

Intra2net Administrator Manual



Intra2net Business Server
Intra2net Security Gateway
Intra2net Network Security

Intra2net Administrator Manual

Intra2net AG

Publication date 20. May 2025

The contents of this manual have been prepared with care. However, the information in this manual is not a warranty of product performance. Intra2net AG shall only be liable to the extent of its sales and delivery conditions and shall not assume any liability for technical inaccuracies and/or omissions. The information in this manual is subject to change without notice. Additional information, as well as changes and version information for Intra2net systems can be found online at <https://www.intra2net.com>

The Intra2net system establishes communication connections depending on the configuration. In order to avoid unwanted charges and data loss, the product should be monitored and backed up at regular intervals. Intra2net accepts no responsibility for loss of data, accidental connection costs or damage caused by the unattended operation of the product.

Intra2net and the Intra2net logo are registered trademarks of Intra2net AG. Company and product names are mostly trademarks of their respective companies or manufacturers.

Copyright © 1999-2025 Intra2net AG. All rights reserved. No part of this manual may be reproduced or reused in any form whatsoever without prior written permission from Intra2net AG.

Intra2net AG
Mömpelgarder Weg 8
72072 Tübingen
Germany

Valid for Intra2net software version 7.0.0

Valid for Intra2net Groupware Client Version 5.0.2

1. Installation	1
1. Welcome	2
1.1. About this Manual	2
1.2. Factory Settings	2
2. Installation on Own Hardware	3
2.1. Hardware Selection	3
2.2. Installing as a Virtual Machine	3
2.3. Location	3
2.4. BIOS	3
2.5. RAID	5
2.6. Installation of the operating system	5
2.6.1. Installation from a USB flash drive	5
2.6.2. Installation from DVD	6
2.6.3. Start of the installation	6
2.6.4. Serial console	6
2.6.5. Solving Compatibility Problems	6
3. Installing as a Virtual Machine	8
3.1. Comparison to Real Hardware	8
3.1.1. Inconsistent performance speed	8
3.1.2. Lower I/O Performance	8
3.1.3. Contact with Unfiltered Network Packets	8
4. Installation on VMware vSphere Hypervisor 4 (ESXi)	10
4.1. Virtual Machine Configuration	10
4.2. Virtual Machine with Direct Internet Access	15
4.3. Installing the Intra2net System	18
5. Installation of Microsoft Hyper-V on Windows Server 2012 R2	20
5.1. Virtual Machine Configuration	20
5.2. Installation of the Intra2net System	27
6. The Console	29
6.1. Intra2net Appliance Micro	29
6.2. Network Cards	29
6.3. DNS and DHCP	30
6.4. Firewall Emergency Mode	30
6.5. Restore to Factory Settings	30
6.6. The Root Password	31
6.7. The Linux Shell	31
7. The Web Interface	32
7.1. Accessing the Web Interface	32
7.2. License Code	32
7.3. The Main Page	32
7.4. The Queue	33
7.5. The Configuration Check	34
7.6. Shutdown necessary	34
2. General Functions	35
8. Intranet	36
8.1. IPs and Networks	36
8.2. VLAN Tagging	36
8.3. Access Rights of a Network Object	37
8.4. Domain and DNS	37
8.4.1. The Intra2net system as local DNS server	37
8.4.2. Integrate another DNS server in the LAN	38
8.4.3. Forward DNS to Other Domains	39
8.4.4. Prevent DNS Rebind	39

8.5. Registering Clients	41
8.5.1. Wake-On-LAN	41
8.5.2. DHCP	41
8.6. DHCP-Server	42
8.7. Entering Ranges	42
8.8. Import/Export Client Profiles	42
8.8.1. Importing Clients	42
8.8.2. Exporting Clients	43
8.9. Intranet Routing	43
9. SSL Encryption and Certificates	44
9.1. Principles and Dangers of SSL Encryption	44
9.2. Correctly Creating Certificates	44
9.2.1. The Computer Name	44
9.2.2. Configuration	45
9.3. Installing Certificates on Clients	45
9.3.1. Installation with Windows	45
9.3.2. Distributing Certificates via Active Directory	48
9.4. User Education and Awareness	49
9.5. Using an External Certificate Authority	49
9.5.1. Certificates from Let's Encrypt	49
9.5.2. Certificates from classic certification authorities	50
9.6. Key Import	51
9.7. Encryption Strength	51
10. Internet	53
10.1. Dial-up with DSL (PPPoE)	53
10.2. Dial-up with DSL (PPTP)	53
10.3. Router with static IP	53
10.4. Router with DHCP or Cable Modem	54
10.5. Router on the Local Network	54
10.6. Router vs. Modem	55
10.7. Official IPs and DMZs	55
10.7.1. Classic Routing	55
10.7.2. Static NAT	56
10.7.3. Proxy-ARP	57
10.8. Automatic Connection	58
10.9. Connection Monitoring	59
10.10. Switching to Other Providers in the Event of an Error (Fall-back)	59
10.11. Bandwidth Management and VoIP Prioritization	59
10.11.1. Bandwidth Management	59
10.11.2. Prioritize VoIP and Real-time Data	61
10.12. Masquerading / NAT	61
10.13. DynDNS	62
10.13.1. Providers	62
10.13.2. Updates and the IP Address Used	62
10.14. External access	63
11. Proxy	64
11.1. Overview	64
11.2. Access to the Proxy	64
11.3. Proxy Configuration	65
11.4. URL Filter	65
11.4.1. Proxy Profile	65
11.4.2. Proxy Access Lists	65

11.4.3. Time Management	66
11.5. Web Content Filter	66
11.6. Proxy Virus Scanner	66
12. Statistics and Data Privacy	68
12.1. Proxy Statistics	68
12.1.1. Proxy Logging	68
12.1.2. Analysis	68
12.1.3. Methodology	68
12.2. Internet Access Statistics	69
12.2.1. Methodology	69
12.3. Speedometer	70
12.3.1. Methodology	70
12.3.2. Sites	71
12.3.3. Data Privacy	72
12.4. Space Usage Statistics	72
12.5. Data Privacy	72
13. Usermanager	74
13.1. User Groups	74
13.1.1. Access Rights	74
13.1.2. Administration Rights	75
13.2. User	75
13.2.1. Settings for Email and Groupware	75
13.3. Import/export of User Profiles	75
13.3.1. Importing Users	76
13.3.2. Exporting Users	76
14. Email	77
14.1. Email Relay	77
14.1.1. Rights	77
14.1.2. SMTP-Submission	77
14.1.3. Dispatch Methods	77
14.1.4. Dispatch via relay server	77
14.1.5. Direct Dispatch	78
14.1.6. Choosing the dispatch method	78
14.2. Receiving emails on the client (POP or IMAP)	79
14.3. Receive emails using the Intra2net system	79
14.3.1. Methods	79
14.3.2. Retrieving individual POP accounts	81
14.3.3. Direct delivery via SMTP	82
14.3.4. Retrieval of collective POP accounts (multidrop)	82
14.4. Forwarding of entire domains	84
14.4.1. Method	84
14.4.2. Recipient Address Check	84
14.4.3. Forwarding of individual POP accounts	87
14.5. Email Addressing	87
14.5.1. Address Settings	87
14.5.2. Email Addresses and Aliases	87
14.6. Email Processing	88
14.6.1. Forwarding	88
14.6.2. Automatic Response	88
14.6.3. Sorting	89
14.6.4. Automatic deletion	89
14.7. Emailfilter	89
14.7.1. Spamfilter	89

14.7.2. Virus Scanner	93
14.7.3. Attachment Filter	94
14.8. DKIM	96
14.8.1. Basic principles	96
14.8.2. Implementation	96
14.8.3. Further standards	97
14.8.4. Prerequisites for use	97
14.8.5. Configuration	98
14.8.6. Filtering and quarantine	101
14.8.7. Header lists and exceptions	101
14.8.8. Rotate the key	102
14.9. Archiving	102
14.9.1. Interface	102
14.9.2. Connecting the MailStore Server	103
14.10. Automatic Transfer	110
14.11. Mailinglist	110
14.12. Additional Settings	110
14.13. Queue	111
14.14. Structure of the mail system	111
14.15. Differences between licenses	111
15. Services	113
15.1. Timeserver	113
15.2. Monitoring via SNMP	113
16. System Functions	114
16.1. License	114
16.1.1. Demo Mode	114
16.1.2. License Code	114
16.1.3. Update Period	114
16.2. Updates	114
16.2.1. Remote Update via Partner Web	115
16.2.2. Rescue System	115
16.3. Backup	116
16.3.1. Backup protection	117
16.3.2. Storage period	117
16.3.3. Remote Storage	117
16.3.4. Restore	118
16.3.5. Procedure for Hard Drive Damage or Hardware Replace- ment	118
16.3.6. Hardware migration with Intra2net support	119
16.3.7. Standby systems	120
16.4. Operation Behind Firewall	122
16.5. Logfiles	123
16.6. Logcheck Reports	123
16.7. Scheduled Shutdown	123
16.8. Inspection and repair of filesystems	124
3. Groupware Client	125
17. Introduction	126
17.1. System Requirements	126
17.2. Overview of Features	127
17.3. Known Limitations	127
18. Installation	129
18.1. Installing the Program	129
18.2. Distributing the Program via Active Directory	130

18.3. Switch from 32 bit to 64 bit	131
19. Setting up a Profile	132
20. Account Configuration	135
20.1. Groupware Account	135
20.1.1. Activate Certificate Check	135
20.1.2. Deactivating the Search Indexer	136
20.2. Importing Existing Data	137
20.2.1. Importing Using Outlook Import	138
20.2.2. Importing Larger Amounts of Emails	141
20.3. Setting up Multiple Accounts and Email Addresses	143
20.3.1. Multiple Server Accounts	143
20.3.2. Multiple Outgoing Mail Identities	145
20.4. Converting Previous Installations of the Groupware Client	148
21. Linking Folders	152
21.1. Linking Own Folders	152
21.1.1. Automatic registration	152
21.1.2. Excluding Folders from Synchronization	153
21.1.3. Update folder list	154
21.2. Linking Shared Folders	155
22. Sharing Folders	157
22.1. Rights	158
22.2. Read Status Shared/Individual	158
23. Folder Linking Expert Mode	159
23.1. Linking Shared Folders	159
23.2. Manual folder linking	162
23.2.1. Switching to Manual Linking	163
23.2.2. Linking an Individual Folder	163
23.2.3. Unlinking a folder	165
24. Additional Features	167
24.1. Folder Hierarchy and ibx_sub	167
24.2. Folder Options	167
24.3. Editing Server-Side Settings	168
24.4. Categories and color assignment	169
24.4.1. Recommendation for shared color assignment	170
24.4.2. Reset local color assignment	170
24.4.3. Changing an existing color assignment	171
24.5. Use Free/Busy Information	172
24.5.1. Outlook 2010 to 2021	172
24.5.2. Outlook 2007	173
24.6. Marking as Private	175
24.7. Reminders in Shared Folders	176
24.8. User-Defined Fields in Contacts	177
24.9. Showing Item Source Text	177
24.10. Backup Folders	177
24.10.1. Backup Data after Restore	178
24.10.2. Backup of local data when resetting to automatic mode	178
24.11. Advice to the User	179
24.12. Log files	180
24.12.1. Submitting log files to support	180
25. Advanced Email Configuration	181
25.1. Retrieve Emails Completely or Only Headers	181
25.2. Notification of New Emails	181

25.3. Marking Moved Emails as Read	182
25.4. Email Reminders and Tracking	183
25.5. Read receipts	184
26. Compatibility and Collaboration	186
26.1. Personal firewalls on the Client	186
26.2. Virus Scanner on the Client	186
26.3. Compatibility with PDAs and Mobile Phones	186
26.4. Other Programs	187
26.4.1. Incompatible Addins	187
26.5. Automatic detection of compatibility problems	188
27. Concept for public folders	189
27.1. Setup	189
27.2. Emails	189
28. Migrating Emails with IMAPCopy	191
29. Migration from Microsoft Exchange	193
29.1. Offline Migration	193
29.1.1. Migration Step-by-step	193
29.2. Migration During Operation	194
29.2.1. Preparing for Migration	195
29.2.2. Migrating Individual Users	196
29.2.3. Shared Folders	197
29.2.4. Final steps	197
30. Reference Information	198
30.1. Synchronizable data	198
30.1.1. Tasks	198
30.1.2. Meetings	199
30.1.3. Notes	200
30.1.4. Contacts	200
30.1.5. Contact Groups	203
30.1.6. Emails	203
30.1.7. All Items	204
30.2. Advanced Registry Settings	204
30.2.1. Store Settings	205
30.2.2. Addin Settings	212
30.3. Data Formats	213
4. Web-Groupware and ActiveSync	215
31. Introduction to Web Groupware	216
31.1. The Display Modes	216
32. Email	217
32.1. Reading and Editing Emails	217
32.1.1. Displaying Emails	217
32.1.2. Deleted Emails	218
32.1.3. Exporting Emails	218
32.2. Sending Emails	219
32.2.1. New Message	219
32.2.2. Append Signatures	220
32.3. Managing Folders	221
32.3.1. Folder Hierarchy	221
32.3.2. Organizing Folders	221
32.3.3. Subscribing to Folders	221
32.3.4. Sharing Folders	223
33. Address Book	225
34. Connecting Mobile Devices using ActiveSync	226

34.1. Introduction	226
34.2. Server Settings	226
34.3. Special Features and Tips	227
34.3.1. Deleting Emails on the Server	227
34.3.2. Synchronization Steps	227
34.3.3. Manage and Resynchronize Devices	228
34.3.4. Synchronize Multiple Calendars or Contact Lists	228
35. ActiveSync with Android Devices	229
36. ActiveSync with Apple iOS Devices	233
37. Reference Information	237
5. Firewall	238
38. Selecting Firewall Rulesets	239
38.1. Rulesets on LAN	239
38.2. Rulesets for the Internet	239
38.3. Packet Routes Through the Firewall	239
38.3.1. Packet Routes on the LAN and Internet	239
38.3.2. Packet Routes for VPN Connections	240
39. Firewall Profile	241
39.1. General Basic LAN Rules	241
39.2. Client Profiles	241
39.3. Provider profile	242
40. Full Rulesets	243
40.1. Components	243
40.1.1. Services	243
40.1.2. Netgroups	243
40.1.3. Netgroups with DNS hostnames	244
40.1.4. Automatic Objects	244
40.2. Rulesets	244
40.2.1. Default Settings	244
40.2.2. Passing Through the Ruleset	245
40.2.3. Linking Rule Criteria	245
40.2.4. The Actions	246
40.2.5. Extra Options	246
40.2.6. Special Features of Provider Rulesets	247
41. Additional Functions	249
41.1. Checking MAC Addresses	249
41.2. Preventing LAN spoofing	249
41.3. Blocking IPs After Too Many Login Errors	249
41.4. Firewall Emergency Mode	249
42. Case Studies and Examples	250
42.1. Example 1: Extending a Simple Client Profile	250
42.1.1. Sample Solution	250
42.2. Example 2: Port Forwarding Only Accessible from an External IP	251
42.3. Example 3: Separate Guest Network	251
42.3.1. Sample Solution	252
42.4. Example 4: Restricted Access from the VPN	253
42.5. Example 5: Web Server in the DMZ	254
42.5.1. Sample Solution	254
6. IPSec VPN	256
43. IPSec Basics	257
43.1. IPSec	257
43.2. Public-Key Cryptography	257

43.3. Certificates	257
43.4. IPSec connections	257
43.5. Algorithms	258
43.6. Limitations	259
43.7. Compatibility with Other IPSec Peers	259
44. Key Management	260
44.1. Own Keys	260
44.1.1. Certificate Authorities (CAs)	260
44.2. Foreign Keys	261
45. Connecting Individual PCs	262
45.1. Method	262
45.2. Preparing the configuration on the Intra2net system	262
45.2.1. Create certificate	262
45.2.2. Default settings for new connections	265
45.3. Automatic configuration for clients on the Intra2net system	265
45.4. Manual configuration on the Intra2net system	267
45.4.1. Prerequisites	267
45.4.2. Default Settings	267
45.4.3. Authentication	268
45.4.4. Configuring the Tunnel	269
45.4.5. Rights	270
45.4.6. Activation	270
46. VPN with the NCP Secure Entry Windows Client	271
46.1. Import	271
46.2. Establish connection	272
46.3. Connection protocols	273
47. VPN with the Shrew Soft VPN Client	275
47.1. Import	275
47.2. Establishing Connection	275
47.3. Connection Protocols	276
48. VPN with Mac OS X	278
48.1. Installation	278
48.2. Generating Certificates	278
48.3. Importing Certificates	279
48.4. Configuring Connections	281
48.5. Intra2net System	284
49. VPN with the NCP Secure Entry macOS Client	285
50. VPN with the Apple iOS devices	288
51. VPN with Android	290
51.1. Preparing the Device	290
51.2. Connection on the Intra2net System	291
51.3. Certificates	291
51.4. Connecting with Android	293
51.5. Simplify Connection Setup	295
52. VPN with the NCP Secure Android Client Premium	298
53. Connecting Complete Networks	302
53.1. Method	302
53.2. Configuration on the Intra2net System	302
53.2.1. Prerequisites	302
53.2.2. Default Settings	303
53.2.3. Authentication	303
53.2.4. Configuring the Tunnel	303
53.2.5. Rights	304

53.2.6. Activation	304
54. VPN with ZyXEL ZyWALL USG	305
54.1. Overview	305
54.2. Preparation	305
54.3. Certificate	305
54.4. Connection	309
54.4.1. IKE / Phase 1	309
54.4.2. IPSec / Phase 2	310
54.5. Intra2net System	313
54.6. Logs	313
55. VPN with Lancom Routers	314
55.1. Overview	314
55.2. Certificate for the Lancom device	314
55.3. Certificate for the Intra2net System	316
55.4. Connecting	317
55.5. Intra2net System	323
55.6. Deleting Certificates	323
56. VPN with Linux	324
56.1. Overview	324
56.2. Generating Certificates	324
56.3. Configuring Connections	325
56.4. Intra2net System	326
57. Solving IP Address Conflicts in VPNs Through NAT	327
57.1. The Problem	327
57.2. Configuration	327
57.3. Same IPs on LAN and Peer	327
57.3.1. Implementation	328
57.4. Multiple Peers with the Same IPs	329
57.4.1. Implementation	330
57.5. Local IPs Defined by Service Provider for Remote Maintenance	330
57.5.1. Implementation	331
58. Error Diagnosis	332
58.1. Reading Logs	332
58.2. The Protocol Format of the Intra2net System	332
58.3. Error in Phase 1	332
58.4. Error in Phase 2	334
7. WireGuard VPN	335
59. WireGuard basics	336
59.1. The WireGuard protocol	336
59.2. Customization by Intra2net	337
59.3. Comparison with IPSec	338
60. Preparing the configuration on the Intra2net system	341
60.1. Own key and interface	341
60.2. External address and firewall	341
60.3. Default settings for new connections	342
61. Connect individual PCs	343
61.1. Concept	343
61.2. Automatic configuration for clients on the Intra2net system	343
62. WireGuard clients	345
62.1. Installation	345
62.2. Configuration	345
62.3. Operating the client	345
62.3.1. Log files	346

62.3.2. DNS name resolution	346
62.4. Special features of the Windows client	347
62.4.1. Protection of private keys	347
62.4.2. Usage without administrator rights	347
62.4.3. Routing for the network Everything (0.0.0.0/0.0.0.0)	348
63. Connection to other Intra2net systems	349
64. Connection with other routers and firewalls	350
64.1. Remote site without own key	350
64.2. Remote site with existing own key	351
65. Connection with AVM FRITZ!Boxes	353
65.1. AVM FRITZ!Box without previous connection	353
65.2. AVM FRITZ!Box with other VPN connection	355
66. Status and error diagnosis	358
66.1. Mainpage	358
66.2. VPN status	358
66.3. Logs	359
8. Appendix	360
A. Licenses	361
A.1. Intra2net Software License Agreement	361
A.2. Licensed software	366
A.3. Notes on return and disposal	367
A.3.1. Separate collection of old equipment	368
A.3.2. Batteries and accumulators and lamps	368
A.3.3. Options for the return of old equipment	368
A.3.4. Data privacy notice	368
A.3.5. Meaning of the crossed out trash can symbol	368
A.3.6. Free collection of used batteries	368
A.3.7. Meaning of the battery symbols	368
B. License	369
B.1. Intra2net Groupware Client License Agreement (EULA)	369
B.2. Licensed Software	373
B.2.1. Info-ZIP	373
B.2.2. JsonCpp	374
Index	375

Part 1. Installation

1. Chapter - Welcome

Welcome to Intra2net's user-friendly solution for connecting your network to the Internet, with minimal effort and maximum security. The Intra2net software regulates the access rights of your individual workstations, sends and manages the team's emails (depending on the selected license) whilst providing the freedom to choose any Internet provider available.

1.1. About this Manual

This manual describes the complete administration of the Intra2net system, from installation to the less frequently needed special functions.

1.2. Factory Settings

The following is a brief summary of the factory settings, for experienced users. What exactly these values mean and how they can be changed will be explained in the following chapters and in Part 2, „General Functions“.

IP Address	192.168.1.254
Netmask	255.255.255.0
DNS-Name	intra
Domain	net.lan
DHCP	Activated
DHCP IP Pool	192.168.1.200 to 192.168.1.250
HTTP proxy (only if included in the license)	Port 3128
Interface only accessible via SSL	Activated
Administrator Login	admin
Administrator Password	admin
Backup Creation	differential backup daily 06:30, 12:30 and 19:00 h, full backup Saturday 22:00 h
Backup Access Protection	activated, set the password under System > Backup > Settings
Email virus scanner (only if included in the license)	active
Email attachment filter (only if included in license)	active for executable files



Caution

Please change your login and password after the first use!

2. Chapter - Installation on Own Hardware

2.1. Hardware Selection

The minimum hardware requirements of the Intra2net software are as follows:

- x86-compatible processor with 64 bit and at least 2 GHz clock speed
- At least 2 GB of memory
- Hard drive with at least 40 GB storage capacity
- Two network cards
- A USB flash drive or CD-ROM drive (only required during installation)

More details about the supported hardware can be found online at <https://www.intra2net.com/en/support/hardware-compatibility.php>.



We recommend only using components or complete devices that are listed here as "certified". Intra2net guarantees optimal compatibility for these products with current and future versions of the software.

2.2. Installing as a Virtual Machine

The Intra2net system can also be installed as a virtual machine. In particular, VMWare vSphere Hypervisor (ESXi) and Microsoft Hyper-V are supported as virtualization platforms. A detailed list of supported virtualization platforms can be found online at <https://www.intra2net.com/en/support/virtualization-platforms.php>.



When installing as a virtual machine, there are a number of points to consider. These mainly concern security when operating as a firewall. Background information and detailed instructions can be found in 3. Chapter, „Installing as a Virtual Machine“.

2.3. Location

Please install the hardware in an area with controllable access (e.g. lockable room). Someone with sufficient system knowledge and physical access can compromise the Intra2net appliance.

Be sure to follow the hardware manufacturer's instructions regarding maximum ambient temperature and air supply. Most devices cannot be operated in an ambient temperature of more than 35 °C.

2.4. BIOS

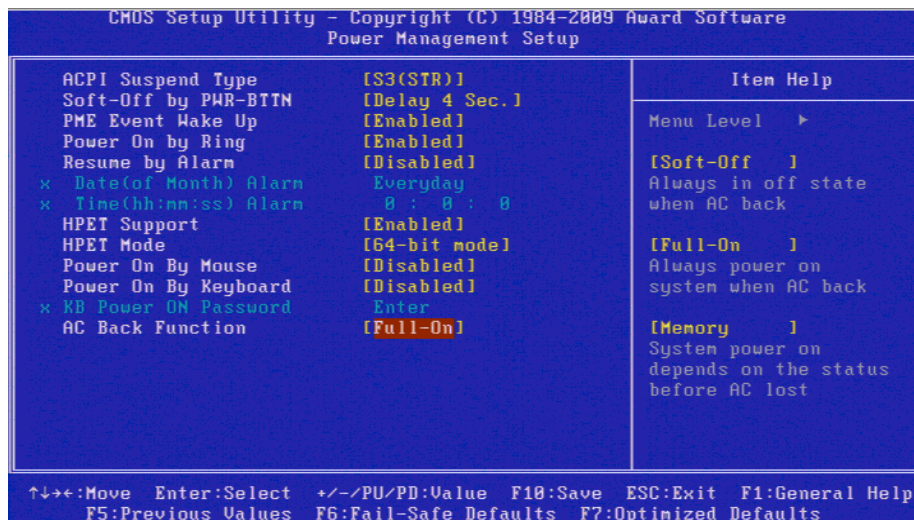
In the BIOS setup some settings should be configured before installing the Intra2net software. Since the BIOS setup differs from manufacturer to manufacturer, the following table lists the most frequently used names for the appropriate settings.

If installing the Intra2net software on a certified HPE server, information regarding the necessary BIOS settings can be found online here: <https://www.intra2net.com/en/support/server-systems.php>.



Date and Time	Should be correct (approx. +-10 min.), because the Intra2net system creates a time-dependent certificate during installation. As soon as an Internet connection is established, the time is set precisely via NTP.
"Restore on AC Power Loss" or "AC Back Function"	To "On" or "Full-On". This means that the Intra2net system will automatically start after a power failure or UPS shut-down. This option is usually found under "Power Management", "Boot Options" or a similarly named menu.
"CSM", "Legacy BIOS" or "UEFI"	The Intra2net system can be operated with classical BIOS as well as with UEFI. A change is still possible even after installation.
"UEFI Secure Boot"	deactivate
"Virtual Install Disk" or "Virtual Driver Disk"	Some server systems offer a virtual drive with this option, which contains drivers for the system or the RAID controller to simplify the installation of Windows or VMWare. Disable this option, as it can interfere with the hard drive detection of the Intra2net system.
"Wake on PCI device" or "Resume by PCI-E device"	Must be enabled in order to make scheduled shutdowns (see Section 16.7, „Scheduled Shutdown“).

Phoenix SecureCore(tm) Setup Utility		
Main		
Boot Features		Item Specific Help
Embedded VGA Control:	[Auto Detect]	Sets the mode of operation if an AC/Power Loss occurs.
Summary screen:	[Enabled]	
NumLock:	[Enabled]	Last State: Restores the previous power state before loss occurred, Off: keep the power off until the power button is pressed. On: It always keep the power on
POST F1 Prompt	[Delayed]	
Restore after AC Power Loss:	[On]	
Splash Screen:	[Enabled]	
POST Speed Up:	[Enabled]	
Extended Memory Testing	[Normal]	
Virtual Install Disk	[Disabled]	
Embedded NIC Port 1 PXE:	[Enabled]	
F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ↔ Select Menu Enter Select ► Sub-Menu F10 Save and Exit		



2.5. RAID

If using a RAID controller, first clarify whether it is a hardware RAID controller or a software RAID controller (also known as BIOS RAID or host RAID). Controllers with their own buffer memory (possibly also with buffer battery) are usually hardware RAID. Most low-cost SATA controllers or SATA controllers integrated on the motherboard are software RAID.

If using a hardware RAID controller, use its BIOS to create a partition that is suitable for the Intra2net system.

If using a software RAID controller, do not configure RAID functions in its BIOS or disable the controller's BIOS by setting the hard drive access to AHCI. The objective is to enable the Intra2net system to communicate with the individual drives separately. This configuration is commonly referred to as JBOD. After installing the Intra2net system on the first hard drive, it is possible to create a RAID array with the second drive in the web interface under System > Hardware > RAID.

2.6. Installation of the operating system

The Intra2net software is based on a full Linux-based operating system. This cannot be installed in parallel with other operating systems on the same device. Should additional software be required on the same hardware, use a virtualization solution.

2.6.1. Installation from a USB flash drive

To create a bootable USB flash drive, you need a USB flash drive with at least 8 GB capacity. The ZIP file that comes with the Intra2net system contains the program rufus.exe to create bootable USB flash drives on Windows.

On a PC with Windows unpack the ZIP archive and start rufus.exe. Use Rufus from the ZIP archive and no other version because it contains modifications necessary for installing. Select the ISO file and the USB flash drive. All other default settings are correct already. During the write process all data on the USB stick will be deleted.

On Linux, you can use the Fedora Media Writer program to create a bootable USB stick. This is either available in your distribution's package manager or can be obtained as a flatpak from Flathub [<https://flathub.org>]. Choose "Custom Image" and then select the ISO file. The write process will erase all data on the stick.

Start the computer on which you would like to install the Intra2net system from the prepared USB stick.

2.6.2. Installation from DVD

Launch the computer using the Intra2net installation DVD. It is possible to use either an internal or USB connected DVD drive.

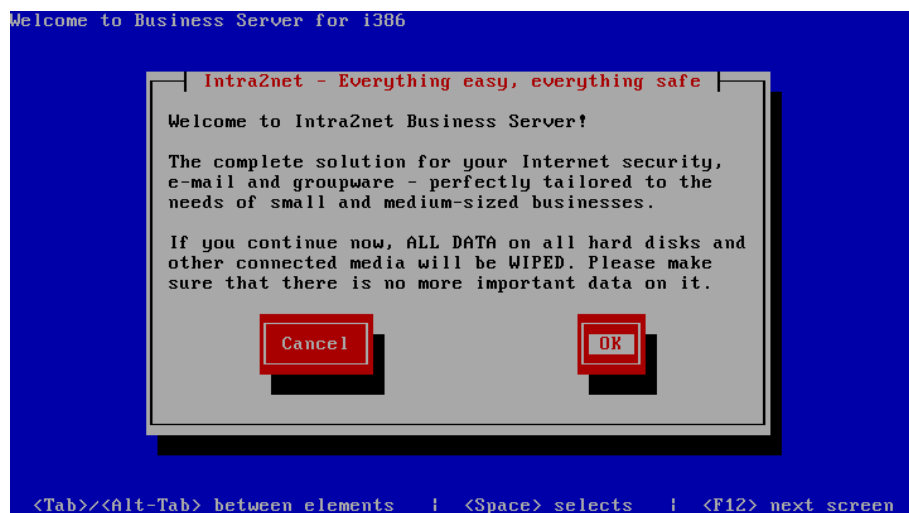
2.6.3. Start of the installation

After the successful start of the installation program you will be prompted to start the installation of the Intra2net system.



Caution

When starting the installation, all data on the attached hard drives will be overwritten. For this reason, please ensure that all hard drives can be safely wiped before installation.



If the installation is completed successfully, there will be a prompt to restart the computer. Remove the DVD or USB flash drive to boot from the hard drive. This will start in the installation console, described in 6. Chapter, „The Console“.

2.6.4. Serial console

If the hardware does not have a normal monitor port, but only a serial console, use a null modem cable or adapter and connect with the parameters 115200 baud, 8 bit, no parity, 1 stop bit. The serial console must be accessed via the first serial port of the system (COM1 or ttyS0). This may have to be adjusted in the BIOS.

Boot the system from the installation media. For classic BIOS, type **serial** in the boot manager and press Enter. For UEFI, select the option marked "serial console" from the boot menu.

2.6.5. Solving Compatibility Problems

If the installation program displays an error message that there is not enough space available on the hard disk, then either a smaller hard disk than the minimum is installed (see Section 2.1, „Hardware Selection“), the actual hard disk was confused with a USB

drive, memory card or a virtual hard disk provided by the BIOS with drivers, or the hard disk was not even found.

Therefore, remove all not needed USB drives and memory cards, which may also be installed inside the case on some systems. Check the BIOS configuration and disable virtual driver drives, see Section 2.4, „BIOS“. Check the configuration of the RAID controller or BIOS RAID, see Section 2.5, „RAID“.

Another reason may be that the hard disk was previously used in a RAID array and now still contains control information for the previous RAID array or inappropriate partitioning data. In this case, perform a format of the hard disk or use a previously unused hard disk.

If the installation program does not start or stops during installation, there is likely a compatibility problem between the hardware and Intra2net software.

First, obtain and install a new BIOS update from the manufacturer of your computer or motherboard. Also check <https://www.intra2net.com>, to ensure that the latest version of the Intra2net installation DVD is being used.

3. Chapter - Installing as a Virtual Machine

3.1. Comparison to Real Hardware

Compared to installing on real hardware, virtualization systems offer a number of advantages such as hardware consolidation, energy conservation or better reliability due to migration possibilities. At the same time, however, there are also the disadvantages described below.

3.1.1. Inconsistent performance speed

The operating system can no longer decide which processes are to be performed exactly when, because the virtualization application can stop or delay the execution of the entire virtualized system.

3.1.2. Lower I/O Performance

The operating system can no longer access the network card or storage hardware directly, but must access a virtualization software component. In order to do this, it is necessary to switch between guest and host multiple times. This not only reduces the maximum possible output, but also increases latency.

If the hard drives are not installed locally on the virtualization server, but are connected via a SAN, for example, the transfer latency via SAN is added. However, very different latency times can be observed on different SAN systems. Systems based on iSCSI tend to have high latency. Fibre Channel or FCoE systems (*Fibre Channel over Ethernet*) tend to have better latency. Additional layers such as storage virtualization can add further latency.

Most tasks of an Intra2net system are typically limited by the latency of hard drive access and not by drive output or lack of CPU performance. This point can therefore significantly impair the performance of an Intra2net system.

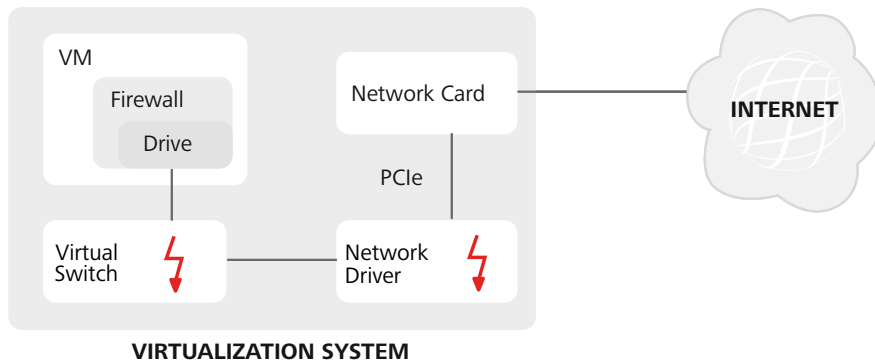
We recommend compensating for this by using faster hard drives (15,000 RPM) or solid state drives.

Furthermore, we do not recommend configuring the virtual disk for the Intra2net system as a dynamically growing / allocated drive, but to assign and allocate it completely from the beginning. If the disk only grows on demand, it costs performance for write accesses. Also, additional administrative information is required, which must be retrieved before access and then possibly adjusted. With classic hard drives, additional repositioning of the read/write heads is required due to the uneven distribution of the blocks.

3.1.3. Contact with Unfiltered Network Packets

If the Intra2net system is used as a router and firewall and thus establishes a connection to the Internet, it comes into direct contact with network packets from the Internet. The Intra2net system is designed to handle non-standard compliant or even malicious packets correctly. Any detected gaps in the drivers or functions are promptly closed through regular updates.

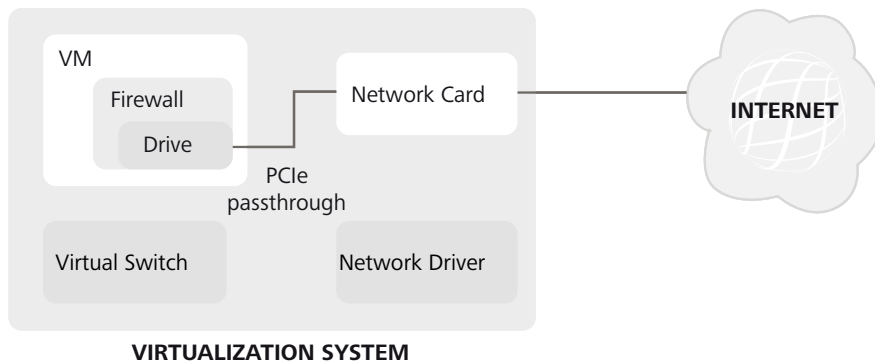
If the Intra2net system is operated as a virtual machine and its network cards are managed via the regular network functions of a virtualization system, the virtualization system is exposed to these packets unfiltered. This usually applies to the network card drivers and the virtual switch.



Virtualization systems are typically not designed to be firewalls. For this reason, driver updates for network cards and virtual switches are not considered to be critical and are therefore distributed and installed less frequently. This ultimately increases the risk of interference or attacks.

Therefore, we strongly advise against connecting network cards directly to the Internet via regular network functions of the virtualization system (typically virtual switches).

Instead, we recommend handing over the respective network cards as complete PCI devices to the virtual machine. The Intra2net system controls the hardware directly via PCI access and the virtualization solution does not come into contact with these network packets in any case.



Caution

Note that this function is not offered by all virtualization systems and is only available with support of the hardware (Intel VT-d or AMD-Vi in processor and chipset as well as appropriate description tables in the BIOS). Therefore, check compatibility from the planning stage.

In addition, when passing through complete PCI devices, live migration of the VM is usually no longer possible. Therefore, a VM must be shut down before migrating to new hardware.

Alternatively, it is possible to use an additional hardware firewall, or install the Intra2net system not as a virtual machine, but on dedicated hardware.

4. Chapter - Installation on VMware vSphere Hypervisor™ 4 (ESXi)

For the base virtualization platform VMware vSphere Hypervisor™ (formerly VMware ESXi™) a permanent, free license is offered at this URL: <http://www.vmware.com/go/get-free-esxi>.

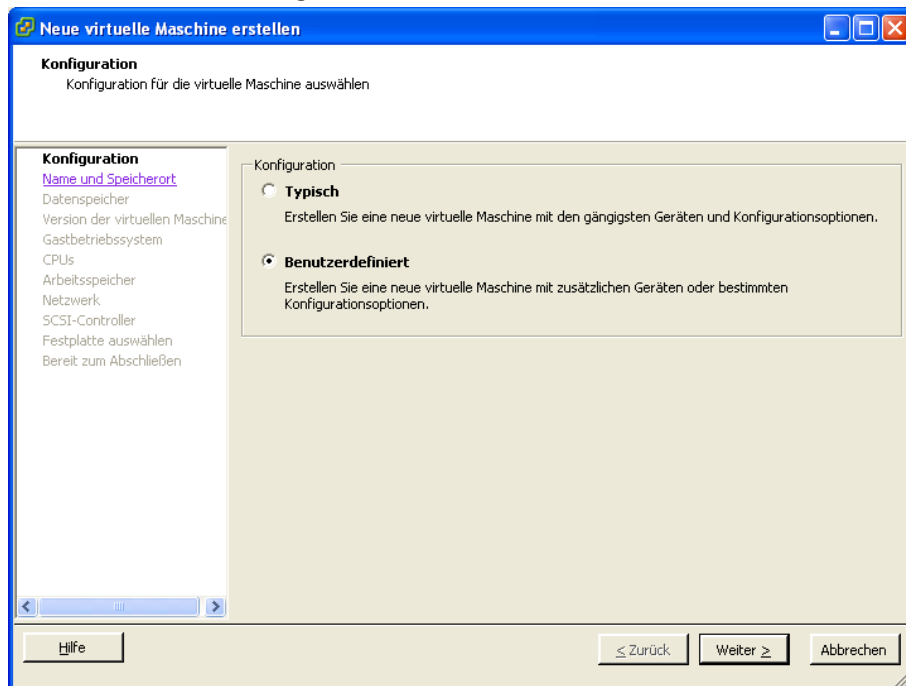
For more advanced management and monitoring functions, they require paid licenses. An overview of the different products can be found at Compare vSphere Editions [<http://www.vmware.com/products/vsphere/compare.html>].

The Intra2net system comes with all drivers and programs required for reliable operation on VMware vSphere Hypervisor™ 4. These are the paravirtualized network driver (VMXNET 3), the paravirtualized SCSI driver (pvscsi) and the open-vm-tools. No additional installation of VMware Tools or other drivers or programs is required.

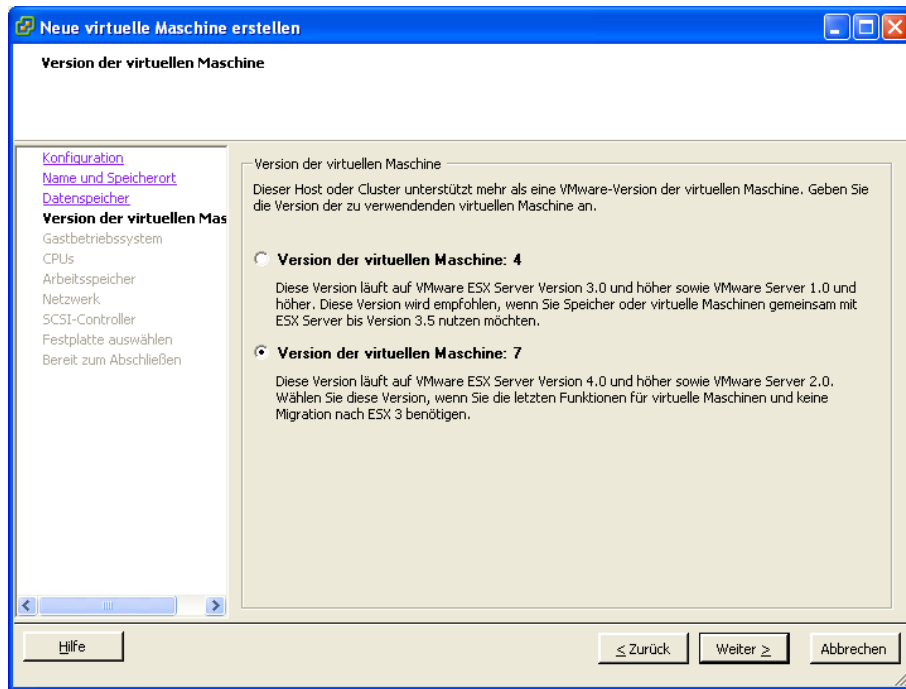
4.1. Virtual Machine Configuration

To install a virtual machine, follow these steps:

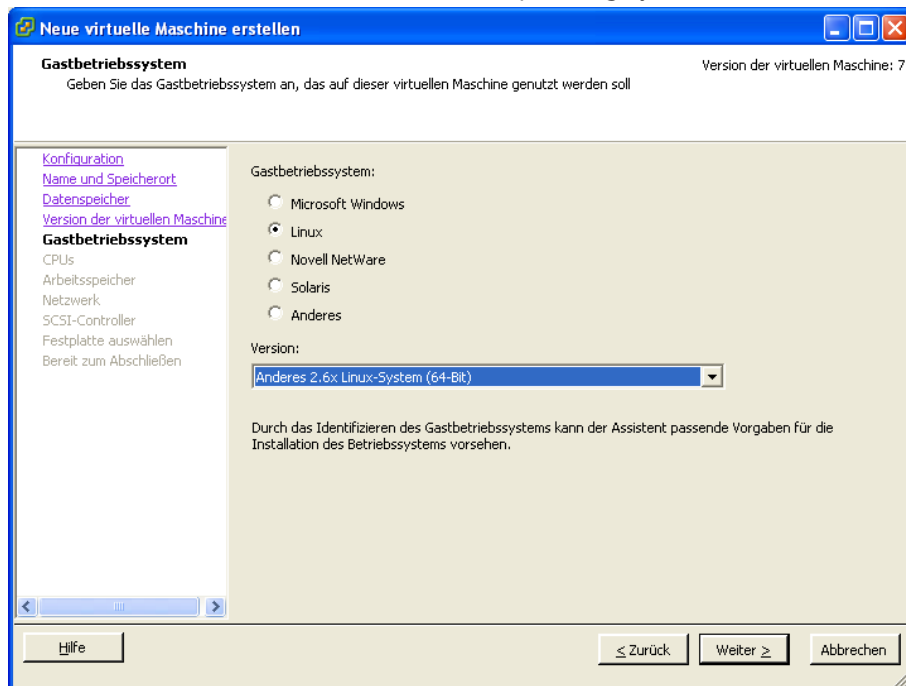
1. Start the vSphere Client, connect to the vSphere server and create a new VM.
2. Select the custom configuration.



3. Name the VM and assign a suitable amount of storage capacity.
4. Choose a virtual machine version 7

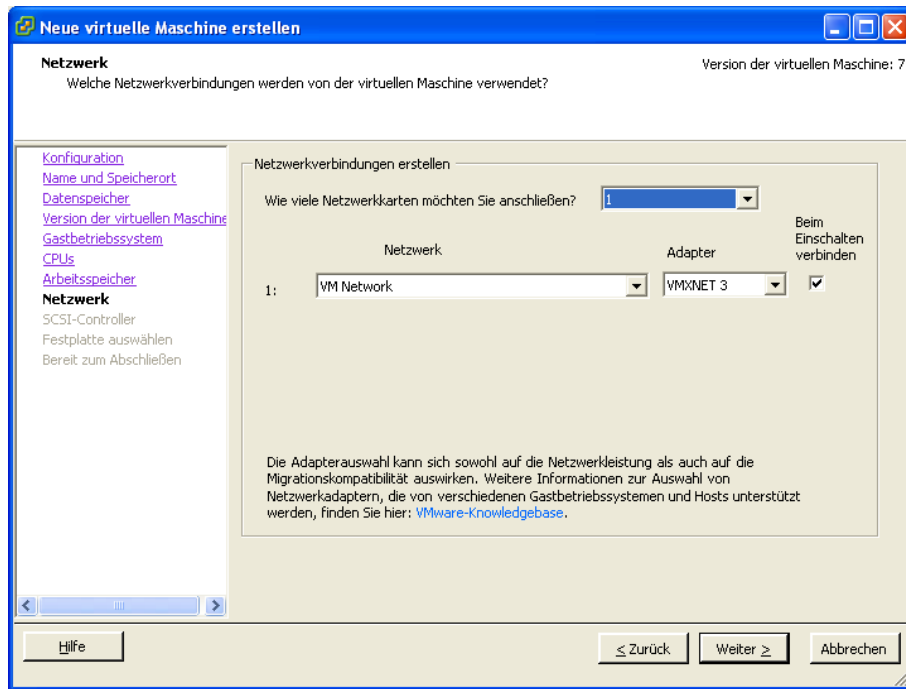


5. Select "Other 2.6x Linux (64-bit)" as the operating system.

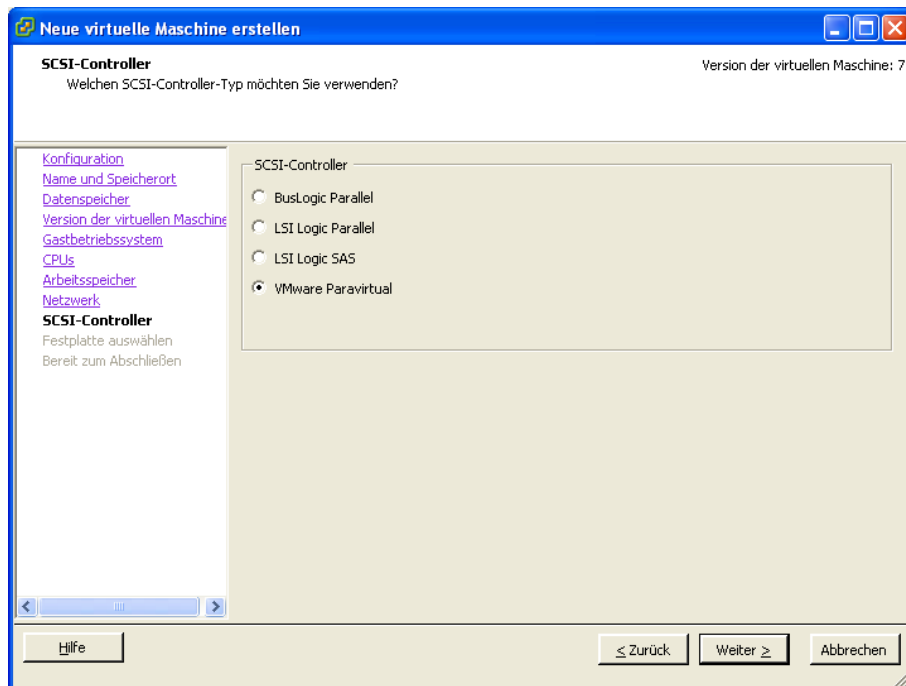


6. Share one or more CPUs for the Intra2net system. The system automatically detects the number of available CPUs at startup and uses them.
7. Allocate enough RAM for the Intra2net system. We recommend at least 2 GB for up to 50 users, and correspondingly more as users increase.
8. Connect "VMXNET 3" type network cards. The number depends on the layout of the local network and the purpose of the Intra2net system.

