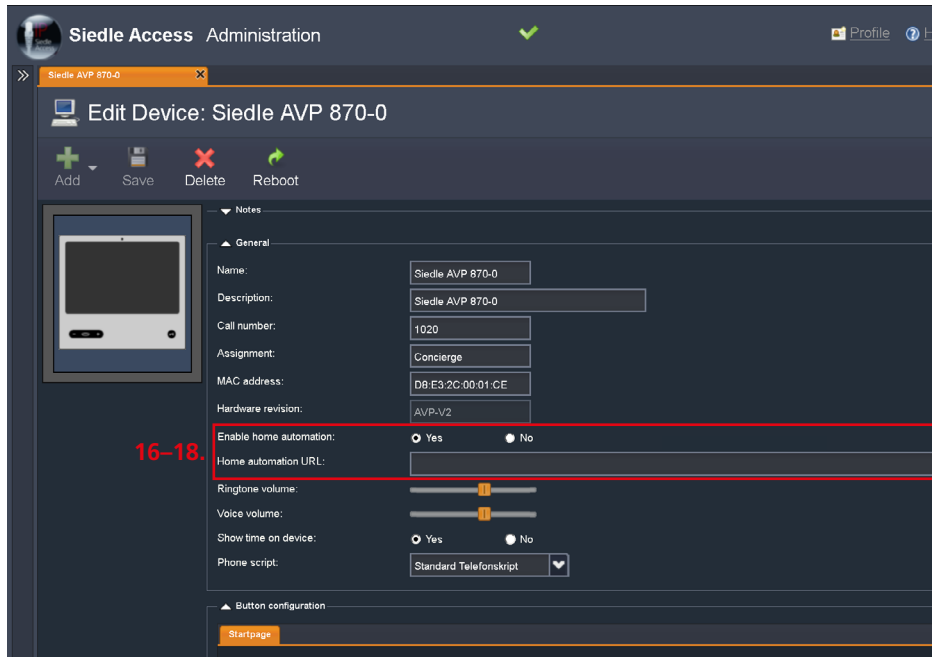
- 8 Click on the hardware terminal.
- 9 The page **Edit device: [name of the hardware terminal]** opens up in the content area.
- 10 Carry out all inputs in the **General** area.
- 11 Assign a meaningful **Name** and **Description** to the hardware terminal to ensure that this is clearly identifiable

### Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

- 12 Check the **Call number** and change it if required, for example to implement your call number system.
- 13 Check the **Assignment** and change/supplement it if required.
- 14 Leave the entered **MAC address** unchanged and change to the next field.

- 15 The **hardware revision** is an information field and cannot be edited.
- 16 Activate the option “Activate building automation”, if you are running a building automation server (Facility Pilot Server) and you want its user interface to be displayed on the AVP (from Access server V 3.1...). If you activate this option, the “URL building automation” input field opens up. Here, the URL of the building automation server must be entered. The “building automation” symbol is displayed on the AVP, this can be used to access the start page of the building automation server. This option is deactivated as standard.



**Note**

- If this option is activated, on the AVP the **Building automation** icon will be additionally displayed on the AVP start page. The user interface of the building automation server is accessed by tapping on the icon.

**17** The **URL building automation:** input box is shown.

**18** In the **URL building automation:** input box, enter the URL address of the building automation server in the form "[http://[IP address with or without port specification]]" (e.g. http://192.168.1.10:8080 or http://192.168.1.10).

**Note**

- The building automation server (JUNG Facility Pilot Server) is not a system component of the Siedle Access system. Integration / display of the user interface takes place using the embedded HTML frame. For commissioning and operation, please use the relevant manufacturer documentation.

**19** Set the **ringtone volume** in accordance with the assumed ambient volume using the slide controller at the hardware terminal (high volume for loud environments).

**20** Set the **voice volume** in accordance with the assumed ambient volume using the slide controller at the door station (high volume for loud environments).

**Note**

- For optimum setting of the ringtone volume and the voice volume, you may have to carry out several tests during function testing.

**21** Activate/deactivate the option **Show time at terminal**, if you wish the system time at the Access server to be displayed (**Yes**) nor not (**No**) (default setting: **Yes**).

**22** Leave the selection **Default telephone script** unchanged under **Telephone script** if you do not wish a secondary signal unit or a surveillance camera to be operated at this door/door station. Otherwise select the required telephone script.

**23** Change to the area **Button configuration**.

**Note**

- Instead of mechanical buttons, at the AVP there is a touch panel, in which a large number of tiles with a large selection of wide-ranging different functions, inscriptions and icons can be configured using the Access system. The configurable functional scope is the same as for the previously configured hardware terminals.

**24** Inscribe the required number of

tiles with a meaningful inscription matching the used functions.

**25** For each tile you wish to configure, select the right icon/symbol in accordance with the overview **Use of symbols – AVP**:

**26** Configure each of the **Tiles** of the hardware terminal with one of the offered functions (**No action**, **Device call**, **User call**, **Group call**, **External call**, **Rerouting to device/ User/Group/External or Scripts and switching functions**), in accordance with the configuration parameters and instructions on the previous pages.

**27** Change to the area **Switching outputs/inputs**.

**28** At the output, define the required application (**No action**, **Free switching time**) and configure it in accordance with the configuration parameters described in the previous pages.

**29** At the input, define the required application (**No action**, **Switching point** or **Signal status**) and configure it in accordance with the configuration parameters described in the previous pages.




























**30** Click on **Save** to take the changes over in the system.

**31** Configure each **AVP** using the same procedure.

## Configure devices

AVP 870-...

### Use of symbols – AVP

 Audio	 Cameras / Door station	 Time-delayed call forwarding on
 Call silencing	 All contacts/Contact – External	 Call forwarding On
 Image view	 Contact – Groups	 All switching functions/ Switching
 Contact – Concierge	 Contact – Internal	 Switching
 Design	 Light switching	 Language
 Cleaning the display	 Microphone off	 System information
 ECO mode	 Mail notification system	 Door release
 ECO mode	 Reset	 Door
 Building automation	 Ringtone Off	 Status display

### Access software concierge (ASC)

In this menu, you can create and configure the Access software concierge (ASC). The ASC is the central switchboard for the entire Access system and can be operated on a Windows-based computer.

#### Remarks

- If the PC with the installed software client is not located in the actual Access network, your system supervisor/network administrator must set up correct routing between the networks by means of a separate network infrastructure. For this, extended knowledge of the network is required.
- Several telephone scripts are available to choose from as standard in the Access system:
- **Secondary signal unit:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.
- **Camera actuation:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.

#### Procedure –

##### Configuring the ASC

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4** The page **Edit user: [name of the user]** opens up in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select **Siedle ASC 170** in this menu.
- 10** The **Create device** page opens up in the content area.
- 11** Carry out all inputs in the **General** area.
- 12** Always assign meaningful names and descriptions.

#### Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

**13** Check the **Call number** and change it if required, for example to implement your call number system.

**14** Check the **Assignment** and change/supplement it if required.

**15** The **software type** is an information field and cannot be edited.

**16** The **Account name** is an information field adopted from the higher-level user and cannot be changed.

**17** The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.

**18** Activate/deactivate the option **Use as autonomous telephone**, if you wish the software client to be used **without (Yes)** or **with (No)** parallel operated hardware terminals (e.g. AHT)(default setting: **Yes = without**).

#### Remarks

- If a hardware terminal is operated in parallel then the software client only shows the video image, while the hardware terminal takes over audio communication.
- If the option **No** is defined, the additional configuration point **CTI device** appears at which the hardware terminal you wish to operate in parallel can be selected. For this, a hardware terminal must be located in the same user.

**19** Under CTI device, select the required device for audio communication if you have deactivated the option **Use as autonomous telephone (No = with)**.

**20** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the software client does not provide a potential-free contact capable of stationary connection.

**21** Click on **Save** to take the changes over in the system.

**22** Download the **ASC** from the login page of the Access server (**Login page > Downloads > Siedle Access software**).

**23** Install the **ASC** on the required Windows-based computer.

**24** Start the **ASC** and log in using the relevant login data (**Account name** and **Password**).

**25** Carry out a test connection.

**26** Configure each **ASC** using the same procedure.

## Configure devices

### ASHT 170-...

#### Access in-house telephone software (ASHT)

In this menu, you can create and configure the Access software in-house telephone (ASHT). The ASHT is a virtual in-house telephone with video transmission facility for the end user which is operated on a Windows-based computer.

#### Remarks

- If the PC with the installed software client is not located in the actual Access network, your system supervisor/network administrator must set up correct routing between the networks by means of a separate network infrastructure. For this, extended knowledge of the network is required.
- Several telephone scripts are available to choose from as standard in the Access system:
- **Secondary signal unit:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.
- **Camera actuation:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.

#### Procedure – Configuring the ASHT

- 1 In the navigation area, click on the **Users** menu.
- 2 The **Users** menu opens up.
- 3 In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4 The page **Edit user: [name of the user]** opens up in the content area.
- 5 Click on **Add**.
- 6 A drop-down menu opens up.
- 7 Select **Device** in this drop-down menu.
- 8 A drop-down menu opens up.
- 9 Select **Siedle ASHT 170** in this menu.
- 10 The **Create device** page opens up in the content area.
- 11 Carry out all inputs in the **General** area.

12 Always assign meaningful names and descriptions.

#### Note

• The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

13 Check the **Call number** and change it if required, for example to implement your call number system.

14 Check the **Assignment** and change/supplement it if required.

15 The **software type** is an information field and cannot be edited.

16 The **Account name** is an information field adopted from the higher-level user and cannot be changed.

17 The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.

18 Activate/deactivate the option **Use as autonomous telephone**, if you wish the software client to be used **without (Yes)** or **with (No)** parallel operated hardware terminals (e.g. AHT)(default setting: **Yes = without**).

#### Remarks

- If a hardware terminal is operated in parallel then the software client only shows the video image, while the hardware terminal takes over audio communication.
- If the option **No** is defined, the additional configuration point **CTI device** appears at which the hardware terminal you wish to operate in parallel can be selected. For this, a hardware terminal must be located in the same user.