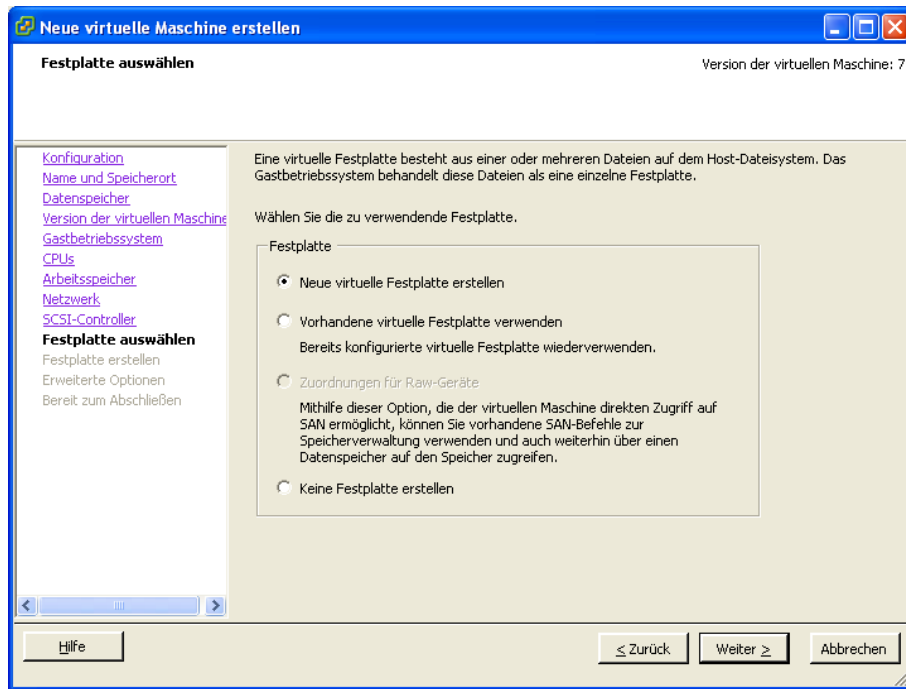
It is strongly discouraged to use network cards directly connected to the Internet in this way. Please refer to Section 4.2, „Virtual Machine with Direct Internet Access“.



9. Select a "VMware Paravirtual" SCSI controller.



10. Create a new virtual hard disk.

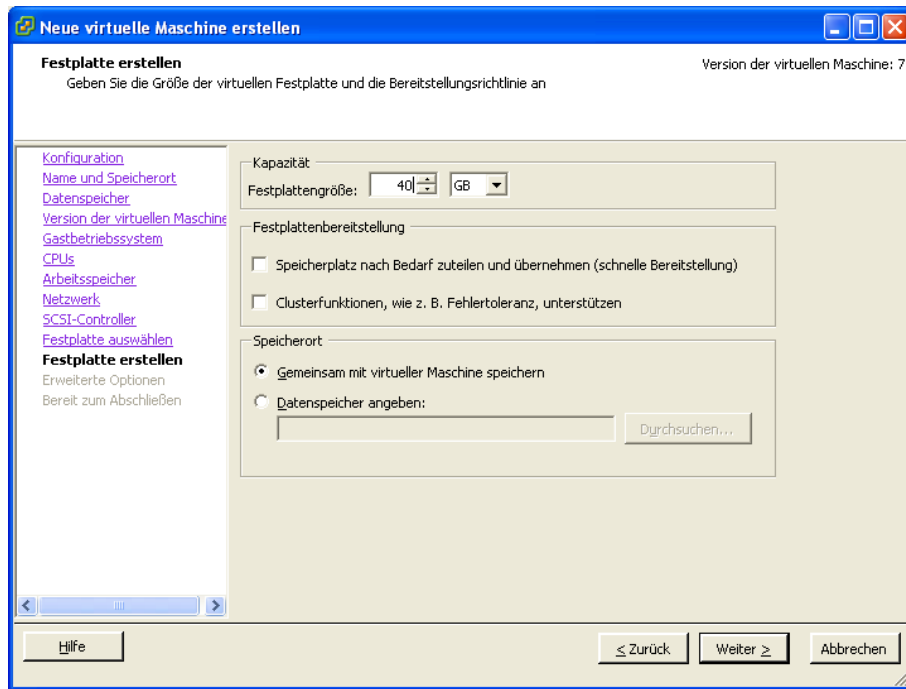


11. Assign a hard disk of at least 40 GB to the Intra2net system. If the Intra2net system is only used for scanning emails and as an HTTP proxy server, 40 GB is sufficient. Only if extensive statistical data is to be stored for many users over a long period of time should more space be required.

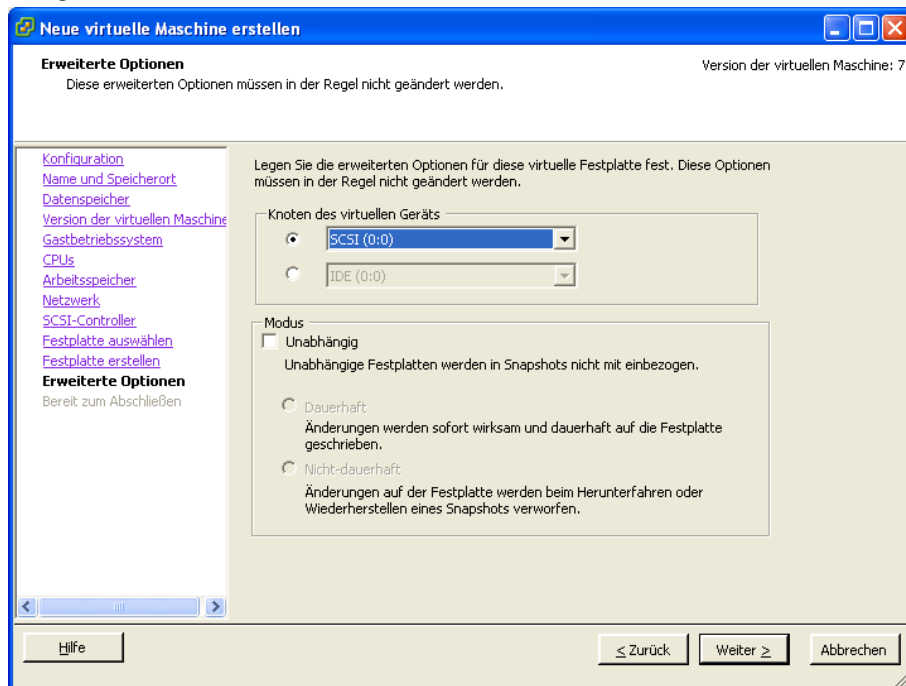
If email or groupware data is permanently stored on the Intra2net system, more hard drive storage is required. The general formula is: (full email volume of all users + statistics) x (number of backup records stored on the system + 2) + 20 GB. The number of backup records stored on the system is at least 1, we recommend 2.

Always allow for some spare capacity, as enlarging the hard disk during operation can only be done by the Intra2net support.

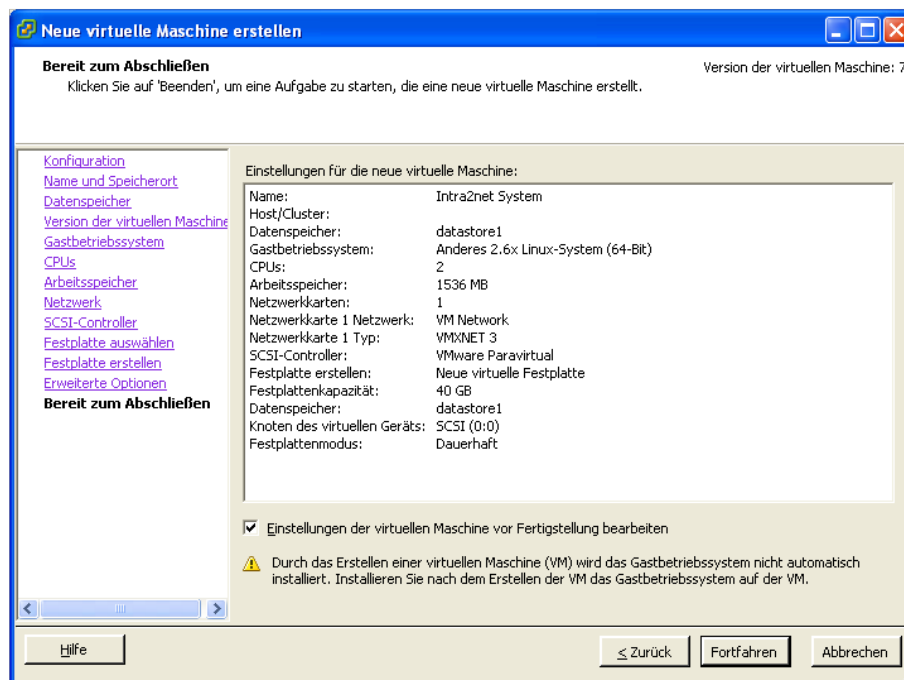
Assign the entire hard disk capacity to the Intra2net system immediately, as this usually leads to faster access times.



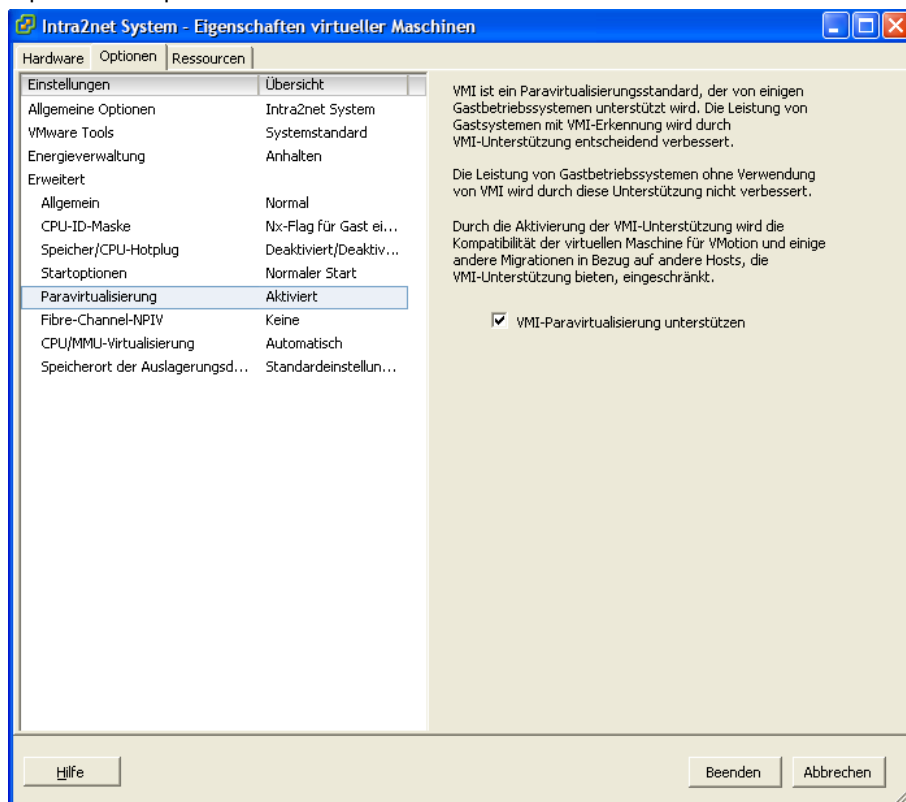
12. Assign the hard disk to node SCSI (0:0).



13. Edit the settings before finishing.



14. Open the "Options" menu and activate "VMI-Paravirtualization".



4.2. Virtual Machine with Direct Internet Access

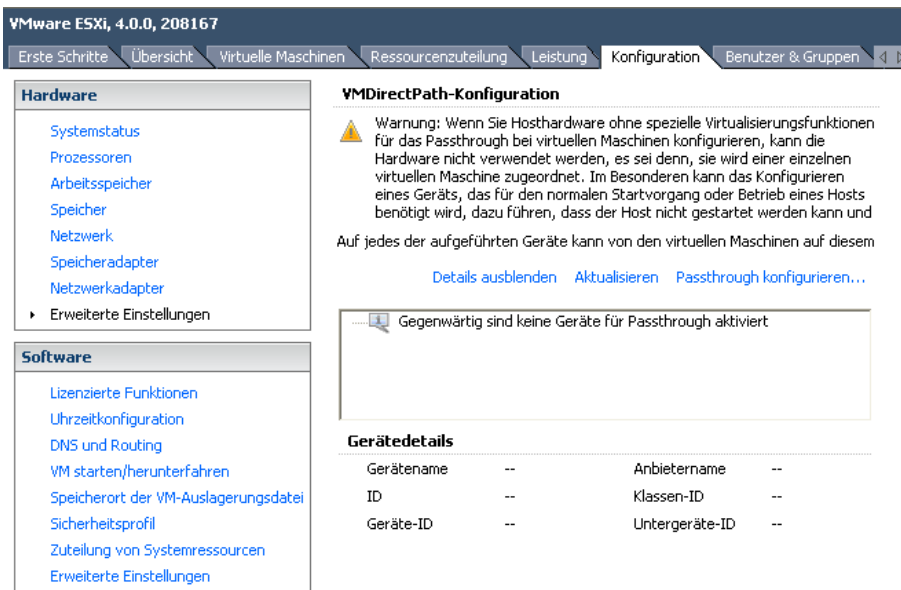
As described in Section 3.1.3, „Contact with Unfiltered Network Packets“, we recommend handing over network cards that are directly connected to the Internet to the VM as complete PCI devices.

This functionality is called VMDirectPath and requires processor, motherboard and BIOS support. Intel calls this VT-d, AMD is called AMD-Vi or IOMMU. These functions are usually implemented only on server systems; computers designed for desktop use often lack full support from all components. See VMware and your hardware vendor for more information.

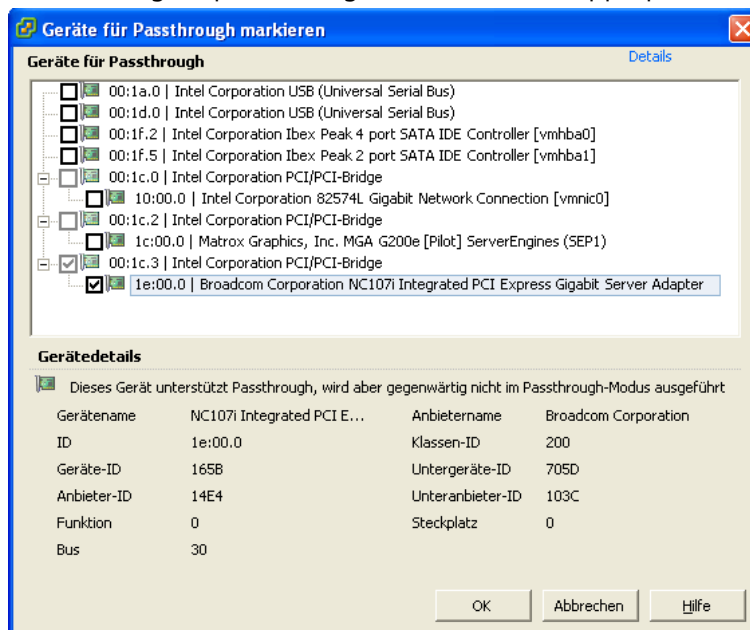
4.2.1. Server Preparation

Before a network card can be transferred directly to a VM, it must be released in the VMware server:

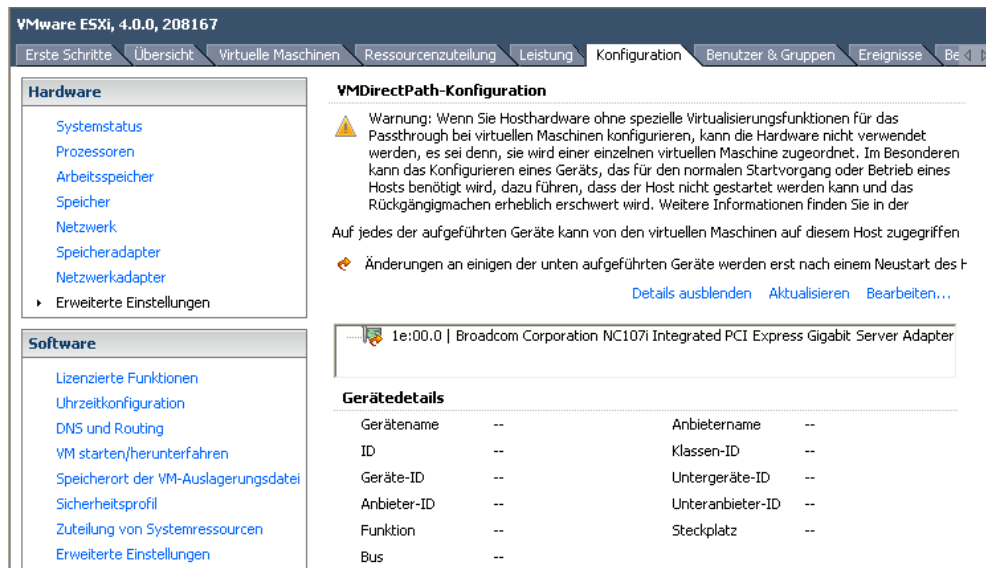
1. Start the vSphere Client and connect to the ESXi server. Select the server itself on the left and open the "Configuration" menu.



2. Click "Configure pass-through" and select the appropriate network card and bridge.



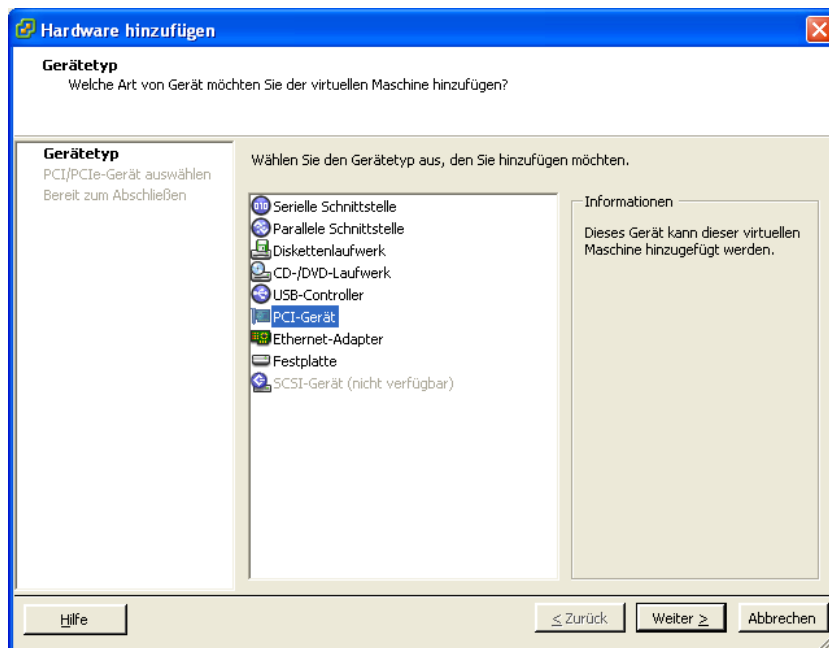
3. The network card is available after restarting the VMware server for VMDirectPath.



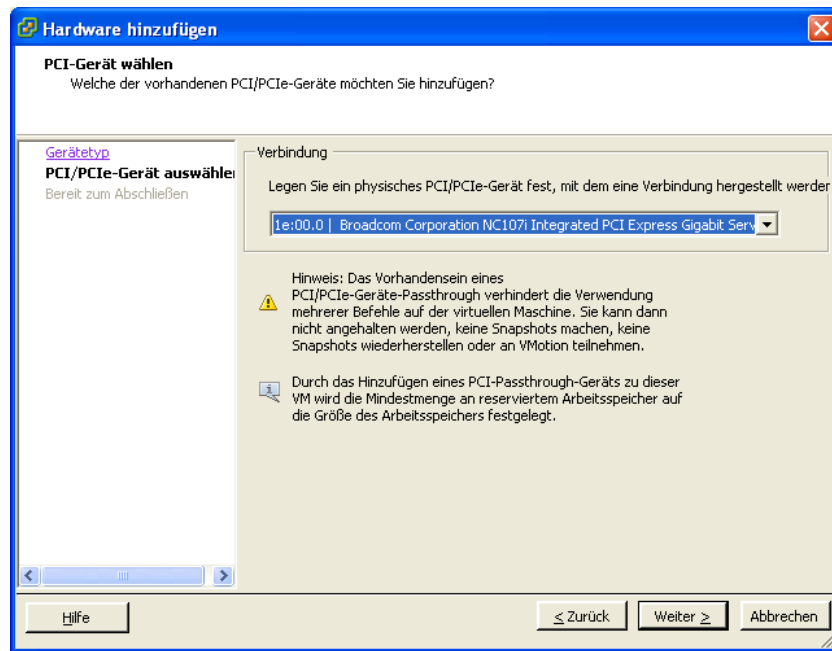
4.2.2. Connecting the Network Card to the VM

The network card can now be installed as follows:

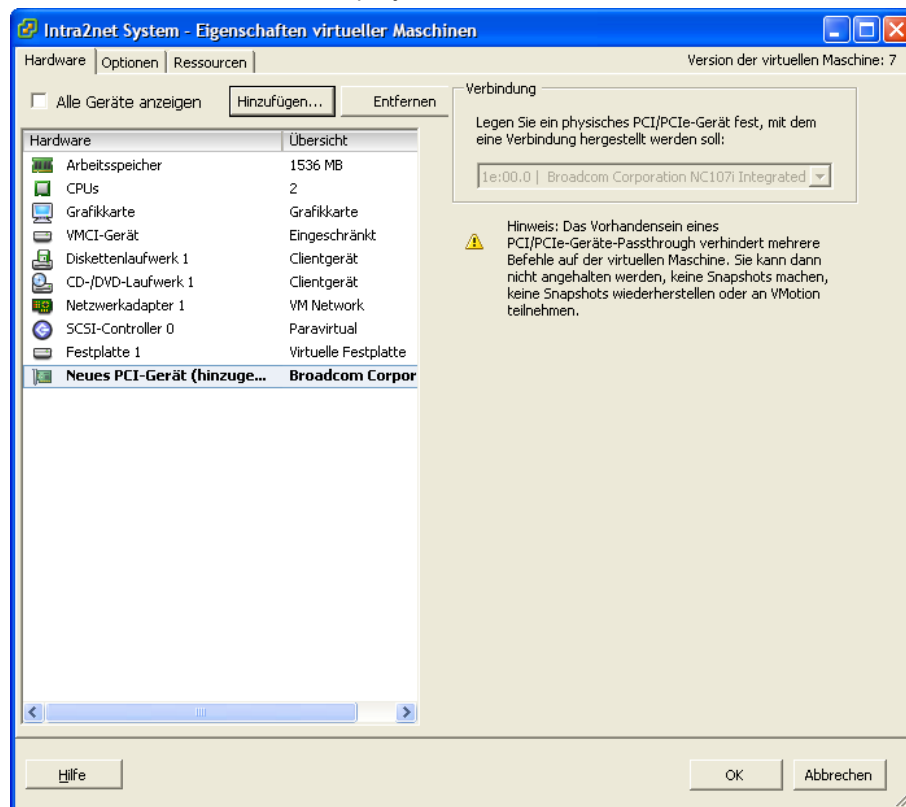
1. Open the configuration of the VM and click "Hardware" on "Add".
2. Add a PCI device.



3. Select the previously enabled network card and close the add dialogue.



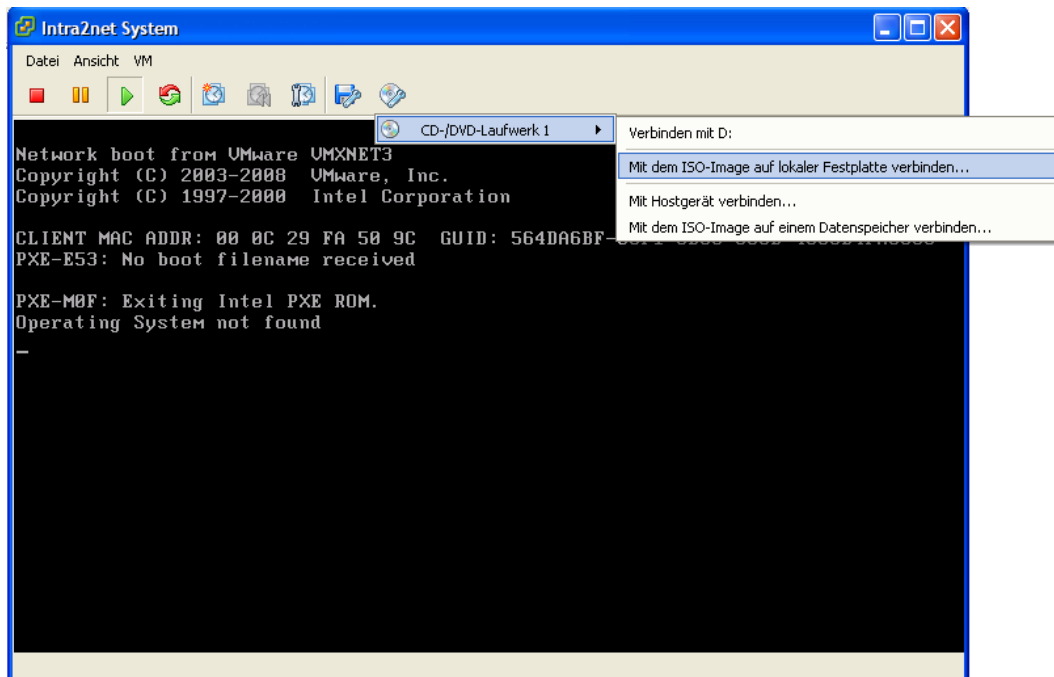
- The network card is now displayed as an additional device.



4.3. Installing the Intra2net System

- Start the virtual machine and open the console.
- The virtual machine tries to boot from the network, but this fails with operating system not found.

3. Click on the CD icon in the console toolbar and use it to add the ISO file of the Intra2net installation CD or a local CD drive to the virtual machine's CD drive.



4. Wait approx. 5 seconds until the CD drive is fully connected.
5. Click in the console to activate it and press the Escape button. The VM now boots from the Intra2net installation CD.

The rest of the installation process is as described in Section 2.6.2, „Installation from DVD“.

5. Chapter - Installation of Microsoft Hyper-V on Windows Server 2012 R2

The Hyper-V virtualization system is part of Microsoft's Windows Server 2012 R2 and can be activated as a part of it.

Additionally, the always-free Microsoft Hyper-V Server 2012 R2 is also available. However, this can only be operated via command line and Powershell, which makes configuration and maintenance much more difficult. Therefore, we can only recommend it to experienced Windows administrators with extensive knowledge of command line operation and we do not offer support for it. For this reason, we recommend using Windows Server 2012 R2 for Hyper-V virtualization.

The Intra2net system contains all of the drivers and software necessary for reliable operation of Microsoft Hyper-V on Windows Server 2012 R2. Additional installation of integration services or other drivers or software is not necessary or possible.



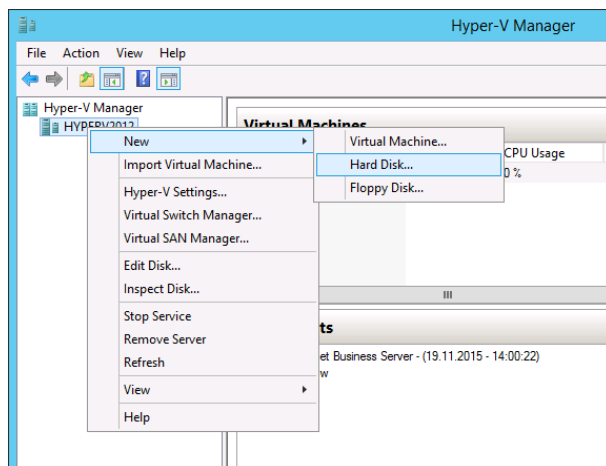
Caution

Hyper-V does not offer the ability to pass through PCI devices such as network cards directly to a VM. We therefore recommend using a Hyper-V virtualized Intra2net system in combination with an additional hardware firewall. Further information can be found in Section 3.1.3, „Contact with Unfiltered Network Packets“.

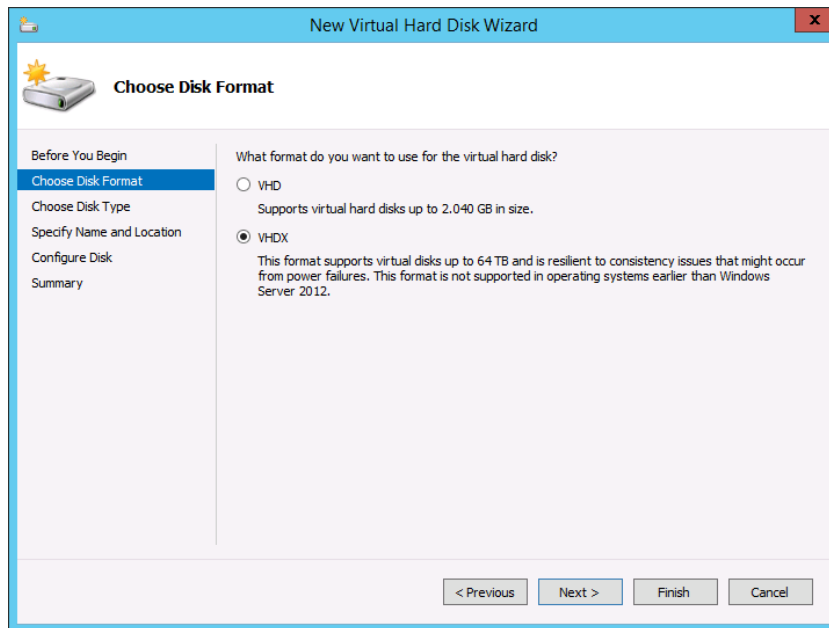
5.1. Virtual Machine Configuration

To install a virtual machine, follow these steps:

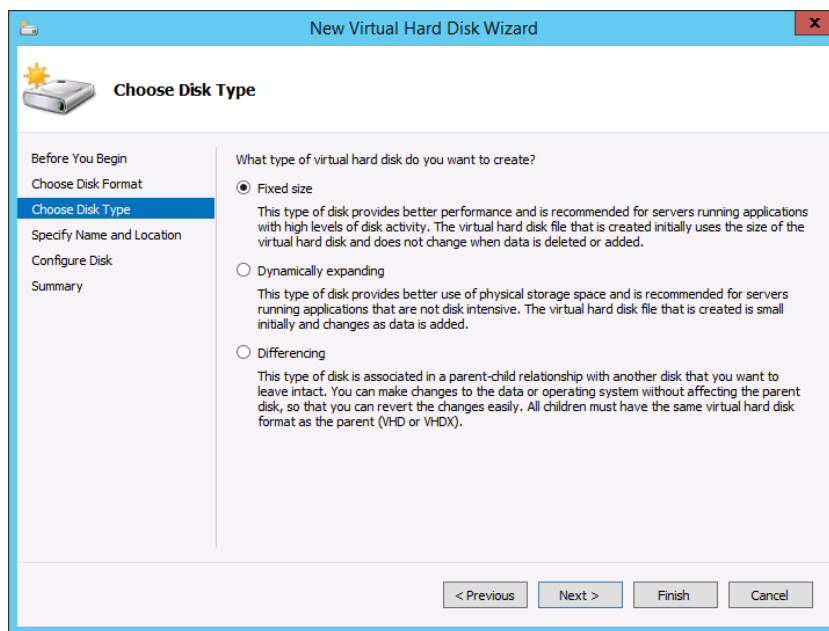
1. Open the Hyper-V Manager and right-click the desired Hyper-V instance. Select "New > Hard Disk...".



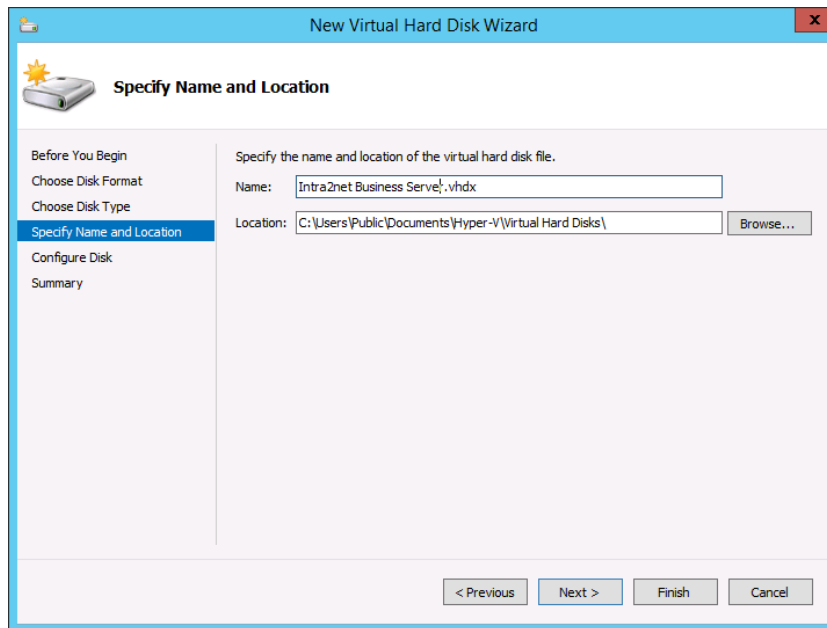
2. Select the "VHDX" format.



3. Select a virtual hard disk with "Fixed size".



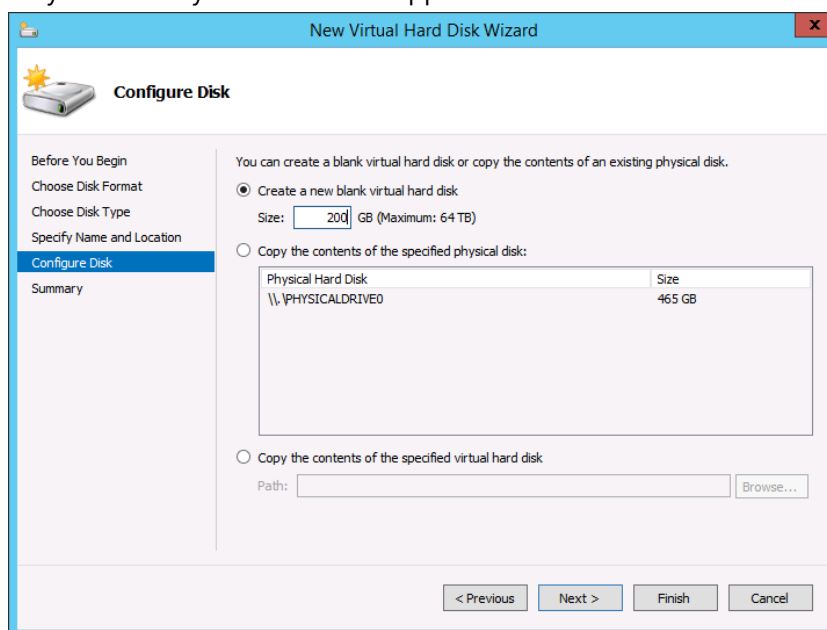
4. Give the virtual hard disk a name that corresponds to the future VM.



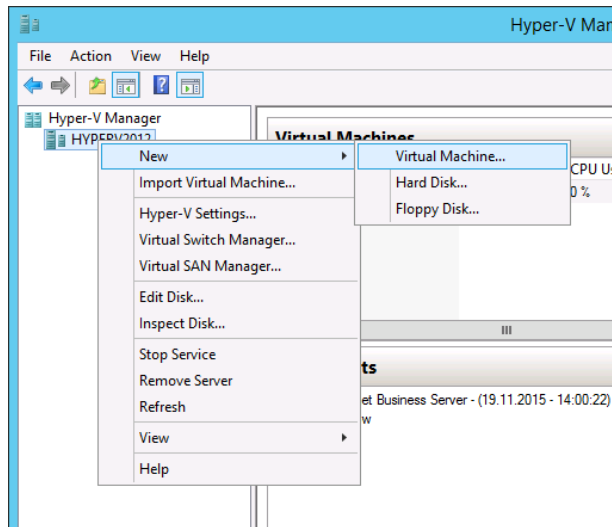
5. Assign a hard drive of at least 40 GB to the Intra2net system. If the system is only used for scanning emails and as an HTTP proxy server, these 40 GB will typically be sufficient. Only if extensive statistical data is to be stored for a long time and for many users, more space will be necessary.

If email or groupware data is permanently stored on the Intra2net system, more hard drive storage is required. The general formula is: (full email volume of all users + statistics) x (number of backup records stored on the system + 2) + 20 GB. The number of backup records stored on the system is at least 1, we recommend 2.

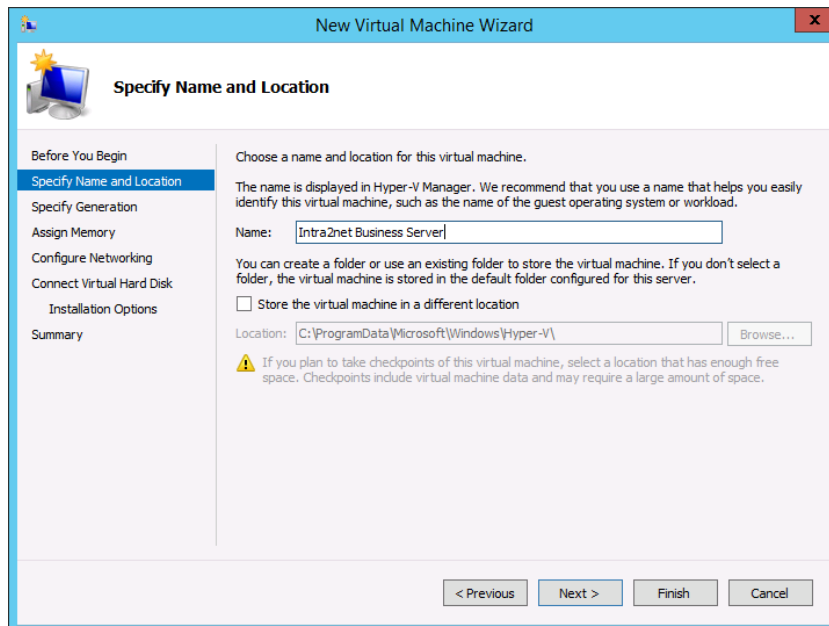
Always allow for some spare capacity, as enlarging the hard disk during operation can only be done by the Intra2net support.



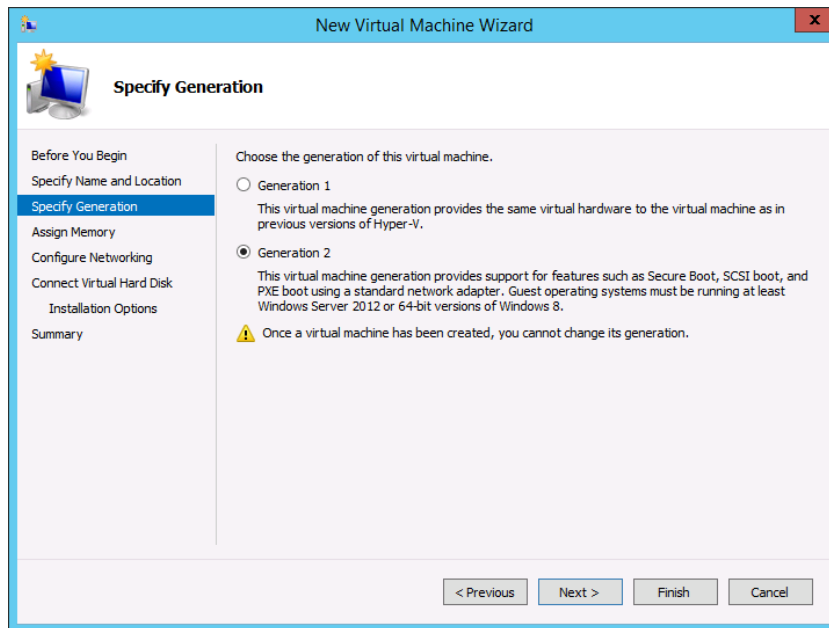
6. Complete the virtual hard disk creation.
7. Right-click the desired Hyper-V instance and select "New > Virtual Machine...".



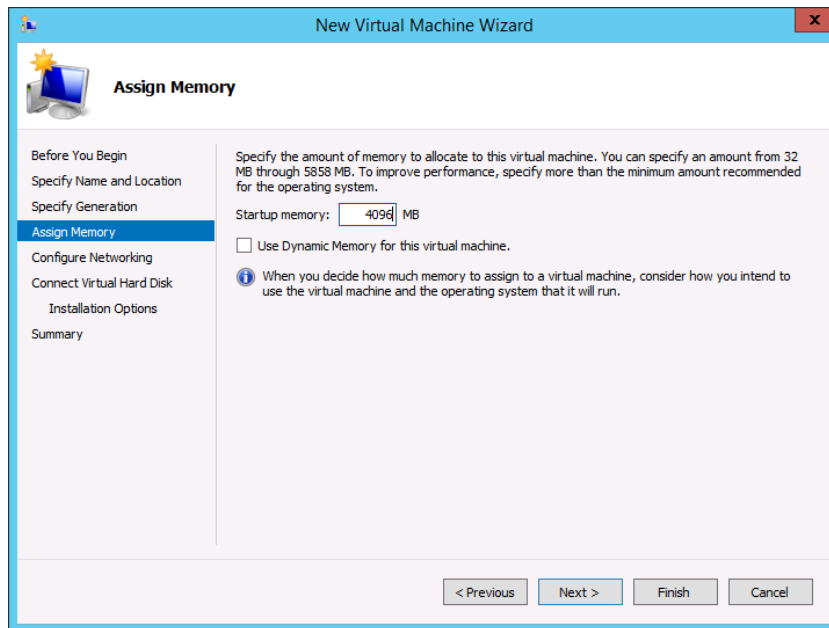
8. Enter the name for the VM.



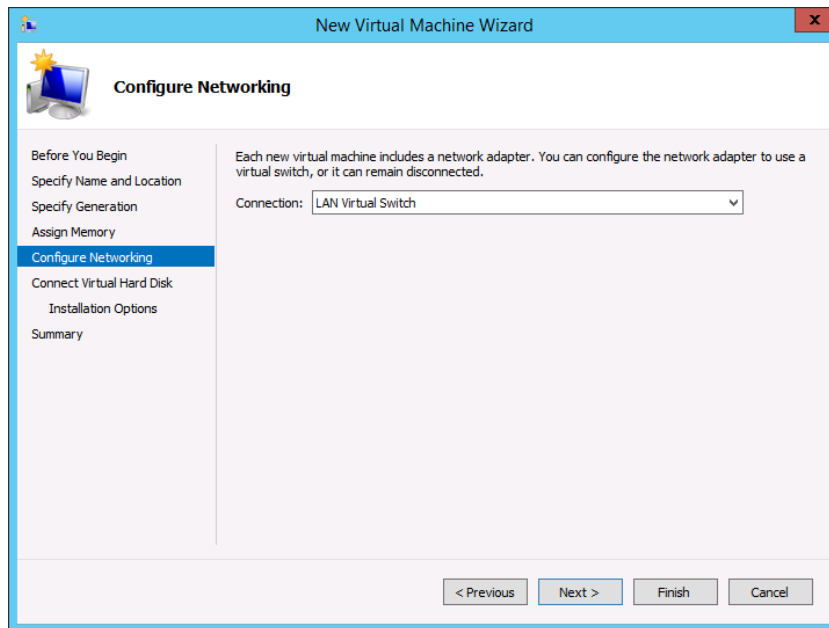
9. Select Generation 2



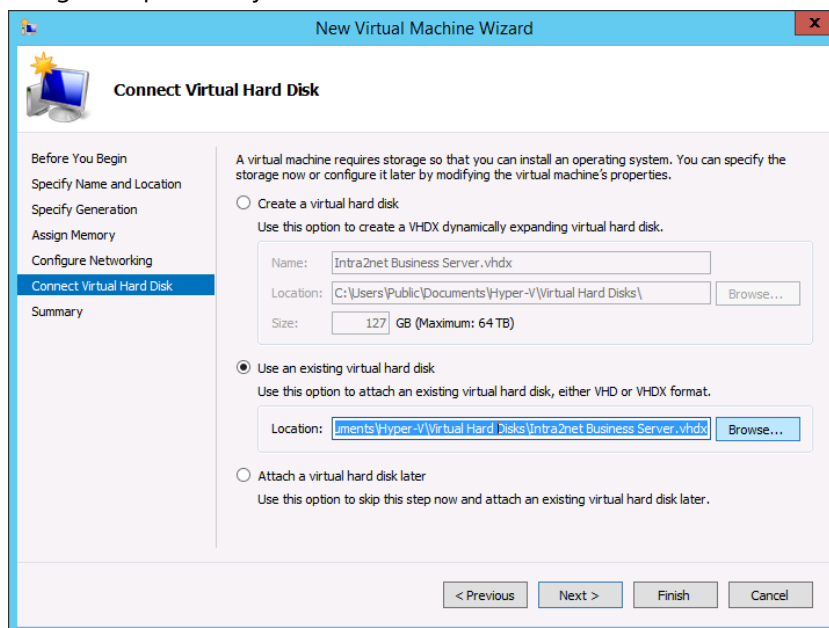
10. Allocate sufficient memory to the VM. Use at least 2 GB. Disable "Dynamic Memory".



11. Connect the VM to the virtual Switch that is connected to the local network.



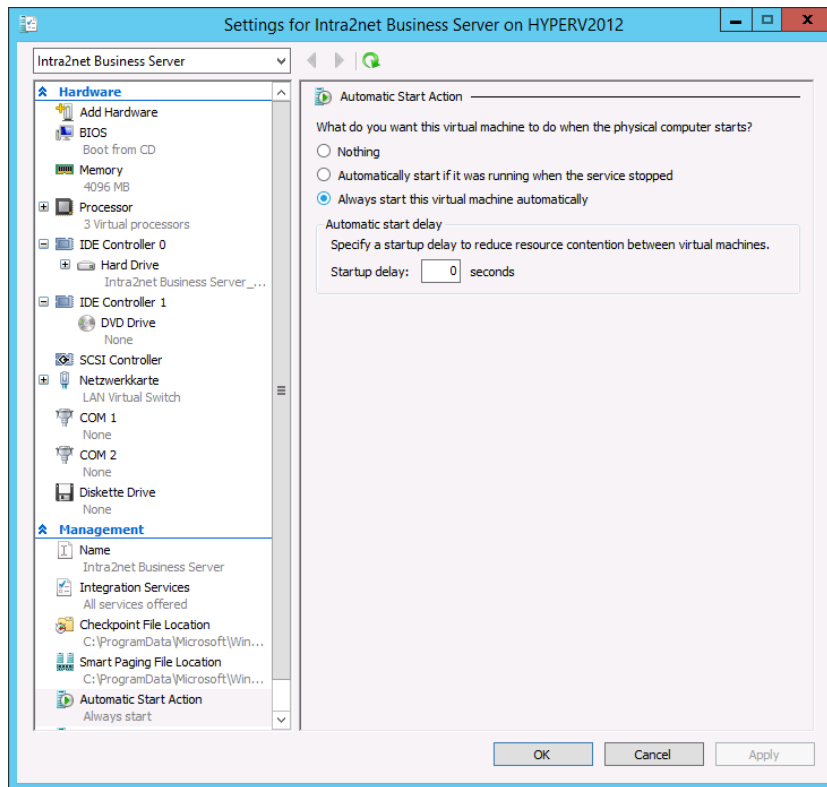
12. Assign the previously created virtual hard disk.



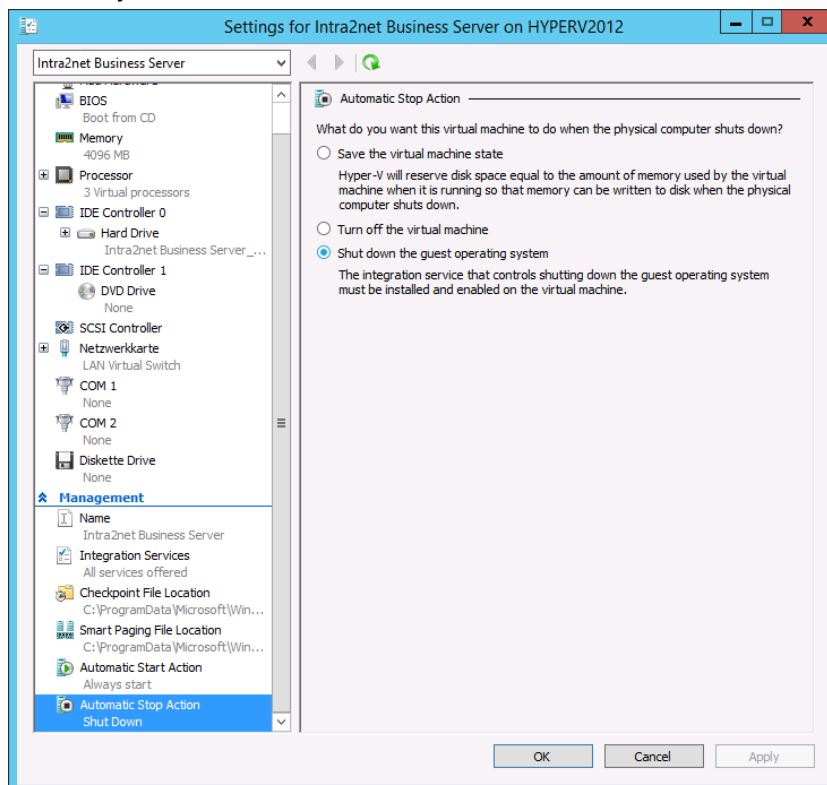
13. Complete the VM creation.