19 Under **CTI device**, select the required device for audio communication if you have deactivated the option **Use as autonomous telephone (No = with)**.

20 Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the software client does not provide a potential-free contact capable of stationary connection.

21 Click on **Save** to take the changes over in the system.

22 Download the **ASHT** from the login page of the Access server (**Login page > Downloads > Siedle Access software**).

23 Install the **ASHT** on the required Windows-based computer.

24 Start the **ASHT** and log in using the relevant login data (**Account name** and **Password**).

25 Carry out a test connection.

26 Configure each **ASHT** using the same procedure.



**Access software module (ASM)**

In this menu, you can create and configure the Access software module (ASM). The ASM is a software module for the integration of indoor devices from other manufacturers such as touch panels into the Siedle Access system.

**Remarks**

Several telephone scripts are available to choose from as standard in the Access system:

- **Secondary signal unit:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.
- **Camera actuation:** Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.

**Procedure – Configuring the ASM**

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4** The page **Edit user: [name of the user]** opens up in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select **Siedle ASM 170** in this menu.
- 10** The **Create device** page opens up in the content area.
- 11** Carry out all inputs in the **General** area.
- 12** Always assign meaningful names and descriptions.

**Note**

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

**13** Check the **Call number** and change it if required, for example to implement your call number system.

**14** Check the **Assignment** and change/supplement it if required.

**15** The **software type** is an information field and cannot be edited.

**16** The **Account name** is an information field adopted from the higher-level user and cannot be changed.

**17** The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.

**18** Activate/deactivate the option **Use as autonomous telephone**, if you wish the software client to be used **without (Yes)** or **with (No)** parallel operated hardware terminals (e.g. AHT)(default setting: **Yes = without**).

**Remarks**

- If a hardware terminal is operated in parallel then the software client only shows the video image, while the hardware terminal takes over audio communication.
- If the option **No** is defined, the additional configuration point **CTI device** appears at which the hardware terminal you wish to operate in parallel can be selected. For this, a hardware terminal must be located in the same user.

**19** Under CTI device, select the required device for audio communication if you have deactivated the option **Use as autonomous telephone (No = with)**.

**20** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the software client does not provide a potential-free contact capable of stationary connection.

**21** Click on **Save** to take the changes over in the system.

**22** Start the **ASM** and log in using the relevant login data (**Account name** and **Password**).

**23** Carry out a test connection.

**24** Configure each **ASM** using the same procedure.

## Configure devices

### Siedle app for Access Professional

#### Siedle app iPhone/iPad

In this menu, you can create and configure the Siedle app for Access Professional for iPhone/iPad. The Siedle app offers the possibility of using Access also in mobile environments.

#### Important!

- A permanent internet connection for both the Access Server and the mobile end device on which the Siedle app is to be run is required for the “Apple Push Notification Service” for commissioning and operating the Siedle app for Access. Local stand-alone operation with apps without connection to the Internet is no longer supported by iOS 11.

- With the switch to APNS, there is no longer a Siedle app call function (if there is no network connection, no telephone connection is established).
- The iOS-capable end device must be located in a network (WLAN or mobile data connection) in which a connection can be established with the Access server. When using a mobile phone network data connection, external access to the Access server needs to be set up. For this, extended knowledge of the network is required.
- Every Siedle app iPhone/iPad being used at the Access system must be used separately and without any other devices in one user. Using together with other users and the devices assigned to them takes place by grouping the relevant users as an automatically or individually defined call group.

#### Procedure – Configuring Siedle app iPhone/iPad

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4** The page **Edit user: [name of the user]** opens up in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select the correct **Siedle app...** for your device.

#### Remarks

- If you have selected the wrong device, switch back to the user display and select the appropriate device via **Add**.
- 10** The **Create device** page opens up in the content area.
  - 11** Carry out all inputs in the **General** area.
  - 12** Always assign meaningful names and descriptions.

#### Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.
- 13** Check the **Call number** and change it if required, for example to implement your call number system.
  - 14** Check the **Assignment** and change/supplement it if required.
  - 15** The **software type** is an information field and cannot be edited.
  - 16** The **Account name** is an information field adopted from the higher-level user and cannot be changed.
  - 17** The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.

**18** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the software client does not provide a potential-free contact capable of stationary connection.

#### Remarks

- Several telephone scripts are available to choose from as standard in the Access system:
- **Secondary signal unit:** Cannot be used here, as the mobile terminal does not make available a stationary connectable potential-free contact.
- **Camera actuation:** Cannot be used here, as the mobile terminal does not make available a stationary connectable potential-free contact.

**19** Click on **Save** to take the changes over in the system.

**20** Check whether the iOS-capable terminal you wish to use fulfils the system requirements for the Siedle app for Access.

**21** Download the **Siedle app for Access** from the Apple App Store to your iOS-capable device (customer's own access account is required for the Apple App Store).

**22** Install the **Siedle app for Access** on your iOS-capable terminal.

**23** Start the **Siedle app for Access** and log in using the relevant login data (**IP address of the Access server, account name and password** of this device).

**24** Carry out a test connection.

**25** Configure each Siedle-App using the same procedure.

# Siedle App for Access Professional for Android panels

## Siedle App Panel (App Android)

In this menu, you can create and configure the Siedle app for Access Professional for Android panels. The Siedle app offers the possibility of using Access on Android touch panels (e.g. JUNG Smart Control...). The app is currently exclusively installed on the JUNG touchpanels in the Smart Control product series.

### Remarks

- If the touchpanel with the installed app is not located in the actual Access network, your system supervisor/network administrator must set up correct routing between the networks by means of a separate network infrastructure. For this, extended knowledge of the network is required. Several telephone scripts are available to choose from as standard in the Access system:
- Secondary signal unit: Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.
- Camera actuation: Cannot be used here, as the terminal does not make available a stationary connectable potential-free contact.

## Procedure –Siedle App Panel (App Android)

- 1** Connect the server hardware to the Access network.
- 2** In the navigation area, click on the Users menu.
- 3** The Users menu opens up.
- 4** Click in the navigation area in the opened Users menu on the folder Not assigned devices, in order to open it.
- 5** The folder Not assigned devices is opened in the navigation area.
- 6** The hardware terminal is displayed following detection by the Access system in the menu Users > Not assigned devices.
- 7** Drag&Drop the still unassigned hardware terminals using the mouse from the folder Not assigned devices to the required position of the Project/folder structure.
- 8** Click on the hardware terminal.
- 9** The page Edit device: [name of the hardware terminal] opens up in the content area.
- 10** Carry out all inputs in the General area.
- 11** Always assign meaningful names and descriptions.

### Note

- The fields Call number and Assignment are automatically issued by the Access system and can be edited at any time.
- 12** Check the Call number and change it if required, for example to implement your call number system.
  - 13** Check the Assignment and change/supplement it if required.
  - 14** Leave the entered MAC address unchanged and change to the next field.
  - 15** The hardware revision is an information field and cannot be edited.
  - 16** Leave the selection Standard telephone script under Telephone script unchanged, as the software client does not provide a potential-free contact capable of stationary connection.

## Important!

A lock screen can be activated on each touch panel, which is activated after a preset waiting time has elapsed. If there is no user interaction on the touch panel, it could also activate during a call if the call takes longer than the preset waiting time. A return to the existing connection dialog is then no longer possible. The call remains active, but cannot be deactivated by the user, and only ends after the system has allowed the call duration to expire.

Please choose a sufficiently long waiting time.  
Recommendation: average length of call + 1-2 minutes

## Configure devices

### SIP video telephone

#### SIP video telephone

In this menu, you can create and configure an SIP video telephone (third party device).

SIP telephones are SIP-2.0-compatible terminals of software clients from third-party manufacturers which can be coupled with the Access system. The configuration of these terminals differs on a manufacturer-dependent basis. In contrast to external telephones connected indirectly to the Access server, a SIP telephone is logged directly onto the Access server, receives an internal direct dial device call number and can therefore be called directly or via the number of the higher-level user. Connection to the Access server takes place via the network with the login data stored here. No telephony routes or configured SIP gateways/providers are necessary for operation.

#### Remarks

- Several telephone scripts are available to choose from as standard in the Access system:

**Secondary signal unit:** Can only be used if this terminal makes available a potential-free contact which is addressable by the Access server.

**Camera actuation:** Can only be used if this terminal makes available a potential-free contact which is addressable by the Access server.

#### Procedure – Configuring the SIP video telephone

**1** In the navigation area, click on the **Users** menu.

**2** The **Users** menu opens up.

**3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.

**4** The page **Edit user: [name of the user]** opens up in the content area.

**5** Click on **Add**.

**6** A drop-down menu opens up.

**7** Select **Device** in this drop-down menu.

**8** A drop-down menu opens up.

**9** Select **SIP video telephone** in this menu.

**10** The **Create device** page opens up in the content area.

**11** Carry out all inputs in the **General** area.

**12** Always assign meaningful names and descriptions.

#### Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

**13** Check the **Call number** and change it if required, for example to implement your call number system.

**14** Check the **Assignment** and change/supplement it if required.

**15** The **hardware revision** is an information field and cannot be edited.

**16** The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.

**17** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the external device does not provide a potential-free contact capable of stationary connection.

**18** Under **Size of audio frame [ms]**, select the length of the audio frame which your SIP telephone supports (e.g. 20 ms).

**19** Click on **Save** to take the changes over in the system.

**20** Connect the external device to the Access network and commission it.

#### Note

- At your external device, select the length of the audio frames **20 ms** (or **40 ms**).

**21** Configure the external device using the configuration data issued by the Access system.

**22** Carry out a test connection.

**23** Configure each external telephone / SIP video telephone using the same procedure.

# SIP audio telephone

## SIP audio telephone

In this menu, you can create and configure a SIP audio telephone (third party device).

SIP telephones are SIP-2.0-compatible terminals of software clients from third-party manufacturers which can be coupled with the Access system. The configuration of these terminals differs on a manufacturer-dependent basis. In contrast to external telephones connected indirectly to the Access server, a SIP telephone is logged directly onto the Access server, receives an internal direct dial device call number and can therefore be called directly or via the number of the higher-level user. Connection to the Access server takes place via the network with the login data stored here. No telephony routes or configured SIP gateways/providers are necessary for operation.