14. Right-click the new VM and open "Settings".

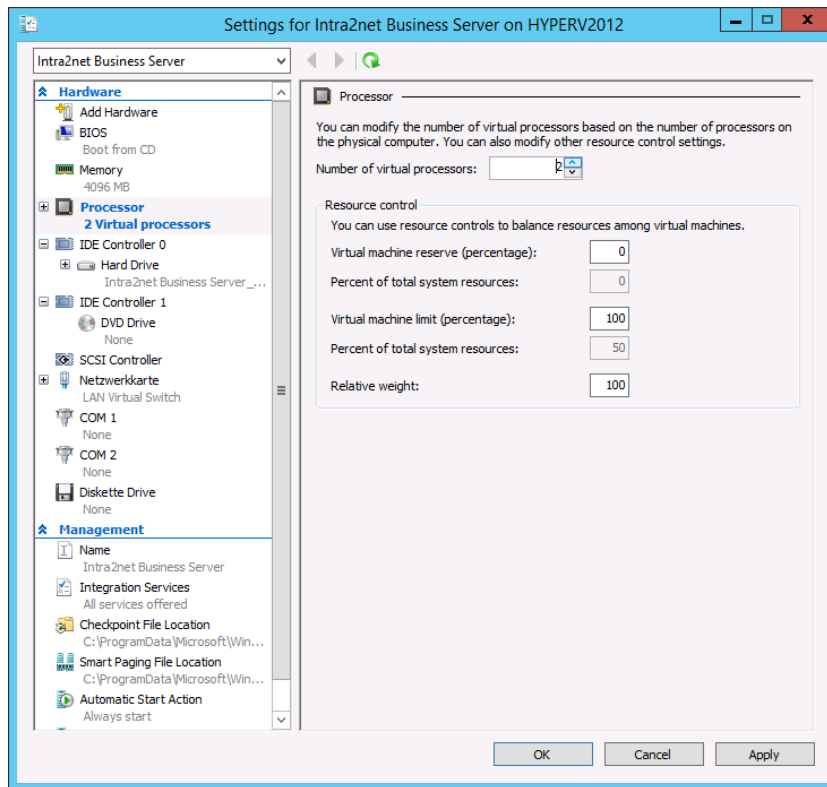
15. Always start the VM automatically so that the VM is always available.



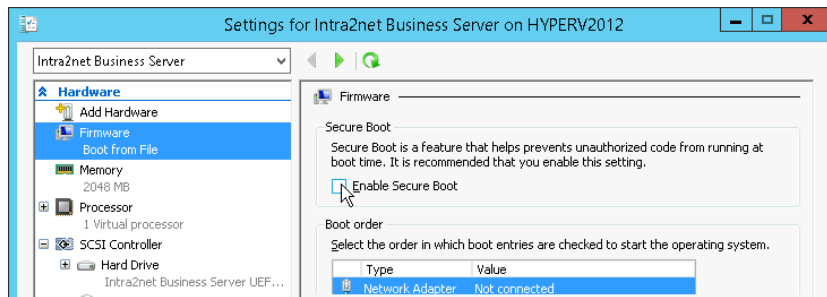
16. Always shut down the VM when the Hyper-V server shuts down. This avoids problems caused by time differences.



17. Increase the number of processor cores allocated, depending on available resources. This setting can be adjusted at a later stage if required.

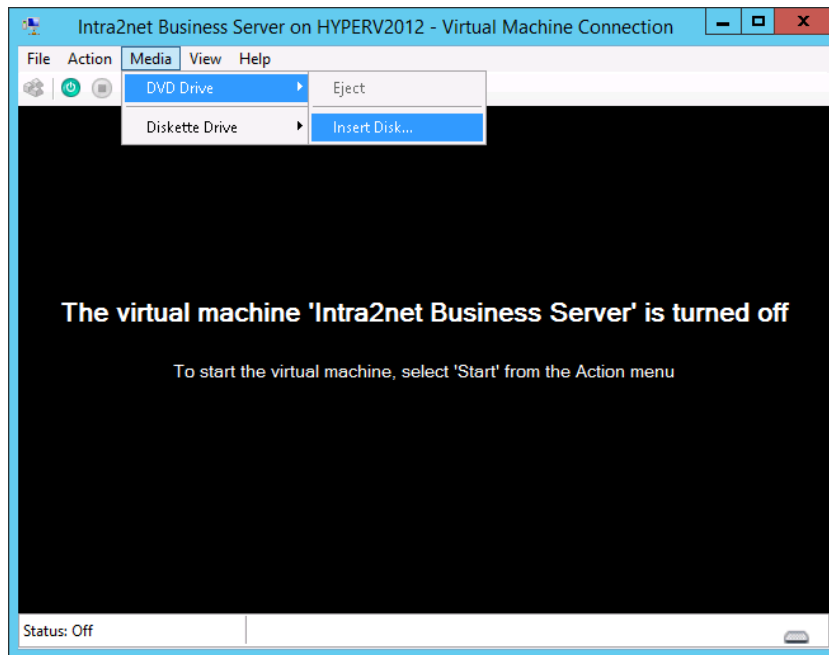


18 Under "Firmware", disable the option "Enable Secure Boot".



5.2. Installation of the Intra2net System

1. Open the new VM by double-clicking it.
2. Open the "Media > DVD Drive > Insert Disk..." menu. Select the ISO file with the Intra2net installation CD. You can download it at <https://www.intra2net.com/>.



3. Start the virtual machine using the green start button.

The rest of the installation process is as described in Section 2.6.2, „Installation from DVD“.

6. Chapter - The Console

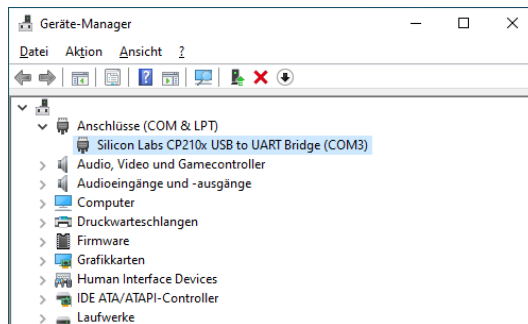
After the initial installation, the Intra2net system starts immediately on the console menu.

This can also be accessed on an already installed Intra2net system by connecting a monitor and keyboard and logging in with the username and password of a member of the administrator group (**admin** by default).

6.1. Intra2net Appliance Micro

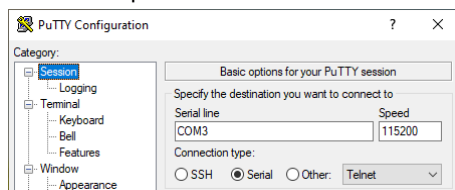
The Appliance Micro does not have a monitor output for the console, it uses a serial console instead. Connect the supplied null modem cable with USB converter to another PC for access. The D-sub/DE-9 connector is connected to the Appliance Micro, USB to the other PC from which the console is to be accessed.

The cable uses a Silabs CP2104 converter. Under Windows you have to download and install the "CP210x Universal Windows Driver" from <https://www.silabs.com>. Then open the Device Manager from the Windows Control Panel and read the COM port number.



A terminal program is required for use. Under Windows PuTTY and TeraTerm are recommended, under Linux picocom.

Select a serial connection in the terminal program, the appropriate port number and set the following parameters: 115200 baud, 8 bit, No Parity, 1 stop bit. With TeraTerm this is done via the menu "Setup > Serial Port", with PuTTY you set the "Connection type" to "Serial", enter the COM port number and under "Speed" the baud rate. Translated with www.DeepL.com/Translator (free version)



6.2. Network Cards

The "Network cards Settings" are used to configure the drivers for the network cards. The cards are automatically recognized and the detected configuration is displayed.

The current connection status is also displayed (x stands for connected, o for disconnected). This is useful for assigning the displayed names of the network cards (`eth0`, `eth1`, etc.) to the correct ports on the device. We recommend labeling the ports with adhesive tape at this point.

Using this menu, an IP address can be assigned to the network cards. During installation, select the IP address that matches the existing local network. Make sure that this IP address is not already used by another device.

The IPs on the local network should originate from one of the designated private network areas. These are:

- 10.0.0.0 / 255.0.0.0 (to 10.255.255.255)
- 172.16.0.0 / 255.240.0.0 (to 172.31.255.255)
- 192.168.0.0 / 255.255.0.0 (to 192.168.255.255)

Use "Intranet (LAN with NAT)" for the local network and "DSL/Router" for the Internet connection. No IPs can be stored for connecting to the Internet, as it takes place at a later point, during the provider configuration.

For more information on the different configuration types for network cards, refer to Section 8.1, „IPs and Networks“.

This menu is opened automatically during initial installation. If something has been changed on the network cards after installation, the Intra2net system must be adjusted to the new configuration using this menu.

6.3. DNS and DHCP

Using this menu, the computer name and the domain of the Intra2net system can be defined.



Caution

In the local network, do not use an official domain (e.g. ending in ".de", ".com" or similar). Use a domain that is only valid locally instead (e.g. ends in '.internal', '.local' or '.lan'). Otherwise, your website will no longer be accessible from the local network and there will often be problems with email delivery.

This menu is opened automatically during initial installation. It is possible to configure a DHCP pool or deactivate the DHCP server function.

6.4. Firewall Emergency Mode

If you have locked yourself out of the web interface with the firewall, access can be briefly re-enabled using this function.

Details can be found in Section 41.4, „Firewall Emergency Mode“.

6.5. Restore to Factory Settings

With this function, the Intra2net system can be restored to the state it was in at the point of supply, or installed for the first time. All settings, user data, passwords, emails, statistics, log files and backups are deleted by the system. Only the version of the Intra2net software remains up to date and is not restored.

The device will then restart automatically.

6.6. The Root Password

The root password is only needed to access the Linux shell and is independent of the administrator password. It is not required for normal operation or administration.

For Intra2net appliances it is randomly generated for each machine individually and stored encrypted at Intra2net. If a dealer or customer wants access to the Linux shell, it can be requested via Intra2net support.

If an Intra2net appliance is replaced by a software version of the Intra2net system, a root password must be entered at the end of installation. Make sure that the password is long enough (at least 10 characters) and cannot be easily guessed (e.g. not a dictionary word). Write the password down and keep it in a secure place (e.g. a safe). Use a completely different password from any administrator, user, or other system.

The root password is part of the installation, not the configuration of the system. It is therefore not included in the backup and is not touched when the configuration is reset to the delivery state.

The root password is also used to protect the boot manager. If the offered boot options need to be changed, the user has to login with username `root` and the root password.

To change the root password, log in via SSH or at the console to run the program `set_root_grub_pwd.sh` on the Linux shell.

6.7. The Linux Shell

The Linux shell is not needed for normal operation or administration.

The Linux shell level can be accessed as a root user from the console and via SSH. Use `ALT+F2` to switch from the Intra2net system console to the Linux shell login.

For a serial console, log in with the `root` login. Then select "Linux shell" from the menu to access the shell.



Caution

Changes to the Linux shell can seriously affect the functionality, stability and security of the Intra2net system. It may not be immediately apparent that this is the case, but rather may only cause problems after a certain period of time, such as after an update.

7. Chapter - The Web Interface

7.1. Accessing the Web Interface

Launch a web browser and open the following URL:

`https://192.168.1.254`

If the Intra2net system is set to a different IP address, that IP address must of course be used.

On the first time visiting the site, the web browser will display a security warning, because the encrypted connection (https) is established with a certificate that is not trusted yet, and does not match the server name. These warnings cannot be avoided with the first access. Nevertheless, open the web page.

For later operation, it is important that such certificate warnings no longer appear. To configure this correctly, see 9. Chapter, „SSL Encryption and Certificates“.

7.2. License Code

The Intra2net system is in demo mode for 30 days after initial start-up. In this demo mode all features of the software can be tried out, except the backups created in demo mode can only be restored with a full license.

As soon as the device has an Internet connection, you can enter a license code under the menu Information > License and thus operate the device fully and continuously.

If you have not entered a license code by the end of the 30-day demo mode, the system will stop functioning, disconnect Internet access, and disallow access to email or groupware.

7.3. The Main Page

With the following user data you can log in for the first time after installation:

Administrator Login	admin
Administrator Passwort	admin

In the upper area of the main page, Internet connections can be established and disconnected with different providers, email transfers can be initiated, and VPN connections can be controlled.

The lower area displays status information.

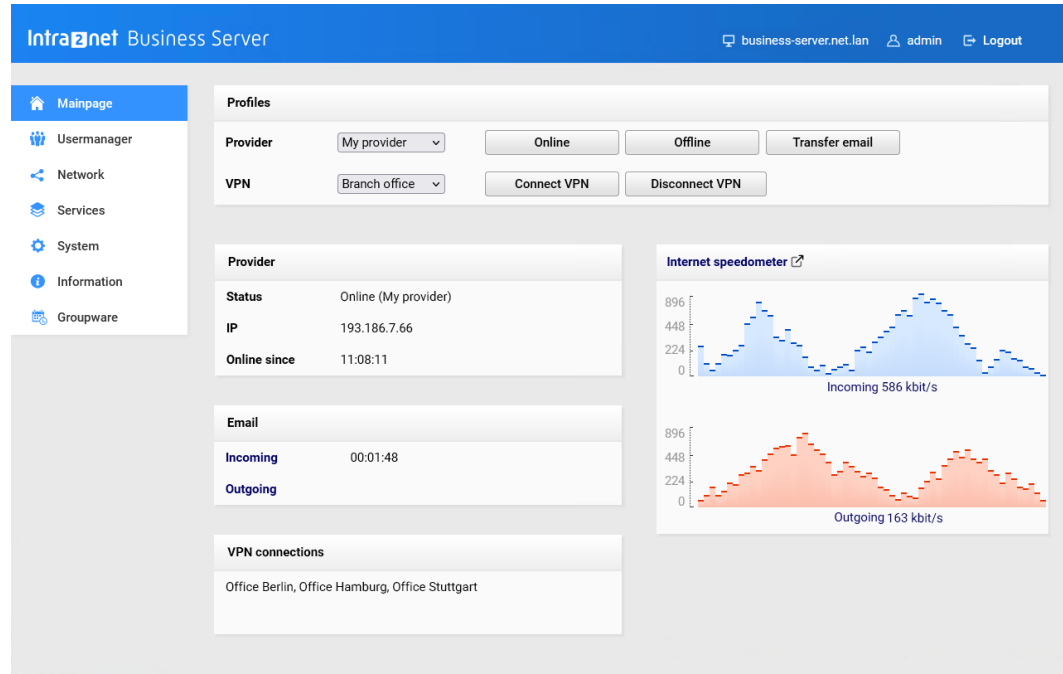
The information area displays status and error messages. Error messages can be removed by clicking on the "OK" button afterwards. Otherwise, they disappear after a certain timeout period (depending on importance and type).

The provider area shows the current provider, IP and timeout.

The email area shows the current email transfer. Clicking "Input" opens a window with a live-log of fetchmail during the email transfer, for error diagnosis during email receipt. Clicking "Output" opens the email queue.

The VPN area displays currently active VPN connections.

The Internet speedometer is displayed on the right. This shows the Internet connection usage within the last minute as a bar chart. The display is divided into incoming (downstream) and outgoing (upstream) traffic. Click on the diagram to access live tracking in the statistics menu.



In the default configuration, everyone who accesses the main page from the local network has the right to see it, as well as establishing and closing connections. This can be changed using the rights of the "All" group. See Section 13.1, „User Groups“.

In the menu on the left-hand side, all menu items that the currently logged in user has access to are displayed in full font color. The menu items to which he has no access are displayed in a faint font color. The latter can still be selected, however, and a login field will open.

7.4. The Queue

Normally, changes to the configuration are enabled immediately by clicking "Save changes". Since this is not practical for some settings (e.g. network configuration or remote maintenance session), there is a queue.

If it is active, all changes are collected. They can be viewed under System > Queue and rejected or activated together.

It can either be activated manually in System > Queue or it is activated automatically when some settings (network, firewall) are changed.

The queue is shared by all users on the system. If no change is made for a certain time, the queue will be deleted automatically. If the queue is active for a longer period of time, there may be problems when configuring new clients via DHCP.

If changes are made that are not valid due to dependencies alone (e.g. changing a network, if there are still IPs in the old network), these changes are normally invalid and displayed

in red as errors. The queue allows such changes, as it is possible to use it to correct the dependencies. If any changes in the queue are to be made, all dependencies must be corrected first.

7.5. The Configuration Check

Under Information > System > Configuration all warnings and errors of the configuration check system are displayed. Since it can sometimes happen that errors are still displayed due to the often complex dependencies, even if they have already been fixed, there is the "Check configuration" function.

7.6. Shutdown necessary

Intra2net systems must always be shut down cleanly before disconnecting the power supply. This is necessary to maintain the integrity of the file system and (if present) RAID mirroring.

Press the power button briefly (=less than 1 second) to shut down. The device beeps, starts shutting down and then switches itself off. Alternatively, you can use the "System > Shutdown" menu.

A scheduled startup and shutdown is also possible, details can be found in Section 16.7, „Scheduled Shutdown“.

Part 2. General Functions

8. Chapter - Intranet

8.1. IPs and Networks

Under Network > Interfaces the system's network cards can be configured.

The following types/modes can be selected for the network cards:

LAN with NAT	Local network. When accessing the Internet, the local IP addresses are converted to the Internet IP of the Intra2net system (network address translation, NAT). This is the default configuration for local networks.
LAN without NAT	Local network. No NAT is used when accessing the Internet. Use this mode for a DMZ (Demilitarized Zone) with official IPs or if the Intra2net system does not provide direct access to the Internet and another router is responsible for NAT.
DSL/Router	Network card used to route access to the Internet. Either via a DSL modem or a router. Which one of them is used is dependent on the type of provider profile used. The provider type and IPs are not set here, but under Network > Provider > Profiles.
Proxy ARP	Local network without NAT using IPs from the router range. A detailed description can be found at Section 10.7.3, „Proxy-ARP“.
unused	not active.

A firewall profile can be assigned to the LAN network cards. This is then valid for all IPs on this network, for which no more specific configuration (e.g. by entering as client or network range) has to be made. Further details are given under Section 8.3, "Access Rights of a Network Object".

8.2. VLAN Tagging

VLAN tagging is the division of a network into virtual subnetworks on the Ethernet level (OSI layer model level 2). For this purpose, each network packet is marked with an additional number, the VLAN tag. A manageable, VLAN-enabled switch can use these VLAN tags to seal off subnetworks or individual devices. The firewall of the Intra2net system can then monitor and control the communication between these subnetworks.

Each VLAN interface appears in the Network > Interfaces menu as a standalone interface. New VLAN interfaces can be created using the "New VLAN" button. The VLAN ID is a freely selectable number between 1 and 4095, and a physical interface is assigned to each VLAN interface.



Hint

Some switches assign a special position to VLAN ID 1. It is advisable to use a VLAN ID of 2 or greater.

By clicking the "Remove VLAN" button, a VLAN interface is deleted. Changes to the VLAN interfaces restart all network services, so the system will temporarily go offline.

For technical reasons it is not possible to create VLANs on DSL/Router interfaces. If the system is offline, the physical interface is switched off and would disable all VLANs. If multiple DSL/Router interfaces are to be bundled on one physical interface, configure the physical interface to the type "not used" and then create as many VLAN interfaces as desired on this interface.

For technical reasons, a maximum of 50 different VLAN interfaces can be used on the system.

For increased security, we recommend connecting LAN and WAN traffic over different physical interfaces instead of relying on VLANs. Incorrect configurations on the switch could otherwise send unfiltered Internet traffic to the local network.

8.3. Access Rights of a Network Object

For each network object (network, client, VPN,...) the same group of rights can be assigned.

Firewall Ruleset	The firewall ruleset is used to check all packets sent by this object (client, network, etc.). A detailed description of the firewall rulesets can be found in Part 5, „Firewall“.
Proxy Profile	Either a proxy profile can be permanently assigned to an object or user authentication can be activated.
Email relaying allowed	Allows sending emails to domains that are not found locally on the Intra2net system. Sending emails must be allowed on the firewall ruleset beforehand.
Allow DNS requests to the Internet	Allow DNS requests that the Intra2net system cannot resolve itself. This function can be used to prevent constant dialing through DNS requests and to block DNS tunnels used by some hackers for data transmission.

8.4. Domain and DNS

The Intra2net system forwards DNS requests to the Internet. For details on how and where to set the currently active provider, see 10. Chapter, „Internet“.

It can also act as a DNS server for the local domain itself or delegate the task to another server.

8.4.1. The Intra2net system as local DNS server

If you do not have a full DNS server in your local network yet, use the Intra2net system as DNS server and configure it as described in this section. If you already use another DNS server (e.g. a Windows Domain Controller), proceed as described in Section 8.4.2, „Integrate another DNS server in the LAN“.

The individual host name and local domain can be set under Network > DNS > Settings. Specify that the local system is responsible for the local domain.

The Intra2net system is then the DNS server for the local domain. All host names entered under Network > Intranet > Clients can be resolved by DNS.

We strongly advise against using the official domain of a company (e.g. "mycompany.com") in the local network. Since the Intra2net system is a DNS server for the local domain, it

cannot answer requests from clients configured in the external DNS server of the web provider, such as "www".

Instead, use a locally valid domain, such as "mycompany.lan". Due to an Internet standard for broadcast DNS, we also advise against using ".local" for such domains, as some Mac OS or Linux versions do not support the name resolution when using ".local" in the local domain.

8.4.2. Integrate another DNS server in the LAN

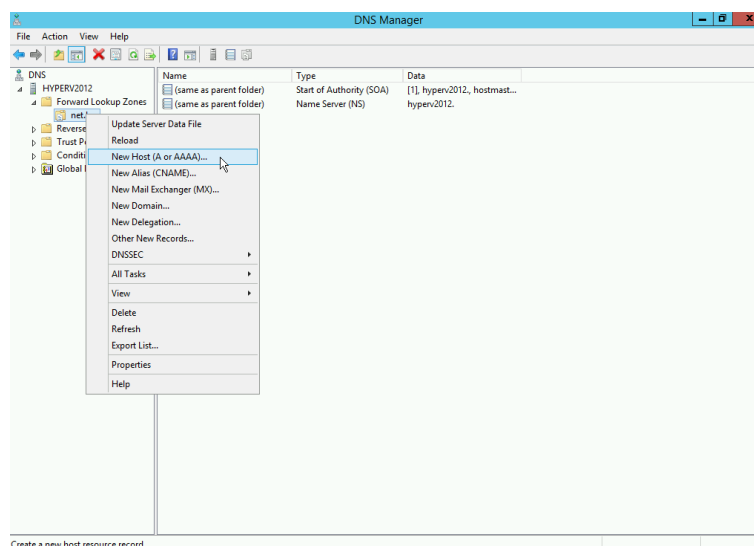
If using a different DNS server for the local domain (e.g. a Windows Domain Controller), enter the host name of the Intra2net system and the domain used in the local network under Network > DNS > Settings. Set the authority for the local domain to "other server". Enter the IP of the relevant DNS server and (if present) the alternative server in the "1." and "2." fields.

On these DNS servers, make sure to allocate an A-entry for the Intra2net system with its IP. For Windows Server, this is described in the following section.

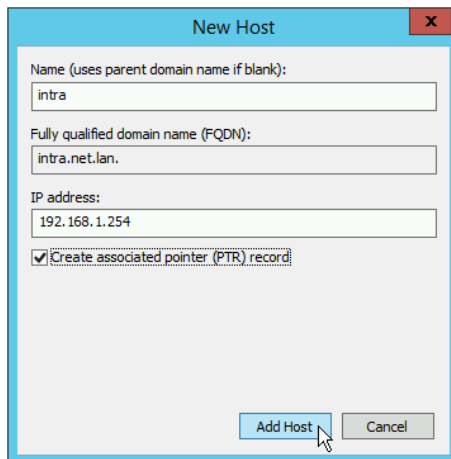
8.4.2.1. Adding the Intra2net system to a Windows DNS server

If you use a Windows DNS server in the local network, it must be able to resolve the name and IP of the Intra2net system so that all computers in the local network can access the Intra2net system under its DNS name. Proceed as follows to create a DNS entry for the Intra2net system:

1. On the Windows server, open the DNS Manager from the menu "Start > Administrative Tools > DNS".
2. In the tree on the left, open the forward lookup zones of your server.
3. Right-click on the local domain you are using and select "New Host (A or AAAA)" from the context menu.



4. Enter the name and IP of the Intra2net system. Create an associated pointer (PTR) record.



8.4.3. Forward DNS to Other Domains

The Intra2net system can forward requests for other non-public domains to dedicated servers. This is useful, for example, if different locations are connected via VPN and names in the local domains of the other locations are to be resolvable.

Enter the domains and IPs of the corresponding DNS servers under Network > DNS > Forwarding.

8.4.4. Prevent DNS Rebind

During a "DNS rebinding" attack, an external DNS server returns an IP from the local network. This may allow an external attacker to force a web browser to establish a remote connection to the local network. Details about this type of attack can be found on Wikipedia [http://en.wikipedia.org/wiki/DNS_rebinding].

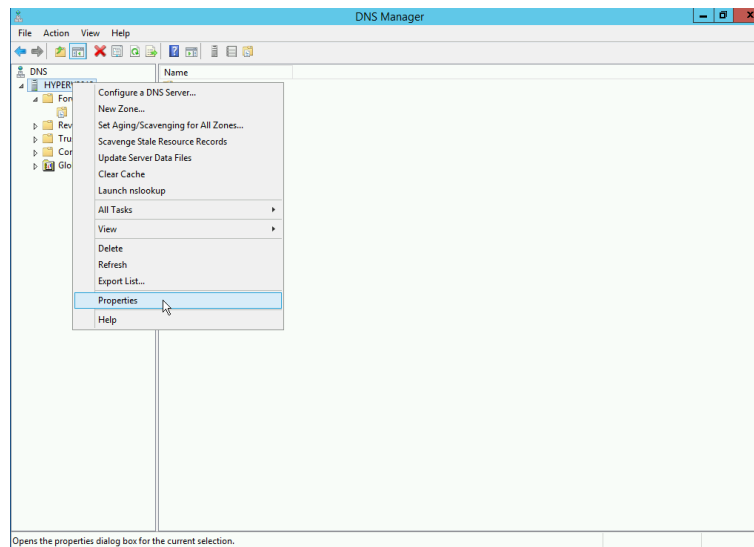
The Intra2net system can effectively prevent these attacks by blocking responses with local IPs from external DNS servers. To avoid malfunctions, only real external DNS servers should be entered under Network > Provider > Profiles : Settings.

All DNS servers that are responsible for local or locally routed domains must be configured for DNS forwarding under the relevant domains. The servers stored there may then respond with local IPs.

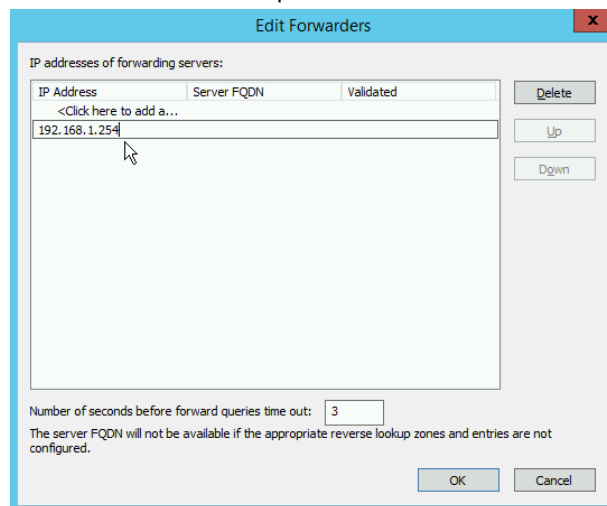
8.4.4.1. DNS rebind protection for Windows DNS servers

Windows DNS servers do not have their own protection against DNS rebind attacks. If you are using a Windows DNS server on the local network and have configured it as described in Section 8.4.2, „Integrate another DNS server in the LAN“, proceed as follows to protect it from DNS rebind:

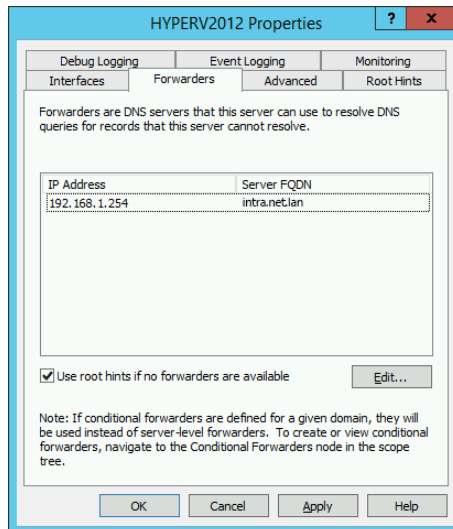
1. On the Windows server, open the DNS Manager from the menu "Start > Administrative Tools > DNS".
2. In the tree on the left, right-click on the DNS server name and open the "Properties" context menu.



3. Switch to the "Forwarders" tab and click "Edit".
4. Enter the IP of the Intra2net system and remove all other entries (e.g. gateway or DNS server of the Internet provider).



5. Now only the Intra2net system is displayed in the forwarders overview. All DNS requests to the Internet now run through the Intra2net system and are protected against DNS rebind.



8.5. Registering Clients

Individual clients can be registered under Network > Intranet > Clients. Each registered client can be assigned its own access rights (see Section 8.3, "Access Rights of a Network Object").

Additionally, the client is automatically available via DNS under its name (primary name and the secondary names specified under "Alias"). An entry for reverse DNS (which DNS name has the IP x?) is also automatically created.

If a MAC address is given, DHCP requests from this MAC are answered with the set IP (static DHCP). If an IP address is entered in the field, click "Detect" to search for the corresponding MAC in the local network.

8.5.1. Wake-On-LAN

"Wake-On-LAN" sends a special IP packet ("Magic Packet") to the specified MAC address. Most computers can be powered on over the network this way. Settings may need to be adjusted in the BIOS of the computer in order to use this feature.

To enable end users to easily use Wake-On-LAN, e.g. to remotely power on their workstations through a VPN, Wake-On-LAN links are offered. By simply opening the link, e.g. with a web browser or script, the Wake-On-LAN function is directly triggered. The link contains all the necessary information, so no further input, confirmation, login or similar is required to trigger the Wake-On-LAN.

The Wake-On-LAN link contains a random value that is used for authentication. If the right to use should be revoked for the previous users, click "Create link". The previous link will be shown. Now click "Revoke current link". This will create a new link and invalidate the previous link.

8.5.2. DHCP

If the client has been set up with dynamic DHCP, the system displays the expiry date of the lease. If it is not renewed by then, the entire entry will be deleted.

It is also possible to enter other rights, aliases or create Wake-On-LAN-links for clients set up with dynamic DHCP. However, since these settings are lost if the computer is not active for a certain period of time (e.g. weekends, vacations, etc.), we recommend removing such clients from the dynamic DHCP pool and assigning another IP outside of the pool. Simply change the IP address and click "Save settings".

8.6. DHCP-Server

The Intra2net system contains a DHCP server. If a MAC address was defined under Network > Intranet > Client, then a querying client is always assigned the corresponding IP. If a MAC is not yet known, the DHCP server assigns an IP from one of the DHCP ranges (see Section 8.7, "Entering Ranges").

Only one DHCP server may be active on a network at any given time. The Intra2net system therefore checks on startup whether another DHCP server is active and deactivates its own when necessary.

Normally the Intra2net system configures itself as the standard gateway and DNS server. Under Network > Intranet > DHCP it is possible to change these values, as well as servers for WINS and NTP time synchronization. If the fields are left blank, the Intra2net system is used.



Caution

We advise against using a different standard gateway. Functions such as port forwarding and accessing local clients via VPN may cease to work.

8.7. Entering Ranges

Under Network > Intranet > Ranges, IP ranges (from-to) can be entered. This allows the entire range to be assigned individual access rights (see Section 8.3, "Access Rights of a Network Object").

In contrast to individual clients, the Intra2net system cannot take over a DNS function for ranges.

If an range is used as a DHCP pool, no rights are assigned to the IPs in said range. An IP from one of the DHCP pools is only assigned to a client when it makes a DHCP request. For this purpose, the client is automatically created under Network > Intranet > Clients.

Should there be multiple different local networks, a separate DHCP pool must be created for each network

8.8. Import/Export Client Profiles

Various settings for clients can be imported or exported in a single file. Either a prepared XML or CSV (Comma Separated Value) file can be uploaded to or downloaded from the Intra2net system. This is particularly useful if there already is a client database from which the data can be exported.

8.8.1. Importing Clients

Here it is possible to upload an XML or CSV file containing client data for import. The field names for the XML import can be found on the DTD, which can be downloaded

from the configuration page. The structure of the CSV format can best be found in a previously exported CSV file. The field "access_right" contains the name of the access right used for this client.



Hint

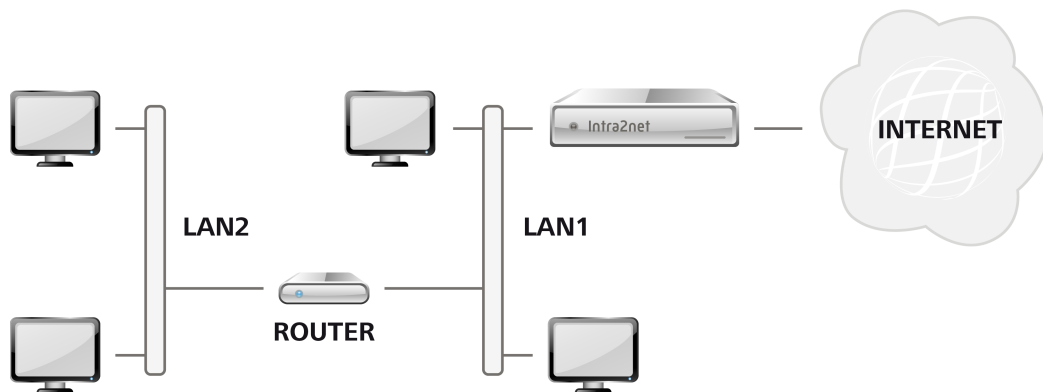
Please note that the access right entered must correspond exactly to the name of an access right in the system.

8.8.2. Exporting Clients

Here it is possible to select the clients for export, either in XML or CSV format. The field names for the XML export can be found on the DTD. In CSV format, the field names are on the first line.

8.9. Intranet Routing

The Intra2net system can route multiple internal networks. For example, this can be useful if multiple companies share an Intra2net system or if separate floors or departments use different networks.



A client or router on the network of the Intra2net system must route between the networks. Enter its IP address in Network > Intranet > Routing, under Gateway IP. If the Intra2net system is to route itself between the networks, connect the other network to one of the network cards of the Intra2net system and enter the network under Network > Interfaces (see Section 8.1, "IPs and Networks").

Routing on the intranet only works for internal networks (on internal network interfaces) and cannot be used to place special routes on the Internet (on the external network interface). Use the provider settings for this purpose, see Section 10.3, „Router with static IP“.

Rights settings can also be specified for an entire routed network. For routed networks, only the rights of the routing itself apply, not the rights of the network through which the gateway is connected, which are specified under Network > Interfaces.

The firewall of the Intra2net system is only effective for connections from the routed network to the Internet and other networks directly connected to the Intra2net system. The firewall does not work for connections between the routed network and the network connected to the Intra2net system and router. In order to be able to use the system firewall between different local networks, these networks must be connected directly to a network interface of the Intra2net system, rather than being connected via a separate router.

9. Chapter - SSL Encryption and Certificates

9.1. Principles and Dangers of SSL Encryption

Encryption ensures that only the client and server know the transferred data. However, somebody can intercept the connection between client and server and can read and change everything from that point onwards (*man-in-the-middle*-attack). To prevent this from happening, the server authenticates itself to the client with a security certificate when the connection is established.

The server sends its certificate to the client and the client checks it according to 3 criteria:

1. The certificate is issued by a Certificate Authority known to the client.
2. The certificate identifies the exact server that the client has connected to. To do this, the client compares the host name it has connected to with the *Common Name*, (abbreviated CN) in the certificate.
3. The current time is within the validity period of the certificate.

Only if all three criteria are correct, can the client be sure that it is connected to the correct server and an attack can be ruled out.

A real-world attack could be described as follows: A hacker sits with a normal notebook at a WLAN hotspot at the airport. He uses special software to redirect all WLAN connections via his notebook. If someone wants to establish an encrypted connection, the software presents the user with a different certificate. This certificate has been legally issued by a trusted Certificate Authority on a domain belonging to the hacker. The only thing that can warn the user that the connection is being tapped and manipulated by the hacker is the browser's warning that the website and certificate do not match.

Warnings of incorrect security certificates should therefore never be ignored.

9.2. Correctly Creating Certificates

9.2.1. The Computer Name

The name (or IP) entered into the web browser, email program, etc. to access the server must correspond exactly with the computer name (CN) in the certificate. This means that if the Intra2net system is to be accessed e.g. via the computer names `intra.net.lan` and `myintra.dyndns.org`, you need 2 different certificates.

The Intra2net system thus allows the configuration of one certificate for the internal interface and another for the Internet interface.

In order for the computer name verification to function consistently, the Intra2net system must be accessible by all clients in the local network under its configured DNS name. Hence, it is important to pay attention to Section 8.4, „Domain and DNS“ and test whether the Intra2net system can be reached by clients in the local network under its full name (including domain).

We advise against storing an IP address as a computer name in the certificate.

9.2.2. Configuration

Open the System > Keys > Own Keys page and create a new key. The name does not matter, but it would be sensible to use the computer name.

At the time of writing, institutions such as the BSI and the German Bundesnetzagentur recommend a key length of 2048 bits and SHA2-256 as a signature algorithm (see algorithm catalogue of the Bundesnetzagentur).

In the field "Computer name (CN)" enter the computer name (see above). All other fields can either be left blank or filled in as desired.

Once the key has been created, it can be used under System > Web Interface > Security. For "SSL Server key (local connections)" select the key for connections to the local network. For "SSL Server key (Internet connections)" select the key for connections to the Internet.

9.3. Installing Certificates on Clients

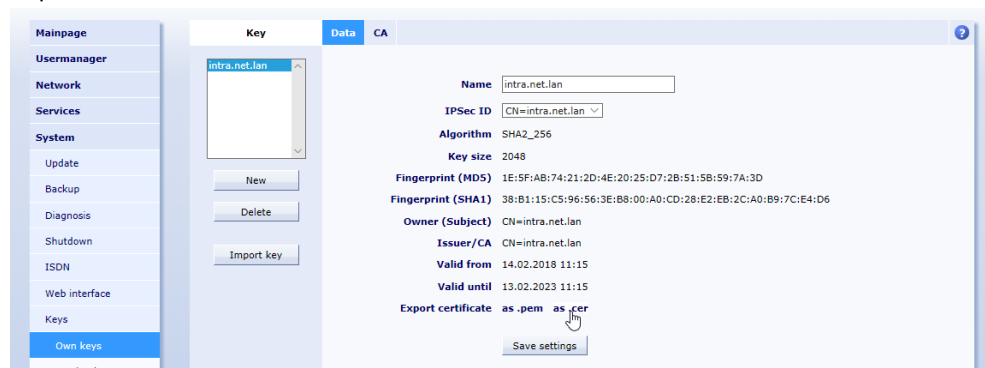
If you have created new certificates yourself, they will not be known on the client. The client software will therefore warn you of a certificate from an unknown Certificate Authority.

Establish a connection and install the certificate on the client. The program should no longer warn of invalid certificates during the following sessions.

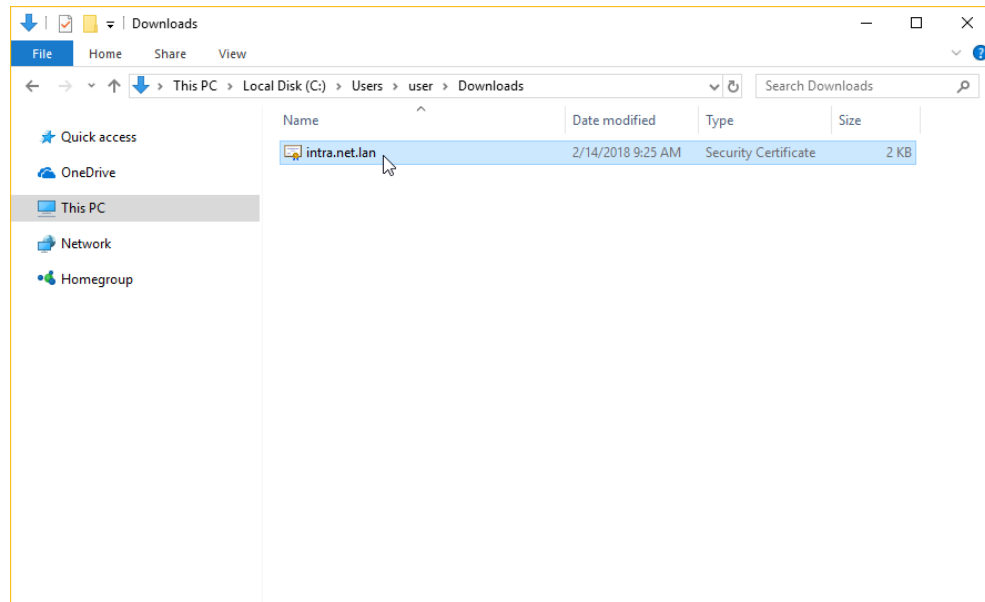
9.3.1. Installation with Windows

The following describes how to install the Intra2net system certificate onto the Windows certificate system. Note that some programs (e.g. Mozilla Firefox) have their own certificate system. If such programs are to be used with the Intra2net system, the certificate must also be installed there.

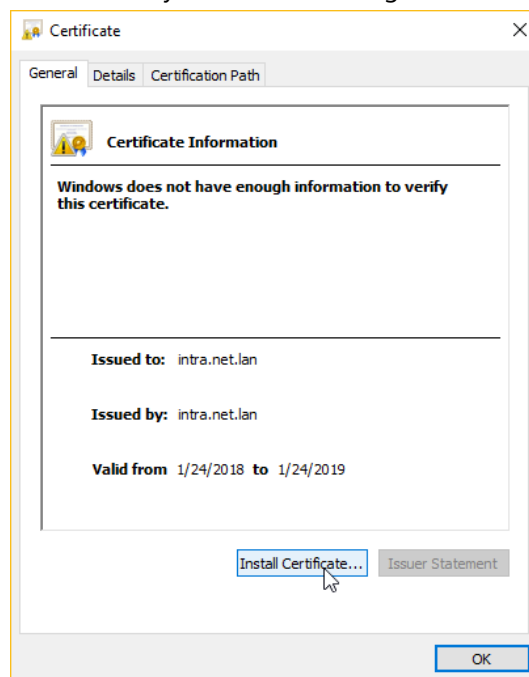
1. Open the web interface of the Intra2net system. It may be necessary to temporarily accept the (still) untrusted certificate and open the connection.
2. Open the System > Web Interface > Security menu and click on the magnifying glass icon beside the "SSL Server Key (local connections)" option.
3. Export the certificate as ".cer" and download it.



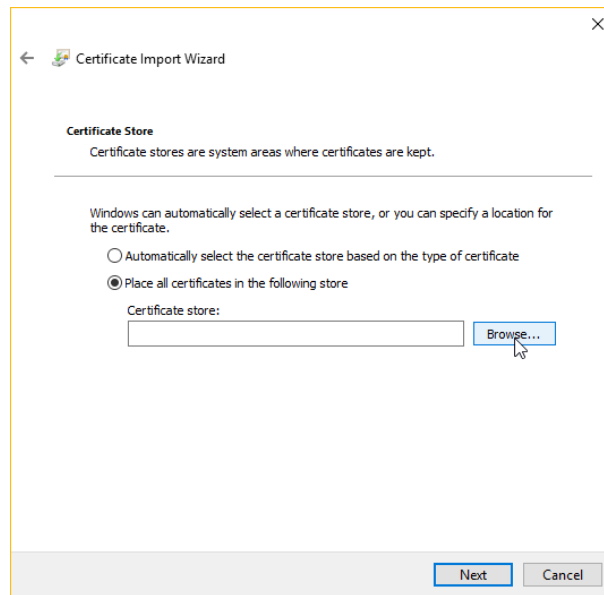
4. Double-click the newly downloaded file in Windows Explorer to open it.



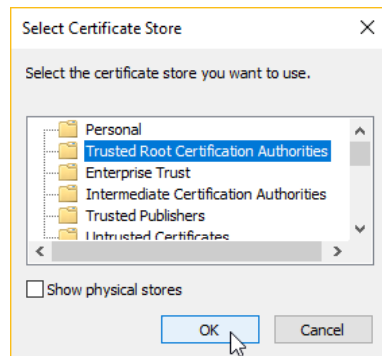
5. In the certificate display, click "Install Certificate". If this option is not available, ensure the necessary administration rights are being used.



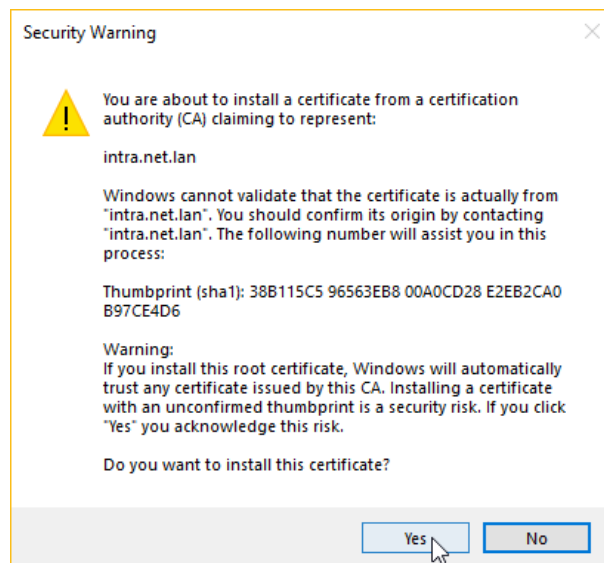
6. A certificate import wizard will open. Click on "Browse..." to select the desired location for the certificate.



7. Select "Trusted Root Certification Authorities" as a certificate location.

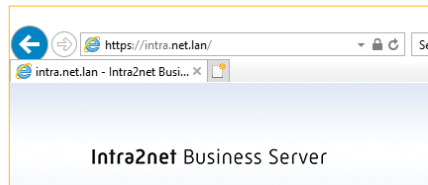


8. Close the wizard. The operating system will display a security warning. Confirm that the installation of the certificate.



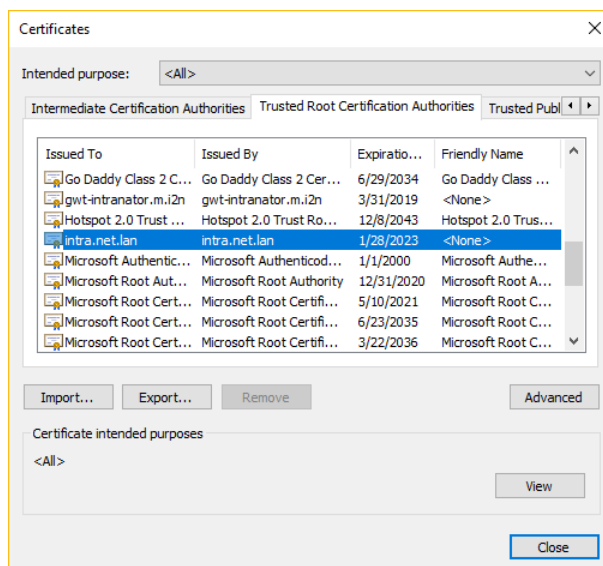
9. Close the Internet Explorer.

10. Open Internet Explorer again, this time without administrator rights, but with normal user rights.
11. Open the Intra2net system interface again. No certificate warning should appear now. A padlock symbol will be displayed next to the URL.



If any problems are encountered with the installation of the certificate, please review the following points:

- In Internet Explorer open "Internet Options", "Content" tab, and click "Certificates". The certificate of the Intra2net system should be listed under the "Trusted Root Certification Authorities" tab.



- If the certificate is not displayed there, check if it is not in another certificate location. Then reinstall it once again ensuring that "Trusted Root Certification Authorities" is the selected destination.
- Some versions of Windows have a known certificate location error. For more information, see <http://support.microsoft.com/kb/932156>.
- We have observed that some systems have problems with the owner of the certificate location, in connection with imaging systems. In this case, the registry editor must be used to change the owner of this key to the current user: HKCU\Software\Microsoft\SystemCertificates\Root\ProtectedRoots. Then assign read access rights for the user.

9.3.2. Distributing Certificates via Active Directory

If the client PCs are managed with an Active Directory, they can be used to distribute the certificate of the Intra2net system to all of them.