## Remarks

Several telephone scripts are available to choose from as standard in the Access system:

- Secondary signal unit: Can only be used if this terminal makes available a potential-free contact which is addressable by the Access server.
- Camera actuation: Can only be used if this terminal makes available a potential-free contact which is addressable by the Access server.

## Procedure – Configuring the SIP audio telephone

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4** The page **Edit user: [name of the user]** opens up in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select **SIP audio telephone** in this menu.
- 10** The **Create device** page opens up in the content area.
- 11** Carry out all inputs in the **General** area.
- 12** Always assign meaningful names and descriptions.

## Note

- The fields **Call number** and **Assignment** are automatically issued by the Access system and can be edited at any time.

- 13** Check the **Call number** and change it if required, for example to implement your call number system.
- 14** Check the **Assignment** and change/supplement it if required.
- 15** The **hardware revision** is an information field and cannot be edited.
- 16** The **password** is an information field adopted from the higher-level user and can only be edited centrally at the higher-level user.
- 17** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the external device does not provide a potential-free contact capable of stationary connection.
- 18** Under **Size of audio frame [ms]**, select the length of the audio frame which your SIP telephone supports (e.g. 20 ms).

**19** Click on **Save** to take the changes over in the system.

**20** Connect the external device to the Access network and commission it.

## Note

- At your external device, select the length of the audio frames **20 ms** (or **40 ms**).

**21** Configure the external device using the configuration data issued by the Access system.

**22** Carry out a test connection.

**23** Configure each external telephone / SIP audio telephone using the same procedure.

## Configure devices

### External telephone

#### External telephone

In this menu, you can create and configure external telephones (external devices). External devices are SIP-2.0-compatible terminals, PC software from external manufacturers or analogue telephones of a telecommunication system connected via an SIP-ATA adapter, which can be linked to the Access system (e.g. VoIP table-top telephone which is integrated via the telephone system and which is called in the event of an incoming call by the Access server).

In contrast to SIP audio/SIP video telephones registered directly at the Access server, an external telephone is not directly logged into the Access server, does not receive an internal direct dial device number and consequently cannot be rung from the Access server, only over the call number of the higher-level user. The connection takes place exclusively over the entered telephony route (direct dial via the local telephone system or an external connection to a different location) and not over the network itself (example: If a user is called, the standard telephone at home should additionally signal the incoming call).

#### Important!

For connection of telephones, a call number plan for these allocated call numbers and a gateway set up for at least one telephone system or one telephony gateway are required (see **Telephony connection > Gateways** menu).

A **Prefix** must be assigned to each gateway. A gateway can be created and configured in the **Telephony connection > Gateways** menu. A prefix should be a number or number combination which is not used for internal calls in the Access system. It is also possible to enter individual complete external call numbers in the call number plan which you wish to explicitly allow or block.

#### Procedure – Configuring external telephones

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area, in the opened **Users** menu, click on the required user within the existing **Project/Folder structure**.
- 4** The page **Edit user: [name of the user]** opens up in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select **External telephone** in this menu.
- 10** The **Create device** page opens up in the content area.
- 11** Carry out all inputs in the **General** area.
- 12** Always assign meaningful names and descriptions.

#### Note

- The **Assignment** field is automatically assigned by the Access server and can be changed at any time.

**13** Check the **Assignment** and change/supplement it if required.

**14** Leave the selection **Standard telephone script** under **Telephone script** unchanged, as the external device does not provide a potential-free contact capable of stationary connection.

**15** Under **Line prefix and call number**, select the **Line prefix** (e.g. 0) used to obtain an external line through which the external telephone can be reached.

**16** Under **Line prefix and call number**, enter the call number used to reach the external telephone.

**17** Click on **Save** to take the changes over in the system.

**18** Carry out a test connection.

**19** Configure each **external telephone** using the same procedure.

### Creating virtual devices – Binary switching device

In this menu, you can create and configure a virtual device (binary switching device).

Binary switching devices can only be created on the relevant folder or sub-folder level and not on the user or device level.

Virtual devices depict switching and control devices within the system. On principle, a virtual device comprises

- a name
- a short description and
- a selectable KNX address which is required for operation.

The precise input required is individually determined for the respective virtual device.

#### Remarks

- To be able to create a virtual device / binary switching device, in the menu **Users > KNX addresses**, a KNX gateway and the KNX address **must have been created and released** for use. Otherwise, no virtual device / binary switching device can be created in the Access server.
- The number of virtual devices / binary switching devices which you can create depends on the number of data points of the acquired Access licence **KNX connection**.

### Procedure – Creating the binary switching device

#### Condition

The KNX gateway and KNX addresses must have been created.

- 1** In the navigation area, click on the **Users** menu.
- 2** The **Users** menu opens up.
- 3** In the navigation area in the opened menu **Users**, click on the **Project** folder or into the position of the existing folder structure in which you wish to create a new user.
- 4** The page **Edit folder: Project / Edit folder: [folder name]** opens in the content area.
- 5** Click on **Add**.
- 6** A drop-down menu opens up.
- 7** Select **Virtual device** in this drop-down menu.
- 8** A drop-down menu opens up.
- 9** Select **Binary switching device** in this drop-down menu.

#### Note:

- If the message **No KNX gateway available** appears, you must first set up a KNX gateway, import the relevant KNX address file into the Access system and release it for use.

- 10** The **Create virtual device** page opens up in the content area.
- 11** Carry out all inputs in the **General** area. Always assign meaningful names and descriptions.

- 12** Change to the area **KNX addresses**.

#### Note:

- The content of the fields **Description** and **Data type** cannot be changed.

- 13** Double click on the input field **(0/0/0)** under **Address**.
- 14** Under **Address**, select **one** of the KNX addresses released for use (can be changed subsequently at any time).
- 15** Click on **Save** to take the changes over in the system.

- 16** Carry out a function test with all created virtual devices / binary switching devices at a later juncture if you have configured these as a selectable function at the **Access devices**.

- 17** Create every virtual device / binary switching device using the same procedure.

#### Remarks

- Depending on the administration of user rights and the position of the virtual devices / binary switching devices in the project / folder structure, a virtual device / binary switching device can be configured as a switching point at a button of an indoor station or a button / tile of a Siedle app or software client.
- Information on the different Access licences is available in the **Planning and System Manual Access Professional**.

# Telephony routes

## Configuring telephony routes

In this menu, you can assign an externally integrated telephone number to any optional internal Access user or a door station as the call designation. The integration of external telephone numbers requires a configured SIP gateway or an SIP provider account. The overview shows the most important information on the created telephony routes (gateway, incoming call number and destination in the Access system).

## Procedure – Configuring telephony routes

- 1 The SIP gateways and/or SIP provider accounts are completely configured with incoming call numbers.
- 2 In the navigation area, click on the **Telephony connection** menu.
- 3 The **Telephony connection** menu opens up.
- 4 In the navigation area, click into the opened **Telephony connection** menu on **Incoming calls**.
- 5 The **Incoming calls** page opens up in the content area.
- 6 Click on **Add** to create a new telephony route.
- 7 In the **Gateway** column, click on the new line in order to select a gateway.
- 8 In the **Incoming call numbers** column, click on the new line in order to select an incoming call number.

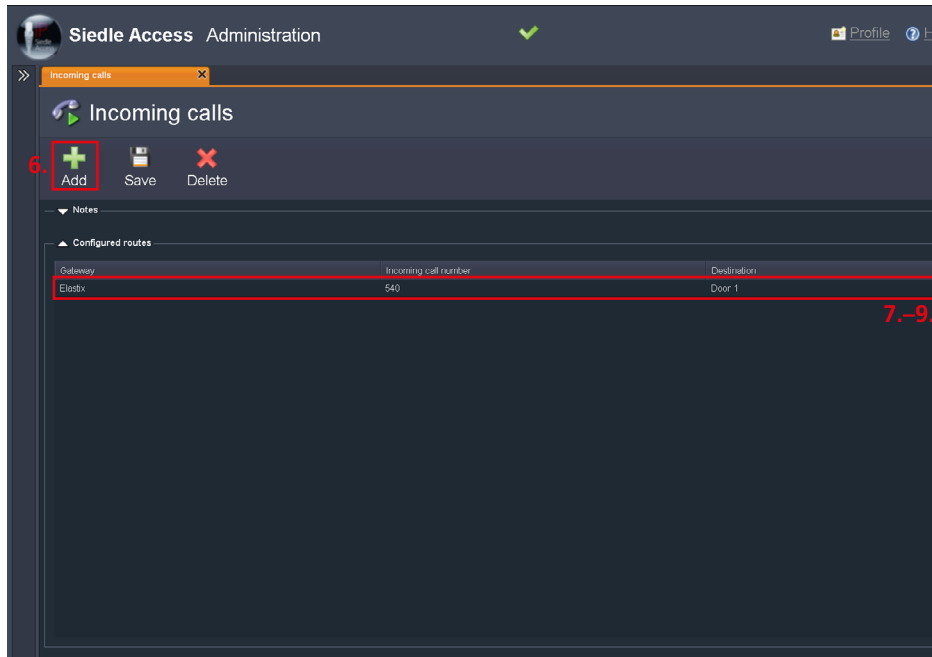
## Note

- If you are unable to select an incoming call number, the configuration of the SIP gateway or the SIP provider account has not been completely carried out.

- 9 In the **Destination** column, click on the **new line** in order to select an internal Access user.
- 10 Click on **Save** to take the changes over in the system.
- 11 You have assigned an internal telephone number to the internal Access user.

## Procedure – Deleting the configured telephony route:

- 12 Select a telephony route from the list.
- 13 Click on **Delete**.
- 14 Click on **Save** to take the changes over in the system.





## Roles and user accounts

### Roles

#### Roles

In this menu, you can create new roles for new or existing user accounts depending on your user rights. In the **Display roles** area, you can access an overview of all roles created in the system, which you can select, edit or delete. The name of the role is required for identification purposes in order to allow the right role to be assigned to a user account.

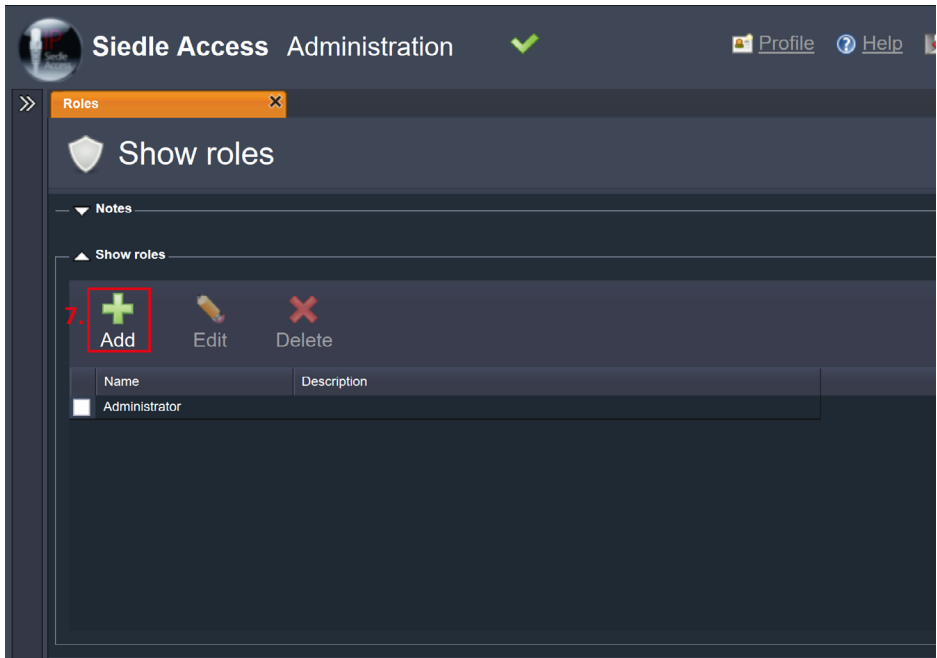
Depending on user rights, you can create new roles and edit or delete existing ones. Every newly created role can be freely named and configured.

#### Note

- Administrators can only process their own profile (user name, password, language etc.) if the **Profile component** is activated in their assigned role (see **Access server > System maintenance > Administrators > Roles**).

#### Procedure – Create new role

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the navigation area, click in the opened **Administrators** folder on **Accounts**.
- 4 The **Administrators** folder opens up in the navigation area.
- 5 In the navigation area, click into the opened **Administrators** folder on **Roles**.
- 6 The **Roles** page opens up in the content area.
- 7 Click on **Add**.
- 8 The **Create role** page opens up in the content area.



# Roles and user accounts

## Roles

**9** In the **Name of administrative role** field, enter a name.

**10** In the **Description** field, enter a meaningful description.

**11** Activate the checkboxes for the allowed **Administration areas** for this role by clicking on the relevant checkbox in the **Access allowed** column.

**12** Click on **Save** to take the changes over in the system.

**13** The role can now be assigned to an administrator or selected when creating a new user account.

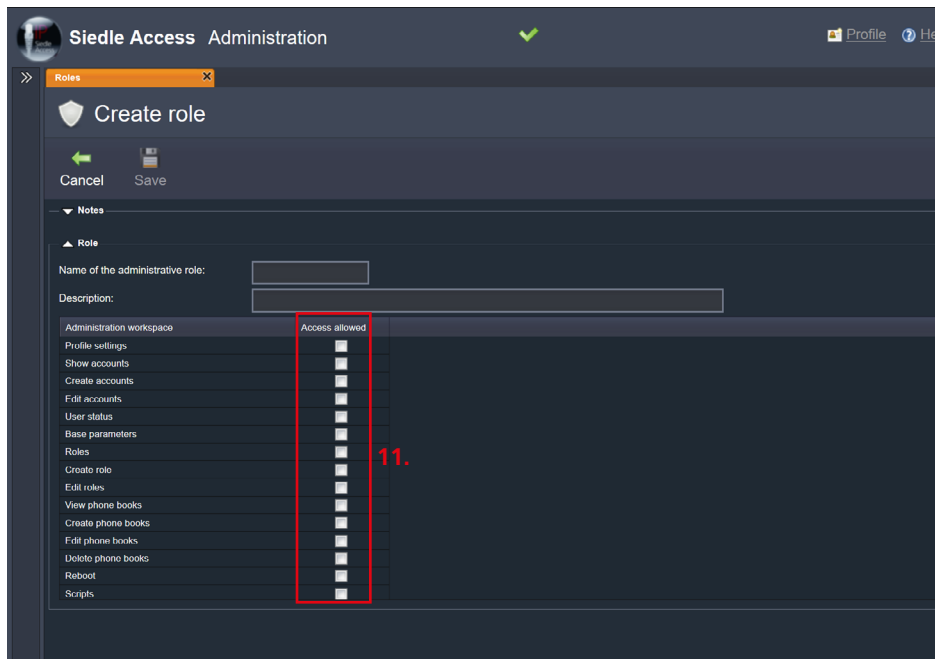
### Procedure – Edit role

**1** Select the role you wish to edit or delete.

**2** Click on **Edit** or **Delete**.

**3** Execute the changes to the **Role**.

**4** Click on **Save** to take the changes over in the system.



# Accounts

## Accounts

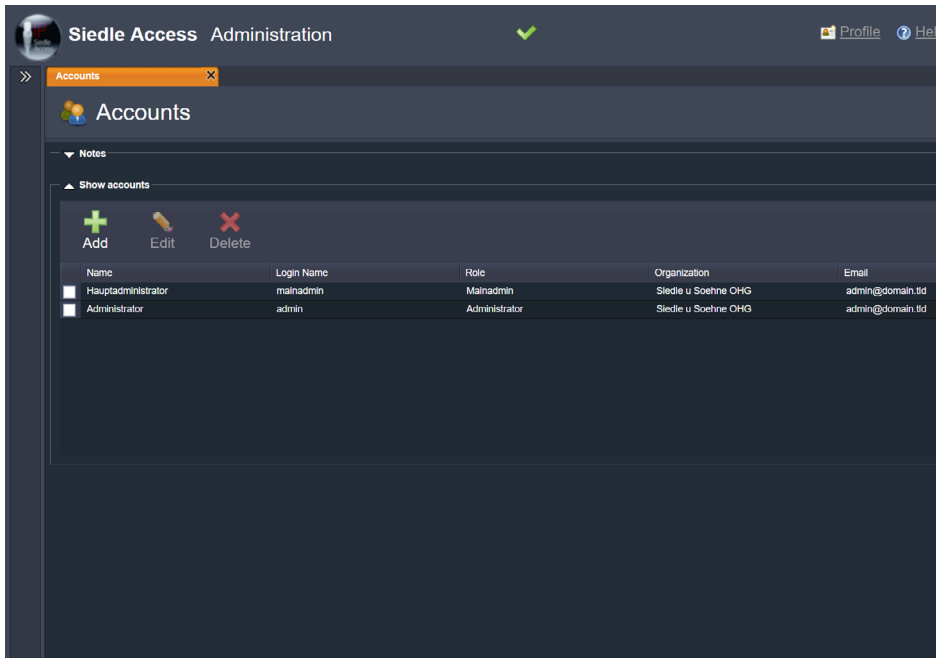
In this menu, you can create and manage new user accounts for accessing the Access system. The scope of user rights of a user account is defined by the assigned role. In addition, here you will find the most important information about the individual user accounts with the respective assigned role. The scope of user rights of a user account is defined by the assigned role. In addition, here you will find the most important information about the individual user accounts on the Access server with the respective assigned role. If the user rights assigned to your user account allow, here you can create new user accounts.

## Authorizations

- Define which folders or groups the new user account will be permitted to read/edit. The access rights to a folder are automatically also assigned to its subfolders (inherited) and the existing subfolders are automatically ticked (recursively inherited rights).
- The column **Explicit** indicates whether the rights of a sub-folder are adopted (inherited) unchanged (**Explicit** not ticked) or whether they deviate from the higher-level folder (**Explicit** ticked).
- In the case of folders which have no higher-level folder, **Explicit** is always set. As soon as you manually change the administration rights of a sub-folder, the field **Explicit** is always set.
- If only the field Explicit is set for a folder, you have no write / read rights over this folder, but you can see it greyed out in the folder structure.

## Remarks

- As standard, a new administrator has no access rights to the user tree or the groups.
- To be able to save a new user account, you must complete all entry fields.
- Administrators can only process their own profile (user name, password, language etc.) if the **Profile component** is activated in their assigned role (see **Access server > System maintenance > Administrators > Roles**).
- If you require different access rights at the Access server, first use the menu **Roles (Access server > System maintenance > Administrators > Roles)** to create the required **Roles** with the relevant access rights (e.g. administrator, area administrator, facility manager).



# Roles and user accounts

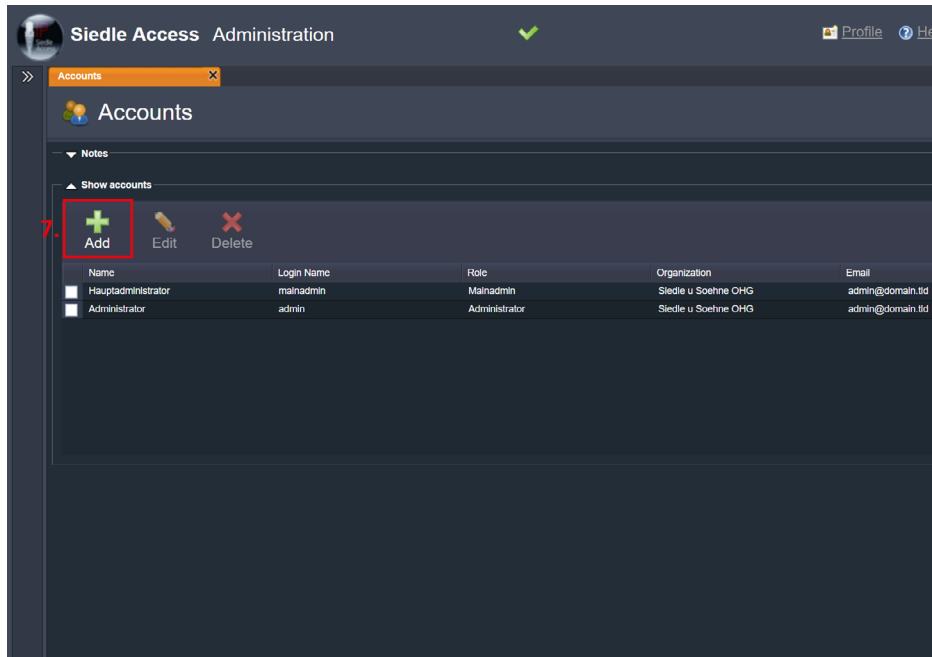
## Accounts

### Creating a user account

If the user rights assigned to your user account allow, here you can create new user accounts and edit or delete existing user accounts.