Export the relevant certificate as a .cer file from the Intra2net system under the menu System > Keys > Own keys.

Then follow Microsoft's instructions for distributing the certificate: <https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy>

Select "Trusted Root Certification Authorities" as a certificate location.

The steps outlined there will create a group policy. Assign this policy to the users and computers on the local network.

After the group policy is deployed, it normally takes up to 2 hours for it to become active automatically on the client PCs. The command gpupdate /force can be used to start an immediate update on a client PC. A few minutes later the certificate should be available in the certificate store.

9.4. User Education and Awareness

1. Users must never become accustomed to accepting browser certificate warnings as they appear. For this reason, the certificates must be configured correctly on computers from the very beginning.
2. Explain to users that they must never, under any circumstances, accept a certificate warning, especially when connecting externally (e.g. web groupware). Instead, an IT manager or an Intra2net specialist retailer should be contacted.

9.5. Using an External Certificate Authority

There are many *Certificate Authorities* (abbreviated CA), which provide the creation of certificates as a service. These certificate authorities are already trusted by most browsers. This means that a certificate does not have to be installed on all clients before use.

Certificate authorities only sign certificates with official, externally accessible DNS names. It is therefore not possible to use a Certificate Authority for local DNS names (such as intra.net.lan) or IP addresses.

There is the choice of classic, commercial certification authorities where the request, verification and issuance of the certificate takes place via the provider's website and for which a small fee per year of validity is due.

Alternatively, the provider Let's Encrypt [<https://letsencrypt.org/>] offers certificates that are issued and renewed fully automatically and free of charge using the ACME protocol. We recommend Let's Encrypt especially because of the easier handling and automatic renewal.

9.5.1. Certificates from Let's Encrypt

Proceed as follows to use a certificate from Let's Encrypt:

1. Configure a DNS name for the external IP of the Intra2net system in an official domain that belongs to you (e.g. **mail.meinedomain.de**). This can normally be set up free of charge and promptly by the webspace provider who manages your own domain. If a dynamic IP is used, set up a dynamic DNS service instead, see Section 10.13, „DynDNS“.

2. Enter the external DNS name in the menu "Network > DNS > Settings" as the computer name for connections from the Internet.
3. An incoming HTTP connection is required to validate the certificate. Therefore select in the menu "Network > Provider > Profiles : Firewall" a firewall ruleset that allows incoming HTTP connections. HTTP connections are only accepted by the Intra2net system while a certificate validation is pending. Otherwise the port is closed.
4. Check how the Intra2net system is connected to the Internet. Check in the menu "Network > Provider > Profiles" the type of the active provider. If it is a (DSL) dial-up line, everything is fine and you can proceed to the next step.

If it is a provider of type with a router, then check if this router assigns an unchanged official IP to the Intra2net system or if it assigns an IP from a private address range via NAT. In the latter case a port forwarding for TCP port 80 (http) must be configured on the router to the IP of the Intra2net system.
5. Create a new certificate signed by Let's Encrypt in the menu "System > Key > Own keys". The verification and issuance of the certificate is fully automated.
6. Switch the certificate used for Internet connections to the new certificate. You can select this in the menu "System > Web interface > Security".
7. You can test whether the new certificate has been issued and installed correctly in the menu "System > Diagnosis > External HTTPS".

Certificates issued by Let's Encrypt are only valid for a few weeks and are automatically renewed by the Intra2net system before expiration. Therefore, the firewall settings and port forwarding described above must remain permanently configured.

9.5.2. Certificates from classic certification authorities

Proceed as follows to use a certificate from a classic certification authority:

1. Configure a DNS name for the external IP of the Intra2net system on an official domain you own (e.g. `mail.mydomain.com`). This can normally be set up free of charge and promptly at the web space provider who manages your domain.
2. Create a self-signed certificate on the Intra2net system and enter the external DNS name under "Computer name".
3. Select a Certificate Authority. Here is a short, summarized list of some providers (alphabetical): Comodo [<https://www.comodo.com/>], DigiCert [<https://www.digicert.com/>], GlobalSign [<https://www.globalsign.com/>], Go Daddy [<https://www.godaddy.com/ssl/>].

Experience has shown that certificates are cheaper to obtain from resellers than directly from providers. Examples of such resellers are (alphabetical) Cheap SSL Shop [<https://www.cheapsslshop.com>] and GoGetSSL [<https://www.gogetssl.com>].

4. Purchase a certificate from the website of the selected Certificate Authority or reseller. A simple, domain-validated SSL certificate is sufficient for a single domain or website. Extended validation (EV), organization validated certificates or wildcard certificates are unlikely to be required. If you have different server types to choose from when ordering, choose `Apache (mod_ssl)`.

5. As the certificate is issued, the Certificate Authority will ask for a *Certificate Request* (or CSR). These can be exported from the Intra2net system using the menu System > Keys > Own Keys : CA . Make sure that you do not allow the certificate request to be generated by the Certificate Authority or dynamically in your web browser, but rather to upload the certificate request generated by the Intra2net system to the Certificate Authority's system.
6. The Certificate Authority will provide 2 items: a certificate and a *Certificate Chain*, *CA bundle* or *Intermediate Certificate*. Import both into the Intra2net system under the menu System > Keys > Own keys : CA.
7. Switch the certificate used for Internet connections to the new certificate. You can select this in the menu "System > Web interface > Security".
8. You can test whether the new certificate has been issued and installed correctly in the menu "System > Diagnosis > External HTTPS".

9.6. Key Import

Normally a private key is created on the Intra2net system and there is no means to export it. Only certificates and public keys issued for the key can be imported using System > Keys > Own Keys : CA menu.

However, if you have a ready pair of private and public keys and want to import them, you can import them using with the "Import keys" button under System > Keys > Own keys.

The pair of keys can be imported either by cut&paste in PEM format but the private key cannot be password protected. Alternatively, the pair of keys can be imported as a PKCS#12 file. You must enter the correct password protecting the file.

Before importing a pair of keys, make sure that you know exactly where it was created and whether this source and the route are fully trustworthy. Anyone who knows the private key can make the data transferred with this key legible. Never let an external Certificate Authority generate a pair of keys, generate the keys locally and send only the certificate request to the external Certificate Authority. Do not allow key pairs to be generated in a web browser, as this will create additional means of attack.

9.7. Encryption Strength

Cryptography and CPU performance has improved rapidly in recent years. Encryption methods that used to be considered secure are now considered cracked and should therefore no longer be used. However, there are still older systems that are not yet able to handle newer processes.

The Intra2net system allows specific control of the available encryption methods, separated by connections in the local network and Internet. This can be found in the "System > Web interface > Security" menu. The settings selected there apply to the connections secured with SSL or TLS for the following protocols or services: The web interface and web groupware, ActiveSync, POP3 (S), IMAP (S) and SMTP-Submission.

The following options are available for each of the two areas:

Normal	Only connections with TLS 1.2 and TLS 1.3 are accepted. Forces PFS for all connections. This is the recommended setting for all connections.
Compatibility for Windows 7	Like "Normal", but TLS 1.0 is also allowed for the IMAP service. This setting is intended to be able to connect email clients with Windows 7 on which TLS 1.2 has not yet been enabled in the registry (see below).
Weak (Windows XP compatible)	Allows weaker encryption and key exchange methods as well as TLS 1.0 to provide compatibility with older operating systems such as Windows XP. However, this setting disables the RC4 method, which is considered broken. With newer systems that support stronger methods, including PFS, they will automatically be negotiated.
Very weak (for testing purposes only)	Allows connections with weak and cracked encryption methods such as RC4, this setting is a security risk and should only be temporarily enabled for testing purposes.

Perfect Forward Secrecy (PFS): ensures that transmitted data cannot be decrypted even if at a later time the private key of the Intra2net system becomes known and a previously recorded transmission is analyzed, with knowledge of the private key.

Windows 7 and TLS 1.2: Windows 7 supports TLS 1.2 in principle, but this support is not enabled by default for all system libraries. This must be done via a setting in the registry. The .reg file with the appropriate settings can be found in the online help of the Intra2net System for the menu "System > Web interface > Security" linked. If TLS 1.2 has been enabled on all Windows 7 clients, the encryption strength should be changed to "Normal".

10. Chapter - Internet

The Intra2net system can be configured for multiple providers. If one provider fails, it can automatically switch to an alternative provider.

10.1. Dial-up with DSL (PPPoE)

The Intra2net system supports DSL with PPPoE as used by Deutsche Telekom. There is no DSL modem built into the Intra2net system, therefore it must be connected to a network interface of a DSL modem and configured to the type "DSL/Router". Only DSL modems with Ethernet connection are supported. Here you can find an overview of VDSL modems recommended by Intra2net [<https://www.intra2net.com/de/support/vdsl-modems.php>].

Many providers supply a router with an integrated modem as part of their contract. Some of these routers can be used in a modem-only mode, sometimes referred to as PPPoE pass-through. If this is possible, this configuration should be set. If this is not possible, the router should be replaced by a dedicated DSL modem. See Section 10.6, „Router vs. Modem“.

For VDSL connections, but also for some ADSL connections, the PPPoE packets must be marked with a VLAN ID for dial-in. For connections that are provided via Deutsche Telekom's infrastructure, this is VLAN ID 7. This VLAN ID must be entered either on the Intra2net system or on the DSL modem, but not on both at the same time.

When setting up a connection with PPPoE, it is important to properly enter the login details. For more information, contact your provider. Ask for dial-up settings for routers.

10.2. Dial-up with DSL (PPTP)

The Intra2net system supports DSL based on PPTP. It is mainly used in Austria, but in some cases it is also used in France and the Netherlands.

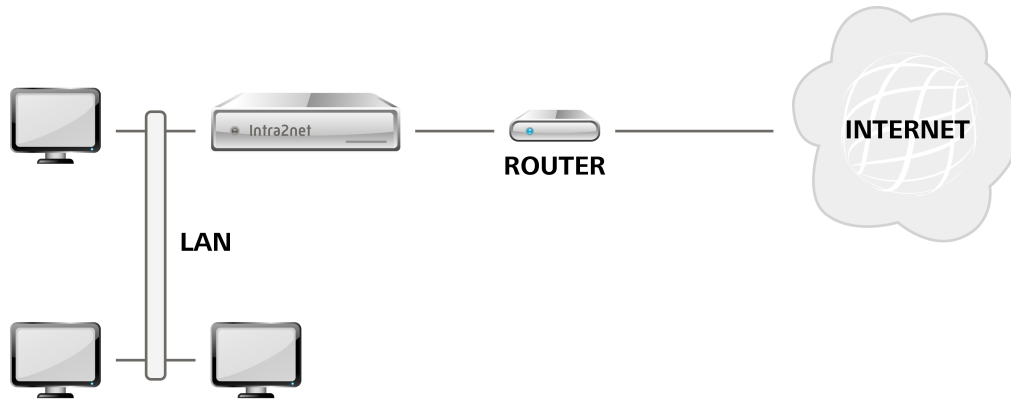
As with PPPoE, the DSL modem is connected to the Intra2net system via an Ethernet interface.

For PPTP connections, the IP of the DSL modem must be set to establish the connection. Most modems use 10.0.0.138. Some providers also allocate this IP via DHCP. Both can be configured on the Intra2net system.

Some providers require a special provider ID (known as the "Phone" field of the PPTP protocol). Leave this field blank and ask the provider for the correct information if problems are encountered during connection setup.

10.3. Router with static IP

A Router with a static IP can be connected to a network interface configured to the type "DSL/Router". The Intra2net system then routes the IP packets directly to it.



Enter the external IP of the Intra2net system in the configuration under "Local IP". This must be in a network together with the router IP. It must not overlap with the local network or one of the locally routed networks (see Section 8.9, „Intranet Routing“).

10.4. Router with DHCP or Cable Modem

This is used when a router is connected to a network interface configured for "DSL/Router". The IPs are requested by the router via DHCP. This method is also used for Internet access via cable connection (broadband cable, e.g. for cable TV), where the Intra2net system is connected to the cable modem and not to a router.

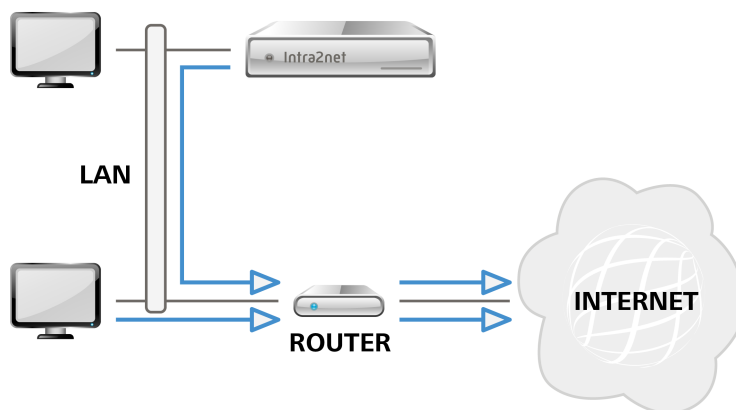


Tip

The cable modem must be turned off for a short period of time when the Intra2net system is connected for the first time, or when the network card is changed. This allows it to adjust itself to the MAC address of the Intra2net system.

10.5. Router on the Local Network

If the Intra2net system is to be used only for limited purposes (e.g. only as an email server), it may be advisable to connect the clients within the local network using a different router. To ensure that the Intra2net system can use another router to access the Internet, although it is not addressed through the external but via the internal interface, there is the provider type "Router in the local network".



Under this configuration, the firewall has very limited functionality. There are also limitations to VPN and port forwarding.

10.6. Router vs. Modem

For most Internet connections, there is a choice between two different connection options:

1. A router typically supplied by a provider assumes the actual dial-up. The Intra2net system is then connected to it using the setting "Router with static IP".
2. The line is connected to a dedicated modem and connected to the Intra2net system. The Intra2net system handles the dial-up.

Variant 1. The router has the advantage of being set up faster, since the router is usually delivered pre-configured by the provider. If this router has additional functionality, such as VoIP, it may also reduce the need for additional devices for specific functions.

Variant 1. A router has the following disadvantages:

- One external IP is used by the router itself. All other devices, such as the Intra2net system, can only communicate via NAT and port forwarding.
- If the Intra2net system is to be accessed externally (e.g. for Activesync, VPN or email delivery via SMTP) port forwarding has to be configured on the router.
- Some routers have difficulties forwarding VPN connections correctly and without interference. This can often be fixed with a router firmware update, but not in all cases. In some cases, we have observed that long-lasting connections, as is common for site-to-site VPNs, do not function reliably and are interrupted after a few days or weeks.
- Very few routers support port forwarding on the local network. This is necessary so that mobile devices (such as laptops) can use both the external DNS name or the external IP for access on the LAN and on the Internet.

Variant 2. A separate modem has the disadvantage that an additional modem is required and dial-up has to be set up once. If necessary, a VoIP upgrade must also be implemented using a separate device and connected to the Intra2net system.

However, there is the advantage that no port forwarding or NAT is required for services, especially the Intra2net VPN. Internal access to the services via the external IP is also possible without difficulty.

10.7. Official IPs and DMZs

If multiple official IPs are available and a server in a de-militarized zone (DMZ) is to be connected, this can be done in three different ways.



Hint

Please note that at least 8 official IPs are needed in order to connect (at least) one server in a DMZ.

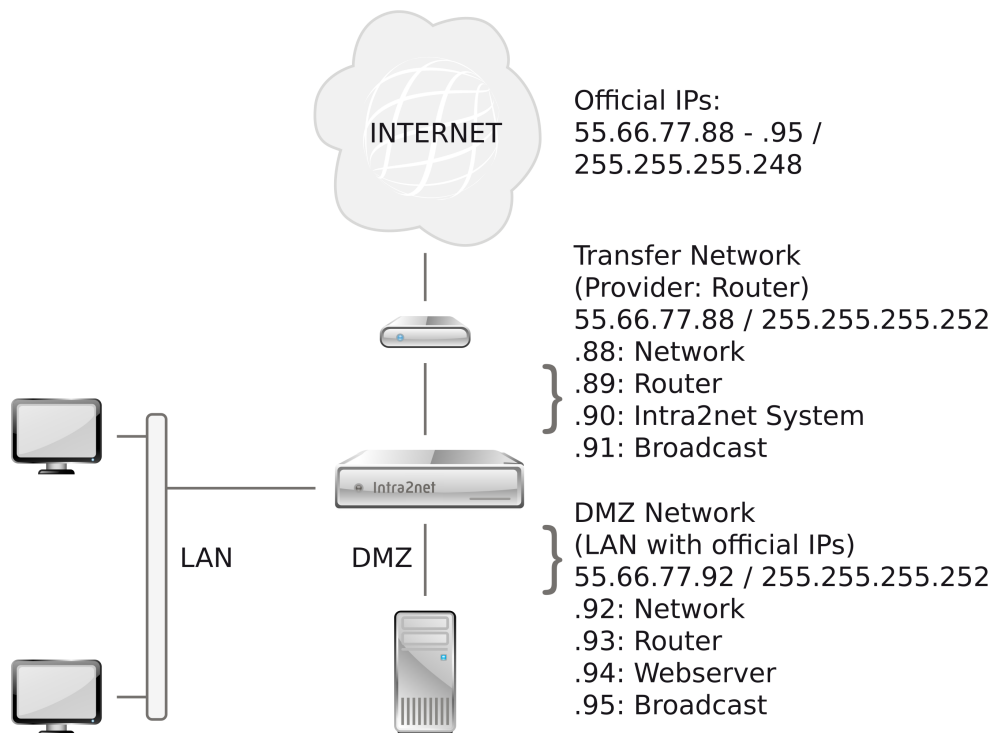
10.7.1. Classic Routing

Advantages	easy to understand, widespread
------------	--------------------------------

Disadvantages	Wasted IP addresses due to network division, subnet routing must be specified on the router
---------------	---

This variant divides the existing network with official IPs into two smaller subnets: A "transfer network" between router and Intra2net system and a DMZ network. Since each subnet always requires two IPs for network address and broadcast and the Intra2net system requires one IP on both networks, only one of the 8 official IPs is available for one server in the DMZ.

On the router it must be specified that the directly connected network (transfer network) has been reduced in size and that the DMZ network is routed via the Intra2net system. Since the user often has no access to a router supplied by the provider, this setting must be made by the provider.



10.7.2. Static NAT

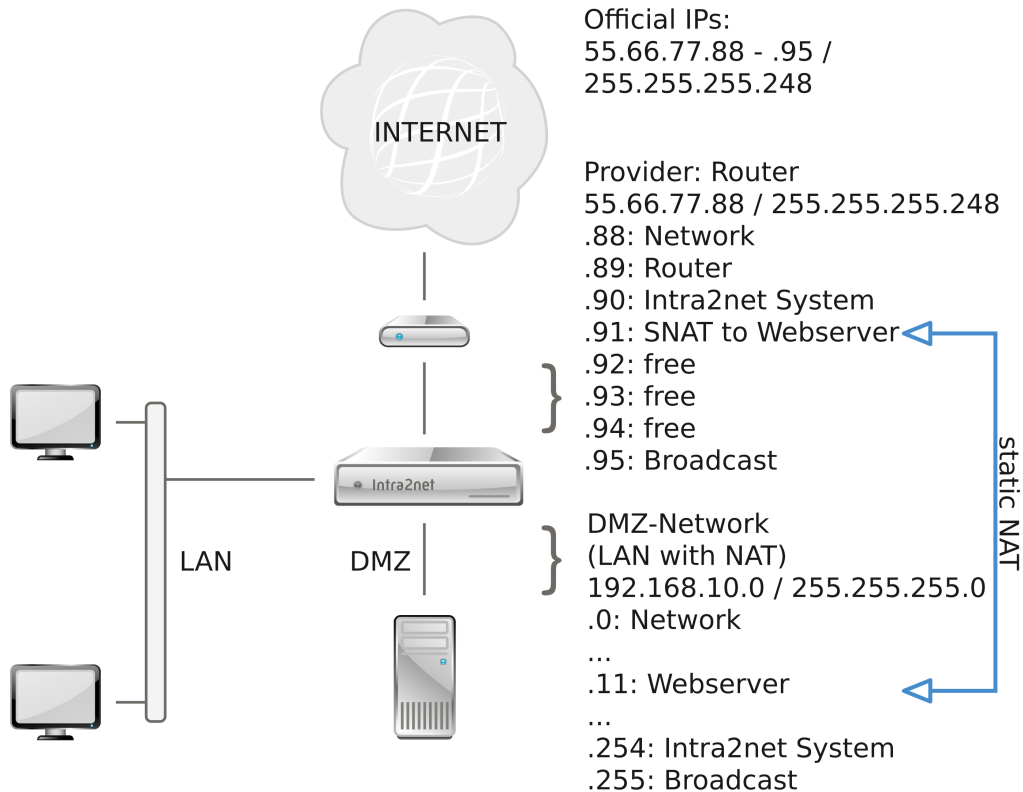
Advantages	flexible, good IP utilization
Disadvantages	does not work with all protocols

In this variant, the DMZ is set up like a normal LAN with IPs from the private address space (e.g. 192.168. x. x). Create all DMZ servers under Network > Intranet > Clients. Then forward the public IP to the server in the DMZ under Network > Firewall > Static NAT.

The Intra2net System automatically answers ARP-requests for the IPs with static NAT as soon as they are in the network between the router and the Intra2net System. Therefore it is not necessary to have any special routing entries on the router for these IPs.

Since the server only knows its IP from the LAN - but not its public one - some protocols do not work, because some protocols also transmit the IP used in the regular data stream.

For some protocols, the Intra2net System can compensate for this (e.g. FTP and PPTP), but not for others (e.g. H. 323).



10.7.3. Proxy-ARP

Advantages	works with all protocols, good IP usage
Disadvantages	more complicated configuration

With Proxy-ARP the network between router and Intra2net system is created again as a DMZ with the same data. Under Network > Interfaces select the type "Proxy-ARP" for the DMZ. Give the Intra2net system in the network the same IP as it was entered under Network > Provider > Profiles. Make sure that all clients in the DMZ network are entered individually under Network > Intranet > Clients. The Intra2net system assumes that all clients not registered there are located in the network between the Intra2net system and the router.

Set the default gateway on the server of the DMZ to the Intra2net system. The Intra2net system now mediates between the two divisions without the clients being affected in any way. For the clients it appears to be a single, larger network. The firewall controls the exchange of data between the two divisions.

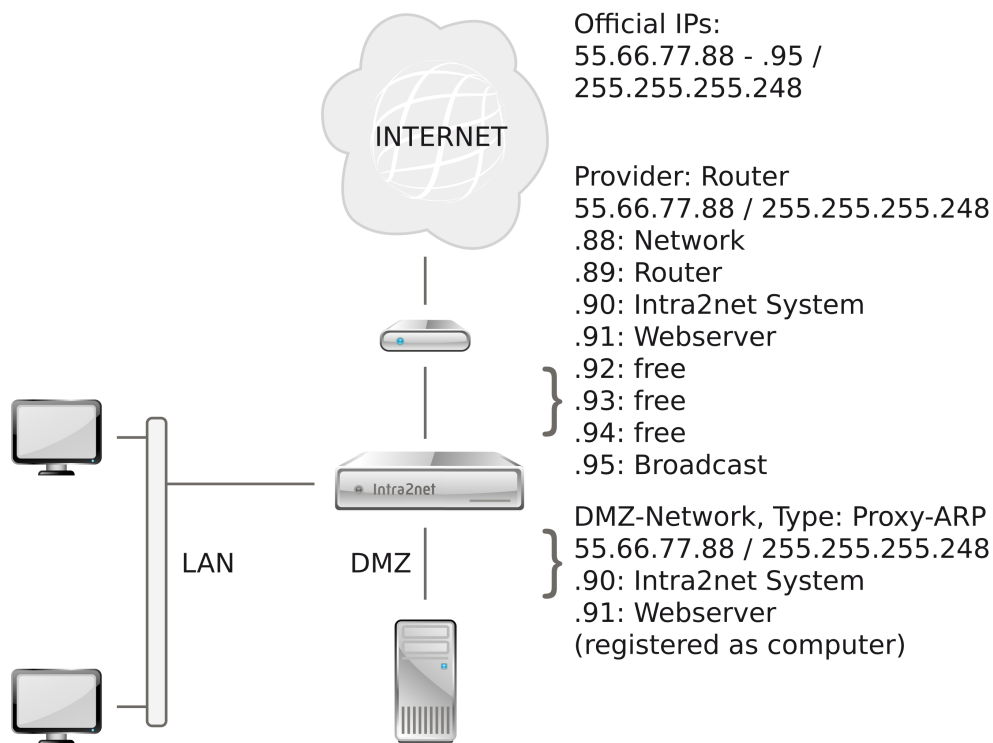
It is not necessary to adjust any special settings for the internal network on the router.



Caution

Initial installation can result in problems with the router's ARP cache. The router will then think that the server is still in the network between router

and Intra2net system. First configure the Intra2net system, then the DMZ server and then restart the router to avoid this problem.



10.8. Automatic Connection

Under Network > Provider > Automatic, define which provider is normally used for connection setup. The connection setup mode will also be configured.

In case of manual connection, the Intra2net system only goes online if a user clicks "Online" on the main page, or a scheduled action (e.g. automatic email transfer) starts.

If a connection is established on demand, the Intra2net system only goes online if a client with firewall access rights wants to send a packet to the Internet. Scheduled actions (e.g. automatic email transfer) also trigger a dialing process.

If the Intra2net system is always online, it will try to keep a connection open at all times.

In case of manual and on demand connection setup, the Intra2net system remains online until the provider terminates the connection (e.g. by forced disconnection) or (if configured) the connection is not used for a certain period of time (connection timeout).

A time can be defined for the Intra2net system to automatically drop the connection. This can be useful, for example, if the provider is to be disconnected after 24 hours at a fixed time of night. After forced disconnection, the connection is only re-established in "always online" mode.

10.9. Connection Monitoring

Connection monitoring is activated by selecting a server list for connection monitoring in the "Services" tab of a provider profile. The connection monitoring then continuously sends ping packets to the peers defined by the server list. If no response is received from half of these servers for a period of 90 seconds, the line is regarded as faulty and the connection is set to offline.

Dial-up access types are first attempted to re-establish connection. If it is not possible to achieve a stable connection through this, a different provider is used, if configured (fallback). In the case of access types without a dial-up procedure, the alternative provider is directly activated. For information on switching to other providers see Section 10.10, „Switching to Other Providers in the Event of an Error (Fallback)“.

Under Network > Provider > Connection monitoring, there are lists of remote hosts which can be pinged for connection monitoring. For normal Internet connections, it is best to use the server list predefined by Intra2net, as it contains servers scattered throughout the Internet, in different data centers, which provides a good overview of the connection status.

When defining your own server lists, it is necessary to ensure that the servers respond to ICMP echo requests (ping). We recommend that at least 4 are listed, preferably 6 to 8, to ensure that one or a few unresponsive servers do not result in a disconnection.

10.10. Switching to Other Providers in the Event of an Error (Fallback)

If the Intra2net system detects that the connection to a provider is disturbed, it can automatically switch to another provider. For this purpose, in the "Settings" of the primary provider tab, the "Fallback provider" option is used to specify a provider, which should be available in the event of an error.

Since an alternative provider is often billed according to time or data volume, or offers a slower line, it is important to switch back to the primary provider automatically. The option "Switches for" is intended for this purpose. After the specified time has elapsed, an attempt is made to reconnect to the primary provider. If it is still not available, a connection to the alternative provider is established again.

The time should not be too short (e.g. 3 minutes) as this will interrupt existing user connections. A longer time interval (e.g. 60 minutes) is recommended.

10.11. Bandwidth Management and VoIP Prioritization

10.11.1. Bandwidth Management

Internet protocols such as TCP are optimized to fully utilize the available bandwidth between client and server in order to transport data as fast as possible. For example, a large amount of data is continuously being downloaded, and an interactive remote maintenance session (where the user performs only one action every now and then) are happening simultaneously. They compete with each other on one line. The download will dominate the line as it is constantly transferring data, and the remote maintenance session packets do not all pass through the line on the first attempt and must be repeated, which is perceived by the user as "stuttering".

Bandwidth management can use rules to ensure that the packets of interactive sessions are not slowed down by large downloads or other large packets of data traffic. This works purely on the basis of packet size and acknowledgment of receipt, without prioritizing special protocol types.

In order for bandwidth management to be effective, it must keep the connection buffers in the modem or router cascaded before the Intra2net system empty and take over the buffering of pending data packets completely by itself. This requires precise knowledge of the bandwidth that is available. If the bandwidth management sends more data to the Internet than can pass through the line, the modem or router will start buffering again. This buffer is not prioritized, which renders bandwidth management ineffective. If the bandwidth management sends less data to the Internet than can pass through the line, the additional bandwidth is left unused.

Precise knowledge of the actual bandwidth is therefore crucial for configuring bandwidth management. We recommend the following procedure for determining the bandwidth (bandwidth management must be deactivated):

1. Open the main page of the Intra2net system in one browser window.
2. In a separate browser window, prepare to download the contents of the installation CD for the Intra2net system from <https://www.intra2net.com>, but do not start it yet.
3. In yet another separate browser window, prepare downloads of 2 other large program files from different vendors (e.g. a Linux Live CD and a free Office package), but do not start them yet.
4. Start all 3 downloads simultaneously.
5. Check the line load in the "Incoming" field of the main page.
6. Small variations in the measurement time and the effects of buffers can lead to erratic utilization. Ignore any anomalous data and calculate the average data transfer rate over a period of approximately 30 seconds.
7. Prepare an email to an external recipient with a large (e.g. 15 MB) attachment, but do not send it yet.
8. Prepare to upload a large file to a cloud storage service provider, but do not yet start it.
9. Send the email with the large attachment. On the main page, watch how the email is queued, scanned and then sent.
10. Start the upload as soon as the email is being transferred over the line.
11. Observe the load on the line in the "Outgoing" field on the main page. Calculate the average as in step 6.
12. Since many Internet access technologies dynamically adapt the bandwidth in response to line disturbances etc., this should be repeated 3 times at different times of the day. Use the lowest values calculated for bandwidth management.

Bandwidth management can be configured in the Network > Provider > Profiles : Firewall menu.

10.11.2. Prioritize VoIP and Real-time Data

If bandwidth management is used, it can further prioritize Internet telephony and the connection of real-time applications. The affected IP packets are detected by DiffServ entries in the packet header. Bandwidth management responds to the DiffServ group Expedited Forwarding (EF). For this, a DSCP value of 46 / 0x2E is used, which corresponds to the entry 184 / 0xB8 in the ToS byte.

Many VoIP devices automatically set the DiffServ group Expedited Forwarding or can be configured accordingly.

We recommend not to connect VoIP devices to the regular local network, but to configure a separate network for all VoIP devices and PBXs, and to connect it to the Intra2net system via a different interface. Ensure that not only different IP addresses are used for this network, but that the Ethernet networks are clearly separated from each other. This has the following advantages:

- VoIP calls can also be prioritized when they pass through a VPN tunnel, (e.g. to another branch office). A prioritization is only possible if a different IP network is used for VoIP and therefore a separate VPN tunnel is used. Otherwise, the VPN's replay protection would prevent a change in the packet order.
- Many manufacturers and service providers of VoIP infrastructure do not apply the same high security standards for security testing, patch management and long-term product maintenance as other IT products. Telecommunication equipment is also used much more often than other IT products, making it more difficult for the manufacturer to maintain. Therefore, VoIP products should be used with increased caution. By separating VoIP devices into a dedicated LAN, the firewall can restrict VoIP devices' access to the rest of the network.
- Large data transfers in the LAN can utilize the network switch to its full capacity. If a separate switch is used for VoIP, the VoIP remains unaffected.

An alternative to using VoIP prioritization is the use of a completely independent Internet access exclusively for VoIP. This allows an even higher quality of service. In addition to this, a connection implemented via another access provider, can also be used as a substitute if the primary Internet access fails (see Section 10.10, „Switching to Other Providers in the Event of an Error (Fallback)“). With this variant, too, the separation between LAN and VoIP network described above must be implemented.

10.12. Masquerading / NAT

All local IP addresses are masked during Internet access and assigned to the external IP of the Intra2net system (n:1 NAT / Masquerading). No NAT is performed just for IPs on networks with "LAN without NAT" mode (see Section 8.1, „IPs and Networks“).

Masquerading can confuse some protocols. The most important ones are corrected automatically by the Intra2net system:

Active FTP, PPTP, IRC, Quake, Cuseeme, Realaudio, Vdolive.

For those missing (e.g. ICQ or Gnutella) the Intra2net system has a Socks 5 proxy server on port 1080, which can be used by all clients with full access without an extra login. It simply requires activation under Services > Proxy > Socks.

For some protocols, it is also necessary to use the "Incoming Socks Connections Enabled" option in the firewall configuration for the relevant provider.

10.13. DynDNS

To remain accessible over the Internet despite changing IP addresses, (e.g. for VPN or external HTTPS access), the Intra2net system can disclose its IP address using the DynDNS service. The Intra2net system notifies a DynDNS provider of its new IP address after every dial-up. A normal DNS name such as `intra.dyndns.org` can then be used to access the Intra2net system under its current external IP.

Under Services > DynDNS it is possible to configure multiple accounts with different DynDNS providers.

10.13.1. Providers

The following DynDNS services are currently supported by the Intra2net system:

Provider	Price	Settings on the Intra2net system
No-IP [http://www.no-ip.com/]	Free of charge (up to 5 entries)	<ul style="list-style-type: none"> Protocol: dyndns Alternative Server: dynupdate.no-ip.com
Dynu [http://www.dynu.com/]	Free of charge	<ul style="list-style-type: none"> Protocol: gnudip-fullhostname Alternative Server: gnudip.dynu.com
ChangeIP.com [http://www.changeip.com/]	Free of charge	<ul style="list-style-type: none"> Protocol: dyndns Alternative Server: nic.changeip.com
DyNS [http://www.dyns.cx/]	\$5 US	<ul style="list-style-type: none"> Protocol: dyns
Dyn [http://www.dyn.com/dns/]	\$25 US / Year	<ul style="list-style-type: none"> Protocol: dyndns
Namemaster [http://www.dyndnsfree.de/]	€12 / Year	<ul style="list-style-type: none"> Protocol: dyndns Alternative Server: dynup.de
DHS [http://www.dhs.org/]	\$5 US / Year	<ul style="list-style-type: none"> Protocol: dhs

All information provided is subject to change and provided without guarantee.

An extensive list of other DynDNS providers can be found here [<http://dnslookup.me/dynamic-dns/>]. However, we cannot guarantee that these providers are all compatible with the Intra2net system.

10.13.2. Updates and the IP Address Used

Under Network > Provider > Profiles : Services it is possible to set whether the DynDNS services should be updated when dialing in for each Internet provider (for redundancy reasons, multiple DynDNS services can be configured at the same time).

The IP address used is usually the external IP of the Intra2net system. However, it is possible that a connection may go through NAT multiple times which could result in a different address being given over the Internet. This can be configured using the setting "Get DynDNS IP from website". The Intra2net system will then first ask a web server for the IP from which the request comes and send it to the DynDNS server.

10.14. External access

The Intra2net system provides access to emails from the Internet via POP3S and IMAPS (encrypted POP3/IMAP4). It is possible to also access the user interface and web groupware from the Internet via HTTPS.

This is configured using the firewall ruleset under Network > Provider > Profiles : Firewall.

For HTTPS connections it is possible to set whether only the webmail system or the complete user interface can be accessed. This depends on which user groups the user is in. The rights for external access are set under Usermanager > Groups : Administration Rights.

For external connections, it is sensible to use a different SSL key from the internal connections, as browsers compare the DNS name of a website with the name in the key, to ensure that no man-in-the-middle attack is being made.

Under System > Keys create an X.509 key using the DynDNS name of the Intra2net system as the host name (CN) (see also Section 9.2, „Correctly Creating Certificates“).

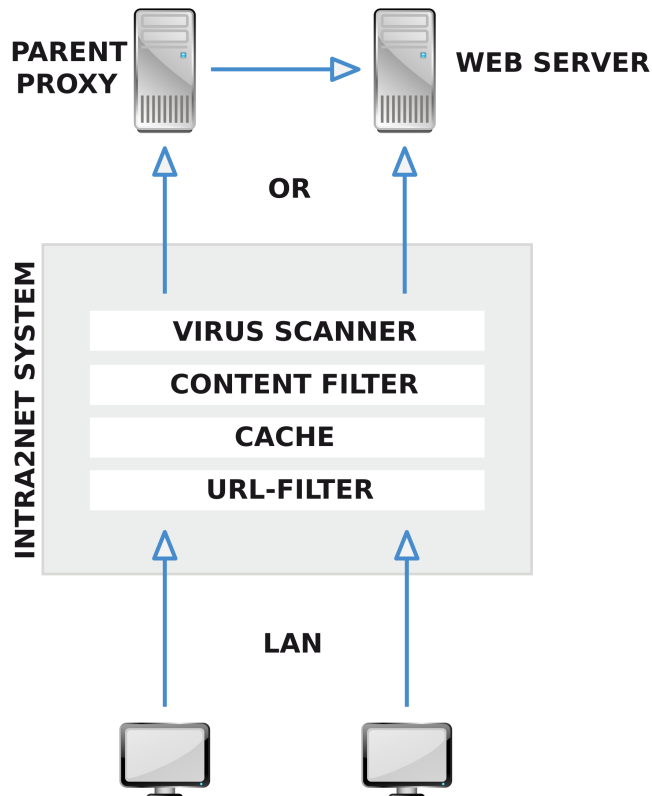
11. Chapter - Proxy

11.1. Overview

The Intra2net system has an HTTP proxy. The proxy can be used for the following functions:

- Acceleration of Access (Cache)
- Filtering unwanted content
- Filtering of dangerous content (viruses, trojans, etc.)
- Logging of all Accesses

The proxy is internally comprised of different modules providing these functions. Since these modules work separately, it is not always possible to configure settings across all modules (e.g. for whitelists).



11.2. Access to the Proxy

The HTTP proxy of the Intra2net system is normally on port 3128, but this can be changed under **Services > Proxy > Settings**.

To use the proxy directly, it must be specified in the browser of each client. The proxy can then be used for HTTP, HTTPS and FTP.

The transparent proxy can also be used for HTTP. There are no requirements to configure anything on the client and the Intra2net system forwards all HTTP requests (transparent

for the client) to the proxy. The Transparent Proxy does not work for HTTPS and FTP. On the Intra2net system, the Transparent Proxy is activated using the clients' firewall rules.

If the proxy is to be used to block access to certain pages, it should be made sure that the proxy cannot be bypassed. This can be done by setting "Forced Proxy" in the client's firewall rule.

11.3. Proxy Configuration

Normally only access to the destination ports 21 and 80, as well as to 443 for SSL are allowed via the proxy. The reason for this is that the proxy's CONNECT function can be generally used for protocols other than HTTP and therefore any firewall restrictions could be bypassed. Some web servers use other ports (such as 81, 8080, etc.). If the clients should be able to use them, they must be entered in the "Allowed ports" or "Allowed SSL ports" under Services > Proxy > Settings.

Normally, the proxy accesses the requested servers directly over the Internet. However, it is also possible that the Intra2net system forwards all requests to another proxy (Parent-Proxy). This can be configured under Network > Provider > Profiles : Services. This means that a different proxy can be used for each provider.

11.4. URL Filter

The URL filter can block pages based on the URL or IP. Access control takes place using proxy profiles. These are either assigned directly to the network object (see Section 8.3, „Access Rights of a Network Object“) or by proxy authentication through the rights of the logged in user (see Section 13.1.1, „Access Rights“).

11.4.1. Proxy Profile

Proxy profiles are configured under Services > Proxy > Profiles. Multiple proxy access lists are combined into one profile.

The following rules apply to grouping.

- If multiple blacklists (marked with "-") are combined, all of their pages are blocked
- If multiple whitelists (marked with "+") are combined, all pages that are not contained in at least one whitelist are blocked
- If both whitelists and blacklists are combined, all pages contained in the blacklists are blocked. If a page is contained in both a whitelist and a blacklist, it is not blocked

11.4.2. Proxy Access Lists

Access lists are managed under Services > Proxy > Access lists. An access list can either be uploaded (for large lists), edited directly in the browser (for smaller lists) or pre-defined. There are also 3 different types of list:

Domain or URL	this option blocks (or allows) a complete domain or URL. For example: "www.sex.com/offer" will explicitly block access to only "www.sex.com/offer" and not e.g. www.sex.com/free
Wildcard	the well-known wildcard "*" can be used to recognize parts of the URL. Example: "*.mp3" - blocks access to all URLs that end with

	".mp3". "*sex*" - blocks access to all URLs that contain "sex" in any part of the URL
Regular Expression	the URLs are checked by POSIX regular expressions. This is only for experts with prior experience

If the "Ban IP addresses of URLs" option has been activated under Services > Proxy > Settings, all domain names in the access lists are resolved and the corresponding IPs are also blocked. This means that it is not possible to bypass the URL filter by entering an IP.

11.4.3. Time Management

It is possible to configure the proxy in such a way that it blocks or releases different pages depending on the time of day and the day of the week. In this way, private websites can be accessed outside of normal working hours or during breaks.

To do this, first define the desired time periods under Services > Proxy > Times. When using blacklists, we recommend creating a time profile for the restricted times (for example, "main working time").

Afterwards, under Services > Proxy > Profiles a profile can be created so that some of the access lists only apply at certain times. To do this, select a time profile from the "Time profile" dropdown menu, then select the appropriate access list and click "<" to add it to the profile.

For example, if erotic pages should never be accessible, but webmail services can be available just outside of normal working hours, add the "erotic" blacklist to the `Anytime` time profile, and the "mail access" blacklist to the `Main working time` time profile.

Note that one proxy profile can only ever contain 2 different time blocks: `Anytime` and one definable time profile.

11.5. Web Content Filter

The Web content filter examines the content of the HTML pages requested via the proxy. If certain words and word combinations occur frequently, the page can be blocked.

Under Services > Proxy > Webfilter, different word categories can be selected and the threshold value set for the response (the "weight of phrase filter" option).

If some domains are to be excluded from the check, they can be entered here.

Each word list contains ratings and calculated dependencies between words. This makes creating and editing very complex. For this reason, it is not possible to customize the word lists. Due to the multi-tiered architecture of the proxy system, it is also not possible to set the threshold value or exception list depending on the individual client or user.

11.6. Proxy Virus Scanner

The proxy virus scanner can scan all of the data that passes through the proxy to detect viruses. First, the complete file is loaded onto the Intra2net system and checked there. If it is virus-free, it is passed to the browser. If it is infected, the transfer is immediately stopped.

Since the user only receives a general error message, all subsequent access to an advisory page is redirected ("locked") at the same time. The virus found, the URL, etc. is displayed there. The user can confirm ("unlock") this by clicking on a link.

If the user is downloading a larger file, they will notice that they must wait for the complete file. In order to give the user feedback on the download progress, the Intra2net system always transmits exactly one 1024th of the data it receives. For example, if the browser shows 50 bytes/sec. then the actual download speed received by the Intra2net system is 50 KBytes / sec.

Multimedia data can also be streamed using the HTTP protocol, and as the virus scanner can only scan complete files, the proxy virus scanner will block it. To make streaming possible, the proxy virus scanner can be deactivated under Services > Proxy > Antivirus for certain data types and for certain domains.

The Virus Scanner allows cloud-based virus detection. Checksums are calculated from executable files and sent to a data center. If the checksums are known to be malicious, access to them is blocked. This significantly reduces the time between the first occurrence of a virus and detection. For data protection reasons, cloud-based virus detection only sends checksums and file names to the data center, and not complete files.

In addition to viruses and Trojans, the virus scanner can also detect adware and spyware. Should such a detected program have utility, then detection can be switched off.

The virus scanner contains a component for detecting macro viruses using heuristic analysis. The detection level for heuristics can be adjusted. At higher detection levels, more macros can be recognized as a virus, but this also could result in an increased proportion of files wrongly detected as a virus.

12. Chapter - Statistics and Data Privacy

12.1. Proxy Statistics

12.1.1. Proxy Logging

Under Information > Statistics > Settings it is possible to configure whether or not the proxy server within the Intra2net system (see 11. Chapter, „Proxy“) should log all website accesses to a log file. Furthermore, these log files can be analyzed and processed automatically.

If activated, the proxy log files are saved as monthly files. These are available in the Information > System > Logfiles menu. They are saved in the standard format of Squid Proxy. The time is given as Unix time in seconds since 1/1/1970 0:00h, UTC. If you want to search the files manually, it is advisable to convert the time by using "Download with normal time".

12.1.2. Analysis

If activated, the proxy log files are analyzed on a monthly basis and displayed as statistics. The current month is always updated on the hour. This statistics are available under Information > Statistics > Proxy.

The statistics can be filtered by web pages, clients or users by using the drop-down menu above. Displaying user logins only makes sense if the proxy is used with authentication.

By default, the rows are sorted by access time. They can be rearranged and sorted by the other values displayed by using the header line.

The statistics can be further narrowed down to individual clients, web pages or days from the overview of web pages, clients and users. This can be done by clicking on the initially displayed column.

By clicking the arrow symbol beside each web page, it can be opened in the browser and its contents can be examined. If a page is to be blocked in the future, it can be marked with the checkbox in the last column and directly added to a URL-blacklist by clicking the button below.

Many websites load their content from different sources, be it text or banner advertising. Hence, there will be servers like google-analytics.com, doubleclick.net etc. in the "Top 50 websites" evaluation, which were loaded passively on websites. This content was not actively visited by a user.

12.1.3. Methodology

The following describes how each access is compiled and converted into the displayed values.

In order to provide an overview, the statistics only stores a shortened name of the visited web address. for example both "http://www.web.com/shopping/" and "web.com/mail/" would become "web.com".

Most web pages consist not only of text formatted in HTML, but also of graphics, flash animations etc. In order to get a meaningful figure for the number of web pages visited,

only the calls for which one of the following data types was transmitted are counted as the number displayed under page accesses:

- text/html
- text/plain
- text/javascript

After retrieving a web page, there is unfortunately no way for the proxy to determine for how long the page has actually been read. Therefore, the proxy statistics can only roughly calculate the duration.

For each first visit to a website, a 60-second retention period is used. If there is another access to the same server within this minute, the time interval is added to the last access period. If the interval between two accesses is more than 60 seconds, the original 60 seconds are reapplied. For the retention period, only calls of data types that are also counted as page accesses are counted (see above).

With period overviews, the number of page views in an hour is summarized and the displayed box becomes darker as more hits have occurred in this hour.

If access to a web page is blocked by a proxy filter mechanism, the access is still logged and evaluated as a normal access. A separate evaluation based on allowed and blocked access is not possible.

12.2. Internet Access Statistics

These statistics can be used to monitor the transmission volume and online time for individual Internet providers as well as the clients connected to the Intra2net system.

For the data of the provider statistics, the effectively transmitted IP data volume (without encapsulation e.g. in PPPoE) and the time that the Intra2net system was online are used. These numbers should match what your provider charges you.

Internet access statistics are updated every 15 minutes; the time of the last update is shown below.

The individual statistics pages such as the monthly statistics of all clients can be exported as a CSV file and then imported into a spreadsheet program for further analysis.

12.2.1. Methodology

The transmission volume of clients is counted as packets that go to the Internet or the proxy server of the Intra2net system. Should the proxy retrieve web pages of an intranet server, these accesses can distort the statistics. If a client sends data into a VPN tunnel, the unencrypted data volume is counted. The data added by encryption, authentication and encapsulation are not included in the calculation.

Email transfers are not included in the transfer volume of a client.

The online time of a client is the time in which a data transfer counted as the transfer volume takes place. If there is a time span between two data transfers that is shorter than the timeout, this time span is also counted as online time. The timeout corresponds to

the connection timeout of the provider set or, if the timeout is switched off, 300 seconds

12.3. Speedometer

This statistic provides a live overview of the traffic on the system, broken down by the clients from which the connections originate.

The speedometer is determined by the connections and data transfers of the last sixty seconds. A continuous average is generated from the transfer volume of the clients during this period. The values of the received and sent bytes, as well as their total are listed in a separate table column. In a further column, the incoming and outgoing volume is also displayed as a bar chart. If a client is registered on the system with a profile or can be uniquely assigned to a defined network range or VPN, the name determined for this purpose is displayed. Clients unknown to the system are shown as their IP address.

The data representation is divided into three tables. In the "Internal Clients" list, clients that have established connections to the Internet or proxy from the intranet via the Intra2net system are listed. Under "External Clients" the data traffic between the Intra2net system and clients on the Internet can be tracked. This includes, for example, data requests from the proxy server and VPN connections. The third table, "Overview", summarizes the traffic in the categories Internal, External and Proxy.

12.3.1. Methodology

As soon as the speedometer page is opened under Information > Statistics > Speedometer, the system starts collecting data on IP connections. Therefore, it takes up to 10 seconds to display data on opening the menu. These are displayed in the tables of the internal and external hosts, depending on their origin.