### Procedure - Creating a user account:

- 1** In the navigation area, click on the **System maintenance** menu.
- 2** The **System maintenance** menu opens up.
- 3** In the navigation area, click in the opened **Administrators** folder on **Accounts**.
- 4** The **Administrators** folder opens up in the navigation area.
- 5** In the navigation area, click in the opened **Administrators** folder on **Accounts**.
- 6** The **Accounts** page opens up in the content area.
- 7** Click on **Add** to create a new user account.
- 8** The **Create administrator** page opens up in the content area.



**9** In the **Administrator** area, enter all data (name, login name, organization and e-mail) of the new user account.

**10** Use an **adequately long** and **secure** password.

**11** Select the correct role for the user account under **Role**.

**12** Under **Language**, select the required language (**German** or **English**) for the administration user interface for this user account.

**13** Under **Time format and date format** select the required display format.

**14** Change to the area **Administrator rights**.

**15** Under **Administrator rights - Folders** assign **Edit** and/or **Read** rights valid for this user account for the displayed folders in the user tree.

**16** Under **Administrator rights - Groups** assign **Edit** and/or **Read** rights valid for this user account for the displayed groups in the user tree.

**17** Check all inputs, your selection and the set assignment of user rights.

**18** Click on **Save** to take the changes over in the system.

**19** The new user account is now ready to use.

The screenshot displays the 'Siedle Access Administration' web interface. The main heading is 'Create accounts'. Below the heading are 'Cancel' and 'Save' buttons. A 'Notes' section is visible. The 'Account' form contains the following fields:

- Name:
- Login Name:
- Password:
- Repeat password:
- Organization:
- Email:
- Role: Choose Role (dropdown menu)
- Language: English (dropdown menu)
- Time format: (dropdown menu)
- Date format: (dropdown menu)

The 'Administrator rights' section shows a table with columns for Folder, Read, Edit, and Explicit. The table lists various folders and their corresponding permissions for the user 'Lipp Michael'.

Folder	Read	Edit	Explicit
Not assigned devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Project	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
... Apartment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
... Pkt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
... Wohnung DG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
... Tot 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
... Testothor 001	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lipp Michael	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

# Roles and user accounts

## Accounts

### Procedure for editing or deleting a user account:

If the user rights assigned to your user account allow, here you can edit or delete existing user accounts.

**1** In the navigation area, click on the **System maintenance** menu.

**2** The **System maintenance** menu opens up.

**3** In the navigation area, click in the opened **Administrators** folder on **Accounts**.

**4** The **Administrators** folder opens up in the navigation area.

**5** In the navigation area, click in the opened **Administrators** folder on **Accounts**.

**6** The **Accounts** page opens up in the content area.

**7** Select an existing user account (e.g. administrator).

**8** Click on **Edit** or **Delete**.

### Note

- The delete process of a user account is always safeguarded by a confirmation prompt.

### Editing administrators

If the user rights assigned to your user account allow, here you can edit or delete existing user accounts.

### Procedure

**9** Select an existing user account (e.g. administrator).

**10** Click on **Edit** or **Delete**.

**11** Adjust the data and rights of the administrators in accordance with the required changes.

**12** Click on **Save** to take the changes over in the system.

### Remarks

- Only enter your Password here if you wish to edit it. A change of password is only effective on the next Login at the Access server.
- Administrators can only process their own profile (user name, password, language etc.) if the **Profile component** is activated in their assigned role (see **Access server > System maintenance > Administrators > Roles**).

The screenshot shows the 'Edit accounts' page in the Siedle Access Administration interface. The page is titled 'Siedle Access Administration' and 'Edit accounts'. It features a 'Cancel' and 'Save' button, a 'Notes' section, and a table for 'Elt: Rechteverwaltung' (Rights Management). The table has columns for 'Folder', 'Read', 'Edit', and 'Explicit'. A red box highlights the 'Notes' section and the table, with a red '9.' next to it.

Folder	Read	Edit	Explicit
Not assigned devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Project	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
... Apartment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
... Pst	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
... Wohnung DG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
... Tost 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
... Testordner 001	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lipp Michael	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## Final assignments

### **Carry out a function check**

#### **Procedure**

Carry out a complete function test of the Access system with all devices and all set up functions (Door call, door dialling, door release, internal call, external call, contacts, phone-books etc.)

### **Handing over the Access system to the customer**

#### **Procedure**

- 1** Carry out a system backup of the Access system.
- 2** Hand over all files (system backup, licences etc....), the system documents and all changed access data to the customer/operator/system administrator.
- 3** After transferring, delete all commissioning files from your commissioning laptop.
- 4** Instruct the customer/system administrator in the Access system and document the system instruction.
- 5** Hand over the Access system to the customer and document the system handover.

**6 Notify the customer/operator/system administrator that he should assign new secure access passwords after system handover, which should not be known to you.**

## Optional administration functions

### Reboot / shut down

#### Reboot / shut down

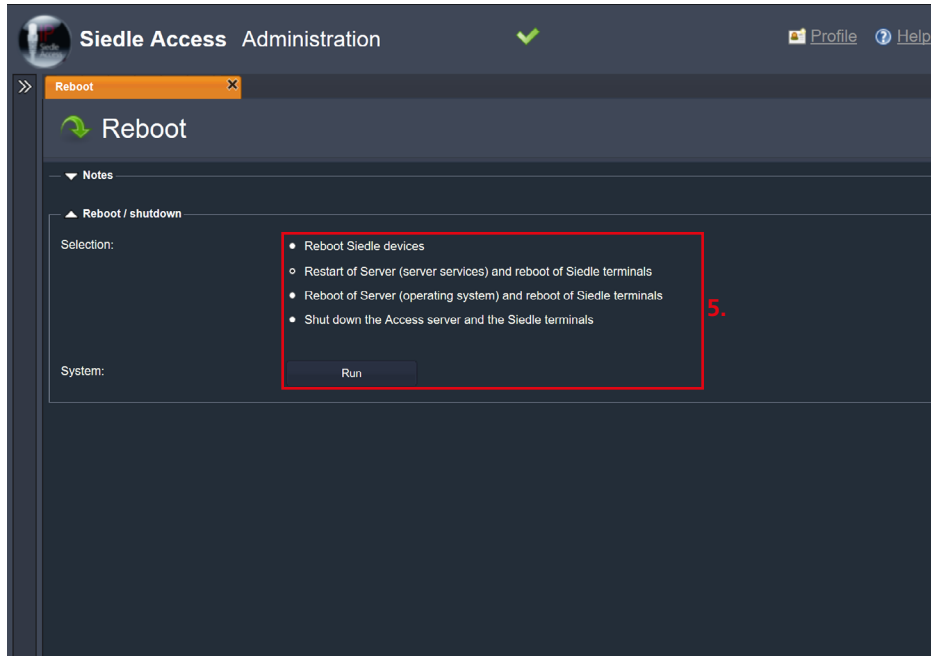
In this menu, you can reboot the Siedle terminals and reboot or shut down the Access server. If you carry out a restart, the Access administration user interface remains disabled for the relevant required time period and then reactivated again after a completed restart.

#### Important!

The user account login remains in existence in the event of a restart.

#### Procedure

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the navigation area, click into the opened **System maintenance** menu on **Reboot**.
- 4 The **System reboot** page opens in the content area.
- 5 Select the relevant option.
- 6 Click on **Execute** to execute the option.



The screenshot shows the Siedle Access Administration web interface. At the top, there is a navigation bar with the Siedle logo, the text "Siedle Access Administration", a green checkmark, and links for "Profile" and "Help". Below the navigation bar, a "Reboot" tab is active. The main content area is titled "Reboot" and contains a "Notes" section. Under "Notes", there is a sub-section "Reboot / shutdown" with a "Selection:" label. A red box highlights a list of four options: "Reboot Siedle devices", "Restart of Server (server services) and reboot of Siedle terminals", "Reboot of Server (operating system) and reboot of Siedle terminals", and "Shut down the Access server and the Siedle terminals". A red number "5." is placed to the right of this list. Below the list is a "System:" label and a "Run" button.



## Help

### • Restart of the Siedle hardware terminals:

Restarts the Siedle Access hardware terminals linked to the Access server immediately. The Access server and the other devices (PC software, Siedle app or non-Siedle devices) remain operational without change.

### • Restart of the server (server services) and restart of the Siedle hardware terminals:

Executes a restart of the Access server without server operating system and the Siedle Access hardware terminals. The software clients and the Siedle app are automatically logged off. Non-Siedle devices are not rebooted.

### • Restart of the server (operating system) and restart of the Siedle hardware terminals:

Executes a restart of the Access server including server operating system and the Siedle Access hardware terminals. The PC software and the Siedle app are automatically logged off. Non-Siedle devices are not restarted.

### • Shut down the Access server and Siedle terminals:

Shuts down the Access server, switches it off and restarts the Siedle Access terminals (**Exception:** The display **Waiting for Server reboot** appears on the AVP) .

The PC software and the Siedle app are automatically logged off.

Non-Siedle devices are not restarted. All system statuses activated are reset when starting up (e.g. activated Doormatic is deactivated, call rerouting set-ups are deactivated, switching outputs are returned to their configured idle status etc.). The Access server can be switched on again manually with the ON button.

# Optional administration functions

## System version

### Version

In this menu, you see an overview of all software statuses existing in the system of the Access system and the Access terminals (hardware and software clients). This page is intended exclusively for your information.

### Note

- If the software client (Concierge = ASC 170 and Access in-house telephone = ASHT 170) has also been updated in a newly delivered version of the Access system, when the older PC client version is next started up, a dialogue appears which allows you to confirm or cancel the software client update. When cancelling, the PC client is closed again. This ensures that all the software clients operated in the Access server are always updated and available in the latest version.
- Please also check for the mobile terminals whether a new version of the Siedle app is available for downloading.

### Procedure – Accessing system information

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the navigation area, click into the opened **System maintenance** menu on **Version**.
- 4 The **Version** page opens up in the content area.
- 5 Take the required information from the content area.

Siedle Access Administration

Profile Help

Version

Version

Notes

Version

Access system version: V 4.0.0 Build 1048

Access components	Version
AS 670-0	V 4.0.010
AHT 870-0 AHT-V1	V 3.0.002
ASC 170	V 4.0.000
ASHT 170	V 4.0.000
AHTV 870-0 AHTV-V1	V 3.0.002
AHF 870-0 AHF-V1	V 3.0.002
AHFV 870-0 AHFV-V1	V 3.0.002
ATLC 670-0 ATLC-V1	V 3.0.002
AVP 870-0 AVP-V2	V 3.2.000

# System backup

## Creating a system backup

In this menu, you can manually create a configuration backup of the Access system.

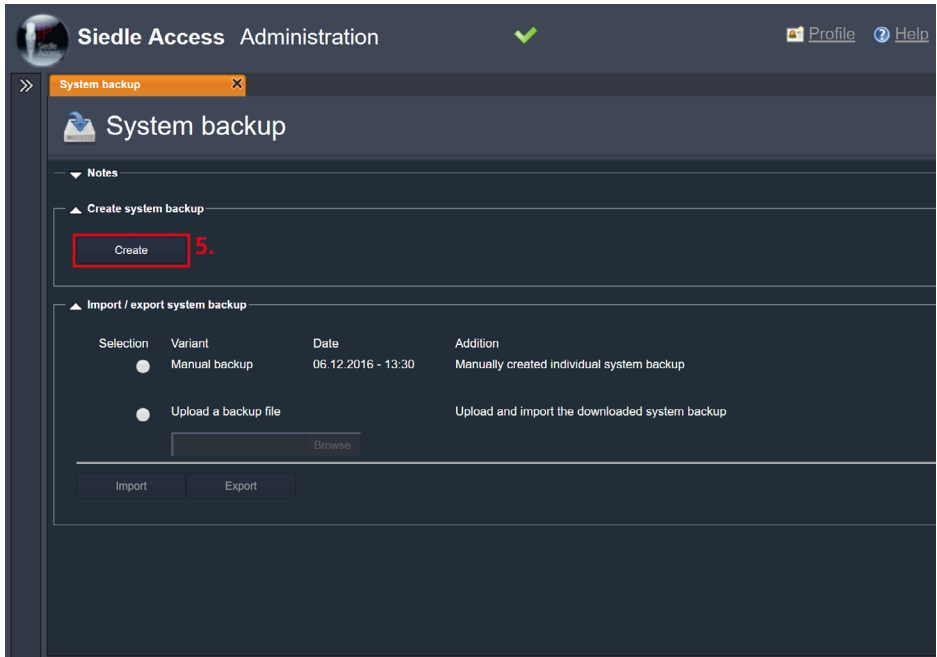
### Important!

- Please plan a suitable time window outside the main operating time of the Access system. Ensure that all affected users are informed of the planned interruption of operation.
- During a backup or restore process, the Access communication System is non-operational for a number of minutes as a system restart is carried out. All system statuses set by users are reset after a restart (e.g. activated Doormatic is deactivated, call rerouting set-ups are deactivated, switching outputs are returned to their configured idle status etc.).

- The following data designations were used for the backup file: backup\_c\_<time stamp>.abf
- The latest version of the manual backup is saved in each case.
- When a new backup is generated, the existing backup is overwritten. The backup file is saved with the latest time stamp on the Access server.
- Export the old backup before creating the new backup, if this is still required.
- In the **Import / export system backup** area and the column **Date** you can see when the last manual backup was created.

## Procedure

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the navigation area, click into the opened **System maintenance** menu on **System backup**.
- 4 The **System backup** page opens up in the content area.
- 5 In the area **Create system backup**, click on the button **Create**.
- 6 Read the notes contained in the confirmation prompt and confirm with **Yes**, if you wish to continue with the backup.
- 7 The system backup is carried out. The process can take some minutes.
- 8 The successful completion of the system backup is confirmed with a message.



# Optional administration functions

## System backup

### Exporting a system backup

In this menu, you can export a configuration backup of the Access system.

### Procedure

**1** In the navigation area, click on the **System maintenance** menu.

**2** The **System maintenance** menu opens up.

**3** In the navigation area, click into the opened **System maintenance** menu on **System backup**.

**4** The **System backup** page opens up in the content area.

**5** In the area **Restore / export system backup**, click on **Export**, in order to download the manual backup.

**6** The dialogue **Open ...** is displayed.

**7** Select **Back up file** and confirm with **OK**.

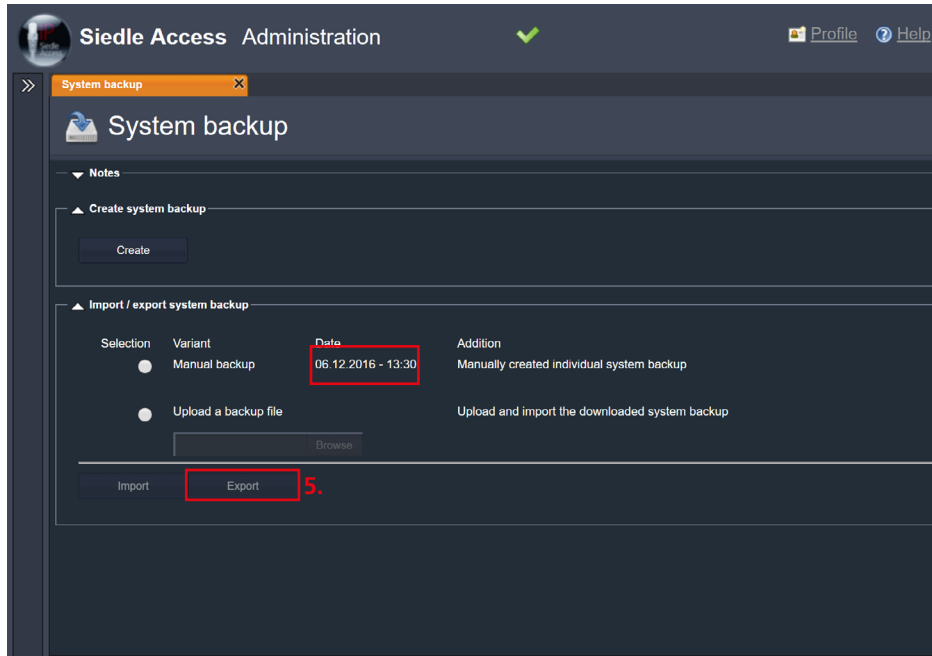
**8** Depending on the browser settings, the backup file is saved in a defined folder or you are asked where you want the backup to be created.

### Notes on system recovery

Following system recovery, the push token stored in the Access system at the time of system backup may no longer match the one in the mobile end device (e.g. due to an app update carried out in the interim). This means that notifications cannot be sent to the Siedle app. Each Siedle app running on the Access system must be logged onto the Access system once after such events.

### Remarks

- The file export is executed as a download over the web browser.
- The backup file is located in the area pre-set by you as the default storage location in the web browser (e.g. Downloads).



### Importing a system backup

In this menu, you can manually restore a configuration backup of the Access system.

#### Important!

- When restoring a backup, the existing data will be overwritten.
- Both the backup saved on the Access server and also a backup saved on a local data carrier can be restored to the system.
- During a backup or restore process, the Access communication System is non-operational for a number of minutes as a system restart is carried out. All system statuses set by users are reset after a restart (e.g. activated Doormatic is deactivated, call rerouting set-ups are deactivated, switching outputs are returned to their configured idle status etc.).

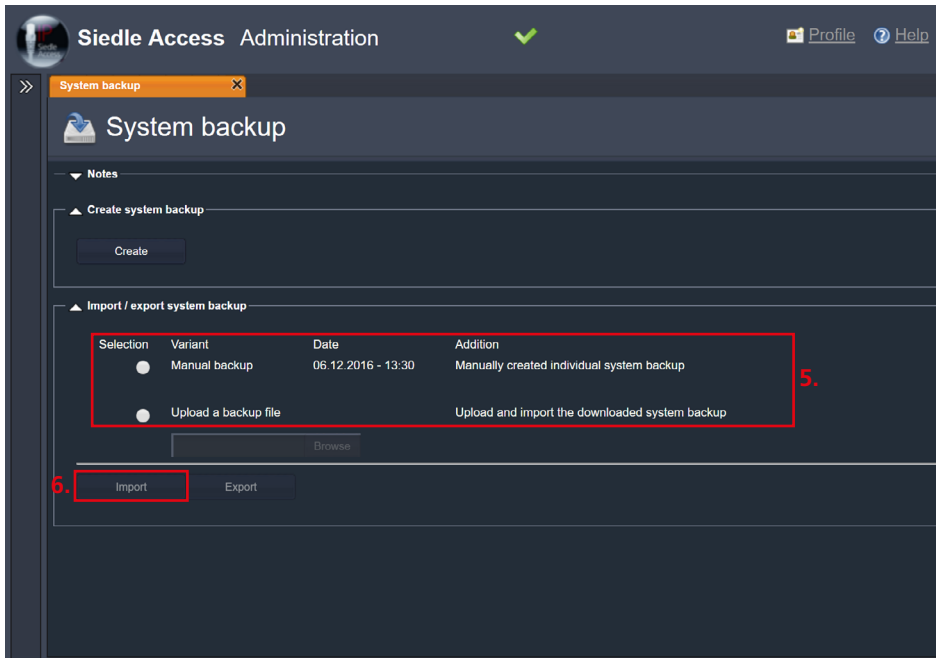
- Please plan a suitable time window outside the main operating time of the Access system. Ensure that all affected users are informed of the planned interruption of operation.