A connection is considered to be *internal* if it starts from a client whose IP address can be assigned to a local address range and the target address is not also local. Otherwise it is considered *external*. This distinction determines the table in which a connection is listed.

The displayed data transmission rates correspond to the running average of the last minute of traffic. These averages are recalculated every ten seconds for each client. Connections for which no traffic is registered for at least one minute are considered inactive and will no longer be tracked. Clients without active connections are removed from the statistics after the connection information has been added to the Internet statistics database. For reasons of efficiency, this does not always happen immediately after the last connection of a client expires, so clients without active connections may remain on the speedometer overview for a certain time.

Connections are classified according to different properties: whether they are external connections and whether the target of the connection is the system's proxy server. The total volume of data for these traffic categories is summarized in a separate table on the overview page. The values on this table refer solely to active connections and do not always reflect the actual bandwidth usage of the WAN uplink. For example, if data traffic is routed through a VPN, there are at least two active connections: one for the tunnel to the peer and one for the data transported over it. Both connections are recorded in the connection overview: The IPsec tunnel built by the Intra2net system is assigned to the external table, the actual connection to the internal. Such overlapping effects can sometimes give the impression that the value specified in the "total" line exceeds the maximum

connection amount. The actual incoming and outgoing traffic can be viewed on the Internet speedometer on the main page.

12.3.2. Sites

The speedometer features are divided into three levels. In addition to the main page, which provides an overview of clients from which data traffic originates, a list of existing connections can be displayed for each client, and in a further step, you can have them filtered according to various criteria.

12.3.2.1. Clients

The main page of the Internet speedometer lists clients from which active connections are originating.

The data is displayed in columns. From left to right:

- The *sequential number* of the entry in the respective table;
- the *IP address* of a client and, if applicable, the internal name of a known client, network range or VPN;
- the *average values* for the volume received and sent in the recording interval and their sum;
- a representation of the incoming and outgoing data traffic as a *Bar chart*.

Above the tables there are two control elements on the main page. A drop-down menu can be used to increase or decrease the number of displayed clients. Using the "Reset" button, you can discard the data currently being recorded and start recording again. The data already registered by the system has been transferred to the statistics database beforehand.

12.3.2.2. Connections

Clicking a client on the main page takes you to its connection table. This gives an overview of the connections that are currently considered active and have been established by the selected client. The available data is presented in nine columns:

- The *sequential number* of the entry in the respective table;
- the *IP address* of the target host;
- the *IP protocol* used for the connection;
- the *target port* and, if applicable, the classification as traffic to the proxy or the service registered with this port (the actually used service can of course deviate from it);
- the *direction* from which the connection was established, i.e. whether it is an incoming, outgoing, external or internal connection;
- the *average values* for volume received and sent at the point of collection, and their sum;

- a representation of the incoming and outgoing data traffic on the given connection as a *bar chart*.

12.3.2.3. Filter

By clicking one of the shown elements on the connection table, you can restrict the connection selection. This takes you to the filter display, in which only connections that match the selected criteria are shown. You can select the IP address of the target client, the transport protocol, the target port, and the connection direction as possible criteria.

12.3.3. Data Privacy

For reasons of data privacy, not all logged connection data is also displayed in traffic tracking.

12.3.3.1. Password Protection

If a data privacy password has been set up for the system, this can also be used to protect the Internet speedometer from unauthorized access, under Information > Data Privacy. The password is always requested when the detailed view of a client is requested: The speedometer main page, on which internal and external clients are shown, can still be viewed by users with administrator rights even if the data privacy password is active.

12.3.3.2. Address Masking

The target addresses of outgoing connections are provided by the system exclusively in a disguised form. The same applies to external system traffic to the ports of HTTP and HTTPS, which usually indicate requests served by the proxy. This mechanism is always active and cannot be bypassed by entering the data privacy password. Specifically, obfuscation means that the lower sixteen bits of the IPv4 address of the target host are ignored. In the web interface the hidden fields are marked with "x". The purpose of this measure is to protect the privacy of users on the intranet while at the same time providing the information necessary for diagnosing data traffic.

12.4. Space Usage Statistics

Information > Statistics > Diskspace displays how the system's individual partitions are working to capacity and have been in the past. The system partition should be working at a relatively constant to slightly increasing load. In normal operation, only a fraction of the capacity of the spool and log partition should be used.

If you notice a high usage of the partition for email, cache and backup and suspect a high volume of emails, you can use user statistics to find out which user is occupying how much space with their emails.

12.5. Data Privacy

In particular, the analysis of the proxy log files allows a precise monitoring of web browsing behavior of individual employees. In many cases such a detailed evaluation conflicts with data privacy standards. The Information > Data privacy page allows you to restrict access to individual critical functions according to the principle of dual control.

Only a particularly authorized employee (e.g. representative of the works council) receives a data privacy password for this purpose. Certain evaluations and the deactivation of the

data privacy password can only be performed if an administrator is logged in and the data privacy password has been entered. If the authorised employee is not assigned administrator rights for their regular user account, it is ensured that only the administrator and the authorised employee can access the statistics together.

The difference between "full access" and access to the proxy statistics without a data privacy password is that the statistics of individual clients and users can only be viewed with full access. Otherwise, only the top 50 web pages are visible, and the accesses cannot be assigned to individual users.

13. Chapter - Usermanager

The Usermanager manages all users, user settings (such as email addresses and forwarding) as well as all access rights (e.g. for administration, proxy, etc.).

For the users themselves only their settings are recorded, the access rights are managed exclusively by the user groups.

13.1. User Groups

Each user receives their access rights from the user groups of which they are a member. A user can be a member of any number of groups.



Tip

A mailing list can be created for a group under Services > Email > Mailinglist. For example, it would be convenient to send an email to all employees by using `<everyone@net.lan>`.

There are 2 special user groups: The administrator group, which has full access rights and is the only one allowed to access the console.

Secondly, the everyone group. All users are members of this group.



Caution

All access rights granted to the "everyone" group are accessible without login and password. So even a guest can access and edit these pages without any additional login.

13.1.1. Access Rights

All rights allowed in any one group of a user are allowed for the user.

Proxy profiles combine all profiles from a user's groups in such a way that all pages allowed in at least one group are allowed for the user. For more information on proxy profiles, see Section 11.4, „URL Filter“.

If the email attachment filter is enabled, incoming emails can be processed using the group with different filter lists. If a user is a member of multiple groups with different filter lists, the filter lists are merged. whitelists have priority over blacklists. For more information about the email attachment filter, see Section 14.7.3, „Attachment Filter“.

Since all users are automatically members of the "everyone" group, the rights of the "everyone" group are effectively the minimum rights that can be assigned to users.

Email quota is the maximum amount of storage space that the group members' mailboxes are allowed to occupy individually (not all members together). If the limit is reached, no new emails will be accepted (error message "450 Over Quota" will be sent to the sender after the email queue time has elapsed). Most IMAP email clients display a warning if they are 90% full. If the user is a member of more than one group, the largest quota from their user groups applies.

With the "SMTP authentication and email relaying" option, it is possible to control whether members of the group can log in to the Intra2net system to send emails to ex-

ternal recipients (SMTP authentication). Note that the members of a group with email relaying from the Internet absolutely require high quality passwords. Otherwise the password can be guessed automatically and the Intra2net system could be misused to send spam.

13.1.2. Administration Rights

Under Usermanager > Groups : Administration Rights, on the lower part of the screen, access to each individual page of the interface can be regulated. In the upper part it can be set whether the rights set below should also be used over the Internet (remote administration) or whether only access to web groupware should be possible.

It is also possible to specify whether setting up and disconnecting Internet and VPN connections is permitted or not.

If the main page is to be hidden without logging in, simply deny access to the "Main Page" right for the "Everyone" Group.

13.2. User

If a user is deactivated, they will no longer be able to log in and new emails will no longer be stored (error message: Over Quota). However, email forwarding is still active. We recommend using this option, for example, for employees who have left the company but may still be likely to receive important emails.

Every user can change their password and email settings on the sub-pages of Usermanager > own profile if their access rights allow it.

All passwords are automatically checked for their quality. Various algorithms for pattern recognition and lexicons are used. The user is warned if the password has a low security level. If a password falls below a minimum quality, it is rejected.

13.2.1. Settings for Email and Groupware

Using the tabs in the Usermanager > Users menu, it is possible to make user-specific settings for the email system. These are described in Section 14.5, „Email Addressing“, Section 14.6, „Email Processing“ and Section 14.7.1.5, „User-Dependent Spamfilter“.

On the Usermanager > Users : Groupware tab, it is possible to define the default folders for the user. For each user, the default email folders (drafts, sent emails, trash) are automatically created by the system. The default groupware folders, on the other hand, are only created when the groupware is first used by this user. The names of the default folders can be retrieved by email clients via the XLIST protocol extension. They are also used by the Webgroupware and ActiveSync.

The settings for webmail are explained in Section 32.2.2, „Append Signatures“, the settings for ActiveSync in Section 34.3.3, „Manage and Resynchronize Devices“.

13.3. Import/export of User Profiles

For a large number of users it can be helpful to create a file externally and then transfer it to the Intra2net system. This can be done easily with the import/export feature. XML files or CSV files (Comma Separated Values) are accepted.

13.3.1. Importing Users

Upload an XML or CSV file containing users for import. The field names of the XML import can be found in the DTD, which can be downloaded from the import/export online help. The structure of the CSV format can be found in a previously exported CSV file.



Hint

Please note that the names of the specified groups must be exactly the same as the names of the groups in the system. The same applies to the detection of email domains.

13.3.2. Exporting Users

Select the users for export, either as XML or CSV format. The field names of the XML export can be found in the DTD. The CSV format can be found in the CSV file.

14. Chapter - Email

14.1. Email Relay

14.1.1. Rights

The Intra2net system includes an SMTP server for sending emails. All network objects (e.g. networks, clients, VPNs,...) with the right "Email relaying allowed" (see Section 8.3, „Access Rights of a Network Object“) and firewall settings that allow access to the SMTP port can use the Intra2net system to send emails over the Internet (relayer) without further authentication.

From local networks without the right "Email relaying allowed" and the Internet it is still permitted after authentication with an active account from the Usermanager (see Section 13.2, „User“) and corresponding rights (see Section 13.1.1, „Access Rights“).

Sending emails to local addresses on Intra2net systems is not relaying and is possible from all networks which the firewall allows access to the SMTP port.

14.1.2. SMTP-Submission

To minimize spam, some ISPs do not allow their customers to connect directly to TCP port 25 (SMTP). This would mean that it would no longer be possible to use the Intra2net system to send emails from anywhere. For this reason, the Intra2net system supports SMTP submissions on TCP port 587.

Simply switch your mobile email client from port 25 to port 587 and enable authentication with your user name on the Intra2net system. You should also enable encryption using TLS (in some programs wrongly referred to as SSL).

14.1.3. Dispatch Methods

Emails sent to the Internet can either be sent directly to the target server or to an SMTP relay server, which then handles further transmission. Relay servers support virtually all website providers, but also some access providers.

To reduce spam, most email servers no longer accept direct emails from IPs used for dial-up or DSL. We therefore strongly encourage the use of a relay server.



Hint

The sending and receiving paths of emails are independent of each other. This means that you can easily receive emails directly via SMTP, for example, while using a relay server for sending them.

14.1.4. Dispatch via relay server

Email relay servers are stored as a relay profiles under Services > Email > Relay.

Almost all relay servers require authentication using login and password via SMTP-AUTH. The old method of SMTP after POP is nowadays rarely used and should be switched to SMTP-AUTH if possible.

14.1.5. Direct Dispatch

Many email providers use rather aggressive methods to reduce the amount of spam they receive. Therefore, the configuration and connectivity of email servers is tested before any email is accepted. In most cases it is recommended to use a relay server (see previous chapter).

If you want to send emails directly, you must first meet the following criteria:

- Static IP address assigned by the Provider.
- DNS reverse resolution (reverse lookup, PTR entry) must be possible for the IP and correspond exactly to the external email server name of the Intra2net system. This is specified under Services > Email > Settings. If you want to use or change reverse resolution, contact your access provider, they must configure this for you. Under System > Diagnosis > DNS you can enter your external IP address and check how the DNS reverse resolution is set.
- The external email server name set under Services > Email > Settings must be resolvable via DNS (forward resolution, A entry) and point to the external IP of the Intra2net system. To create this DNS entry, contact your web space or domain provider.
- The assigned IP address should be registered to the customer and not the provider. This can be checked using RIPE at <http://www.ripe.net/>.

14.1.6. Choosing the dispatch method

Normally, all emails are sent using the same method and configuration. This is configured in the Services > Email > Relay menu in the "Default" profile. If required, different sending methods can be used based either on the currently active Internet provider or on the sender address of an email.

A sending method that is dependent on the currently active Internet provider is particularly useful if the emails are to be sent directly by the primary provider, but with a fallback provider this is not possible because of the external IP address used, for example.

In this case, create a new profile of the type "Provider" under Services > EMail > Relay. Under Network > Provider > Profiles : Services, these profiles can then be selected for all Internet providers that are not to use the default sending method.

A relay profile dependent on the sender address of an email is particularly necessary if emails are to be sent via relay servers, but none of the relay servers in question allows emails to be sent with arbitrary sender addresses. In this case, several relay servers or different logins on the same relay server can be selected to match the sender domain or individual sender address.

In this case, under Services > Email > Relay, create a new profile of the type "Sender" and select the appropriate sender address or sender domain.

For the sender domain type, the domains must always be specified in full. Subdomains are not automatically treated like a superordinate domain, separate profiles must be created for them.

The priority of the relay profiles is as follows:

1. Single sender address
2. Sender domain
3. The relay profile assigned to the currently active provider

14.2. Receiving emails on the client (POP or IMAP)

Each user automatically receives an email account with their name on the Intra2net system. This account can be accessed via POP3 and IMAP4, no extra configuration is necessary on the Intra2net system.

We recommend using the IMAP protocol to transfer emails from the Intra2net system to the client, as IMAP offers the following advantages:

- All emails (including emails stored in folders) are made centrally accessible. They are also accessible via webmail, notebook or smartphone.
- The IMAP protocol allows you to download just parts of an email. For example, when checking for important emails via a mobile network, it's not necessary to download large attachments in order to see the email contents.
- Multiple users can access one account at the same time. Therefore, in the case of shared accounts (such as info or sales) there is no chance of multiple employees answering one email.
- Through the IMAP rights management, it is possible to give other users certain rights (e.g. read-only rights) for individual folders. For example this can be helpful for the secretarial office or a holiday substitute.
- Emails on the Intra2net system are automatically included in the backup and are thus never lost due to a malfunctioning computer.
- All emails are on the server, therefore a crashed email program or switching to another program will never result in a loss of emails.

The Intra2net system internally uses the Cyrus mail server. It was developed by Carnegie Mellon University and is used for the management of multiple 10,000 email accounts. Larger folder structures or folders with 100,000 emails can be supported without complications.



Hint

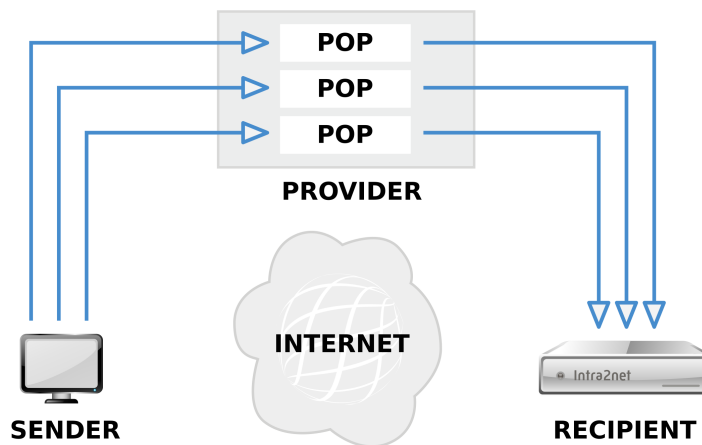
When using POP3, we strongly advise against activating the "Leave emails on the server for *n* days" option in the email client, because the POP3 protocol lacks the functionality required for reliable operation. Please use IMAP instead.

14.3. Receive emails using the Intra2net system

14.3.1. Methods

There are 3 different methods for receiving incoming emails using the Intra2net system.

14.3.1.1. Retrieving individual POP accounts



A POP mailbox is created for each email address of a provider. The Intra2net system collects each of these mailboxes separately and delivers the contents to the recipient.

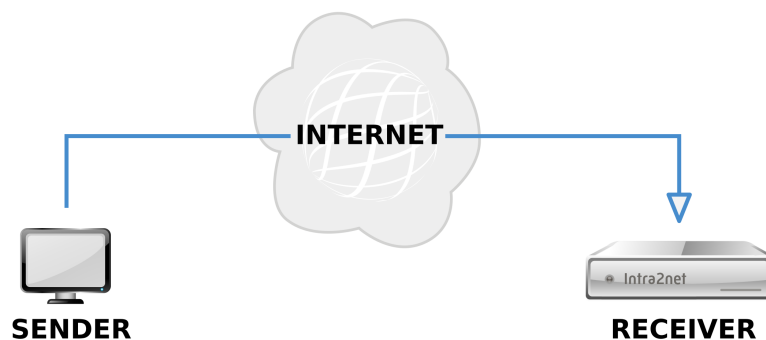
Advantages:

- Available with almost all providers
- No undeliverable emails (bounces) as the provider knows all valid addresses

Disadvantages:

- Many accounts may require more administrative workload
- Accounts are processed sequentially. With a large number of accounts, more time is required for processing

14.3.1.2. Direct delivery via SMTP



The sender can send emails directly to the Intra2net system without any intermediary provider.

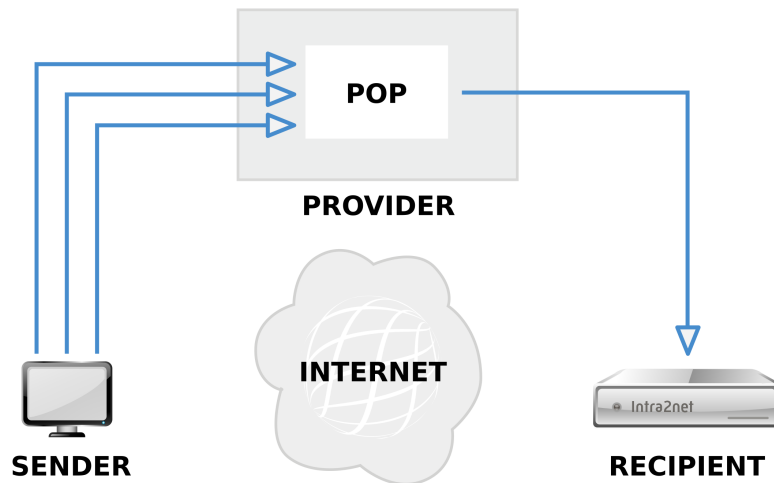
Advantages:

- New emails arrive immediately
- No undeliverable emails (bounces)

Disadvantages:

- A static assigned IP address is required

14.3.1.3. Retrieval of collective POP accounts (multidrop, catch-all)



All emails for a domain are collected by a provider in a single POP account. The Intra2net system accesses this account and distributes the emails to the appropriate recipients.

Advantages:

- Reduced administration effort, as only one account has to be maintained by the provider.

Disadvantages:

- No standard for multidrop header line
- It works correctly with only a few providers (multiple recipients in one domain, BCC,...)
- Undeliverable emails (bounces) cannot be avoided

14.3.1.4. Recommendation

We recommend that up to a maximum of 15 users access individual POP accounts. If there are more users, direct delivery via SMTP would be the appropriate option.

We do not recommend using POP collective accounts (multidrop, catch-all).

14.3.2. Retrieving individual POP accounts

If emails are to be fetched from a single POP3 account with a provider, this can be configured under Services > Email > Polling. You can enter any number of external accounts for a given user.

Under "Encryption" you can set the extent of encryption for the connection to the server. With some poorly configured servers, automatic encryption detection causes connection setup problems. The "None" mode is meant only for this purpose.

14.3.3. Direct delivery via SMTP

If you have a static IP, it is possible to send emails directly from the sender to the Intra2net system. To do this, you must have your static IP registered as MX (*MaileXchange*) in the domain by your domain provider (usually the one who is also responsible for the website). You must also open the SMTP port in the firewall (see Section 39.3, „Provider profile“).

The direct delivery of incoming emails via SMTP is completely independent of the sending of emails. The strict criteria for direct email dispatch from Section 14.1.5, „Direct Dispatch“ are not relevant here and sending via a relay server is easily possible.



Caution

Do not use the Intra2net system with dynamic IPs and DynDNS for direct SMTP reception, even if some DynDNS providers offer this. If an IP address change or line fault occurs, third parties could be able to receive your emails.

14.3.4. Retrieval of collective POP accounts (multidrop)

The Intra2net system can retrieve emails for a domain via multidrop from a POP3 account and then distribute them.



Caution

Because of the serious disadvantages (see above) Intra2net does not recommend the use of this method!

The Provider must offer the capability of storing all emails for a domain in one account or of setting up a "catch-all" account to which all emails with unknown recipients can be sent.

Additionally, a multidrop header is required for distribution, which the mail server of the provider must include in the email header. The real recipient (Envelope / RCPT-To) of the email is saved here.

However, there are different types of multidrop headers:

Normal Header	It is called X-Envelope-To:, Envelope-to:, X-Original-To: or X-RCPT-To: and contains only the recipient's email address. This type is mainly offered by Exim Software. Enter the header name (with a colon) in the "Multidrop Header" field.
Qvirtual	It is called Delivered-To: and is mainly used by Qmail. It contains a domain identifier before the actual recipient address. Enter the domain name in the "Multidrop Header" field. Examples are "mbx-yourdomain.com" or "yourdomain.com-"
Received	The email does not contain a multidrop header. The Intra2net system tries to determine the recipient address from the received information in the header. This can cause problems for some providers. Some emails are then sent to the postmaster (see Section 14.12, "Additional Settings"). This option is therefore only intended as an emergency solution in case a provider does not transfer a multidrop header.



Tip

If the provider is not able to reliably insert envelope headers, it is advisable to set up a domain for a different provider (e.g. 1&1) for just a few euros per month (e.g. "mycompany-mail.com"). The previous provider can then forward all emails to the new domain 1:1.

Example 14.1. Sample excerpt from an email header with a normal envelope header

```
Received: from localhost (localhost.localdomain [127.0.0.1])
  by fire.local (8.11.6/8.11.6) with ESMTP id g3SMO2D10977
  for <gerd@localhost>; Wed, 29 Apr 2015 00:24:02 +0200
Envelope-to: gerd@klickmich.de
Delivery-date: Tue, 28 Apr 2015 21:22:01 +0200
Received: from pop.kundenserver.de [212.227.126.129]
  by localhost with POP3 (fetchmail-5.9.0)
  for gerd@localhost (single-drop); Wed, 29 Apr 2015 00:24:02 +0200 (CEST)
Received: from [4.43.46.11] (helo=intra.net.lan)
  by mxng00.kundenserver.de with smtp (Exim 3.22 #2)
  id 17luF3-0007Sd-00
  for gerd@klickmich.de; Sun, 28 Apr 2015 21:21:50 +0200
Message-Id: <j60jo.a5626@intra.net.lan>
To: gerd@klickmich.de
Subject: Test
```

A simple "To:" is not a multidrop header!

Example 14.2. Sample excerpt from an email header with Qvirtual header

```
Return-Path: <k.schuster@irgendwo.de>
Delivered-To: klickmich.de-m.muster@klickmich.de
Received: (qmail 29628 invoked from network); 30 Jun 2015 14:47:38 -0000
Received: from moutng1.kundenserver.de (212.227.126.171)
  by pluto.link-m.de with SMTP; 30 Jun 2015 14:47:39 -0000
Received: from [212.227.126.162] (helo=mrelayng1.schlund.de)
  by moutng1.kundenserver.de with esmtp (Exim 3.22 #2)
  id 17OfzF-0003jP-00
  for m.muster@klickmich.de; Tue, 30 Jun 2015 16:47:37 +0200
Received: from [217.81.153.239] (helo=intra.net.lan)
  by mrelayng1.schlund.de with asmtip (Exim 3.35 #1)
  id 17OfzF-0002Mf-00
  for m.muster@klickmich.de; Tue, 30 Jun 2015 16:47:37 +0200
Received: from storm (storm.net.local [172.16.1.2])
  by intra.net.lan (8.11.6/8.11.6) with SMTP id g5UElmd25862
  for <m.muster@klickmich.de> Tue, 30 Jun 2015 16:47:48 +0200
Message-ID: <001d01c22045$12856700$020110ac@storm>
From: "Karl Schuster" <k.schuster@irgendwo.de>
To: <m.muster@klickmich.de>
Subject: Beispiel
```

The "Delivered-To:" header is of interest here. In this example, the domain name is "klickmich.de". Enter these in the "Multidrop Header" field in the Intra2net system.

If the multidrop header is not set correctly, all emails where the real recipient is not set to To: will be sent to the postmaster. These include e.g. emails with BCC:, forwarded emails, emails from mailing lists or spam.

14.4. Forwarding of entire domains

14.4.1. Method

For each domain, it is possible to forward emails to another mail or groupware server (e.g. Microsoft Exchange or Lotus Domino) and not to users of the Intra2net system. This forwarding is done after virus scanning, banned attachments and the global spam filter.

Forwarding can be configured for each domain under Services > Email > Domains : Forwarding.

It is possible to change the destination domain of the forwarded emails. For example, if you receive the domain **example.com** on the Intra2net system and specify "Domain address change" as **xyz.com**, the target addresses in all forwarded emails will be changed to ...@xyz.com. This is especially useful if you do not want to reconfigure a destination server.

14.4.2. Recipient Address Check

If an email cannot be delivered, the sender must be informed of this with a non-delivery message (*Bounce*). Of course, this also applies if the destination domain exists, but not the user. If spammers send a lot of emails to invalid recipients in a short time, this mechanism can result in 2 problems:

- Each of these non-delivery messages must be delivered to the sender which results in additional load. Furthermore, many spam addresses are wrong and as a result a further non-delivery message (*Double-Bounce*) is generated from the other side, which increases the load further.
- Some recipients consider non-delivery responses to emails that do not originate from themselves as spam. If there are too many of them in a short time, it can happen that the IP of the Intra2net system is added to a spam blacklist. As a result, many normal emails would no longer be delivered or end up in a recipient's spam folder.

These problems can be solved by preventing the Intra2net system from accepting emails with invalid recipients. In this case, the sending server is responsible for generating the non-delivery message, or in the case of a spam server, none at all.

If a domain is assigned to the Intra2net system, the system recognizes all valid recipient addresses and rejects invalid addresses immediately before receipt. No special configuration is required, as this is done automatically.

If, on the other hand, a domain is given to another server, only this server knows the valid addresses. In order to enable the Intra2net system to reject emails on receipt, there are two procedures described below.

14.4.2.1. Receiver address check via SMTP requests

Before an email is accepted, the Intra2net system asks the receiving server whether the address is valid. For the check, an SMTP connection to the target server is established and the target address is checked with the `RCPT TO:` command.

It is important that the receiving server responds in case of an invalid address with an error code in the range of 500 (e.g. `550 Recipient address rejected: User unknown`).

Many servers in the default configuration accept the address first and then send a non-delivery message later. For some servers, direct rejection can be activated by changing the settings. However, this is not possible with some server programs (such as Microsoft Exchange before version 2007). In this case, a recipient address check via SMTP cannot be used.

14.4.2.2. Recipient address check via Active Directory and LDAP

With this method, the Intra2net system regularly reads the list of all valid email addresses on an LDAP server (e.g. Active Directory). When an email is received, this list can be used to immediately determine whether the address is valid or not.

The Intra2net system requires a valid login on the LDAP server. The LDAP login (bind DN) is usually entered as a complete Distinguished Name (e.g. **CN=username, CN=user, DC=mycompany, DC=local**). However, many servers also accept a simple user login if it is located directly in the LDAP search base.

If you are using a standard domain without additional organizational elements or similar, you can enter the user login as an LDAP login for Microsoft Windows Server 2000 and 2003. For Microsoft Windows Server 2008, enter the user's first name and last name separated by a space. Both times the Intra2net system will automatically select the appropriate Distinguished Name.



Caution

We strongly advise against using an account with administrative rights. The password has to be stored internally in plain text on the Intra2net system, which, in case of a successful attack on the Intra2net system, it could be used to compromise the LDAP server.

The LDAP search base is the starting point in searching for LDAP queries: A Distinguished Name (DN) of the root node of the subtree to be searched (e.g. **DC=mycompany, DC=local** for the active directory domain "mycompany.local").

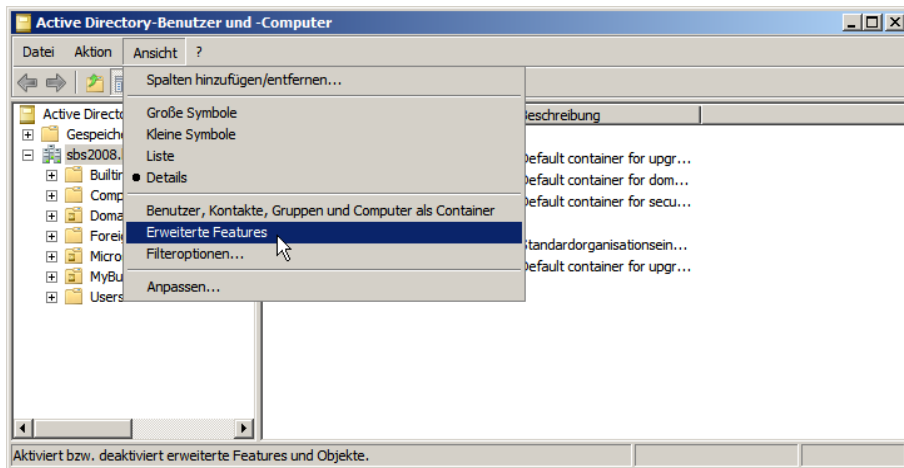
If the LDAP server is an Active Directory, set the structure to Active Directory. If it is an LDAP server with systems other than Active Directory, you have to specify a search filter (e.g. **(mail=*)**) and the name of the result attribute (e.g. **mail**).

Immediately after the recipient address check has been configured, the Intra2net system will attempt to read the data via LDAP. This must be regularly carried out. The interval for this is set under Services > Email > Automatic.

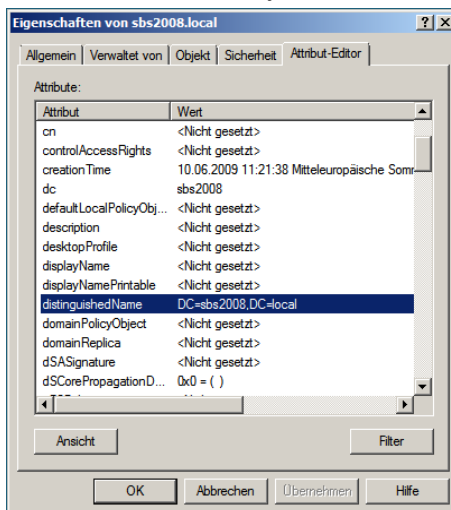
14.4.2.2.1. LDAP paths on Windows servers

If you have trouble finding the appropriate LDAP paths for your Windows server, the following describes how to access this data.

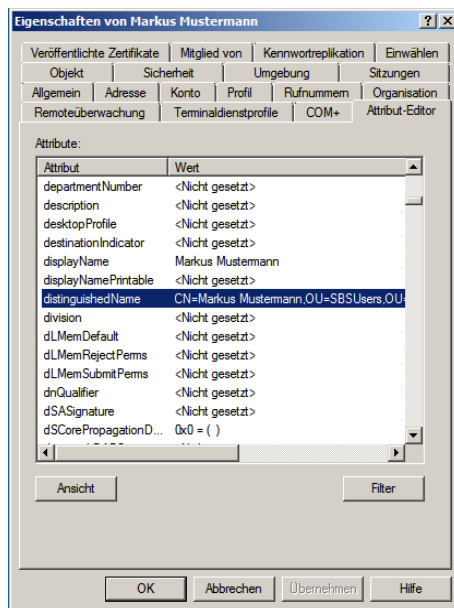
1. Open the management console for "Active Directory Users and Computers". You will normally find them under "Management".
2. In the menu "View" activate the option "Advanced Features".



3. Right click the domain and open the "Properties" dialog.
4. In the "Attribute Editor" tab, you will find the "distinguishedName" attribute. Enter this in the Intra2net system as the LDAP search basis.



5. Close the domain's property view and locate the path of the user you want to use to retrieve the data.
6. Right click the user and open the "Properties" dialog.
7. In the "Attribute Editor" tab, you will find the "distinguishedName" attribute. Enter this in the Intra2net system as an LDAP login.



14.4.3. Forwarding of individual POP accounts

If you want to retrieve individual POP accounts and then forward the emails directly to another server, proceed as follows: Set up the retrieval as described under Section 14.3.2, „Retrieving individual POP accounts“. Forward at least one domain to the appropriate destination server. If you are not already forwarding a domain, set up an internally valid domain for this purpose only (e.g. `net.1an`).

Under Services > Email > Polling, do not select a local user of the Intra2net system as recipient, but enter an email address in the forwarded domain. The emails from the POP account will then be delivered to the entered address on the target server after the usual filters (viruses, attachments, spam).

14.5. Email Addressing

14.5.1. Address Settings

Normally, all system users can be reached in one domain. This can be disabled under Services > Email > Domains : Settings. In doing so, only the addresses that are explicitly specified are valid within a domain.

It is also possible to specify that emails to unknown recipients in this domain are not blocked ("550 User unknown"), but forwarded to the postmaster.

14.5.2. Email Addresses and Aliases

Each user can be reached under their username in all domains where the "All system users valid" option is active. In addition, aliases with which the user can also be accessed can be set up for each user under Usermanager > User : Addresses.

The aliases, like normal names, can be valid for all domains or only for a specific domain. This makes it possible, for example, to forward the address "Info" for multiple domains to different users.

If an address is entered for "@local domains", this means that it is valid for all domains where the "All system users reachable" option is active.

It is also possible to enter aliases for external domains. This may be necessary for an automatic response (see Section 14.6.2, "Automatic Response"). In addition, emails to such addresses are delivered locally immediately and do not go through the provider. If no domains are used on a system, but only individual POP accounts, you can save the transfer of internal emails to the provider and back.

A complete name can be entered for each alias. This is used as the sender for webmail.

14.6. Email Processing

14.6.1. Forwarding

Under Usermanager > User : Forwarding, you can configure user-dependent email forwarding. With the "Email copy" option, the email is sent to the entered address(es) and additionally stored in the user's account. With the "Email redirection" option, the email is only forwarded and is no longer stored in the user's account.

If required, the email copy can be linked to the automatic response timer. To do this, set forwarding to "Send copies during vacation to" and configure a period of time under Usermanager > Users : Vacation.

If the email is to be forwarded to multiple recipients, enter their addresses separated by commas.



Caution

Never use "Email redirection" for a user who functions as postmaster, always use "Email copy". If there is a problem with sending emails, even the postmaster would not be able to receive emails. Emails can be lost. Since it is not possible to retrieve error notifications locally, troubleshooting may be considerably more difficult.

14.6.2. Automatic Response

Under Usermanager > Users : Vacation you can activate the automatic reply (Vacation Mode). Then each email is automatically answered with a specified response. To avoid an accidental email storm, a single response is usually sent to each recipient only once a day.

In order to prevent mailing lists or spam emails from being answered automatically, vacation mode only responds to emails in which a recipient address assigned to this user is entered in the To: - or Cc: header lines of the email.



Caution

You must therefore enter all externally accessible email addresses and email aliases of this user in the "Addresses" tab (particularly the external POP accounts). Otherwise, vacation mode cannot function.

The automatic reply can be activated and deactivated on a scheduled basis. If you enter a date for "from", the automatic response is activated on this day at the set hour. If you enter a date for "until", the automatic response will be deactivated on this day at the set

hour. You can also leave one of the date fields blank, in which case the automatic answer is active from now until the set time or from the set time until it is switched off again in this menu.

14.6.3. Sorting

Under Usermanager > Users : Sorting, you can create server-side sorting rules. Compared to sorting rules in the client program, they have the advantage that they are executed directly on receipt of the email and work reliably even without a running mail client.

You can create any number of sort rules. For each rule, an action (move to subfolder, forward, reject, delete) is defined. If one or all (adjustable) sorting criteria are fulfilled by an email, the action is performed.

All email headers (e.g. recipient, sender, subject) can be used as criteria for sorting. Any number of criteria can be combined for a rule.

14.6.4. Automatic deletion

Under Usermanager > User : Groupware you can set times after which emails are automatically deleted.

On the one hand, emails can be automatically deleted from the recycle bin. This option is active by default when creating new users and is set to 30 days.

On the other hand, emails in all folders of a user can be deleted after a configurable time. This is particularly interesting for the implementation of data protection specifications. This deletion only affects folders with emails, groupware data is not automatically deleted.

Only the date of receipt of the email (IMAP INTERNALDATE) is used to calculate the deletion time, not the date set by the sender ("Date:" header line) or the moment when an email was moved to a new folder. For emails imported from other systems, it is therefore important that the date of receipt has also been imported correctly.

The deletion is automatically performed daily at night. This means that deletion does not usually begin immediately after the setting has been saved.

14.7. Emailfilter

14.7.1. Spamfilter

14.7.1.1. SMTP Filtering

If you receive your emails directly via SMTP, as a first step in spam filtering, you can have emails from known spam addresses rejected immediately before they are accepted. This reduces the load on the system and avoids unnecessary data transfer.

If the "Check IPs via DNS at SMTP level" option in the menu under Services > Emailfilter > Spam > Settings is active, the IP of each server that wants to deliver emails directly via SMTP is checked using DNS. Multiple block lists are queried. If the IP is listed on multiple block lists at the same time as a spam sender, the email is rejected by the server.

If the IP of the sending server is only present on a few or no block lists, the email is accepted and checked by the next level of the spam filter.

14.7.1.2. Flagging

The Intra2net system contains a multi-level spam filter. An email is categorized both by spam-typical criteria (special words, many exclamation marks, invalid sender addresses, etc.) and by a bayesian word filter. The bayesian word filter can calculate spam probability by comparing word combinations with a pre-trained word base.

In addition, DNS-based network tests can be performed. It checks whether the email addresses and URLs contained in the email appear in different blacklists. Since this check is also performed for each internal email, you should only activate this option if your Internet connection is not charged by time or dial-up attempt.

Additionally, the Intra2net system can also check emails using the Razor network. The Razor Network is an association of email recipients. In the Razor network, spam emails are manually marked as spam. This information is then distributed via the Razor network. The more people classify an email as spam, the faster it is filtered out.

If the spam filter is activated (under Services > Emailfilter > Spam > Settings), a spam score is determined for each email and stored in a special email header. However, this does not delete or move an email. The score is stored in the header "X-Spam-Level:". It is calculated by $(\text{spam points} + 100) * 10$, which means that the value is always positive and an integer, which makes it possible to compare it in most other programs. In addition, a detailed description of why an email is spam or not is stored in the "X-Spam-Status:" header.

14.7.1.3. Thresholds

The higher the spam score, the more likely it is to be spam. Values lower than 4 are typically indicative of non-spam emails. With values between 5 and 8, the probability of spam is higher, but there is still a risk of it being a desirable email. With values of 8 and higher, the email is extremely likely to be spam.

The lower the threshold, the more emails are filtered out. At the same time, however, there is a greater risk that an important email will be sent to the spam folder.

In the Intra2net system, a distinction is typically made between three categories: desired email, potential spam and spam.

The potential spam is intended for emails that have clear spam characteristics but cannot be clearly classified as spam. It is advisable to check these emails regularly (e.g. weekly) manually.

Spam is an email that has been definitely identified as spam. These emails do not normally need to be checked manually. However, in the event of erroneous configurations it is still advisable not to delete these emails immediately but to keep them for a few days.

As a reasonable compromise, the thresholds 5 for potential spam and 8 for spam have proven to be appropriate for most cases.

14.7.1.4. Global Spamfilter

Under Services > Emailfilter > Spam > Global the global spam filter can be activated. It filters all received emails - regardless whether they go to a local user or get forwarded. Therefore, we recommend the Global Spam Filter especially in cases where emails are not permanently stored on the Intra2net system but forwarded to another server.

14.7.1.4.1. Actions

The following filter actions can be configured separately for spam and potential spam. This allows the two categories to be treated differently.

The "Modify email subject" option ensures that each affected email is preceded by "****SPAM****" or "****POTENTIAL SPAM****" in the subject line. This makes sense especially when emails are delivered normally.

With "normal delivery" the concerned emails continue their normal process and are not stopped or redirected. This is particularly useful in combination with changing the subject and a filter rule on the target server. The filter rule on the target server can then store the emails in an appropriate subfolder based on the subject.

The "redirect" option redirects the affected emails to a group address. If you are using an account on the Intra2net system, please make sure to activate the user-dependent spam filter and have the spam emails deleted automatically after some time. Otherwise, there is a risk that the spam account will grow indefinitely.

14.7.1.4.2. Quarantine

The spam quarantine stores detected spam emails, keeps them waiting for a specified time and then deletes them. If necessary, mis-identified emails can be released from quarantine and delivered normally.

The spam quarantine itself is available under Services > Emailfilter > Quarantine > Spam. It contains the detected spam emails of all recipients together. Therefore, it is normally only accessible to users with administrative rights. It can also be made accessible with a data protection password under Information > Data privacy, only using the 4-eye procedure.

The report function is available to give each recipient an overview of their filtered emails. When activated, each recipient will automatically receive an email with an overview of all filtered emails within the specified delivery times.

The report email contains a link under the data for each filtered email that can be used to release the relevant email from quarantine. The report emails are sorted by increasing likelihood of spam.



Hint

Since the report emails contain the subject lines of the filtered emails, it is possible that an additional spam filter installed on the destination server or client may incorrectly identify the report emails as spam.

If you use an additional spam filter it is recommended to enter the postmaster address of the Intra2net system (found under Services > Email > Settings) in your whitelist. The postmaster address of the Intra2net system is used for sending the reports.

14.7.1.5. User-Dependent Spamfilter

The user-dependent spam filter can be individually configured for each user on the Intra2net system. It is able to store detected spam emails in special IMAP subfolders belong-

ing to the user. We therefore recommend using the user-dependent spam filter in cases where the emails are to be finally stored on the Intra2net system.

If an email reaches a user who has activated the spam filter under Usermanager > Users : Spamfilter, the email is scanned. The user spam filter has a two-stage structure. There is a threshold value for potential spam emails as well as a threshold value for "real" spam. If the email has a spam point value greater than or equal to the entered threshold value, it is not deleted but placed in the IMAP subfolder "Potential Spam" or "Spam" belonging to the user. If desired, spam emails can also be forwarded to a central collection address.

Additionally, every user has the option to influence this by using a blacklist (all senders or recipients listed are always classified as spam) and whitelists (all senders or recipients listed are never classified as spam).

When a user accesses their emails via IMAP, the subfolders are directly visible. It may be necessary to reload the folder list in the email program and subscribe to the folders (subscribe). Spam emails remain on the server when accessed via POP3. The user should therefore regularly check the "potential spam" folder for incorrectly filtered messages via webmail.

14.7.1.6. Trusted Servers

In standard mode, the spam filter checks all received email headers to see if their IPs are included in DNS blacklists. In optimized mode, only the IP of the sender's last server is checked. This further increases the spam detection rate and reduces the potential for false positives. The currently used mode can be found under "Services > Emailfilter > Spam > Trusted servers".

In order to distinguish the IP of the last sending server from falsified data, the system needs to know which servers are trustworthy. An SMTP server is considered trusted if it can be assumed that it does not distort the received lines in the email header and truthfully inserts its own received record. One can normally assume that all servers configured for receiving and processing their own emails are trustworthy, since their operators are bound by contract.

The Intra2net system automatically tries to determine the trusted servers, using an adapted procedure for each email receiving method.

Trusted servers for direct SMTP and POP multidrop accounts: The Intra2net system automatically queries the servers responsible for receiving emails (MX record of the domain) for each configured domain via DNS. These servers are added to the list of trusted servers.

In the following cases, it may be necessary to adjust the list of Trusted Servers:

1. The emails are accepted by the server responsible for receiving the emails (MX record of the domain) and then forwarded to another server (e.g. for checking or caching) before they are sent to the Intra2net system. Here, the IPs or DNS names of all intermediate servers must be entered in the list of "Additional trusted servers".
2. The Intra2net system gets to see other data for its own domain via DNS in the local network than "outside" on the Internet. This configuration is usually called "split DNS". Here, the IPs of all externally responsible servers (MX record of the domain) must be entered in the list of "Additional Trusted Servers".

3. The emails for domain A are received by a server, rewritten to domain B and then forwarded to the Intra2net system or a server responsible for domain B. The Intra2net system only knows domain B. Here the original domain A must be included in the list of "trusted domains".

Trusted Servers for individual POP accounts: The Intra2net system automatically checks all email servers entered under Services > Email > Polling via DNS. These servers are treated as trusted. In addition, each server name is shortened to the second level domain, e.g. the server name "pop.1and1.de" is translated to the domain "1und1.de". The email servers responsible for this domain (MX entries) are queried and additionally saved as trusted servers.

In the following cases it may be necessary to adjust the list of Trusted Servers:

1. The provider uses different servers for their own emails from those of their customers. In this case, enter the domains of all email addresses used by you in the list of "Trusted Domains".
2. The emails are received by the provider on one server, e.g. forwarded to another server for checking and then again held ready for collection on another server. In this case, you must enter the IPs or DNS names of all intermediate servers used for checking in the list of "Additional trusted servers".
3. Emails are received from one domain and automatically forwarded to another domain. The Intra2net system then retrieves the forwarded emails. In this case, enter all original domains that are being forwarded into the list of "trusted domains".

Based on the last 1,000 spam emails, the Intra2net system is able to detect whether the list of trusted servers is correct. After this calibration, the spam filter switches to the optimized mode if possible. The calibration is checked hourly during operation.



Hint

After changing the trusted servers or domains, up to 1,000 spam messages are required before the spam filter automatically switches to the optimized mode.

14.7.2. Virus Scanner

Under Services > Emailfilter > Antivirus you can activate the email virus scanner. If it is activated, all emails passing through the Intra2net system (incoming, outgoing, forwarded, etc.) are checked for viruses.

If a virus has been found, it is quarantined under Services > Emailfilter > Quarantine > Virus and can be inspected by an administrator.

If a virus is found, warnings can be sent to the administrator and the recipient. Warnings are only sent to local recipients.

The virus scanner features cloud-based virus detection. Checksums are generated by executable files and sent to a data center. If the checksums are known to be malicious, the email is blocked. This significantly reduces the time between the first appearance of a virus and its detection. For data protection reasons, the data center receives only checksums and file names, not complete files.

In addition to viruses and Trojans, the virus scanner can also detect adware and spyware. Should such a detected program have utility, then detection can be switched off.

The virus scanner contains a component for detecting macro viruses using heuristic analysis. The detection level for heuristics can be adjusted. At higher detection levels, more macros can be recognized as a virus, but this also could result in an increased proportion of files wrongly detected as a virus.

14.7.3. Attachment Filter

Email attachments may contain new, unknown viruses. These must be delivered to a computer as an executable files before they can cause damage. The Intra2net system can scan email attachments and block particular file types. This will ensure that no executable file can reach a computer on the intranet via email.

The attachment filter examines attachments based on the file extension and MIME type. Additionally, it performs a type identification on the data actually contained within the email. Archives such as ZIP or RAR, as well as PDF are unpacked and scanned.

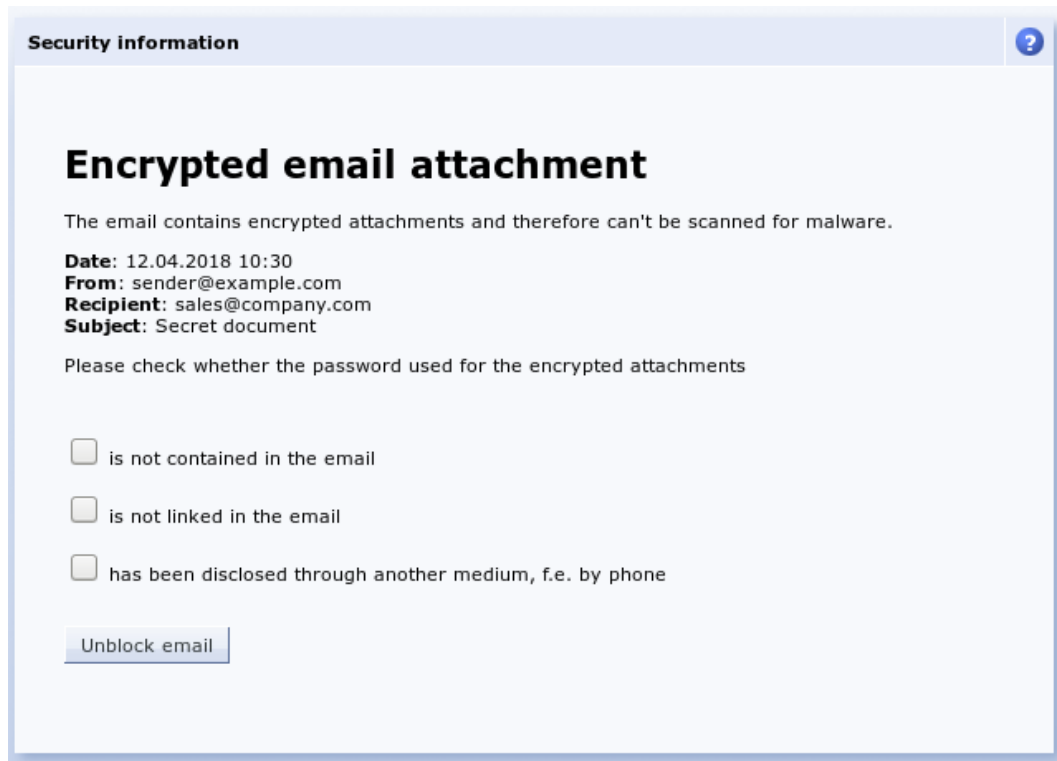
Under Services > Emailfilter > Attachment > Filter Lists, you can create filter lists for attachments. There is a distinction between whitelists and blacklists. Whitelists only allow known and approved attachments to pass through, whereas blacklists allow everything other than the listed entries to pass through.