#### Procedure

- 1** In the navigation area, click on the **System maintenance** menu.
- 2** The **System maintenance** menu opens up.
- 3** In the navigation area, click into the opened **System maintenance** menu on **System backup**.
- 4** The **System backup** page opens up in the content area.
- 5** In the **Import/export system backup** area, select the type of backup you wish to import:
  - **Manual backup** on the Access server **or**
  - **Upload the backup** from an external storage location.

With the option **Upload backup**:  
**a)** Click on **Browse**.  
**b)** Navigate in your Windows Explorer to the storage location of the backup file.

- 6** Click on **Restore**.
- 7** Read the notes contained in the confirmation prompt and confirm with **Yes**, if you wish to continue with the backup.
- 8** The backup is imported. The process can take some minutes.
- 9** Successful completion of the system restoration is confirmed with a message.
- 10** Check all the basic parameters in full, carry out any corrections and save them.



## Optional administration functions

### Saving the protocol

#### Saving the protocol

In this menu, you can export the server and terminal protocols from the Access system in order to archive them.

#### Procedure

**1** In the navigation area, click on the **System maintenance** menu.

**2** The **System maintenance** menu opens up.

**3** In the navigation area, click into the opened **System maintenance** menu on **Logging**.

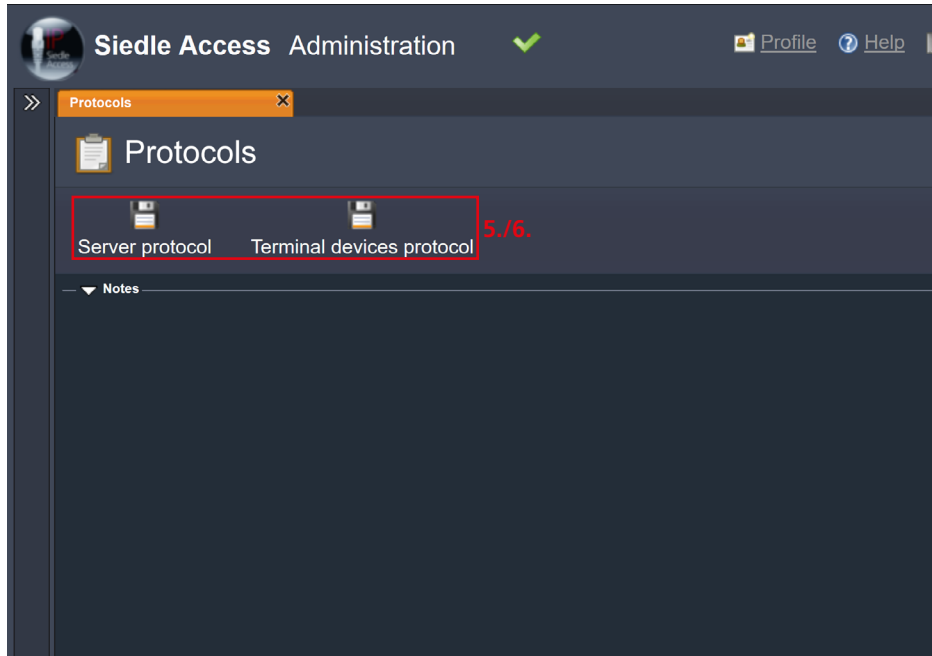
**4** The **Logging** page opens up in the content area.

**5** Click on **Server protocol**, to export the complete system protocol (server + users) including all the included protocol levels.

**6** Click on **Terminal protocol**, in order to export the user protocol (without server).

#### Remarks

- The server and terminal protocols are automatically deleted after a time period defined by you.
- You can change the time period with a prescribed range of 5-15 days in the menu **System maintenance > Basic parameters > Data management**.
- If you wish Access protocols to be permanently retained, these must be saved manually at regular intervals from the Access system. The possibility to export protocols is primarily intended for servicing purposes.
- If servicing is required, have the current protocol files to hand.



## View user status

### View user status

In this menu, you can view the current status of all Access users (not devices) created in the Access system. An Access user is a user to which one or more Access terminals can be assigned.

### Existing status:

- **OFFLINE:** No device of the Access user is currently logged into the Access server / is active.
- **IDLE:** At least one device of the user is logged into the system, is active and can be called.
- **CALL:** The user has started a call; the target call number is located in the column **Call destination**.
- **BUSY:** The user is on the telephone; the target call number is located in the column **Call destination**.
- **RING:** The user is being rung; the number of the caller is located in the column **Call destination**.
- **DND: Do Not Disturb** – the user has activated the call barring function and cannot be reached.

### Remarks

- Only the status of the Access user is displayed.
- It is not possible to display the status of individual Access terminals of an Access user (exception: 1 Access user is only assigned to 1 Access terminal).

The screenshot shows the Siedle Access Administration web interface. At the top, there is a header with the Siedle logo on the left, the text 'Siedle Access Administration' in the center, and a green checkmark on the right. Below the header is a navigation bar with a 'User status' menu item highlighted in orange. The main content area is titled 'User status' and contains a table with the following data:

Status	Call number (A-TLN)	Destination number	Name
IDLE	201		Haupteingang
IDLE	206		R. A. Munsch
OFFLINE	210		T. Matt
OFFLINE	1004		Sabine Test
OFFLINE	1002		R. Balthasar
OFFLINE	1008		XYZ
OFFLINE	1012		TD-Testgerät
OFFLINE	1010		Concierge
OFFLINE	1021		Lippl Michael

# Optional administration functions

## System characteristics

### System characteristics

In this menu, you can delete Access terminals which fail to complete the login process correctly due to a fault, and transfer them to the "Non-assigned devices" folder. These devices are displayed on the dashboard as "Devices in the log-in process" and remain there. Access terminals must be separated before being deleted from the Access system. After the completed delete process, they must be reconnected to the Access system. In addition, you can release process IDs of running or uncompleted critical Access processes.

### Procedure – Deleting assigned devices:

- 1 In the navigation area, click on the **System maintenance** menu.
- 2 The **System maintenance** menu opens up.
- 3 In the navigation area, click into the opened **System maintenance** menu on **System messages**.
- 4 The **System messages** page opens up in the content area.
- 5 In the **Important system messages** area under **Unassigned devices**, click onto the relevant line of the unassigned device you wish to delete.
- 6 Click on **Delete** to delete the unassigned device.

### Procedure – Releasing critical system processes (process IDs):

- 7 In the area **Release process ID** click onto the relevant line of the process you wish to release.

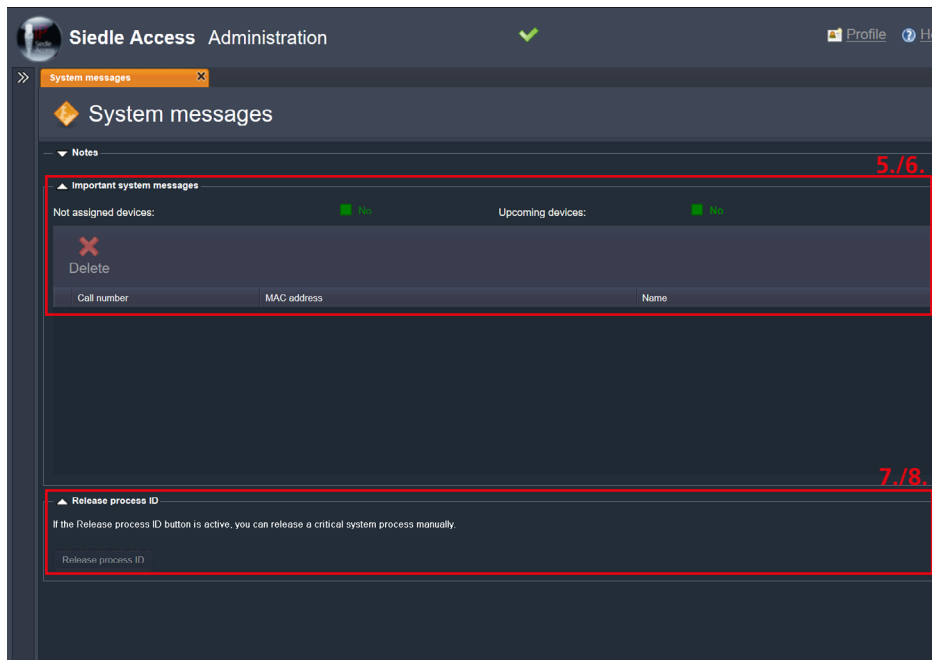
- 8 Click on **Release process ID** in order to release a critical process which has not been properly completed.

### Remarks

- The **Release process ID** is only active if a critical process has been started.
- If you start a critical Access process and are not able to complete it properly due to a technical fault, manual interruption or processing error, it is not possible to start other critical processes. In such cases, the incomplete process must be released in order to restore full functionality of the Access system.

### Critical processes are:

- Restart
- Update
- Creating a system backup
- Importing a system backup
- Saving basic parameters





## Connecting to external networks

### Connecting to external networks – Access gateway

Access terminals (hardware and software) can also be operated in your customer network. For this, you must connect the Access network to the existing customer network over the Access Gateway. The Access Gateway physically separates the two networks, and there is no possibility of infiltration into the Access network from the customer network. In this way, several independent customer networks can be linked to the Access network.

#### Important!

In contrast to the Access software clients, all Access hardware terminals additionally require the DHCP options transferred by the Access system in the **customer's network**. The IP settings to be configured refer to the customer network linked to the Access network, if Access hardware terminals are required to be operated in it. If the customer's own DHCP server is not able to distribute additional DHCP options, the DHCP server service of the Access Gateway must be used in this customer network and the DHCP server service of the customer router/gateway switched off.

### Configuring the Access Gateway

Operation of the Access Gateway AGW 670-... requires the Access server V. 2.1.3 Build 938 as a minimum requirement. If applicable, a software upgrade/update must be carried out at your Access system.