14.7.3.1. Encrypted Attachments

Encrypted archives (protected with a password) cannot be scanned by the attachment filter. In practice, there are often viruses that are sent in encrypted archives and whose password is contained in the text of the email or an attached image. Therefore, it is generally recommended to filter out encrypted archives.

Some companies handle a significant proportion of communication with encrypted PDF files. In this case, it is possible to define exceptions for encrypted PDFs. These only apply to certain sender addresses defined in the corresponding field. Since the sender address of emails can easily be falsified and it has been observed in practice that, f.e. on infected systems of business partners, the email programs are systematically harvested by the attackers for email addresses communicating with each other, it is not recommended to let encrypted attachments pass completely unfiltered.

The recipient should always check emails with encrypted attachments to ensure that the used password is not contained or linked in the email itself, but has been previously established by the other communication partner using an alternative method such as telephone. To point out the necessity of this check to the receiver, it is possible to use "send hint with unblock link to recipient". Instead of the attachment, the recipient receives a link under which they must confirm the necessary checks and then release the attachment itself.



14.7.3.2. Office Macros

Because Office files can contain executable components (macros, VBA script, etc.), it is possible to scan Office files for such elements. By using the "by filter list" option, no specific Office file filtering is carried out, only the settings defined under "File extensions" will apply. By using the "with suspicious macros" option, Office files are opened and any existing macros are extracted and analyzed. If an Office file contains macros that fulfill multiple common malware criteria, the file is blocked. With the "with any macro" option, all Office files that contain macros are automatically filtered.

14.7.3.3. Standard Filterlist and Groups

There are predefined filter lists "All Permitted", "All Forbidden" and "Executable Files". Under Services > Emailfilter > Attachment > Settings you can define global settings for the attachment filter and the "Default filter list". The default setting is "Executable files". Outgoing emails and domain forwarding are also filtered through this default list.

Incoming emails use the filter list of the user groups. This can be assigned under Usermanager > Groups : Rights. By default, all user groups use the default filter list. If one user is a member of multiple groups with different filter lists, the filter lists are merged. Whitelists have priority over blacklists. This, for example, makes it possible to block all executable files, while still permitting them for the administrator group.

14.7.3.4. Unblocking

If an email is filtered, it is quarantined under Services > Emailfilter > Quarantine > Attachment and the administrator is notified. The email can easily be released or deleted later. Alternatively, it is possible for incoming emails to be delivered without the (potentially dangerous) attachment. The original email with attachment is still kept in quarantine and can be released if necessary.

Access to the quarantine can be allowed, as with any other menu item, under Usermanager > Groups : Administration rights for any user group, just like any other menu item.

14.8. DKIM

14.8.1. Basic principles

The SMTP protocol used to transport emails does not provide any way of verifying the sender address of an email. In principle, sender addresses can therefore be falsified and recipients cannot know who an email really comes from. This facilitates attempts at fraud, spam, phishing and the like.

DKIM was developed to be able to check whether an email really comes from the specified sender (`From:` header). The protocol provides for a check at domain level, so it is up to each sender domain itself to decide whether and which mechanisms it provides to prevent forgeries within the sender domain. As a recipient, you can therefore only rely on DKIM to ensure that the domain is correct, but not the address within the domain.

With DKIM, the sender's email server adds a digital signature to every email sent and inserts it in an additional header (`DKIM-Signature:`). At the same time, the public key used to create the signatures is published in the domain's DNS entry. Each recipient can now check whether the email has really been signed with the correct key. This works independently of the sender's server. The email can therefore be sent or forwarded via any server without affecting the verification.

In principle, each sender can decide for themselves whether or not to sign their emails with DKIM. This allows a gradual introduction. However, some recipients or their email service providers have decided to reject unsigned emails in general. This puts pressure on all senders to also sign their emails, as otherwise they will no longer be able to communicate with these recipients by email.

14.8.2. Implementation

With DKIM, the sender decides which parts of an email to sign and which not to sign. The list of parts contained in the signature is stored together with the signature in the `DKIM-Signature:` header and is not stored centrally in the DNS. This makes it possible to sign each email differently and, for example, to use a different configuration for some recipients.

The `From:` header must always be signed. However, it is strongly recommended that you also sign `Date:`, `Subject:`, `Reply-To:`, `Sender:`, all MIME headers, all content headers and the actual content of the email (*body*). This is because if an attacker gets hold of an email with a valid signature, they can change all unsigned parts without invalidating the signature. An email in which only `From:` is signed would then correspond to a blank cheque and should therefore be avoided. In the Intra2et system, several lists of headers to be signed are predefined in the menu "Services > Emailfilter > DKIM > Headers".

In addition to the list of signed parts, the `DKIM-Signature:` header also contains the so-called *selector*. The selector is the name of the public key entry in the DNS and can be freely selected. Based on the selector, the recipient knows where to get the key to verify the signature. Several selectors can be used simultaneously for one domain. This makes sense, for example, during a key rotation or when using several email servers.

14.8.3. Further standards

SPF: is an alternative standard for verifying the sender of an email. This involves storing a list of IP addresses in the DNS that are authorised to send emails for a domain. However, this leads to several problems:

- Emails can no longer be forwarded normally as the forwarding server is not on the list of authorised IPs. The Sender Rewriting Scheme (SRS) is provided as a workaround, but this only partially solves the problem and causes new problems.
- SPF only checks the *Envelope Sender* transmitted at SMTP level, not the `From:` header displayed by the recipient's email client. The *Envelope Sender* can only be viewed by the recipient via detours such as the source code display.

Intra2net advises against using SPF due to these disadvantages and recommends using DKIM.

DMARC: is a standard that the administrator of a domain can use to communicate that all emails sent legitimately from this domain must be signed with DKIM or fulfil the SPF requirements. This can be used by the recipient to reject all emails that do not fulfil these requirements. DMARC is therefore based on DKIM and/or SPF.

14.8.4. Prerequisites for use

An important part of implementing DKIM is ensuring that outsiders are not able to obtain valid DKIM signatures. This is particularly relevant in connection with email forwarding, sorting rules, mailing lists, web forms and the like. To prevent this, the Intra2net system automatically blocks all incoming emails from untrusted systems without a valid DKIM signature with your own domain as the sender. This also prevents forgery of the sender address for your own domain.

However, this means that correct signing must be considered for all legitimate email paths before DKIM is introduced. In particular, consider external users who access the email provider directly, devices such as scanners and printers in the local network, emails with status or error information from services such as backup servers, NAS, UPSs, building automation and similar, automated reports such as those from time recording, warehouse management, accounting, etc., as well as emails from external web servers such as web shops, contact forms and similar.

Emails can be signed in the following ways:

- Delivery of the email to the Intra2net system from the local network via SMTP, encryption of the connection with TLS, authentication with a valid user. The user must be a member of a group that has the right to authenticate SMTP from the local network.
- Delivery of the email to the Intra2net system from the local network via SMTP, the IP of the SMTP client has the right "Email relaying allowed" (see e.g. "Network > Intranet > Clients"). TLS and authentication are then optional.
- Delivery of the email to another email server in the local network. Although this server does not perform DKIM signing itself, it forwards outgoing emails to the Intra2net system.

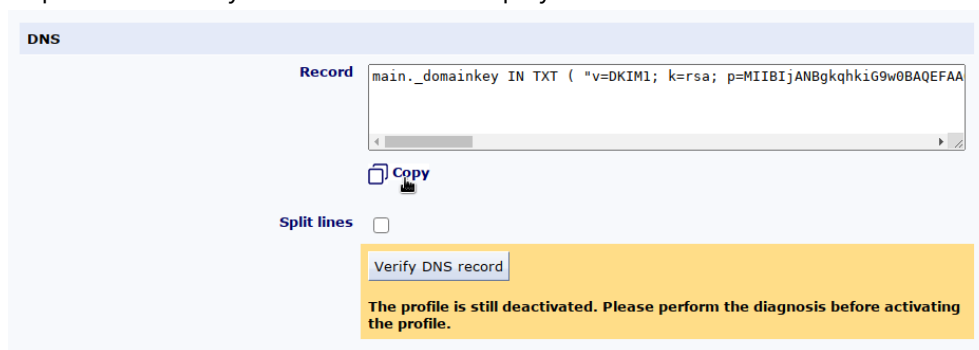
- Delivery of the email to the Intra2net system from the Internet via SMTP, encryption of the connection with TLS, authentication with a valid user. The user must be a member of a group that has the right to authenticate SMTP from the Internet.
- Delivery of the email to the Intra2net system via Activesync. The user must be a member of a group that has the right to use Activesync.
- Delivery of the email to another server or service that also signs emails using DKIM. Such services are offered by some web hosting or email providers. This service may use a different valid DKIM selector than the Intra2net system. Such a service must sign via DKIM, the use of SPF is not sufficient for the emails to be accepted by the Intra2net system.

Make sure that every email that uses your own domain in the sender is always sent via one of the above-mentioned channels.

14.8.5. Configuration

Proceed as follows to sign emails with DKIM:

1. Make sure that the requirements from Section 14.8.4, „Prerequisites for use“ are met and check all legitimate email paths for your own domain.
2. Create a new key of the type "DKIM" in the menu "System > Keys > Own keys". Choose any name for "Selector", but limit yourself to lower case letters and do not use any spaces or special characters apart from the hyphen. A key length of 2048 bits is recommended as a good compromise between security, computing time and data size in the DNS.
3. Create a new profile in the menu "Services > Emailfilter > DKIM > Profiles". Select your own domain as the sender domain and use the DKIM key you have just created. We recommend starting with the standard list as the list of headers to be signed.
4. Be sure to leave the profile deactivated first and save the settings. After saving, the required DNS entry for the selector is displayed at the bottom of the menu.



DNS

Record main._domainkey IN TXT ("v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAA

Copy

Split lines ☐

Verify DNS record

The profile is still deactivated. Please perform the diagnosis before activating the profile.

5. Go to the administration portal of the provider responsible for the domain. This is usually the provider who is also the web hosting provider. There, open the DNS administration for the selected sender domain.
6. Add a new entry, host name or record of the type `TXT`. The name for the entry is the selector with `._domainkey` appended, as it is displayed in the menu of the Intra2net system under "Record" at the front.

7. You can also copy the content of the entry from the Intra2net system display. The exact format required differs between DNS providers. This is because the required entry is longer than 255 characters and must therefore be split according to the DNS standard. Some DNS providers perform this separation themselves, while others require the user to do this. You can use the "Split lines" button to display both variants in the Intra2net system. There are also differences between the DNS providers as to whether or not the quotation marks must be included.

DNS-Record hinzufügen

Typ **TXT**

Hostname

Wert

TTL

Vorschau main_domainkeyexample.com 300 IN TXT

```
"v=DKIM1; k=rsa;
p=MIIBIJANBgqhkiG9w0BAQEFAAOCAQ8A...
a9sweus9EBKsYrxqZLgXReS/
CFyNicXZ6y6TeAZOANu7rN5Zs9vMddCVhtz...
fj0h4nLWY81SR5sAQnPCgmMmmHfj5+RhE/
JBceav+alcQtyhMj0jsdC0OeDLrvj4V9Hv/
2LCBdrZcdYWsMDSzfYfjC7GjvvHPAdWwkdF...
6FFB9CwDV8YJJY6VSgxuHvxgjFg/KPA/
7ZPwIDAQAB;"
```

Menu of a DNS provider as an example. The appearance varies depending on the DNS provider.

8. If the DNS provider gives you the option to do so, then first use a short *TTL* (time-to-live, validity period) for the DNS entry, e.g. 5 minutes or 300 seconds. In the event of a configuration error, this allows you to correct it immediately without having to wait for the incorrect entry to expire.
9. Save the new DNS entry in the interface of the DNS provider and wait until the new entry is published on the DNS servers. In most cases, this is completed after a few minutes, but the exact duration varies depending on the DNS provider.

<input type="checkbox"/>	TYP	HOSTNAME	WERT	SERVICE 圖	AKTIONEN
<input type="checkbox"/>	MX	@	mx00.ionos.de	Mail	
<input type="checkbox"/>	MX	@	mx01.ionos.de	Mail	
<input type="checkbox"/>	A	@	217.160.223.176	-	
<input type="checkbox"/>	TXT	main_domainkey	"v=DKIM1; k=rsa; p=MIIBIJANBgqhkiG9w0BAQEFAAOCAQ8A..."	-	
<input type="checkbox"/>	A	ftp	217.160.223.176	-	
<input type="checkbox"/>	A	www	217.160.223.176	-	

10. In the Intra2net system, click on "Verify DNS record" and start the DKIM diagnosis. The Intra2net system then checks whether the DKIM entry can be retrieved correctly in the DNS. In the event of an error, see Section 14.8.5.1, „Solving DKIM configuration errors“.

11. Once the diagnosis has been successfully completed, you can activate the new DKIM profile in the menu "Services > Emailfilter > DKIM > Profiles". From then on, all emails with the configured sender domain will be signed and unsigned emails from this domain will be blocked if they do not come from a trustworthy system.

14.8.5.1. Solving DKIM configuration errors

If the diagnosis fails, check the following points depending on the exact error message displayed.

The DNS entry was not found:

- First check whether the entry has not yet been updated by the DNS provider. Depending on the DNS provider, this can take between a few seconds and several hours. This should be described in the documentation or administration interface of the DNS provider.
- Check next whether the sender domain is also used locally or whether there is a forwarding to it. In this case, the responsible local DNS server is also displayed in the diagnostic output. It is recommended that you also store the DKIM entry in this local DNS server. In this case, however, the diagnostics can only check the entry in the local DNS server and not the one visible to others on the Internet.
- Compare the exact spelling of the entry / host name and the correct type "TXT" displayed in the Intra2net system with the data from the DNS provider.

Syntax error or incorrect public key:

- Compare the content of the DNS entry between the data displayed in the Intra2net system and that of the DNS provider. The data there must be identical. Pay particular attention to the beginning and end as well as spaces.
- If the DNS provider's administration interface provides for several lines, then use the representation with split lines, if it only provides for one line, then without.
- Try omitting or adding quotation marks at the beginning and end.
- The DNS provider's administration interface may offer the option of displaying or downloading the complete DNS zone file for diagnostic purposes. This can be helpful to recognise transmission errors. A standard-compliant zone file should contain the entry exactly as it is displayed in the Intra2net system with activated "Split lines".

Please note that if you retrieve an entry created once from the DNS provider and then change it there again, the old value is normally still stored temporarily in the DNS cache for the stored TTL / validity period. You should therefore wait for the TTL to expire before restarting the diagnosis.

Depending on the DNS servers used, you can avoid this waiting time by clearing the DNS cache of the Intra2net system in the "Network > DNS > Settings" menu. However, this is only possible if the Intra2net system queries the root name servers as an independent DNS resolver and does not use other DNS resolvers.

14.8.6. Filtering and quarantine

After activating DKIM for a sender domain, the Intra2net system must block all emails that claim to come from this domain but are not DKIM-signed or come from a trusted system. This is necessary to prevent signature fraud, see Section 14.8.4, „Prerequisites for use“.

Emails blocked in this way end up in the DKIM/DMARC quarantine by default. This quarantine can be found under "Services > Emailfilter > Quarantine > DKIM/DMARC". The emails can be viewed and analysed there and emails that have been incorrectly filtered can be released again.

You can control the behaviour of the filter under "Services > Emailfilter > Settings". It is recommended that these emails are first quarantined for a few weeks after the introduction of DKIM. During this time, the administrator can ensure that all email paths of their own domain are actually configured correctly without emails being inadvertently rejected and deleted. In the event of an error, these emails can then be forwarded via one of the paths described in Section 14.8.4, „Prerequisites for use“.

If the Intra2net system retrieves incoming emails from an external email provider via POP (see menu "Services > Email > Polling"), the quarantine must be used permanently, as the emails to be blocked have already been accepted by the email provider when they arrive at the Intra2net system. It is then too late to reject them at SMTP level.

If incoming emails from outside are received via SMTP and the MX record of the email domain points to the Intra2net system, it is advisable to switch the action for unsigned emails to Reject after an introductory period of a few weeks. The notification emails to the administrator for quarantined emails will then no longer be sent.

14.8.7. Header lists and exceptions

Lists with the email headers to be signed can be configured under "Services > Emailfilter > DKIM > Headers". It is normally recommended to use the predefined standard profile, as it contains all relevant headers and makes it very difficult for a potential attacker to falsify emails or misuse existing signatures.

However, it can happen that a server legitimately changes emails between the sender and certain recipients, causing the DKIM signature check to fail at the final recipient of the email. This happens, for example, when labels such as "[external]" are inserted in the subject line or a mailing list is used that inserts its name in the subject line or appends brief instructions for use to the email text. For these cases, the Intra2net system offers the option of defining exception rules for certain recipients and signing fewer headers there.

First select a suitable list of headers under "Services > Emailfilter > DKIM > Headers" or create a new one. Then go to the menu "Services > Emailfilter > DKIM > Profiles" and create a new recipient profile. Enter either an entire recipient domain or a single recipient email address. Select the desired header list and save.

The setting stored in the recipient profile is then used for all emails that are to be sent to the set recipient email address or domain and whose sender address is in a domain for which a DKIM profile is active. This setting takes precedence over the settings for the sender domain.

As the sender server can freely select the list of headers to be signed, no changes need to be made to the DNS or the selector.

14.8.8. Rotate the key

In principle, the key belonging to a DKIM selector can be used indefinitely. In some cases, however, the key should be replaced with a new one immediately:

- Misuse of the key by others is clearly recognised or suspected
- A server on which the private key was stored was infiltrated by unauthorised persons or at least suspected of having been infiltrated
- An employee who had access to the private key has left the company
- A service provider, such as an IT service provider, web hosting provider or email provider, with whom the private key was stored, has been cancelled

In addition to these events, it is recommended to rotate the keys every 1 to 5 years to prevent the key from being broken with a lot of computing power and to adapt the key length to the current state of science and technology.

To rotate the key, proceed as follows:

1. Create a new key of type "DKIM" in the "System > Keys > Own keys" menu. Use a different selector than for the previous key.
2. Create a new profile in the menu "Services > Emailfilter > DKIM > Profiles". Enter the same sender domain, use the new key and be sure to keep the new profile deactivated first.
3. Also configure the new DNS entry with the DNS provider, leave the previous DNS entry there and then start the DKIM diagnosis. See Section 14.8.5, „Configuration“ for a detailed description.
4. If the diagnosis was successful, activate the queue in the "System > Queue" menu.
5. Deactivate the previous DKIM profile and activate the new one. Leave the previous profile in place and do not delete it yet. Both changes are first queued and do not take effect immediately.
6. Now execute the queue to switch seamlessly from the old to the new profile.
7. As emails signed with the old profile may still be in transit and must be able to be checked later by the recipient, the profile and the associated DNS entry must remain in place. The earliest possible deletion date is displayed in the menu "Services > Emailfilter > DKIM > Profiles".

14.9. Archiving

14.9.1. Interface

The archiving interface of the Intra2net system can be configured under "Services > Email > Archiving". The interface can be used to process emails in various formats

and thus be configured to match whichever archiving software used. The different archiving methods are as follows:

Email copy to	A copy of every email is sent to this address. The original recipients of the email are listed in the headline <code>X-Envelope-To</code> .
POP3 multidrop mailbox (MailStore)	A copy of each email is stored in a special multidrop mailbox from which archiving software can retrieve it via POP3. For emails with multiple recipients, a separate email is stored in the multidrop mailbox for each recipient. The sender is stored in the <code>X-Envelope-From</code> header, the recipient in the <code>X-Envelope-To</code> header.
Single files (BSMTP format)	Each email is written to a single file in BSMTP format. The BSMTP format is described in RFC 2442 [http://tools.ietf.org/html/rfc2442]. Only one email is stored in each file, multiple recipients are specified in single <code>RCPT-TO</code> lines.
Single files (EML/RFC822 format)	The content (header and body) of each email is written to a single file. This is usually called EML format and was initially described in RFC 822 [http://tools.ietf.org/html/rfc822]. Only one email is stored in each file, and a separate file is created for each recipient. The sender is stored in the headline <code>X-Envelope-From</code> , and the recipient in the headline <code>X-Envelope-To</code> .
MailStore Proxy	Individual emails are stored in files compatible with the MailStore Proxy format. This allows the Intra2net system to be connected to a MailStore server like a MailStore Proxy. For installation instructions, please refer to Section 14.9.2, „Connecting the MailStore Server“.

If the spam filter is active on the Intra2net system, emails detected as spam can be excluded from archiving. Select a threshold value from which emails should not be archived. We recommend using a value of 8. For further details on spam thresholds, see Section 14.7.1.2, „Flagging“

If you have selected an archiving mode that stores files, you can access them using a Windows share. You must select a login and password for this share. The archiving interface only provides complete files. The interface ensures that no incomplete or partially written files are visible or accessible.



Caution

The archiving software is responsible for ensuring that emails are deleted from the interface immediately after archiving. The interface share is not designed to permanently store email files and can block email transfer if the files are not retrieved regularly.

14.9.2. Connecting the MailStore Server

The MailStore Server [<https://www.mailstore.com/>] can be used to archive all emails routed through the Intra2net system. There are two different archiving options to choose from: via multidrop mailbox or via Mailstore proxy. Since the Mailstore proxy interface has been deprecated by Mailstore, the connection via POP3 multidrop mailbox is recommended.

14.9.2.1. Connecting the MailStore Server via POP3 multidrop mailbox

The MailStore Server [<https://www.mailstore.com/>] is connected to the Intra2net system via a separate POP3 mailbox. A copy of each email passing through the Intra2net system is created in the POP3 multidrop mailbox. The Mailstore server regularly retrieves this multidrop mailbox and archives the emails. The additional program "Mailstore Gateway" is not required.

Unlike the other archiving methods of MailStore Server (such as IMAP mailbox or Exchange Server), this ensures that all emails are archived. It is impossible for a user, an incorrectly configured sort rule, or bug to delete emails before they are archived.

Follow these steps for installation:

1. Install MailStore Server as described in the manufacturer's manual: <http://en.help.mailstore.com/>.
2. Set the archiving mode of the Intra2net system under Services > Email > Archiving to "POP3 multidrop mailbox" and enter the login details for the mailbox.

Note the login (e.g. **mailarchive**).

3. Open MailStore Client, log in with administrator rights and open the "Administrative Tools" menu.
4. Use the "Create New" button to make every user of your system available to MailStore Server. It is particularly important that all email addresses including aliases and user redirects are entered in the "Email addresses" field.

The screenshot shows the 'User Properties' dialog box for a user named 'johndoe'. The dialog is divided into several sections:

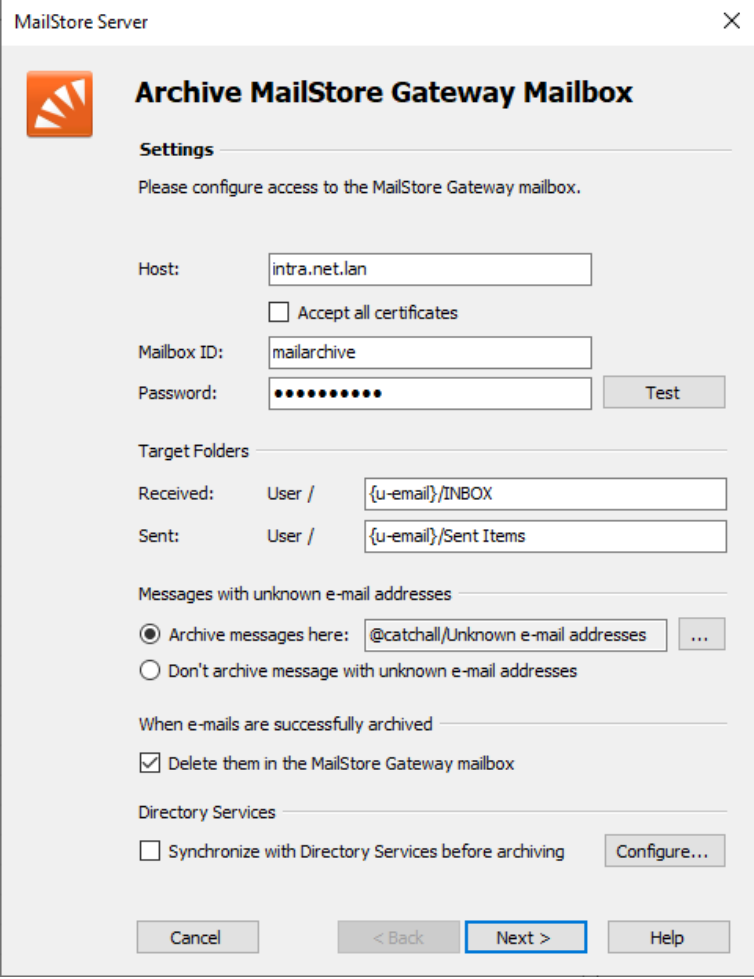
- General Information:**
 - Login Name: johndoe
 - Full Name: John Doe
 - Authentication: MailStore-integrated (dropdown), Password... (button)
 - ☐ User is an Administrator
- Integration (optional):**
 - LDAP DN String: (empty text box)
 - E-mail Addresses: johndoe@example.com, johndoe@intra.net.lan (comma separated)
 - POP3 User Names: (empty text box, comma separated)
- Privileges:**
 - ☒ Log on to MailStore Server
 - ☒ Change Password
 - ☒ Archive E-mail: Unlimited (dropdown)
 - ☐ Export E-mail: Unlimited (dropdown)
 - ☐ Delete E-mail
- Folder Access Table:**

Folder	Access	
johndoe	Read, Write	

At the bottom right of the table are buttons: 'Add New...', 'Edit', and 'Delete'. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

5. In the "Archive E-mail" menu, select "E-mail Servers" and then the "Mailstore Gateway Mailbox" option.
6. Select the option "Other E-mail server".
7. Enter the server name and the assigned password. As mailbox ID, use the login listed in the Intra2net system in paragraph 2 (e.g. **mailarchive**).

Have the emails deleted from the gateway mailbox if archiving was successful (important!).

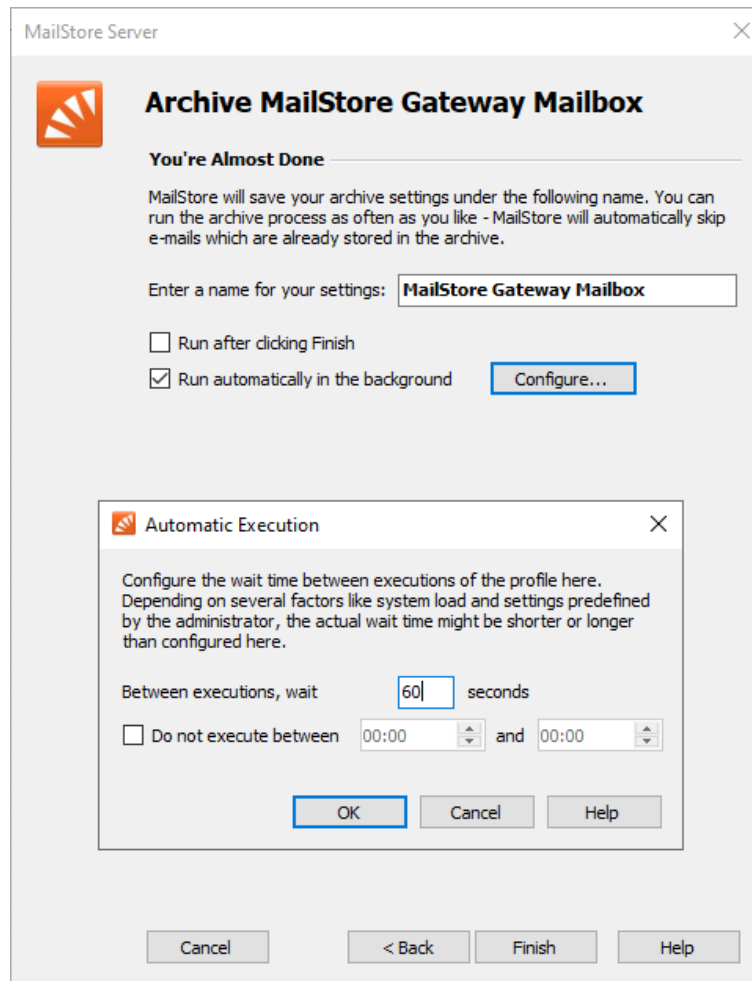


The screenshot shows the 'MailStore Server' window with the title 'Archive MailStore Gateway Mailbox'. It contains several sections for configuring email archiving:

- Settings:** Includes fields for 'Host' (intra.net.lan), 'Mailbox ID' (mailarchive), and 'Password' (masked with dots). There is an 'Accept all certificates' checkbox and a 'Test' button.
- Target Folders:** Includes fields for 'Received' (User / {u-email}/INBOX) and 'Sent' (User / {u-email}/Sent Items).
- Messages with unknown e-mail addresses:** Includes a radio button to 'Archive messages here:' with a field containing '@catchall/Unknown e-mail addresses' and a '...' button, and an option to 'Don't archive message with unknown e-mail addresses'.
- When e-mails are successfully archived:** Includes a checked checkbox for 'Delete them in the MailStore Gateway mailbox'.
- Directory Services:** Includes a checkbox for 'Synchronize with Directory Services before archiving' and a 'Configure...' button.

At the bottom, there are buttons for 'Cancel', '< Back', 'Next >', and 'Help'.

8. Run the profile in the background automatically every 60 seconds.



9. Save the configuration.

14.9.2.2. Connecting the MailStore Server proxy interface

The connection of the MailStore Server via the proxy interface has been deprecated. We recommend Section 14.9.2.1, „Connecting the MailStore Server via POP3 multidrop mailbox“ instead.

The MailStore Server [<https://www.mailstore.com/>] is connected via the MailStore Proxy interface on the Intra2net system. Each email sent through the Intra2net system is duplicated and stored in a special format on the archive interface. MailStore Server will then regularly retrieve the files from the interface and add them to the archive.

Unlike the other archiving methods of MailStore Server (such as IMAP mailbox or Exchange Server), this ensures that all emails are archived. It is impossible for a user, an incorrectly configured sort rule, or bug to delete emails before they are archived.

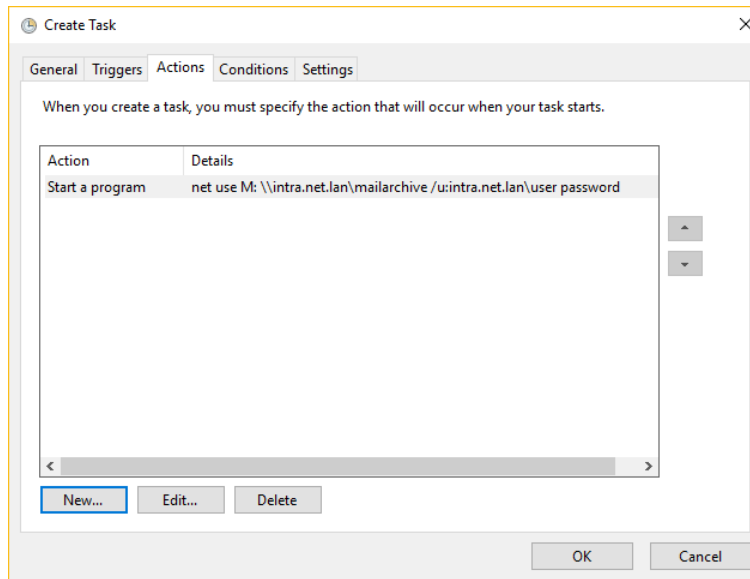
Follow these steps for installation:

1. Install MailStore Server as described in the manufacturer's manual: <http://en.help.mailstore.com/>.
2. Set the archiving mode of the Intra2net system to "MailStore Proxy" under Services > Email > Archiving, and enter the login details for the share path.

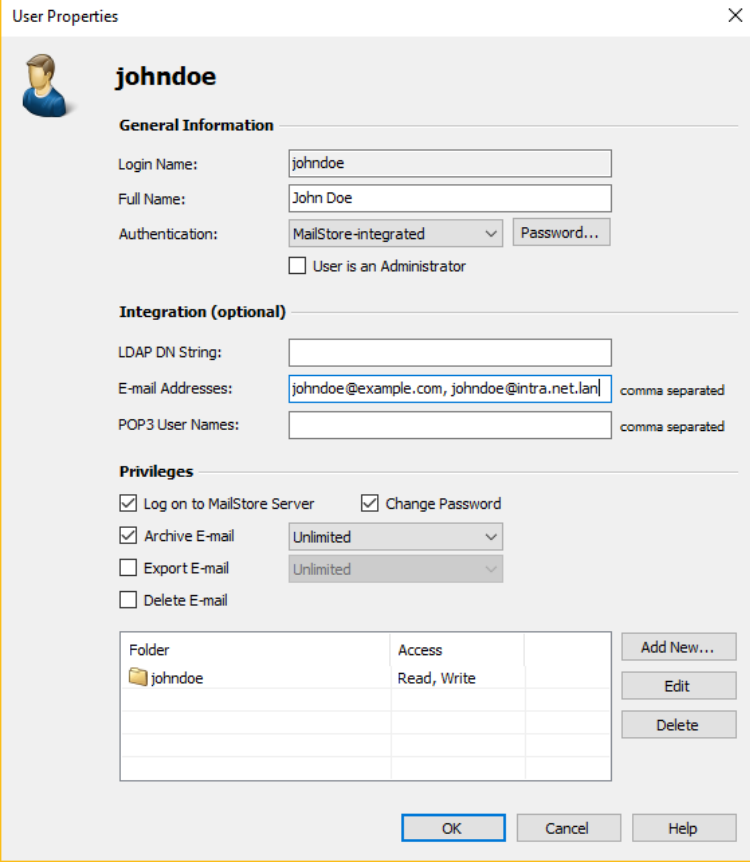
- On the computer with MailStore Server, open Windows Task Scheduler from Windows Administration.
- Create a new task. Allow the task to be executed with the **SYSTEM** user account and with the highest privileges.

- Add a new trigger for the task. Let the task start on an event and select "Microsoft-Windows-NetworkProfile/Operational". The source is "NetworkProfile" and as the event ID enter 10000. This will start the task as soon as the network is operational.

- Add a new action. Let the program **net** start and provide the parameters **M: \\intra.net.lan\mailarchive /u:intra.net.lan\user password**. Use the name of your Intra2net system and the login details you have chosen instead of "user" and "password". If the drive letter M: is already assigned elsewhere on your computer, please select a different one. Note the space between **M:** and **\\intra.net.lan....**



7. Save the new task and restart the computer with MailStore Server.
8. Check that the network drive M: was connected correctly after system startup. Note that only the Windows system user has access to the network drive. All other users are denied access or see a "unconnected network drive". If you see this, the connection works correctly. If no network drive should be displayed at all, there is an error.
9. Open MailStore Client, log in with administrator rights and open the "Administrative Tools" menu.
10. Use the "Create New" button to make every user of your system available to MailStore Server. It is particularly important that all email addresses including aliases and user redirects are entered in the "Email addresses" field.



User Properties

johndoe

General Information

Login Name: johndoe

Full Name: John Doe

Authentication: MailStore-integrated Password...

☐ User is an Administrator

Integration (optional)

LDAP DN String:

E-mail Addresses: johndoe@example.com, johndoe@intra.net.lan comma separated

POP3 User Names: comma separated

Privileges

☒ Log on to MailStore Server ☒ Change Password

☒ Archive E-mail Unlimited

☐ Export E-mail Unlimited

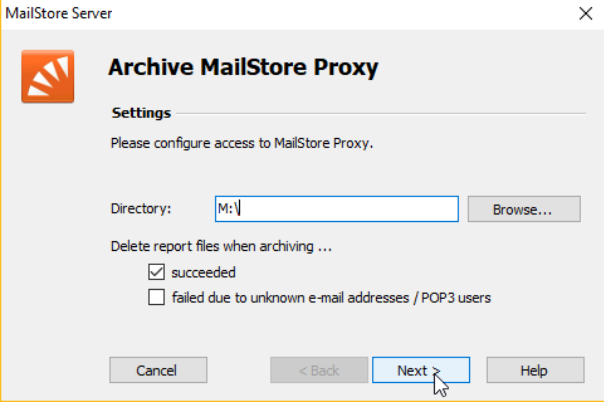
☐ Delete E-mail

Folder	Access
johndoe	Read, Write

Add New... Edit Delete

OK Cancel Help

11. Open the "Email archive menu" and configure a new "MailStore Proxy" archiving profile.
12. Select the newly connected drive letter as the directory and delete the report files, if the archiving was successful (important!).



MailStore Server

Archive MailStore Proxy

Settings

Please configure access to MailStore Proxy.

Directory: M: Browse...

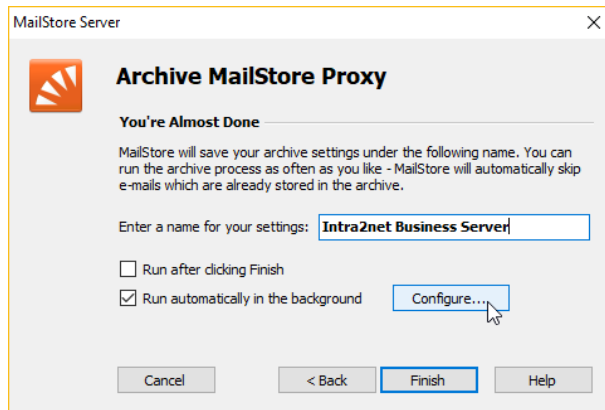
Delete report files when archiving ...

☒ succeeded

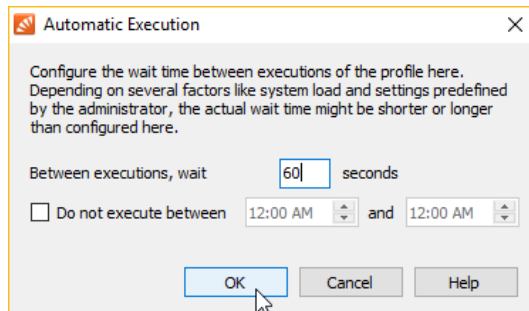
☐ failed due to unknown e-mail addresses / POP3 users

Cancel < Back Next > Help

13. Run the profile in the background automatically.



14. Allow the profile to run every 60 seconds and save the profile.



14.10. Automatic Transfer

The Intra2net system can automatically collect and send emails at regular intervals. This can be configured according to days of the week under Services > Email > Automatic.

For the transfer, a connection is established with the default provider (see Section 10.8, „Automatic Connection“) if there is no connection yet. Once the transfer has been completed, the connection is automatically disconnected if there is no one else connected.

While the Intra2net system is online, emails are always immediately sent.

14.11. Mailinglist

The Intra2net system comes with a powerful mailing list management system. In addition to user groups, you can set up mailing lists under Services > Email > Mailinglists.

In addition to internal users and groups, external email addresses can also be added. If the Intra2net system does not manage a domain via multidrop or SMTP, there is the problem that the distribution list does not have an externally accessible email address. To solve this, you can set up a POP3 account under Services > Email > Polling, from which emails for the mailing list are collected. At the same time, the email address entered under "External Mailing List Address" is also included as a reply address in all emails to external members.

14.12. Additional Settings

Under Services > Email > Settings you can configure some additional settings for the email system.

The postmaster is the user who receives messages regarding errors and undeliverable messages. There is a system-wide standard postmaster and it is possible to set an individual postmaster for each domain (under Services > Email > Domains). Emails sent by the system use the postmaster's address as the sender. If you have not defined a domain in the system, you should enter a valid address at "External address of the postmaster", as many servers do not accept emails from invalid senders.

Emails cannot be of unlimited size as they must be temporarily stored and unpacked for further processing (e.g. virus scan, etc.). The spool partition whose space is limited is used for this. 100 MB has proven to be a reasonable limit. Very few systems will accept or send larger emails.

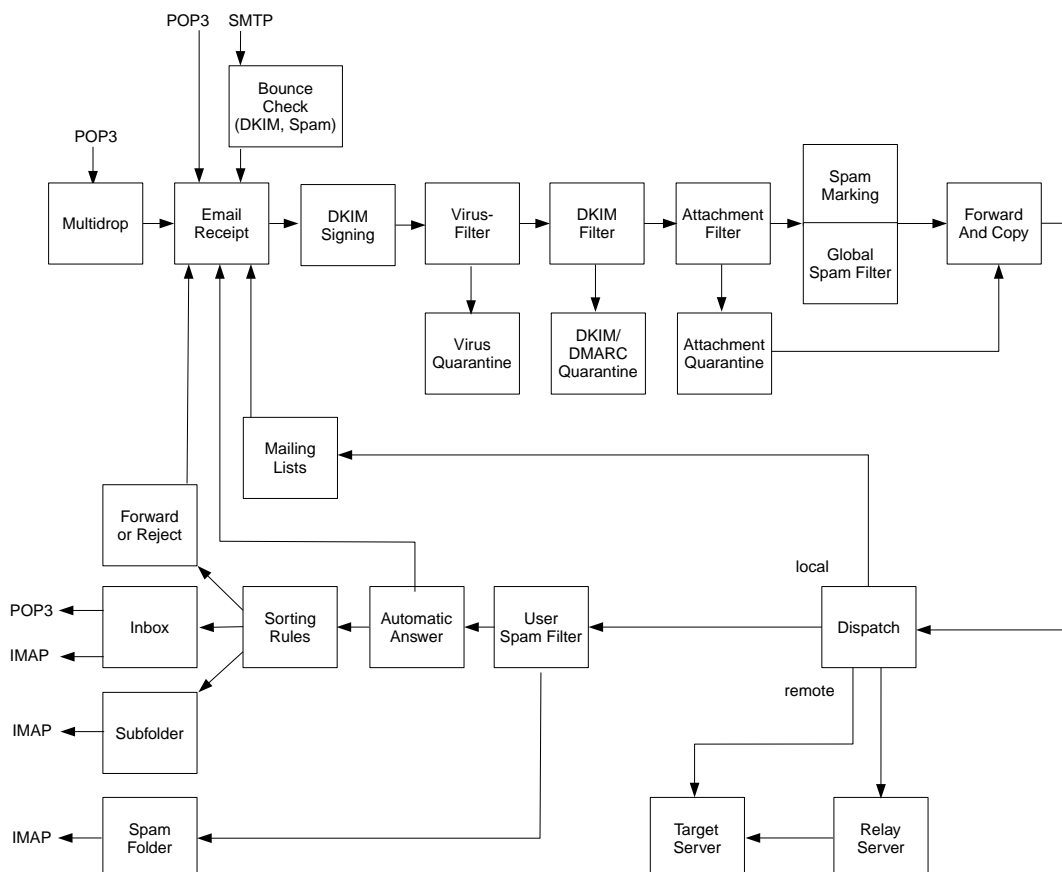
14.13. Queue

Before an email is sent to an external recipient, it is queued under Services > Email > Queue.

There are also emails that cannot be delivered on short notice due to server errors.

An administrator can delete these emails from the queue or download them.

14.14. Structure of the mail system



14.15. Differences between licenses

Intra2net licenses with Mail Security feature:

- Acceptance of emails from individual POP accounts, direct delivery via SMTP and from collective POP accounts
- Forwarding of entire domains
- Forwarding of individual email addresses
- Recipient Address Check
- Spamfilter with quarantine
- Attachment Filter
- Email Antivirus
- DKIM signing and filtering
- Interface for email archiving

Intra2net licenses with mail server additionally support:

- Permanent storage of emails on the Intra2net system
- Email retrieval using clients (such as Outlook) from the Intra2net system via POP3 and IMAP
- Vacation Mode
- Email sorting
- User-based spam filter
- Mailinglists
- Webmail and Web-Groupware
- ActiveSync

15. Chapter - Services

15.1. Timeserver

As soon as it is online, the Intra2net system keeps its own time updated by synchronizing itself with time servers on the Internet.

The time servers used can be set under Services > Time synchronisation. By default, time servers from a public pool are used. More information about this pool can be found at <http://www.pool.ntp.org>.

Computers from the intranet can use the Intra2net system as a source for their own time. The NTP and SMB protocols can be used for this purpose. To use the NTP protocol, it is possible to use a separate NTP program or enter the Intra2net system as the Internet Time Server in the clock properties under Windows. To use the SMB protocol, regularly (e.g. on every system startup) run the following command with administrator privileges:

```
net time \\intra.net.lan /set /yes
```

Of course, the local name or IP address of your Intra2net system must be used.

15.2. Monitoring via SNMP

Under Services > Monitoring > SNMP it is possible to configure whether and how the Intra2net system should provide data for monitoring via SNMP. This data can then be accessed and evaluated by a central SNMP monitoring service.

The Intra2net system does not offer information using the insecure SNMP versions 1 and 2, but only using the newer, secured version 3. User name, password and authentication protocol (MD5 or SHA1) must be specified for the authentication of the monitoring service with the Intra2net system.

It is sensible to have the monitoring service not only log on to the Intra2net system, but also encrypt all transmitted data. To do this, select an encryption password and an encryption method (AES or DES). It is recommended to use the secure AES if the monitoring service supports this. If "Only encrypted data transmission" is then enabled, the monitoring service must encrypt correctly in order to access the data of the Intra2net system.

If the Intra2net system is to be monitored from the local network, the firewall settings for the computer with the monitoring service must allow this. For example, a simple computer profile can be created and an additional service "snmp" can be added to it. If the Intra2net system is to be monitored over the Internet, set up a VPN connection between the monitoring server and the Intra2net system. The data can then be queried using these.

The Intra2net system uses SNMP to provide various information about CPU and memory usage, I/O load, hard disk usage, network utilization, number of error messages, Intra2net software version, and status of the RAID array. In order for this information to be usefully evaluated by a monitoring program, a description of the data is usually required as *Management Information Base* (short MIB). These are linked in the online help of the Services > Monitoring > SNMP page.

16. Chapter - System Functions

16.1. License

16.1.1. Demo Mode

After installation, the system will be in demo mode. You will then have 30 days to explore all of the features. The range of features corresponds to an Intra2net Business Server with the only restriction that backups cannot be restored and system updates are unavailable.

Internet access and email traffic will be blocked after 30 days. However, configuration data and emails are retained.



Hint

The Intra2net system updates its system time as soon as it is online. If the system time deviated considerably during installation, it may be that the time period for the demo license is calculated incorrectly. In this case, reinstall the Intra2net system.

16.1.2. License Code

If a license has been purchased, it can be imported into the system and activated. For this purpose, the Intra2net system requires an internet connection. It should therefore already be configured and default provider set correctly (see Section 10.8, „Automatic Connection“).

Enter the full license code under Information > License. A complete license code consists of 5 blocks of 4 characters each, separated by hyphens (e.g. **A1B2-C3D4-E6F7-G8H9-I0J1**).

If the new license is missing functions that are currently actively used on the Intra2net system, a conflict occurs when the license is imported and the new license is not activated.

These particular functions can now be disabled. They are listed in the Information > License menu. An attempt to import the license can now be made again.

16.1.3. Update Period

Each license includes feature, security, spam filter and virus scanner updates for 1 year. This period counts from the first registration or check for updates. The end date is displayed on the Information > License page.

If the license for new updates has expired, the system continues to run normally in its current state. All updates released up to the expiry date can still be installed. In addition to the updates for the Intra2net system, the updates for the virus scanner and spam filter will no longer work. Both functions are highly dependent on contemporary data, which is why the filter rates tend to deteriorate rapidly after only a few days.

16.2. Updates

The Intra2net system contains an update system with which it can always be kept updated to the latest software version. This is necessary to quickly resolve any security issues and provide customers with new features and functionality. In this way, the Intra2net system virtually cannot be "obsolete".

Updates are always downloaded and installed over the Internet from the Intra2net server. The use of manual file import is only intended for emergencies and is then handled together with Intra2net support.

Under System > Update > Settings the update settings can be configured. In the standard configuration, the Intra2net system checks for new versions on a daily basis and notifies an administrator. The update can then either be installed immediately or delayed. The standard provider is used for dialing into the Internet (if not already online) (see Section 10.8, „Automatic Connection“).

The Intra2net system reboots after each update. If multiple updates are being installed simultaneously, each update is executed step by step, from version to version and a reboot is performed after each step. Therefore, an update can take a long time over multiple versions. Please do not switch off the Intra2net system during the update process!

The current version of the Intra2net software can be found under Information > Version.

The virus databases are updated separately from the Intra2net system updates. In the standard configuration, the Intra2net system checks for new virus databases every hour and installs them all automatically.

In addition to the hourly checks for new virus databases, there is the option to push the update system via DNS within minutes of a new virus database being released. The update system then downloads and automatically installs new virus databases in the normal way. When using this option, we recommend still running the regular hourly updates. The transmission of the version information via DNS is not cryptographically secured and can therefore be disrupted easily compared to the communication with the update servers of Intra2net, which is completely secured by HTTPS.

The Spamfilter database is also independent of the Intra2net system updates. This is automatically updated daily by default.

16.2.1. Remote Update via Partner Web

Update installation can be centrally managed from the Intra2net partner web. This can be convenient for distribution partners with a larger number of Intra2net systems. The prerequisite for this is to activate the function "Enable remote update management" under System > Update > Settings on the device itself. The activation for the partner web is completed approx. 5 minutes after saving on the device.

On the partner web individual Intra2net systems can be selected and then updated to the latest version at a specified time. The installation command is sent during the next update check. If the set time is already in the past, the update will be installed the following day.

16.2.2. Rescue System

Before new software is installed during an update process, a copy of the current status of the system partition is created. The actual update process begins after that. This copy is called a rescue system, and can be booted on demand instead of the normal system. It always reflects the status of the system prior to the last update.

The rescue system is started automatically if an update could not be installed completely, e.g. because of a hardware error or because a user switched the device off during the update process.

If necessary, the rescue system can also be launched manually, e.g. if an update has caused errors in the system. For this purpose, the rescue system can be activated on the device's console i.e. with a monitor and keyboard connected to the device, in the boot manager's menu shortly after starting the device.

The rescue system can be used normally in the majority of cases. However, there are functional limitations: Users can not be created, deleted or renamed. Furthermore, no updates can be imported to the rescue system. It is therefore recommended that the problem that led to the activation of the rescue system be resolved as soon as possible, and that the system be returned to the primary system.

If the rescue system has been activated due to an error during the installation of an update, there are the following methods for returning to the primary system and trying the update again:

- Contact Intra2net support. The primary system can then be reset by remote maintenance.
- Create a backup from the rescue system, copy it to an external storage, reinstall the system, and then restore the backup. Proceed as described in Section 16.3.5, „Procedure for Hard Drive Damage or Hardware Replacement“.

16.3. Backup

The Intra2net system contains the current configuration data and all emails and groupware data as well as statistics, log files and the email attachment quarantine. Therefore a regular backup is important.

Since the emails and groupware data can quickly grow to a large volume, a full backup may take many hours. Therefore, the system offers the possibility to create not only full backups, but also differential backups. These then only contain all changes since the last full backup. They can be created much faster and therefore allow to back up the data several times a day.

In the default configuration the Intra2net system creates a full backup once a week on Saturday at 22h and a differential backup three times a day at 6:30h, 12:30h and 19h on all days except Sunday. This means that the full backup can run the whole Sunday without disturbing the employees with increased system load. At the same time, the three backups per day provide only a small window for data loss should there ever be serious problems.

You can adjust these default settings to your requirements in the menu System > Backup > Settings or also trigger a backup manually.

If a differential backup is to be created manually or via the defined time control, but there is no full backup yet, a full backup will be created automatically instead.

The backups contain all emails, groupware data, the configuration, the license, the various email quarantines, the statistical data and the proxy server log files. Not included in the backup are the email queue, the email archiving interface and the system log files. In

addition, flags set for individual emails via IMAP are not saved in the backup. Email flags are information such as "read"/"unread", "marked", as well as user-defined flags that are offered by some email clients other than Outlook. This applies to categories in Thunderbird, for example.

16.3.1. Backup protection

The backups contain all emails, groupware data and the configuration with passwords of email retrievals, among others. It is therefore essential to protect them from access by unauthorized persons.

As basic protection of the backups, access can be restricted to a computer or user. By default, access to the backups is restricted to a user with a randomly generated password. Change this password to enable access.

For extended protection, the backups can be encrypted. The symmetrical AES-128-GCM method is used for this. The password entered is converted to a key block directly after entry using the script method and only this key block is stored in the internal configuration database. This means that the password used cannot be later read out of the configuration database.



Caution

Make sure to keep the password safe and check the exact spelling via the eye button next to the input field. If the password is lost, there is no realistic possibility for Intra2net to make the backup readable again.

For an optimal level of protection, it is recommended to change the password at least every 5 years. On one hand, the script parameters are adapted to current threat scenarios if necessary, and on the other hand, a regular exchange prevents the reuse of initialization vectors.

16.3.2. Storage period

Backups are always created exclusively on the local hard disk of the system and then initially kept locally as well. This primarily serves the purpose of fast restore in the most common case in the field, which is the accidental deletion of important emails by a user.

The backups of the last three days are kept on the system itself in the default configuration. For differential backups, the associated full backup is always kept as well, even if it is older than the set period.

Once the first backup sets have been created on a system, you will find statistics about the time and space required in the System > Backup > Settings menu. Use this data to adjust the frequency and storage duration to your requirements and available storage space.

16.3.3. Remote Storage

Of course it is not enough to store the backup only on the Intra2net system, because e.g. the hard disk could break.

Therefore the backup sets can be downloaded via HTTPS or SMB/CIFS (Windows share) from the Intra2net system to another computer. This can be done e.g. by an automatically

started batch file or by including the directory on the Intra2net system in an existing backup program.

Another option is automatic remote storage. If this function is active, the Intra2net system automatically uploads the backup files to a target server as soon as they are created. This can be done via FTP or SMB protocol. The Intra2net system can also automatically delete old backup records via SMB.

16.3.4. Restore

To restore backups, the backup sets are uploaded to the Intra2net system via SMB/CIFS to the `restore` share.

The same access protection settings as for downloading the backups apply to this share, see Section 16.3.1, „Backup protection“. If you want to restore a differential backup, both the files of the differential backup and those of the corresponding full backup must be copied.

The restore can be started under System > Backup > Restore.

There are multiple ways to restore backups: Full (configuration and emails), only the configuration (all emails are deleted!) or only the emails of one user.

The emails of a user can also be restored to an IMAP subfolder of a user. For example, if certain important emails were deleted by mistake, they can be retrieved without overwriting newer emails.

The Intra2net system can restore backups of old versions. The configuration of the backup runs internally through the update process. However, it is not possible to restore backups from newer versions.

16.3.5. Procedure for Hard Drive Damage or Hardware Replacement

After a hard drive failure or when the Intra2net system hardware is replaced, we recommend following the procedure below. We strongly advise against transferring data from the Intra2net system using hard drive imaging programs or similar solutions. In the case of a hard drive defect, the defects would simply be copied as well, and in the case of new hardware, even minimal differences in hard drive size often cause problems with the system.

For Hardware Replacement

1. Plan the hardware migration and the time required for it. To do this, go to the "System > Backup > Settings" menu and look at the "Forecast" section. Double this time to account for backup and restore.

Depending on the predicted time needed, consider the variant described in Section 16.3.6, „Hardware migration with Intra2net support“.

2. Deactivate the email and groupware system under Services > Email > Settings so that no new incoming emails are lost
3. Start Backup

4. When using email archiving: Check whether the archiving interface has been completely collected and emptied
5. Copy the completed backup to another computer

For Defects and Hardware Replacement

6. Download current installation image for the Intra2net System from www.intra2net.com [<https://www.intra2net.com>] and install it on a USB storage device.
7. Boot from USB storage device and install Intra2net System
8. Enter the IP range of your local network in the installation dialogue
9. If the new hardware has 2 hard drives, activate disk mirroring on the web interface now, under System > Hardware > RAID. Be sure to enable RAID at this point, it will take much longer after restoring the backup.
10. On the Intra2net system web interface, open and set a new password for the backup share (menu System > Backup > Settings)
11. Copy the backup from the other computer to the restore share of the Intra2net system
12. Restore the backup with configuration and emails to the Intra2net system
13. Activate the email and groupware system again, if it had previously been deactivated
14. Configuration, emails and statistics are restored and working as normal

When restoring email and groupware data from a backup, the internal identifiers (*UID-VALIDITY*) of all email folders must be changed to maintain data integrity. Most IMAP-based email clients recognize this and resynchronize all data from the server. If many clients do this at the same time, this can lead to increased system load. Email clients can also only be used to a limited extent for a certain period of time. Hints how this is handled by the Intra2net Groupware Client can be found in Section 24.10.1, „Backup Data after Restore“.

16.3.6. Hardware migration with Intra2net support

If you plan to replace the hardware, you can proceed as described in Section 16.3.5, „Procedure for Hard Drive Damage or Hardware Replacement“. With this procedure however, the system is not usable during the creation of the backup and when restoring it. With a larger volume of emails, this can take several hours and thus become a problem. In addition, the issue about changing the *UIDVALIDITY* of the email folders and the resulting resynchronization of the emails by the clients must also be taken into account.

Therefore Intra2net offers an alternative that avoids these disadvantages. With the help of Intra2net support, the new hardware can be updated to the current data status in the background and without interrupting the users. This process then runs e.g. over night. The next day, only the data that has changed since then needs to be transferred and the configuration applied. Therefore, the downtime is limited to about 15 to 30 minutes. Also, the *UIDVALIDITY* of the email folders are preserved, so the email clients do not have to resynchronize.

Prepare the following:

1. New hardware is in the same local network as the previous Intra2net system
2. Has a different IP address configured than the previous system (the IP of the previous system is taken over later).
3. Internet access via a provider profile of the type "Router in local network", router is the previous Intra2net system in the LAN
4. The same version of the Intra2net system is installed as on the existing system
5. Monitor and keyboard are available for accessing the console
6. There is *no* need for an additional or modified license, the previous license can be easily transferred to the new hardware.

Then contact Intra2net support to make an appointment for the hardware migration. Please note that this is considered Consulting and the time actually spent for the migration will be billed according to the price list.

The initial setup of the data transfer can be done completely via remote support. For the migration on the 2nd day, a trained IT technician should be on site to, among others, correctly identify the network cards and adapt the cabling.

16.3.7. Standby systems

To reduce the recovery time in the event of an error, a standby system can be used. Two variants are possible here:

16.3.7.1. Cold standby

A cold standby system is a system in the local network that can promptly take over the function, configuration and data of a failed primary system. For this purpose, a suitable device is kept ready in the local network. The Intra2net system is installed there in the suitable version and everything is prepared for fast takeover of the data.

Unlike the hot standby system, however, user data is not synchronized to the cold standby system every few minutes.

16.3.7.1.1. Set up and switch over

Configure the system as follows:

- When selecting the hardware, make sure that the standby system
 - has the same or a higher number of network cards
 - has the same or a larger hard disk capacity
- Install the current version of the Intra2net system
- You need a separate license for the standby system. This is always an Intra2net Network Security (I2N-INS-100) regardless of the license of the primary system.
- If two hard disks are available, set up the RAID array before
- Assign the system an IP in the local network of the primary Intra2net System

- Set up a provider profile of type "Router in local network" and use the IP of the primary Intra2net System as router IP
- The version level on the standby system must always be the same or higher than that of the primary system. It is therefore best to always install an update on the standby system first and only start the update of the primary system when it has been successfully completed on the standby system.
- On the primary system, configure remote backups to be automatically copied directly to the `restore` share of the standby system

If the primary system fails, proceed as follows:

1. Switch off the primary system
2. If the primary system is switched on and connected again at this moment, network disruptions and loss of email and groupware data can occur.

Therefore, secure the primary system against inadvertent restarting, e.g. by removing the mains cable and sealing the power supply socket with an appropriately labelled adhesive tape.

3. Restore the last backup set uploaded by the primary system completely on the standby system (menu System > Backup > Restore, Restore type "Configuration, statistics, emails and groupware data")
4. If the system asks you to select the license to be restored, select the license of the primary system.
5. Plug additional network cables (e.g. Internet connection) from the primary system to the standby system.
6. Wait until the standby system has fully restored the backup and restarted itself automatically.
7. Should network connection problems occur, it is possible that the assignment of the network cards of the standby system is different from that of the primary system.

In this case, connect a monitor and keyboard, log in to the console with a user from the administrator group and check the assignment of the network cards in the menu "Network card settings". Disconnect a network cable. The connection will then be shown as disconnected at the corresponding network card number in the menu. You can then exchange the assignment between 2 network cards using the corresponding option.

16.3.7.2. Hot standby

The disadvantage of cold standby, especially with an Intra2net Business Server with a larger stored email volume, is that it must be restored to disk and this step extends the recovery time.

Hot standby circumvents this problem by continuously synchronizing email and groupware data to the standby system. In addition, continuous synchronization drastically reduces the maximum time between last backup and failure.

A hot standby system can be set up remotely by Intra2net technicians. If you are interested, please contact your distributor or the Intra2net sales department.

16.4. Operation Behind Firewall

If the Intra2net System is not used directly on the Internet, but behind a firewall, some connections have to be allowed on it.



Hint

Intra2net has the right to change the IP addresses behind the DNS names at any time and without prior notice. Only changes to the DNS name will be announced in advance. If your firewall does not accept DNS names and cannot update them regularly, it is advisable to either check the DNS names on a regular basis or to release all connections from the Intra2net system to the corresponding ports.

Intra2net systems must be able to establish connections (outgoing connections) to the following targets:

Target	Protocol	Target Port / Packet Type	Function
update.intra2net.com	TCP	443 (https)	System updates, anti-spam updates, licenses, coordination of antivirus updates
avupdate.intra2net.com	TCP	443 (https)	Antivirus Update Data
*.avcloud.intra2net.com	TCP	443 (https)	Antivirus cloud for real-time scanning of virus checksums
avfpc.intra2net.com	TCP	443 (https)	Antivirus cloud for real-time queries of false positives
*.intra2net.pool.ntp.ntp.org or NTP server of choice	TCP and UDP	123 (ntp)	Time Synchronization
support.intra2net.com	TCP	5000 to 5050	Manufacturer Remote Maintenance
Your DNS Server	TCP and UDP	53 (dns)	Name Resolution
Multiple Servers	TCP	2703	Razor Spam Detection
Multiple Servers	ICMP	Echo-Request (Ping)	Connection Monitoring

Other possible services to be activated are email (POP3 and SMTP) as well as HTTP, HTTPS and FTP for the Intra2net system proxy.

If you want to use the services listed below, you must open the corresponding ports for incoming connections from the Internet:

Protocol	Destination port	Function
TCP	443 (https)	Web groupware, Activesync, remote maintenance

Protocol	Destination port	Function
		Note: The port number used for web groupware and remote maintenance can be changed. Active-sync works on port 443 only.
TCP	80 (http)	Issuing and renewing certificates via Let's Encrypt
TCP	25 (smtp)	Receive incoming emails via SMTP (MX record points to external IP)
TCP	587 (smtp-submission)	Sending emails by external users
TCP	993 (imaps)	Retrieval of emails and groupware data by external users
UDP	500 and 4500	Incoming VPN connections

16.5. Logfiles

Under Information > System > Logfiles, the Intra2net system provides access to the internal log files of the system. They can either be downloaded or viewed in a livelog.

The log files are rotated daily, or as soon as they reach a certain size. The number of old log files stored on the system can be configured over the days after which the log files are to be deleted at the latest. The maximum size the files may reach is automatically calculated by an algorithm from available space, the share of the affected file in the total log volume and the number of days for which the logs are to be kept.

16.6. Logcheck Reports

Under Information > System > Report the Intra2net system can be configured to send a daily evaluation of the events stored in the log files by email. This is done with Logcheck and Fireparse.

If the recipient is external (e.g. the distributor), it is advisable for security reasons to encrypt these emails. The Intra2net system offers PGP- and GnuPG-compatible encryption with password (symmetrical encryption with 256-bit AES).

16.7. Scheduled Shutdown

In order to save power, the Intra2net system can switch off automatically when it is not needed. In the System > Shutdown menu, it can be programmed to switch itself off at certain times. If you receive emails directly via SMTP, you should not use this function, otherwise emails could be returned to the sender as undeliverable. Also VPN, web-groupware, remote maintenance, port forwarding etc. do not work while the system is switched off.

The system switches itself back on at the programmed time. This requires BIOS support. In the BIOS, an option like "Wake on PCI device" or "Resume by PCI-E device" usually has to be enabled.

Use the Test button to test this function before utilizing it. The system shuts down and has to switch itself on automatically after 3 minutes. If this does not happen, settings have to be adjusted in the BIOS.

16.8. Inspection and repair of filesystems

At startup, the device automatically checks the consistency of the filesystems. If an error is detected, the system aborts.

Details are only displayed on the console. Therefore, connect a monitor and keyboard to the device. An error is indicated with `Filesystem check failed` clearly displayed. Press a key to restart the device.

On restart the boot manager is displayed for a short time. The boot manager starts the normal system after a few seconds. Instead, select "Filesystem repair attempt".

In this mode, the system examines all filesystems more closely and automatically attempts to repair any detected damage. If a filesystem has been repaired, the system displays the result for a few seconds and then moves to the next filesystem. At the end, the system reboots automatically.

Do not switch off the system while the filesystem repair attempt is running, as this can cause even more serious damage to the filesystems.



Caution

Do not attempt to repair the filesystem if you suspect that the hard disk is damaged. This could irreparably damage the filesystem.

A damaged hard disk is suspected if corresponding messages were previously displayed on the main page of the Intra2net system or in the system messages, the RAID status is not OK or unusual noises can be heard from the hard disk.

If you suspect a damaged hard disk, please contact Intra2net support. Alternatively, you can make a low-level copy of the defective hard disk (e.g. with `dd_rescue`) and then try to repair it using the copy.

Part 3. Groupware Client

17. Chapter - Introduction

17.1. System Requirements

Operating System	<ul style="list-style-type: none"> • Microsoft Windows 11 (64 Bit with Intel x86 Platform) • Microsoft Windows 10 (32 and 64 Bit with Intel x86 Platform) • Microsoft Windows Server 2016 (64 Bit) • Microsoft Windows 8 / 8.1 (32 and 64 Bit with Intel x86 Platform) • Microsoft Windows Server 2012 R2 (64 Bit) • Microsoft Windows 7 (32 and 64 Bit) • Microsoft Windows Server 2008 (32 and 64 Bit) <p>It is possible to operate in terminal server environments.</p>
Microsoft Outlook	<ul style="list-style-type: none"> • Microsoft Outlook 2021 • Microsoft Outlook 2019 • Microsoft Outlook 2016 • Microsoft Outlook 2013 • Microsoft Outlook 2010 • Microsoft Outlook 2007 (minimum SP1) <p>32- and 64-bit versions of Outlook are supported.</p>
Server	Intra2net Business Server version 6.0.0 or higher



Caution

Only one version and bit variant of Microsoft Office products may be installed on the system. Different versions of Outlook and other Office components, as well as different versions of Outlook at the same time (as partially supported by Outlook 2013, so-called side-by-side installations), cannot be used reliably with the Groupware Client.

Also if Office related apps (including "My Office", "OneNote", and "Office Lens") are installed from the Microsoft Store, this can lead to an incompatible side-by-side installation. These apps are pre-installed on some versions of Windows and must be uninstalled via the Microsoft Store.

We also advise against using Click-to-Run installations of Microsoft Office 2013, as we have observed some Click-to-Run-related malfunctions in this version. Instead, use a fully local offline installation.

17.2. Overview of Features

- Shared access to emails, appointments, contacts, tasks and notes
- Folders of other users can be shown anywhere in Outlook and can be freely locally named
- Backup of groupware data and emails on the server
- Background synchronization of all folders
- Adjustable synchronization frequency by folder
- Simultaneous use of multiple server accounts and email addresses within one Outlook profile
- Simultaneous connections with several different servers, e.g. to share data between head office and branch offices
- Configuration of server-side out-of-office mode and email forwarding within Outlook
- Use and update of free/busy information together with the Intra2net system.
- Web access to emails, appointments, contacts, tasks and notes (Intra2net Business Server feature, see 31. Chapter, „Introduction to Web Groupware“)
- Data synchronization with mobile devices via ActiveSync (Intra2net Business Server feature, see 34. Chapter, „Connecting Mobile Devices using ActiveSync“)

17.3. Known Limitations

The following features supported by Microsoft Outlook cannot be used in conjunction with the Intra2net Groupware Client:

- The Intra2net Groupware Client cannot be used with a Microsoft Exchange data file on the same profile. However, it is possible to work together in different Outlook profiles on the same PC without any problems.
- Limitations on handling invitations when using the account on multiple devices or with shares.

Incoming invitation emails, appointments created from them and self-created appointments with invitations should only be accepted or edited with the Groupware Client and only on one device. Otherwise the appointment may be duplicated, incorrect messages to the organizer or incorrect display of the invitation status may occur.

- Changed attendees of a recurring element in a recurring appointment
- Full-day appointments series that extend over several full days
- Journal feature
- Linking groupware items with each other (e.g. between a contact and an appointment)
- Attaching files to groupware objects (not to emails). Files attached to groupware objects are not written to the server and are therefore not visible to other users or devices. If

the object is modified by another device or user, the attachment is removed. They are also not included in the backup.

- Task assignments received by email cannot be processed
- Email tags for tracking and tracing with dates are not written to the server and are therefore not visible to other users or devices. It is also not included in the backup. Therefore, use the method described in Section 25.4, „Email Reminders and Tracking“ instead of the tag for tracking.
- If an email is both answered and forwarded, only one of the two is displayed as a status in Outlook.
- It is not possible to rename shared folders of other users. Only the owner can rename folders.
- No automatic execution of client-side sort rules in Outlook. Instead, use server-side sort rules as described in Section 24.3, „Editing Server-Side Settings“.
- Outlook's "undo" function is not supported.
- Automatic response to read receipts requested by the sender of an email (*Message Disposition Notification* (MDN)). See Section 25.5, „Read receipts“.
- The Groupware Client is designed for up to 500 folders, 50,000 objects per folder and email and groupware data of up to 10 GB (accounts connected in a data file, measured on the server, e.g. via the menu "Information > Statistics > Users").

If these values are exceeded, disruptions may occur. These include, but are not limited to, delays in responding to user input, delays in synchronizing changes, and program crashes.

- The fixed maximum size of the data file is 50 GB (for Outlook 2007: 20 GB). The data file contains all linked folders, regardless of whether they are own folders or shared ones of other users. When the maximum size is reached, the data file is irreparably damaged and all data must be freshly synchronized in from the server.

Using the option "Only headers" (see Section 25.1, „Retrieve Emails Completely or Only Headers“) you can save space in the data file.

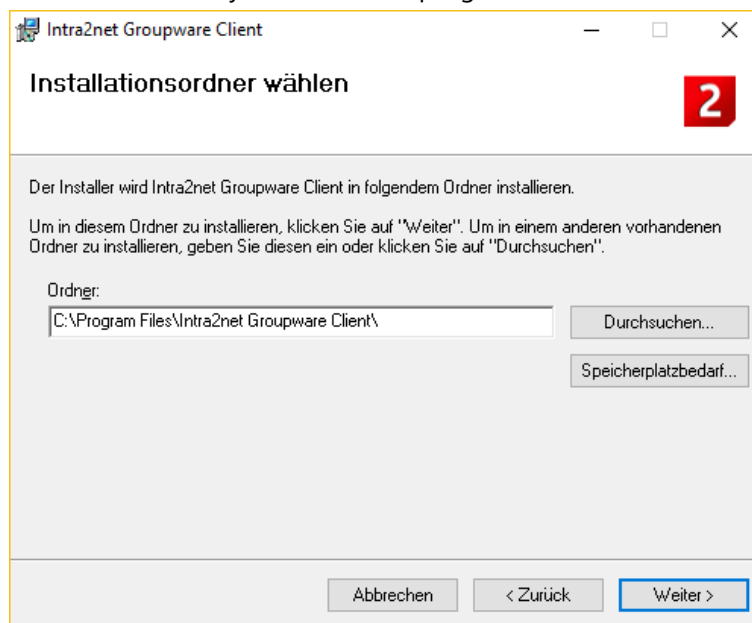
- In the quick search function of Outlook (but not in the advanced search), while the search is running, search hits appear in random order first. Once the search is complete, it can be sorted. In addition, deleted items cannot be excluded from the quick search.
- Unable to use the "Notifications" folder name at the top level of the data file.
- Folder names that differ only by upper and lower case from other folder names on the same level as well as folder names that start or end with spaces are not supported. This is a limitation of Outlook.

Please also note the following Section 30.1, „Synchronizable data“.

18. Chapter - Installation

18.1. Installing the Program

1. Unpack the ZIP archive in which the program is delivered. It contains 2 MSI files. Use the file with the suffix `-win32` if Outlook is installed in the 32 bit version and the file with the suffix `-x64` for the 64 bit version. Call the corresponding MSI file with the Windows Installer.
2. Follow the instructions on the screen and read the End User License Agreement (EULA) carefully. This can also be found at Section B.1, „Intra2net Groupware Client License Agreement (EULA)“.
3. Select the directory for where the program should be installed and press "Continue".



4. If no Outlook profile has been created for the groupware client so far, it is possible to create a suitable profile directly from the installation program. Enter the user and account data.

Enter the complete DNS name including the domain of the Intra2net Business Server under Server, do not enter any IP addresses. If the client should also be able to access from outside the local network, use the external DNS name of the Intra2net system. Again, do not use an IP address, but register a DNS name for your server with your domain provider or DynDNS provider.

Under Username, enter the login exactly as it is specified on the Intra2net Business Server under Usermanager > Users. In the Username field, do not add an @ and a domain name.

For correct operation, the data file must be stored on a local drive of the client PC. The use of network drives leads to disturbances in data synchronization and in sending emails.

If the groupware client needs to be configured later, the necessary steps are described in 19. Chapter, „Setting up a Profile“.

5. Continue with the setup in 20. Chapter, „Account Configuration“.



Hint

To enable all options for the Outlook profile generation, the installation program sets the following value in the registry:

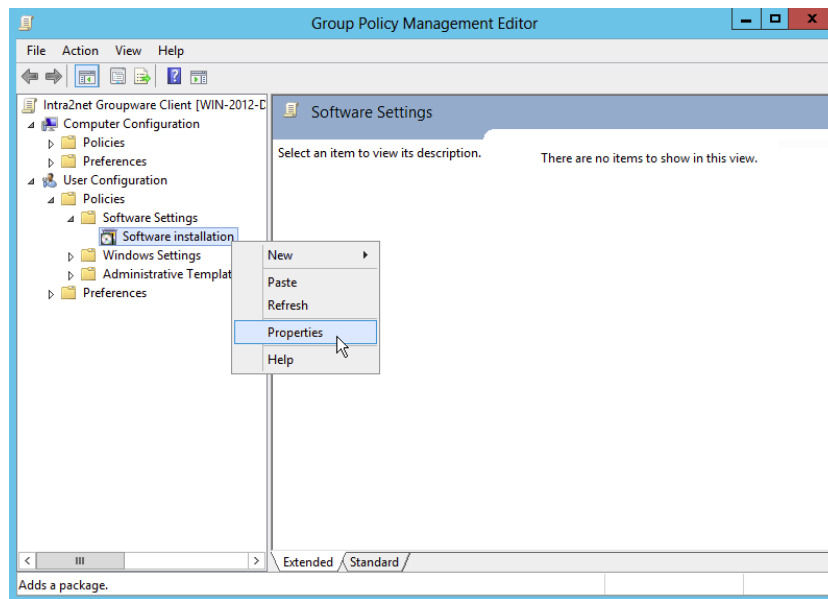
Key HKCU\Software\Policies\Microsoft\Office\16.0\Outlook\setup,
name DisableOffice365SimplifiedAccountCreation, type REG_DWORD,
value 1

18.2. Distributing the Program via Active Directory

The program is delivered as an MSI file and can be distributed and updated via Active Directory on the computers of a Windows domain. Instructions for software distribution via Active Directory can be found at <http://support.microsoft.com/kb/816102>.

Note that the program must be installed with the "Basic" user interface option:

1. Start the Group Policy Management Editor and open the hierarchy tree up to "Software Installation"
2. Right click on "Software installation" and open "Properties"



3. Select the "Basic" user interface option.



4. Only now add the MSI of the groupware client to the software installation policy.

18.3. Switch from 32 bit to 64 bit

If you have installed Outlook and the Groupware Client in the 32 bit version and now want to change to the 64 bit version or vice versa, please proceed as follows:

1. Close Outlook and all other components of Office
2. Uninstall the Groupware Client
3. Uninstall Microsoft Office
4. Install Microsoft Office in the new bit variant
5. Install the Groupware Client in the new bit variant

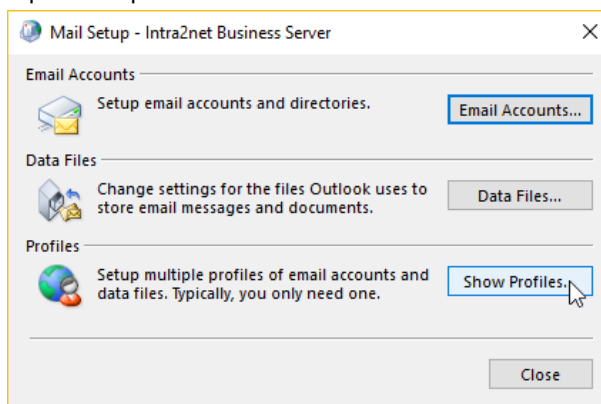
The Outlook profile and the data file(s) of the Groupware Client can be used unchanged. Only if you switch from a higher Outlook version to a lower one (e.g. from Outlook 2019 to Outlook 2013) at the same time, you have to create a new profile and data file to ensure the complete consistency of the data.

19. Chapter - Setting up a Profile

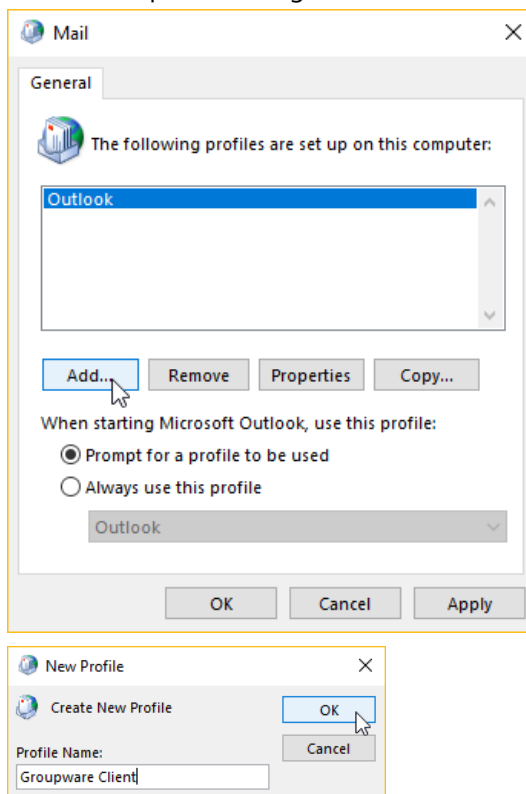
To use the groupware client, a new Outlook profile must be created. Largely independent of the installed version of Outlook, this is done through the control panel, and is described below.

Existing data can be imported into the new profile after the basic configuration. This is described in Section 20.2, „Importing Existing Data“. Adding the groupware client to an existing profile is not recommended.

1. After opening the Windows Control Panel, navigate to "Mail (Microsoft Outlook)", or "Mail". The exact name of the menu item depends on the versions of Windows, Outlook and the chosen system language. For some versions of Windows, it may be necessary to first display all items in the Control Panel.
2. Open the profile editor



3. Add a new profile and give it a name



4. Select "Manual setup or additional server types" and then "Other" and "Intra2net Business Server".

The first screenshot shows the 'Add Account' window with the 'Auto Account Setup' section. It has a title bar with a close button. Below the title bar, it says 'Auto Account Setup' and 'Manual setup of an account or connect to other server types.' There are two radio buttons: 'Email Account' and 'Manual setup or additional server types'. The 'Manual setup or additional server types' radio button is selected. Below it, there are input fields for 'Your Name', 'Email Address', 'Password', and 'Retype Password'. The 'Email Address' field has an example: 'ellen@contoso.com'. The 'Password' field has a note: 'Type the password your Internet service provider has given you.' At the bottom, there are buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

The second screenshot shows the 'Add Account' window with the 'Choose Your Account Type' section. It has a title bar with a close button. Below the title bar, it says 'Choose Your Account Type'. There are four radio buttons: 'Office 365', 'POP or IMAP', 'Exchange ActiveSync', and 'Other'. The 'Other' radio button is selected. Below it, there is a text box for 'Email Address' with an example: 'ellen@contoso.com'. Below that, there is a list box with the text 'Connect to a server type that is listed below' and 'Intra2net Business Server' selected. At the bottom, there are buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

5. Enter the user and server data.

Enter the complete DNS name including the domain of the Intra2net Business Server under Server, do not enter any IP addresses. If the client should also be able to access from outside the local network, use the external DNS name of the Intra2net system. Again, do not use an IP address, but register a DNS name for your server with your domain provider or DynDNS provider.

Under Username, enter the login exactly as it is specified on the Intra2net Business Server under Usermanager > Users. In the Username field, do not add an @ and a domain name.

For correct operation, the data file must be stored on a local drive of the client PC. The use of network drives leads to disturbances in data synchronization and in sending emails.



Hint

If this dialog is not displayed, Microsoft Outlook is not installed correctly or in an incompatible configuration. Therefore, cancel at this point and fix the Outlook installation problem first. Then start again with step 1.

First check the Section 17.1, „System Requirements“, especially the point with side-by-side installations triggered by apps from the Microsoft Store (e.g. "My Office", "OneNote" and "Office Lens"). Then try a repair installation of Microsoft Office.

6. Outlook can open the newly created profile automatically on startup if desired.

7. Continue with the setup in 20. Chapter, „Account Configuration“.

20. Chapter - Account Configuration

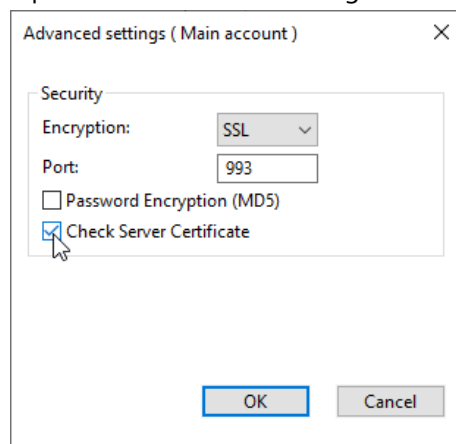
20.1. Groupware Account

To complete the installation, the settings described in the following sections must be configured.

20.1.1. Activate Certificate Check

Activate the certificate check when using an IMAP connection. This means that passwords are only sent using secure connections. This setting is especially important when connecting to the server over the Internet.

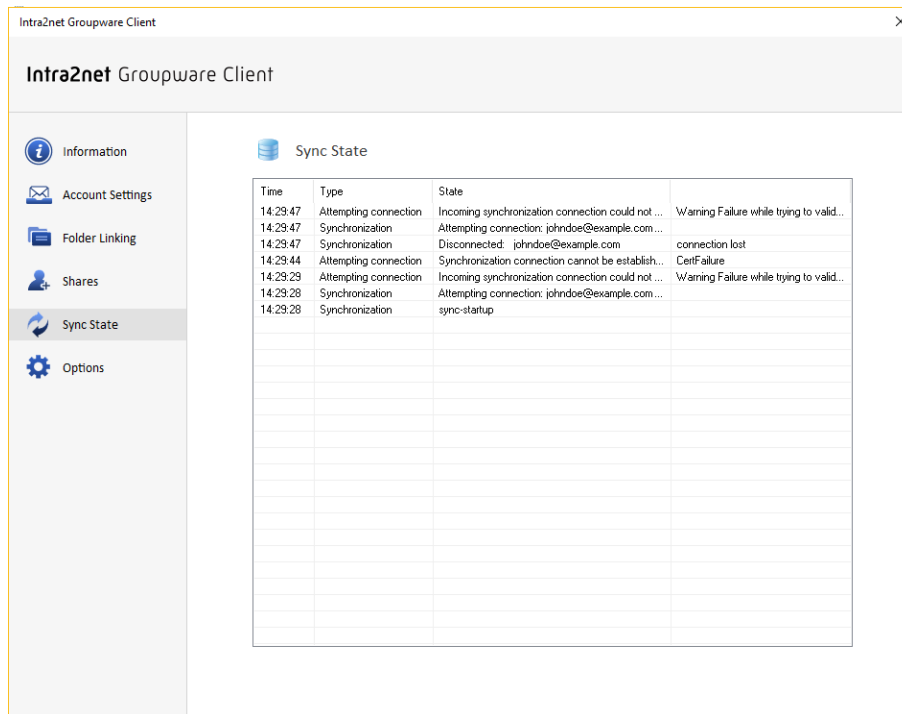
1. Start Microsoft Outlook and open the profile with the Intra2net Groupware Client.
2. Open the menu "Groupware Client", "Account settings".
3. Open the "Advanced Settings" menu and select Check Server Certificate.



4. Click "Save" to save the settings.
5. Open the "Sync State" menu of the groupware client and check that the connection can still be successfully established.

20.1.1.1. Procedure for Certificate Errors

If a `CertFailure` is displayed in sync state, the server's certificate is not considered trustworthy.



In this case, the following points should be verified:

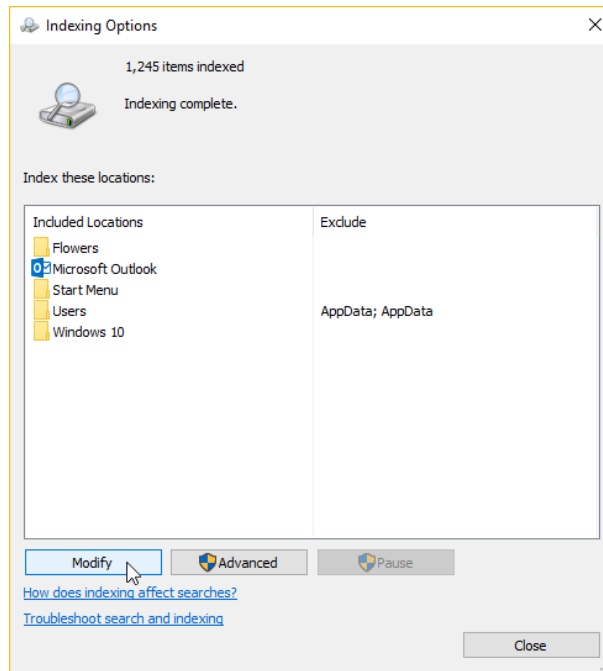
1. First check that the complete DNS name of the server, including the domain, is specified in the groupware client, as opposed to an IP.
2. If the DNS name is a local domain or if the certificate was not created by an external certification authority, the certificate must be registered as trusted in Windows. Follow the steps described in Section 9.3, „Installing Certificates on Clients“.
3. Lastly, check that the server's certificate was created correctly. See Section 9.2, „Correctly Creating Certificates“

20.1.2. Deactivating the Search Indexer

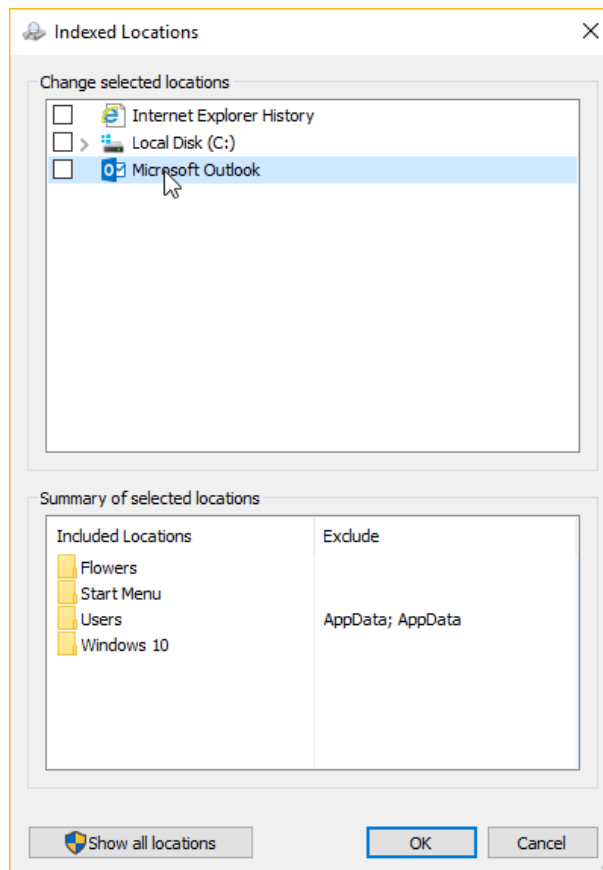
Windows has a central service for indexing user data, which can then be searched through the system wide search function. This service is called Search Indexer.

By default, the search indexer also attempts to index data from Outlook, but this is not supported by the Groupware client in this way. In many cases, this leads to performance bottlenecks and a sluggish response to user interaction in Outlook. Most importantly, the startup process of Outlook will also be prolonged. Therefore, we advise against allowing the search indexer to index Outlook. Proceed as follows:

1. Open the Windows Control Panel, then "Indexing Options".
2. Select "Modify".



3. Uncheck "Microsoft Outlook".



4. Confirm the settings with "Ok" and close the indexing options.

20.2. Importing Existing Data

If Outlook was previously used with a different profile and it is required to continue with the pre-existing data on Intra2net Groupware Client, proceed as described below.

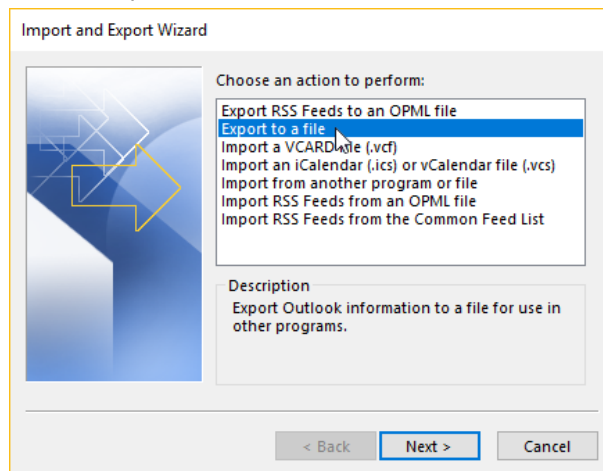
When using Outlook with Microsoft Exchange, the complete migration process is described under 29. Chapter, „Migration from Microsoft Exchange“.

20.2.1. Importing Using Outlook Import

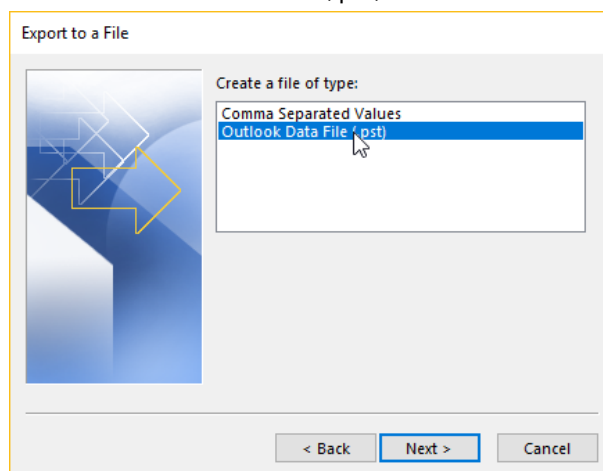
If the data to be imported has a size of up to about 1 GB, it can be easily imported into the Groupware Client using the procedure described here. If the emails to be transferred have sum up to a larger amount, this method can still be used, but will take longer. A faster import is then normally possible with the method described under Section 20.2.2, „Importing Larger Amounts of Emails“.

20.2.1.1. Exporting Current Data

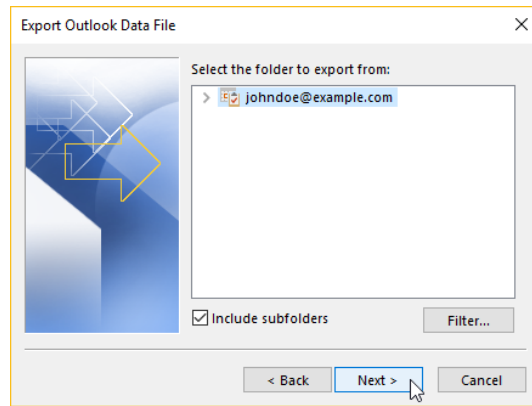
1. Open Outlook with the old profile containing the data to be imported. It may be necessary to change the profile that is opened by Outlook using the Windows control panel, under "Mail (Microsoft Outlook)", or "Email "
2. Open "File", "Open "
3. Select "Export to a file".



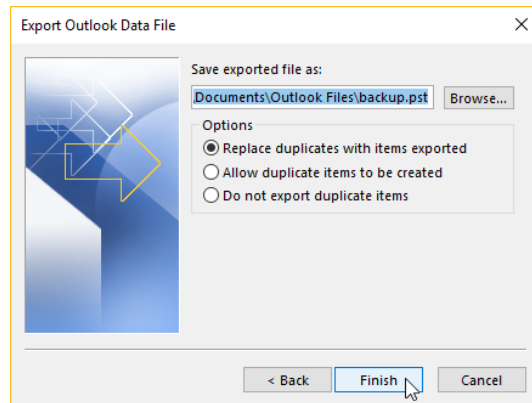
4. Select "Outlook Data File (.pst)".



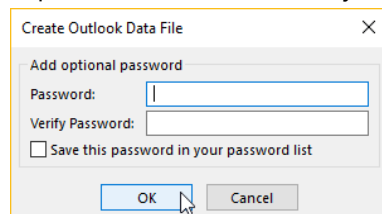
5. Select the required data file, including subfolders.



6. Select the directory and file to which you want to export the data.



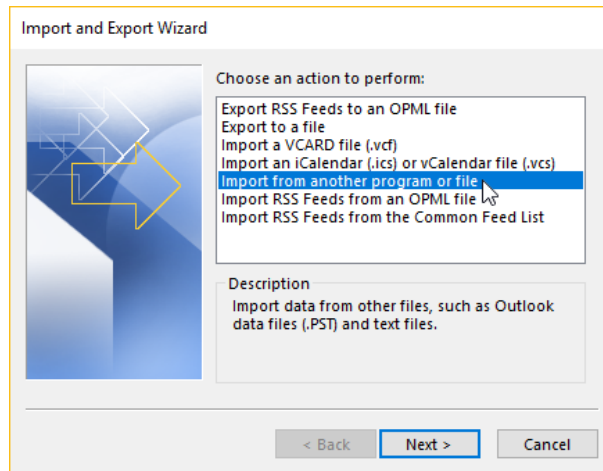
7. A password is not necessary



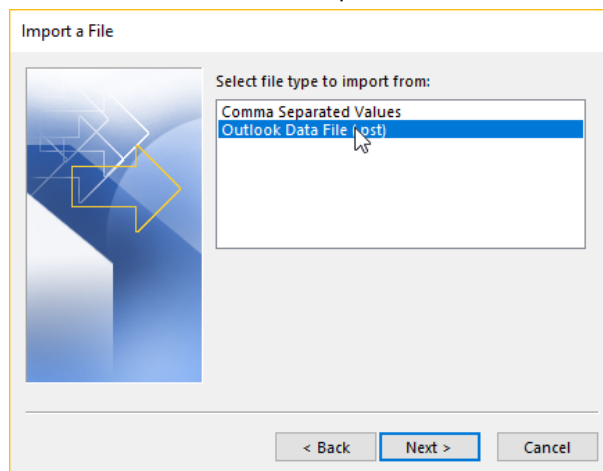
8. Wait until Outlook has exported all data.
9. Close Outlook.

20.2.1.2. Importing to the Groupware Client

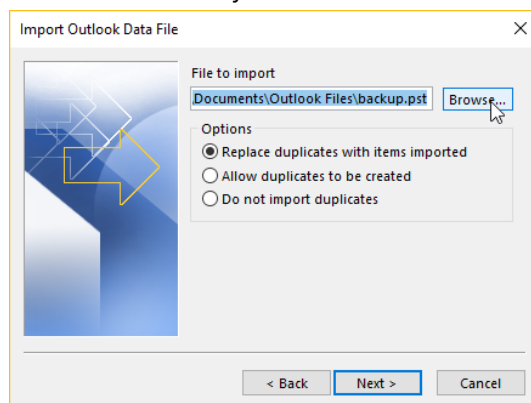
1. Open Outlook with the Groupware Client profile. It may be necessary to change the profile that is opened by Outlook using the Windows control panel, under "Mail (Microsoft Outlook)", or "Email "
2. Open "File", "Open "
3. Select "Import from another program or file".