#### Configuration:

- **IP address:** IP address of the Access Gateway in the customer network.
- **Subnet mask:** Subnet mask of the IP address range in the customer network.
- **Gateway:** Gateway IP address of the customer router / gateway in the customer network for connection to the internet.
- **DNS:** DNS IP address of the customer router / gateway in the customer network for connection to the internet.
- **Multicast IP video:** Multicast IP address for Access server video stream transmission.
- **DHCP:** DHCP server service of the Access Gateway for the customer's own network can be enabled or disabled.
- **Start IP:** Start IP address for the IP address assigned by the DHCP server service in the customer's own network.
- **End IP:** End IP address for the IP address assigned by the DHCP server service in the customer's own network.
- **Password:** Access password for the Access Gateway (default: siedle).

### Remarks

- SIP services / telephone systems cannot be directly connected over the Access Gateway.
- Alternatively, you can connect the SIP services / telephone systems from the customer network to the Access server by the use of additional hardware (e.g. Session Border Controller – SBC), or if technically possible, you can carry out direct connection in the Access network.
- Using the video multicast IP, video streams are transmitted by the Access server to the Access network and over the customer networks connected to the Access Gateway.
- The video multicast IP addresses in the Access server and in the Access Gateway **must be identical**.

**Recommendation:** Even if you wish the video stream to be transmitted exclusively in the Access network/ server using unicast, we recommend ensuring that the video multicast IP in the Access server and Access Gateway agree. This ensures the right configuration in case of future modifications or changeover to multicast operation.

## Connecting to external networks

### Configuring the Access Gateway (continued)

#### Procedure – Access Server

- 1 The laptop and Access Server must be in the same network. If necessary, adjust the network address of the laptop.
- 2 Open the Firefox browser and enter the valid server address. The login window will open up. Enter the pre-set account names **admin** and the password **admin**.
- 3 Open the menu **System maintenance > Basic parameters > Server index tab**.
- 4 Make a note of the **Video multicast IP (e.g. 224.3.0.59)**.
- 5 Log out of the Access server.

#### Procedure – Configuring the Access Gateway

- 1 Decide on an IP address range for the customer network if you do not already have one.
- 2 The laptop and Access Gateway must be in the same network. If necessary, adjust the network address of the laptop. (LAN socket **Customer**).
- 3 Open the Firefox browser and enter the IP address **192.168.240.1/setup**.
- 4 The login window will open up.
- 5 Enter the pre-set user name **admin** and the password **siedle**.
- 6 The Access Gateway configurator opens.

The screenshot shows the Siedle Access Administration web interface. The top navigation bar includes the Siedle logo, the text 'Siedle Access Administration', a green checkmark, and links for 'Profile' and 'Help'. Below the navigation bar, there is a breadcrumb trail: '>> Base parameters'. The main content area is titled 'Base parameters' with a gear icon. A 'Save' button is visible. Below this, there are tabs for 'Notes', 'Server', 'Location', 'Date and Time', 'Data management', and 'Telephony'. The 'Server' tab is selected, showing a list of server configurations. The 'Server' list has a sub-header 'Server'. The configuration fields are: 'Server name:' with the value 'ibx'; 'Hardware ID:' with the value 'AAAA-BBBB-CCCC-DDDD-EEEE'; 'IP address:' with the value '10.32.246.10'; 'Video Multicast IP:' with the value '224.3.0.59', which is highlighted with a red box and labeled '6.'; 'System language:' with a dropdown menu set to 'English'; and 'Hide Captcha during login' with a checked checkbox.

**7** If you operate the Access Gateway as a DHCP server, untick the checkbox next to **DHCP**.

**8** Enter a freely selectable **Start IP address** for the DHCP address range.

**9** Enter a freely selectable **End IP address** for the DHCP address range.

**Note**

- The IP address range you require and the existing IP addresses of the Access Gateway can be freely selected.

**10** Enter the previously noted video multicast IP address from the Access server under **Multicast IP video**. The video multicast IP addresses in the Access server and in the Access Gateway **must be identical**.

**11** Allocate the DNS IP address of the customer router/gateway in the customer network (e.g. for the internet connection).

**12** Allocate the gateway IP address of the customer router/gateway in the customer network (e.g. for the internet connection).

**13** Allocate a subnet mask (e.g. 255.255.255.0).

**14** Check whether the previous IP address of the Access Gateway can continue to be used, or if necessary change it.

**15** Click on **Save Gateway data**.

**16** Note all changed settings in the provided fields of the Access Gateway product information.

**17** Change to the **Password** index tab.

**18** Allocate a new **Password** for the Access Gateway.

**19** Click on **Save Gateway data**.

**20** Note the newly allocated password in the provided field of the Access Gateway product information.

**21** Log out of the Access gateway.

**Accessibility**

- [IP address AGW]: Calls up the administration interface of the Access system (via the AGW)
- [IP address AGW]/setup: Calls up the administration interface of the AGW

**Gateway configurator**

gateway password **save gateway data** **15.** log

gateway (V 1.17)

IP address:	192.168.240.1
subnet mask:	255.255.255.0
gateway:	192.168.240.254
DNS server:	
multicast IP video:	224.3.0.59 <b>8.-14.</b>
DHCP:	<input checked="" type="checkbox"/>
start IP:	192.168.240.10
end IP:	192.168.240.199

# Index

Access device protocol	15, 168	Configuring necessary services and options	38	Firewall – Necessary ports	81
Access gateway	161	Configuring the Access video panel (AVP with KNX)	131	Firewall – Video multicast IP addresses	82
Access in-house telephone software	136	Configuring the static IP address	20	Getting started – Setting up the Access system	80
Access server variants	7	Connecting and switching on the server hardware	13	Handing over the Access system to the customer	151
Access Service Center	3	Connecting to external networks	161	Import the Access user licence and optional Access application licences	97
Access software module	137	Creating project	111	Important changes	5
Access system overview	6	Creating and configuring folders/subfolders	113	Incoming calls	144
Access system version – Important changes	5	Creating and configuring users	116	Individually defined call groups	121
Access software concierge	135	Creating contacts	110	Installation and operating conditions	18
Accessing the Access system	83	Creating a project	111	Installation process	68
Accounts	147	Data management	93	Installing the Access system	66
Acoustic button acknowledgements	101	Date and time	92	Installing the Firefox browser	80
Activating a remote connection	56	Default gateway	21	Installing the server operating system	18
Activating the IP address range	48	Defining exclusions in the IP address range and server time delay	42	KNX addresses	99
Activating the security code request	86	Defining the IP address range	41	Legal notice	4
Additional functions at the login window	84	Defining the WINS server	47	Licence agreements	84
Additional scripts	98	Device commissioning	15	Licences	10, 97
Administration graphic user interfaces	88	Device types	124	Location parameters	91
AHF/AHFV/AHT/AHTV 870-...	128	Device-specific settings	16	Log servers function	52
Apple Push Notification Service (APNS)	12	DHCP options	44, 50	Logging in with security code	86
AVP with KNX	131	DHCP server service	25	Logging in without security code	84
Basic parameter	90	Differentiation between users and call groups	112, 116, 123	Logging into the server operating system	19
Boot server host name	54	DNS server	21, 46	MAC address label	15, 168
Bootfile name	55	Domain name	46	Maintenance contract	11
Button configuration	128, 131	Door station (ATLC)	115, 124, 125	Menu structure	
Carry out a function check	151	Downloading and installing the Access system	66	Access Professional	87
Changing the password	7, 19, 83, 84, 85	Editing already defined call groups	120	Microsoft .NET Framework 3.5/ 4.6.1	62, 63
Checking the safety warning message	69	External device licences	97	Models	124
Commissioning – Access system	13	External telephones	142	Modifying the NTP server services configuration	58
Commissioning possibilities	16	Facility Pilot Server	131	Name of the server service	40
Commissioning requirements	13	Final assignments	151	Navigation area	89
				Necessary ports – Firewall	81

Network configuration	17	Starting the server manager	22
New in this version	88	System backup	155
NTP server	12, 53	System characteristics	160
Optional Access licences	97	System conditions	9
Optional administration functions	152	System information	154
Ordering Access licences	96	System overview	6
Protect your network!	4	System update	76
Protect your property!	4	System updating procedure	74
Reboot / shut down	152	Telephone directories	109
Recommended commissioning sequence	14	Telephone systems	12, 102
Requirements imposed on virtualization	9	Telephony	94
Restart the system	72	Telephony link	103
Roles and user accounts	145	Telephony routes	144
Safety remarks	4	Test period	10
Saving the protocol	158	Time server	51
Scope Wizard	39	Time synchronisation in the Access system	12
Server	90	Uninstall process	77
Server hardware	8	Uninstalling the Access system	77
Servicing	4	Updating the Access system	74
Setting up the Access system	80	User accounts	147
Setting up the server operating system	18	User interface language	85
Set-up of building automation in AVP with KNX (Facility Pilot Server)	131	User rights system	80
Shut down	152	Validity of the IP configuration	43
Siedle Access device protocol	15, 168	Version	154
Siedle app for Access Professional	138	Video multicast IP addresses	82
Siedle App for Access Professional for Android panels	139	View user status	159
SIP audio telephone	141	Virtual device	124, 143
SIP provider account	106	Virtual machine	8
SIP video telephone	140	Virtualization	9
SIP-Gateway	103		
Specifying IP address for routers/gateways	45		
Start page (dashboard)	88, 95		

## As-delivered status / Factory settings

---

### Accessing the Access system

Remote access / Direct access

see page 83

---

---

IP address of the Access Server

192.168.1.1

---

Subnet mask

255.255.255.0

---

---

Password – server operating system

SiedleAccessMain2015

---

---

Password – Access server administration

admin

---

User name

admin

---



# SSS SIEDLE

S. Siedle & Söhne  
Telefon- und Telegrafengeräte OHG

Postfach 1155  
78113 Furtwangen  
Bregstraße 1  
78120 Furtwangen

Telefon +49 7723 63-0  
Telefax +49 7723 63-300  
[www.siedle.de](http://www.siedle.de)  
[info@siedle.de](mailto:info@siedle.de)

© 2016/12.18  
Printed in Germany  
Best. Nr. 210006190-00 EN