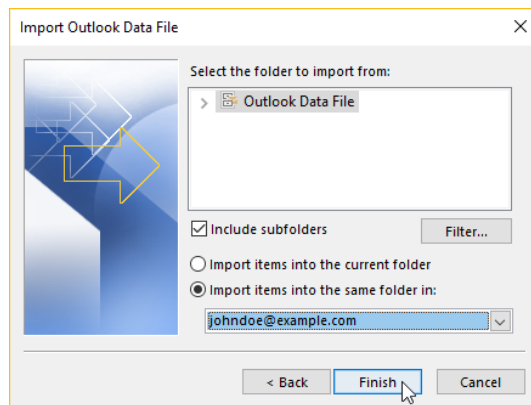
4. Select "Outlook Data File (.pst)".



5. Select the directory and file into which the data was exported.



6. Import the data including subfolders to the current data file, into the same folder.



7. Wait until Outlook has imported all data.
8. The Groupware Client starts to write the data to the server in the background during the import. However, this usually takes longer than importing the file into Outlook and therefore continues to run in the background even after the import is completed. The progress can be followed in the "Groupware Client", "Sync State" menu.

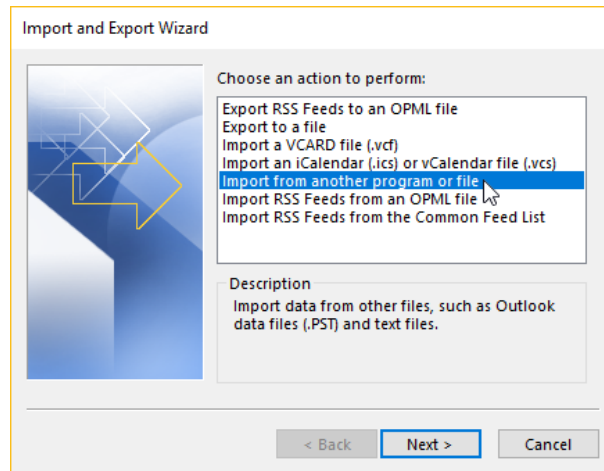
20.2.2. Importing Larger Amounts of Emails

To use existing data with the Groupware Client which contains large amounts of emails, the method described here is recommended.

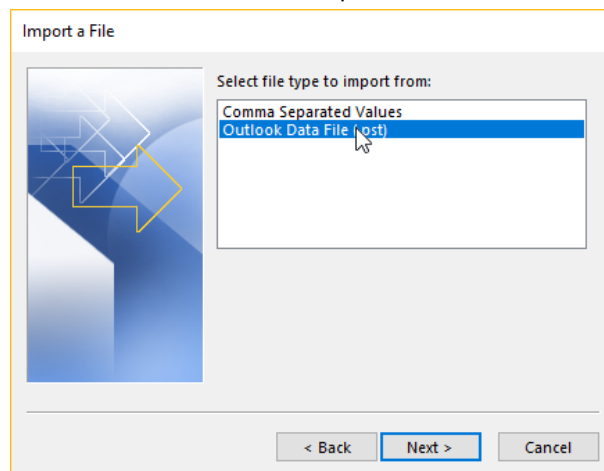
It is necessary that the emails are on an IMAP accessible server. Most email servers are reachable by IMAP by default, or at least this feature can be activated as an option. Using an additional program, the emails can be copied directly from the previous server to the Intra2net system via Outlook. However, only the emails can be copied via IMAP, not the groupware data. The groupware data (calendar, contacts, tasks and notes) is usually not so large and can therefore be transferred via the import/export function of Outlook.

Should the data volume be less than approximately 1 GB, or the emails are not on a server accessible via IMAP, use the method described under Section 20.2.1, „Importing Using Outlook Import“.

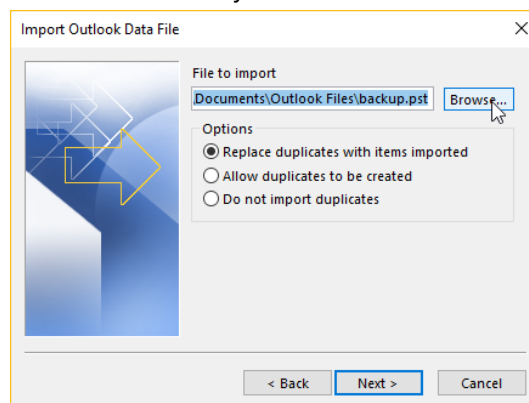
1. Transfer the emails from the previous server as described in 28. Chapter, „Migrating Emails with IMAPCopy“.
2. Export the data from the existing Outlook profile as described in Section 20.2.1.1, „Exporting Current Data“.
3. Open Outlook with the Groupware Client profile. It may be necessary to change the profile that is opened by Outlook using the Windows control panel, under "Mail (Microsoft Outlook)", or "Email "
4. Open "File", "Open "
5. Select "Import from another program or file".



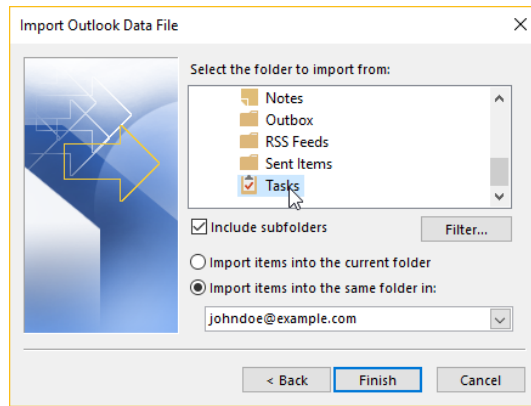
6. Select "Outlook Data File (.pst)".



7. Select the directory and file into which the data was exported.



8. Do not import all data, just the folders with groupware data (calendar, contacts, tasks and notes). Select the first folder with groupware data, in this example `Tasks`.



9. Repeat the import process for all other groupware folders.

20.3. Setting up Multiple Accounts and Email Addresses

It is possible to use multiple accounts on the server and multiple email addresses simultaneously within one Outlook profile. This is useful, for example, to connect a company-wide account such as "info" or to be able to effectively represent a colleague.

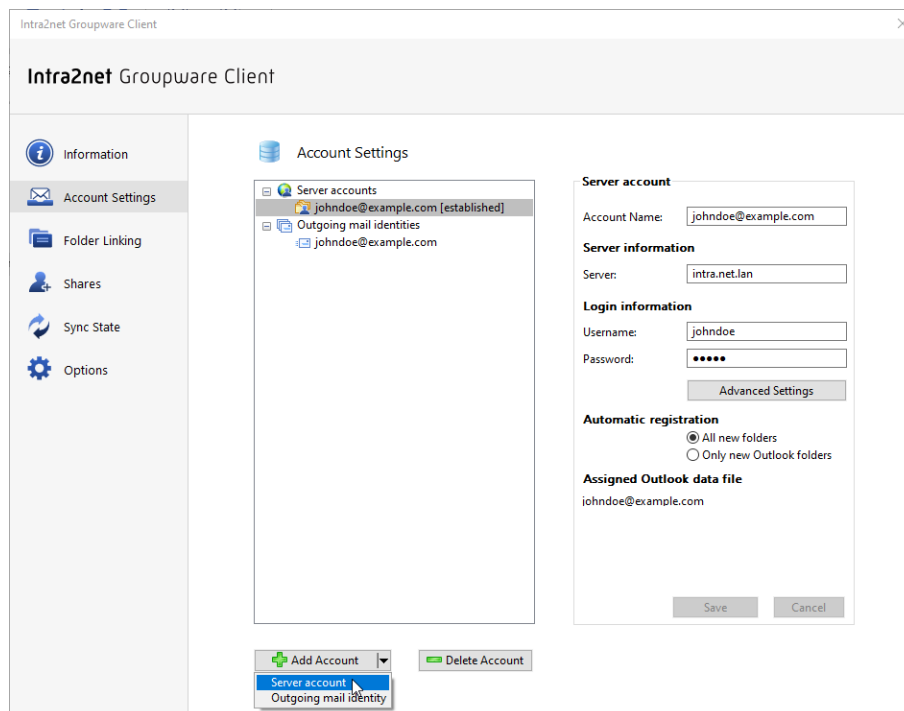
20.3.1. Multiple Server Accounts



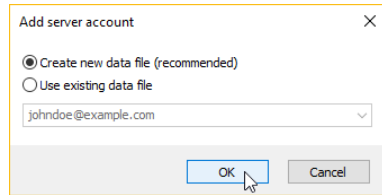
Caution

Only use the Groupware Client menus described below to configure accounts. Do not use Outlook's account settings.

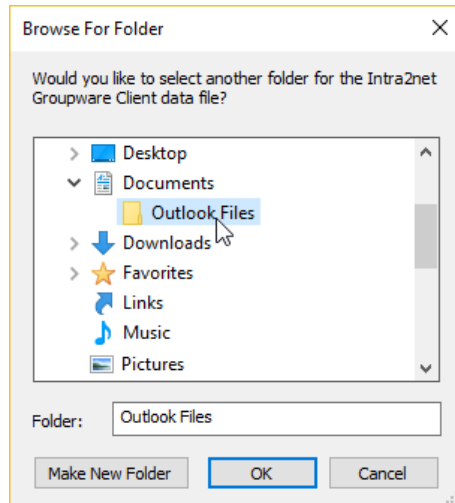
1. Open the menu "Groupware Client", "Account settings".
2. Under "Add Account", select "Server Account".



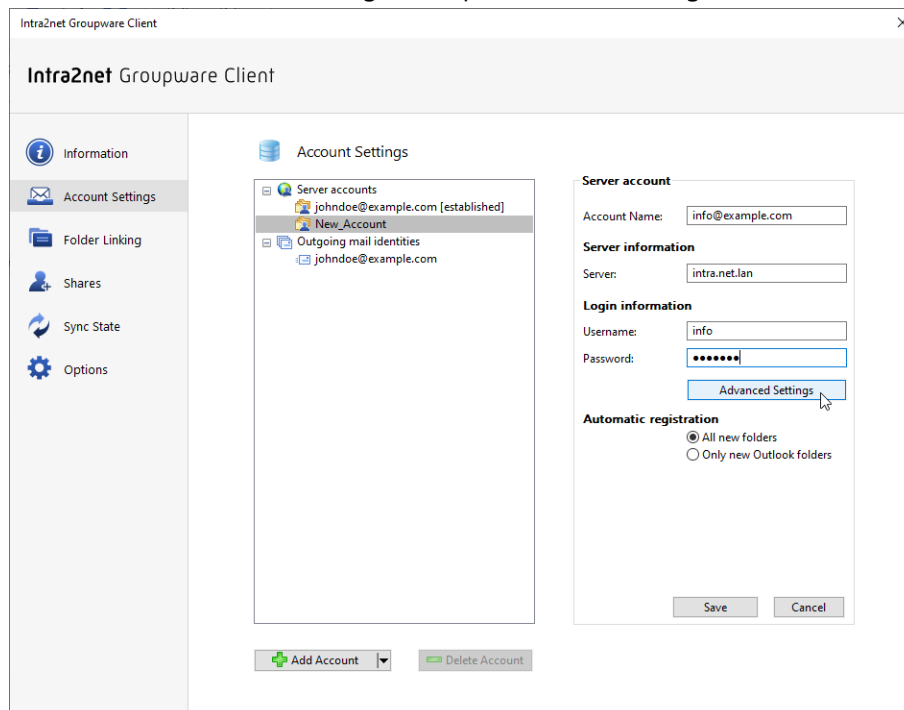
3. Select "Create new data file" if you want to insert the entire account as an additional data file. The "Use existing data file" option is intended for cases where only individual folders of the new account are to be connected in the "Shared folders" directory.



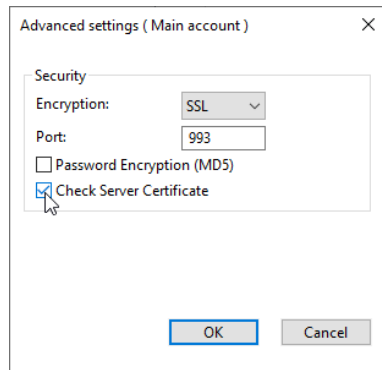
4. Select the folder in which you want to store the new data file.



5. Enter the full server name, login and password and assign an account name.



6. Open "Advanced Settings" and turn on the server certificate check.



7. Save the settings.

20.3.2. Multiple Outgoing Mail Identities

It is possible to configure any number of different email sender addresses, regardless of the number of server accounts. If necessary, different folders can be defined for storing the emails sent for these sender addresses.

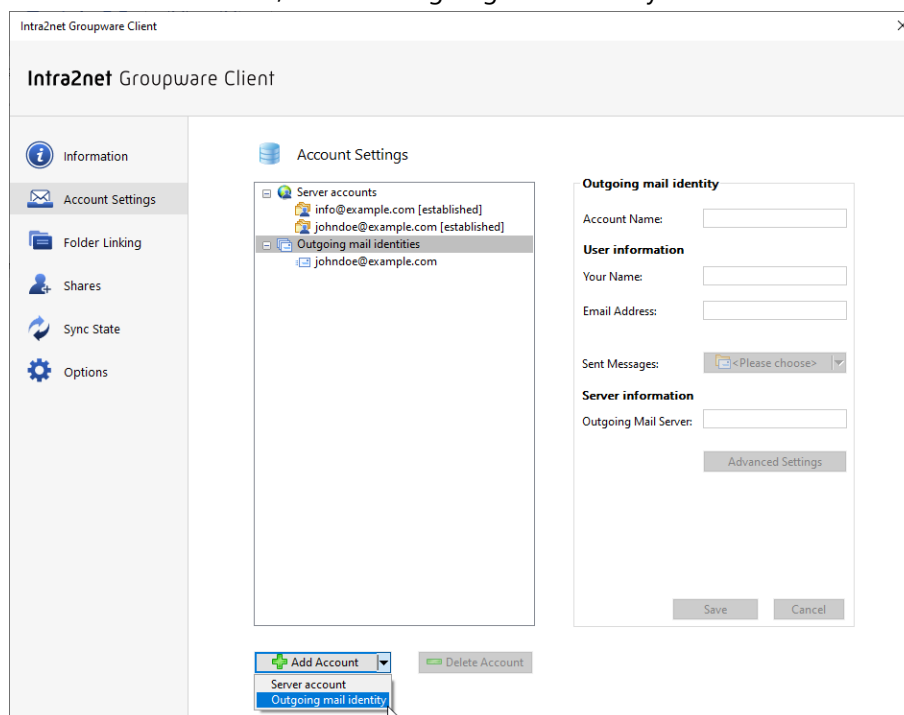


Caution

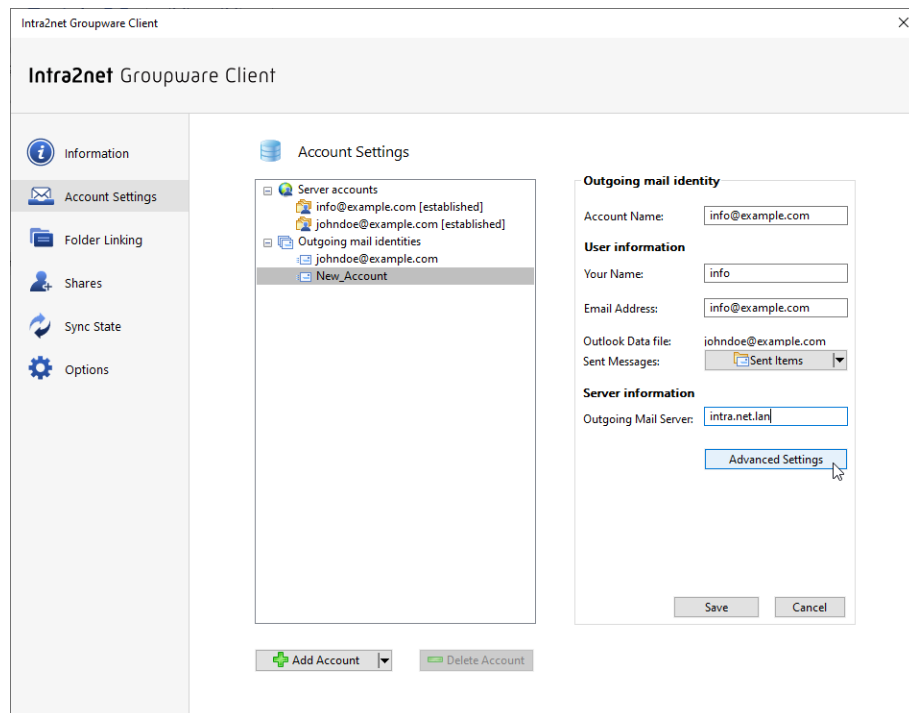
Only use the Groupware Client menus described below to configure accounts. Do not use Outlook's account settings.

Proceed as described below to create new sender addresses.

1. Open the menu "Groupware Client", "Account settings".
2. Under "Add Account", select "Outgoing Mail Identity".

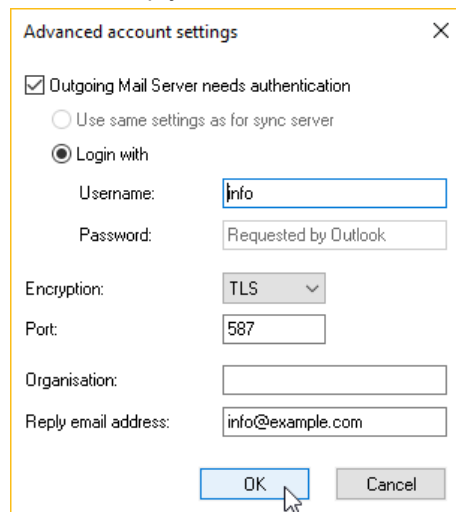


3. Enter the user name, email address, outgoing mail server, and assign an account name.

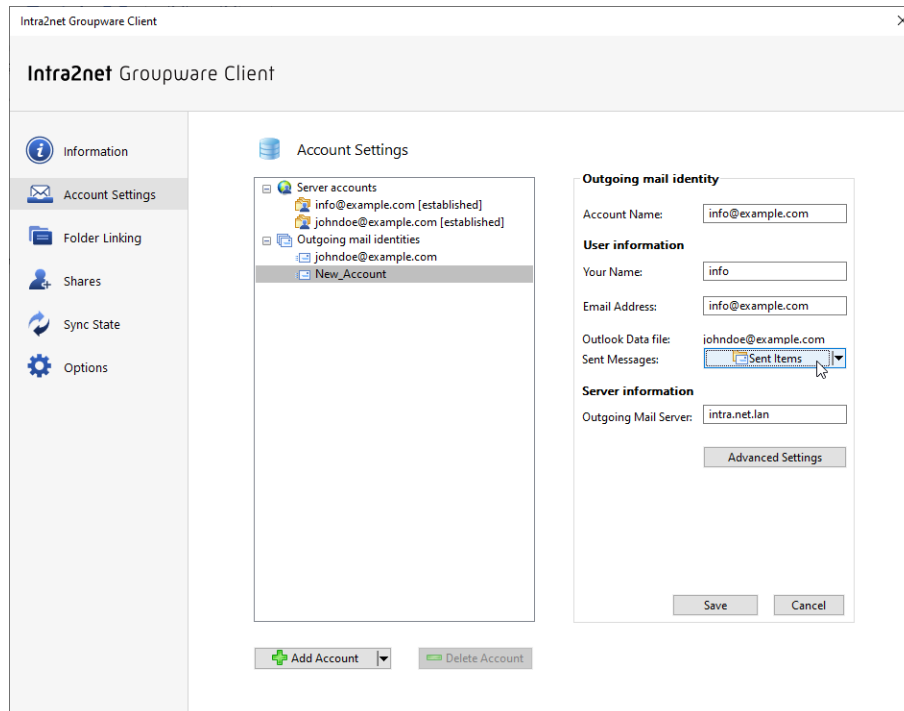


4. Open "Advanced Settings", activate encryption via TLS and set the port used to 587.

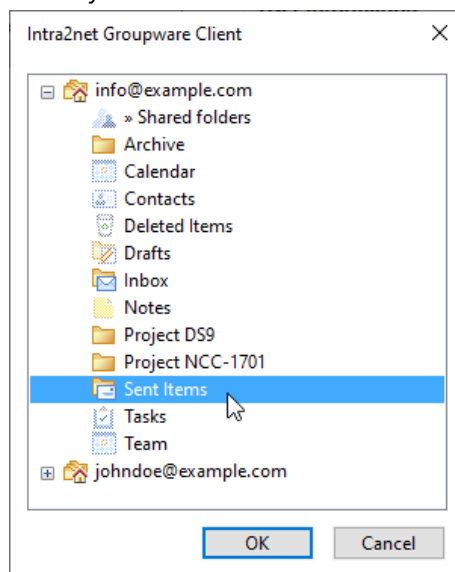
If necessary, authentication can also be activated and an organization name and a different reply address can be entered.



5. Click on the selection box beside "Sent messages".



6. Select the folder in which you want to store messages sent with this Outgoing mail identity.



7. Save the settings and restart Outlook.

20.3.2.1. Folder Selection for Sent Messages

If several different sender addresses have been configured for a server account, it is often advisable to store the sent messages in different folders depending on the sender address used. If one sender address is used by several users, it may be advisable to store the sent messages in a shared folder. To do this, the folder for the sent messages can be selected differently for each outgoing mail identity.

The following specifics apply if sent messages are to be stored in a folder other than "Sent Items":

- Sent emails are first stored in the "Sent Items" folder. A few minutes later, they are automatically moved to the selected folder.
- The "Sent Items" folder is automatically excluded from synchronization with the server. Therefore, make sure that other users of this account on the server do not continue to use "Sent Items". Synchronization in the opposite direction, i.e. from the server, still takes place.
- It is not possible for an outgoing mail identity to use the "Sent Items" folder while another outgoing identity uses a different folder in the same data file to store sent emails.

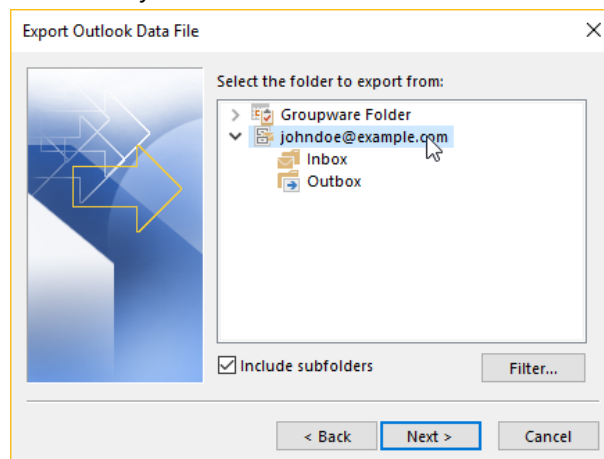
In this case, set folders other than "Sent Items" for all outgoing mail identities.

20.4. Converting Previous Installations of the Groupware Client

If the Intra2net Groupware Client was previously only used to synchronize the groupware data, and a separate IMAP data file managed by Outlook was used for emails, it is possible to switch the email processing to the groupware client.

The following describes how to make this conversion.

1. Use the Import/Export function to create a backup copy of the local data file for the emails. The export steps can be found under Section 20.2.1.1, „Exporting Current Data“. Only select the data file used for emails as the data source.



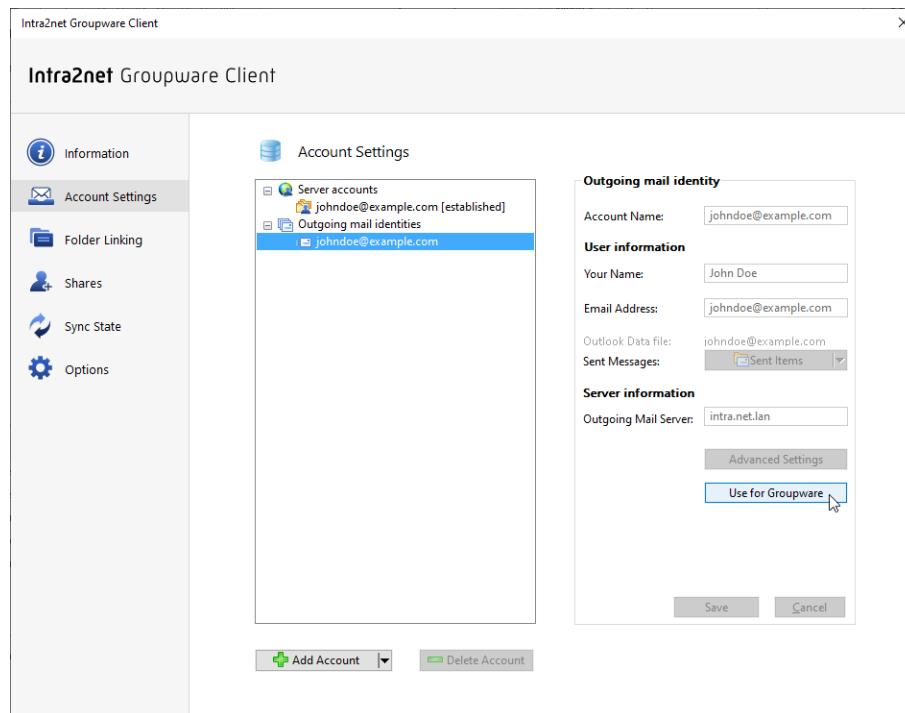
2. Open the newly exported backup copy by going to "File", "Open and Export", "Outlook data file" and check if it contains all email folders and if they are complete. Then close it again.



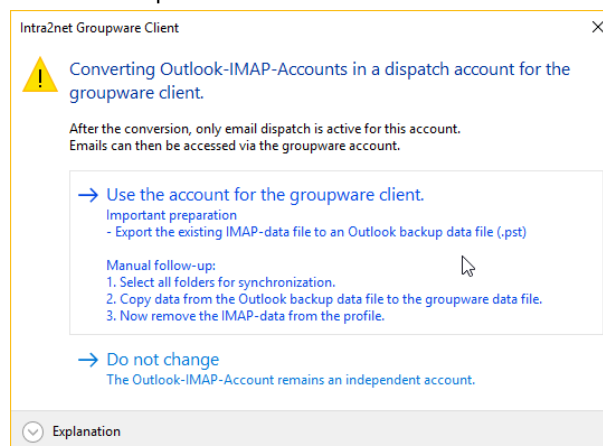
Caution

Without a complete backup, it is possible that emails may be lost.

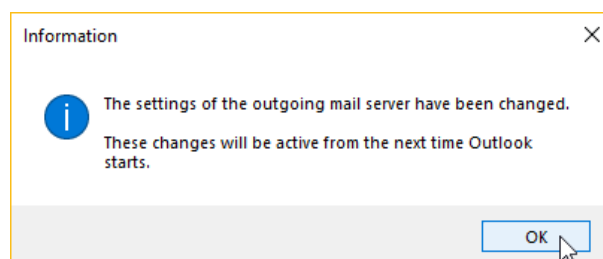
3. Open the menu "Groupware Client", "Account settings".
4. Under "Outgoing mail identities" select the previous IMAP account and click "Use for Groupware".



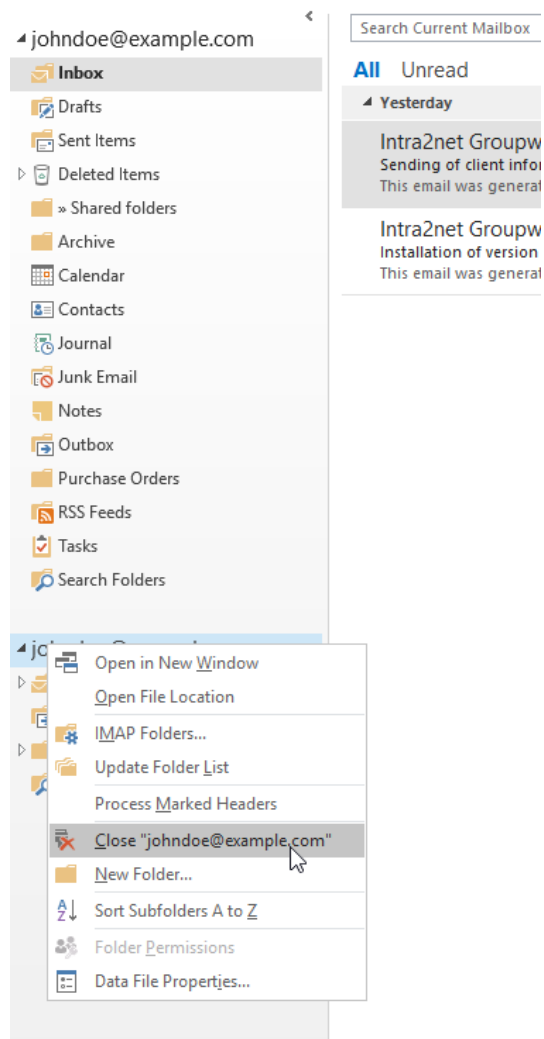
5. Having created a backup copy of the email data beforehand, the confirmation prompt can be accepted with "Yes".



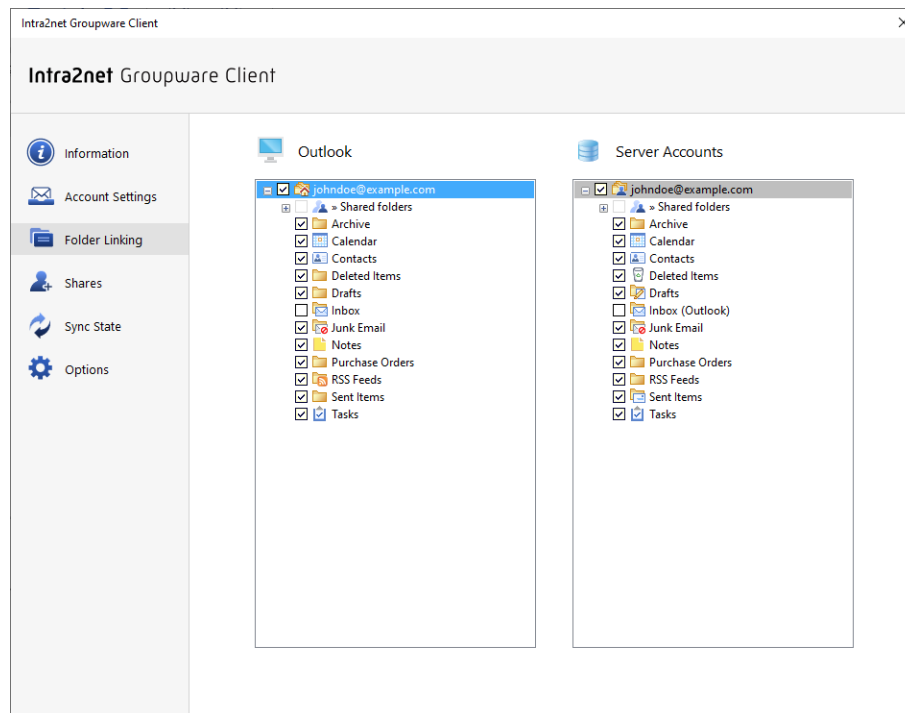
6. Quit Outlook, wait until the Outlook process is truly finished (see Task Manager) and restart it afterwards.



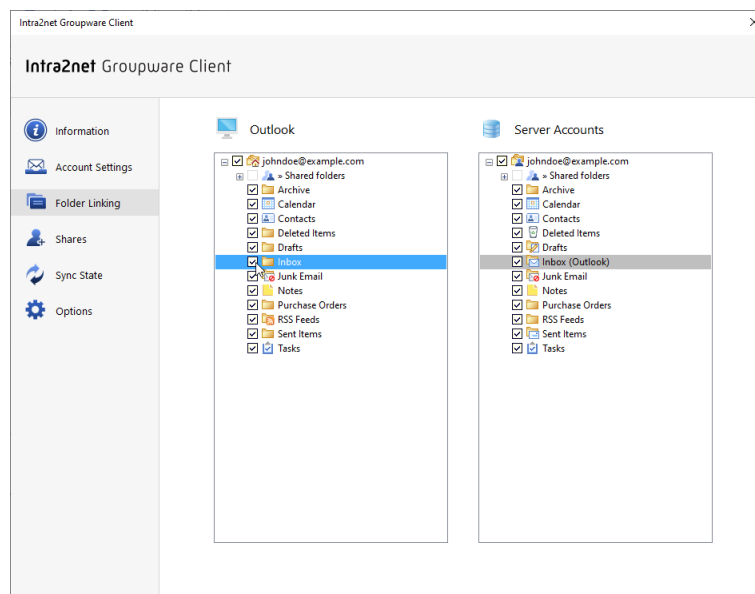
7. In the folder tree on the left-hand side of Outlook, the data file for the email account may still be displayed in some cases. This must then be removed. To do this, right-click on the data file and select "Close 'data file name'". The previous IMAP data file is recognizable by the fact that it *does not contain* a "Shared folders" folder.



8. Open the "Groupware Client" menu, and click "Folder Linking".
9. The missed checkmarks in front of the email folders indicate that they are not synchronized by the groupware client. This can be amended as follows:



10. Click on the checkbox in front of the folder name on the left side (Outlook) and check the box.



11. Repeat the previous step for all email folders.
12. You can follow the progress in the menu "Groupware Client", "Sync State".
13. After the synchronization is finished, check the content of the email folders for completeness.

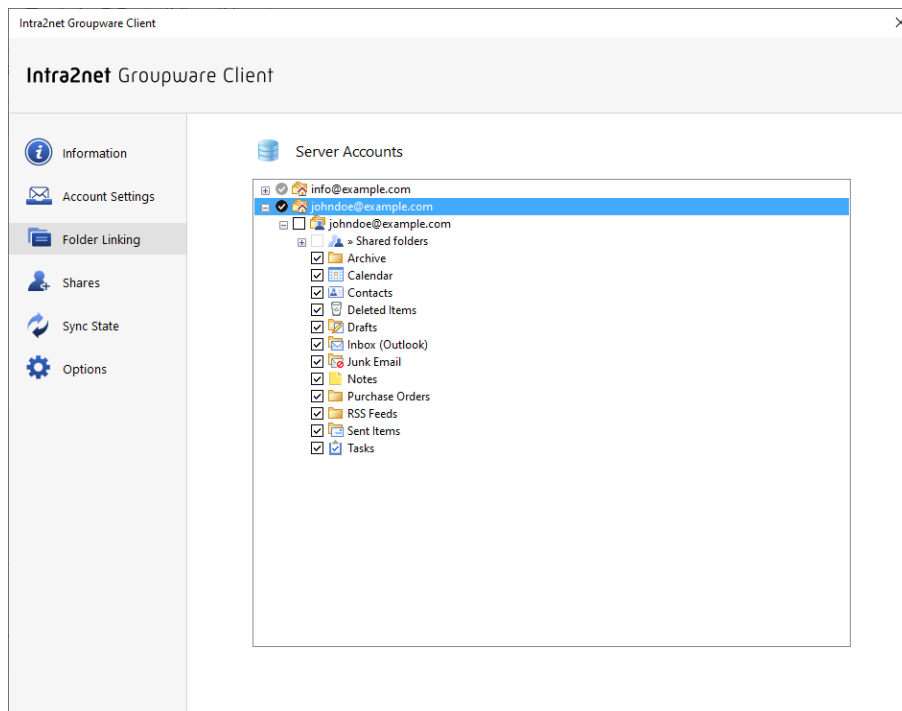
If entire folders or individual emails are missing, they can be copied from the backup created at the beginning. To do this, open the backup copy as an additional data file ("File", "Open", "Open Outlook Data File") and drag

21. Chapter - Linking Folders

The menu "Groupware Client > Folder Linking" controls which folders on the server account should be linked to the local Outlook data file.

This menu always displays the list of folders on the server. Linked folders (marked by set checkbox icon) then appear at the corresponding place in the folder hierarchy also within the local Outlook data file.

When a folder is linked, it means that all contents are synchronized between the local Outlook folder and the server folder.

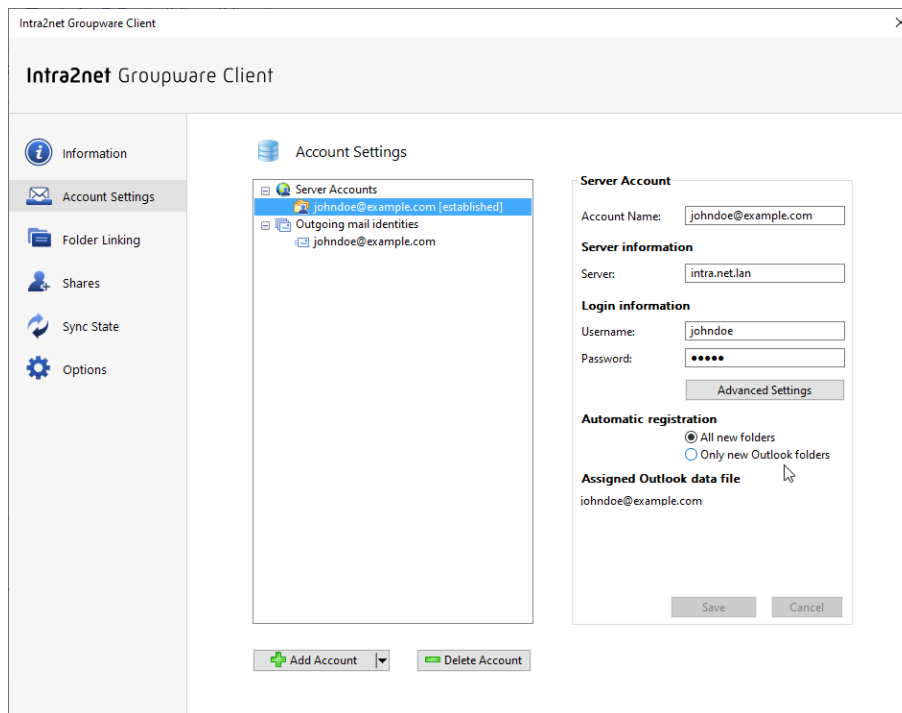


This chapter describes the standard mode for folder connections. Alternatively, there is also the expert mode, which is described in the 23. Chapter, „Folder Linking Expert Mode“.

21.1. Linking Own Folders

21.1.1. Automatic registration

By default, all folders owned by the server account are linked to the Outlook data file and, conversely, all new folders created locally are also created and linked on the server. This corresponds to the "All new folders" option in "Automatic registration" in the "Groupware Client > Account Settings" menu.



In some cases it may make sense that newly created folders on the server are not automatically connected and synchronized with the Outlook data file. E.g. if this would make the data file too large. In this case you can switch to "Only new Outlook folders". Folders newly created locally in Outlook will then continue to be automatically linked, but folders newly created on the server will no longer be linked. You will then have to click on them individually in the "Folder Linking" menu to link them.

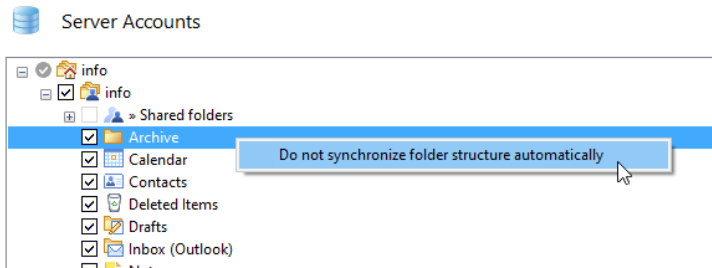
If own folders are deleted, renamed or moved in Outlook, this change is always immediately applied to the server as well.

21.1.2. Excluding Folders from Synchronization

It may be useful to keep folders only locally in the Outlook data file and not synchronize them with the server. E.g. it can speed up the deletion process if you do not synchronize Deleted Items with the server. Another example is the Drafts folder, the synchronization of which can conflict with the automatic saving of emails opened for editing and not yet sent.

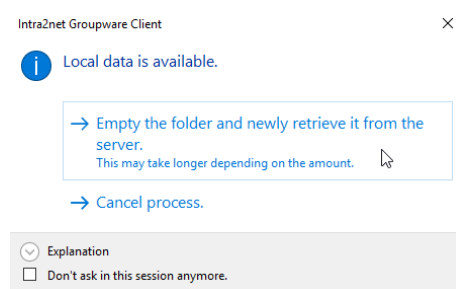
Another desired configuration can be to automatically synchronize new folders created on the server by default, but to exclude a few parts of the folder hierarchy.

For both you can use the function "Do not synchronize folder structure automatically". You can find this in the menu "Groupware Client > Folder Linking" if you right-click a folder there.



Note that a folder configured in this way always remains in the local Outlook data file with its contents, but the folder and its subfolders are exclusively local and are no longer synchronized with the server. If necessary, the subfolders can be deleted in Outlook. However, the folder itself must remain in order to get the exception from synchronization. If the folder were deleted from the local Outlook data file, it would be created again the next time the folder structure is synchronized, and its contents would be re-synchronized from the server.

If you want to undo the setting, set the checkbox of the folder again. In order to resume synchronization, all locally existing data and all subfolders must first be deleted and replaced by the content on the server. The user is informed about this in a dialog and must launch the deletion.



21.1.3. Update folder list

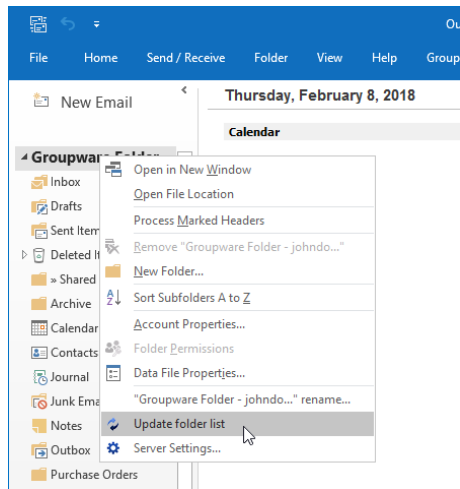
Server-side changes to the folder structure, e.g. folders newly created or renamed on the server, are detected in the background when Outlook is started and periodically thereafter and applied to the local Outlook data file. This process runs every 60 minutes



Hint

This only affects the folder structure itself, but not the content of the folders. For synchronization of the contents see Section 24.2, „Folder Options“.

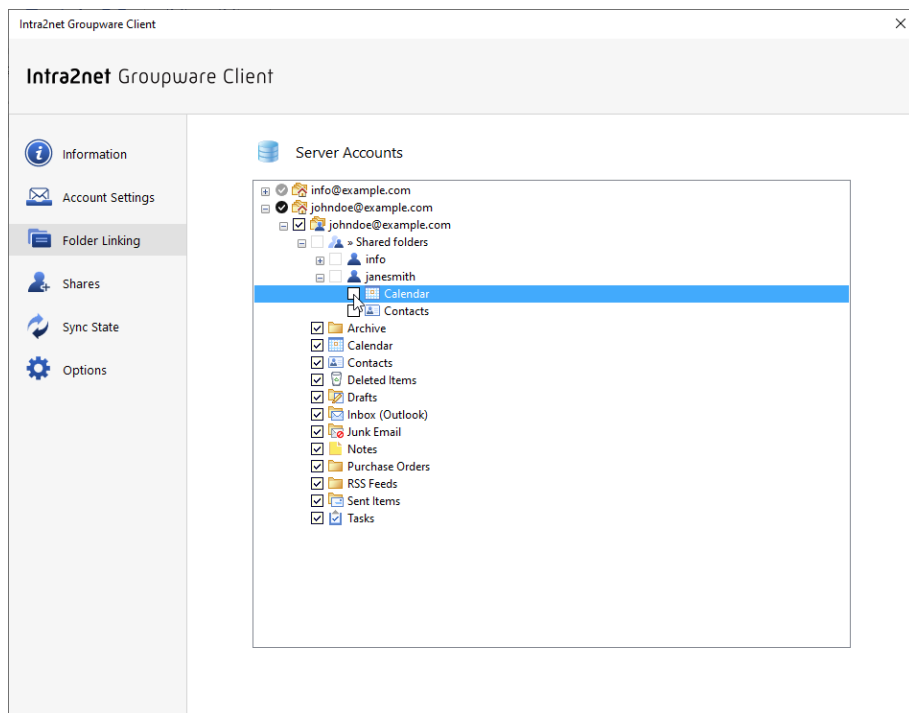
You can instruct the Groupware Client to update the folder structure immediately by right-clicking in the folder list to open the context menu of a folder managed by the Groupware Client and selecting the "Update folder list" option. This will update the folder structure of the entire Outlook data file.



21.2. Linking Shared Folders

If a folder has been shared with you or a group of which you are a member, you will see a notification about it in the Inbox the next time you start Outlook. Unlike own folders, new shared folders are not automatically linked.

Use the menu "Groupware Client > Folder Linking" and there the item "»Shared folders" to link shared folders and thus make them usable in Outlook. Click the checkbox icon to link or unlink a folder.



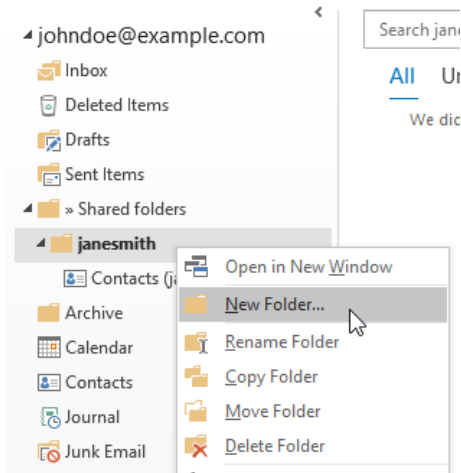
If you have the "Folder" right to a shared folder, you can delete the folder or create new subfolders. It is not possible to rename shared folders. Only the owner of the folder can do this. To delete subfolders, you need the "Folder" right for each subfolder.



Caution

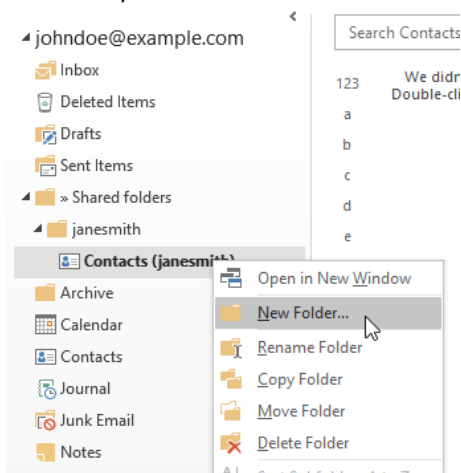
Creating and moving shared folders is not possible on the top folder level of a user account. Even if Outlook allows to create folders in this level, they are not linked to the server and are located purely locally in the Outlook data file.

Example:



Only the owner of an account is able to create folders on the top folder level or move them there.

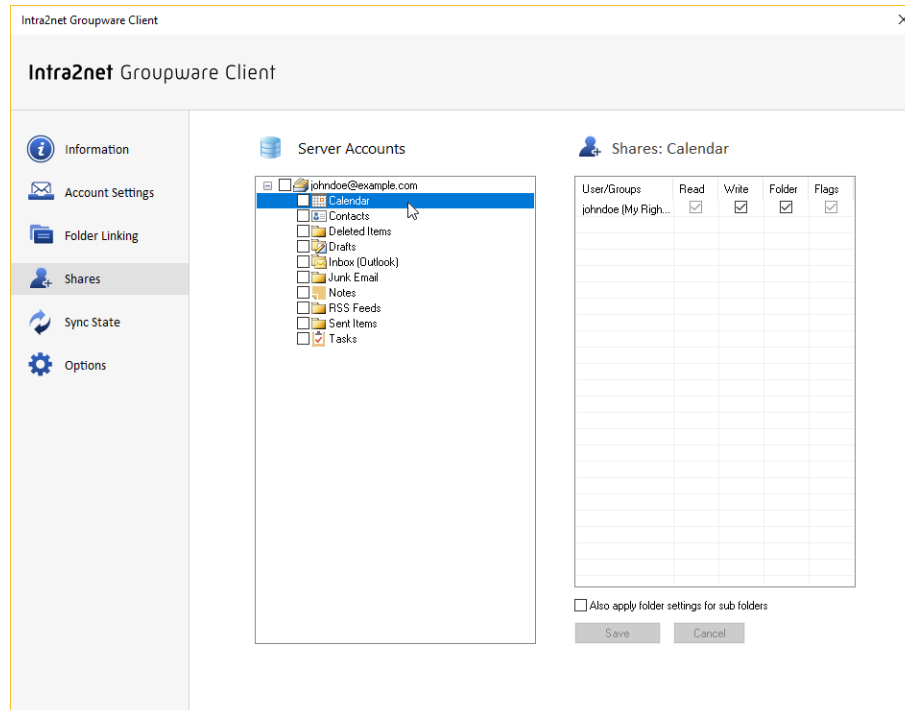
However, the creation of folders below a linked folder are synchronized to the server. In the example, a new folder is created below "Contacts".



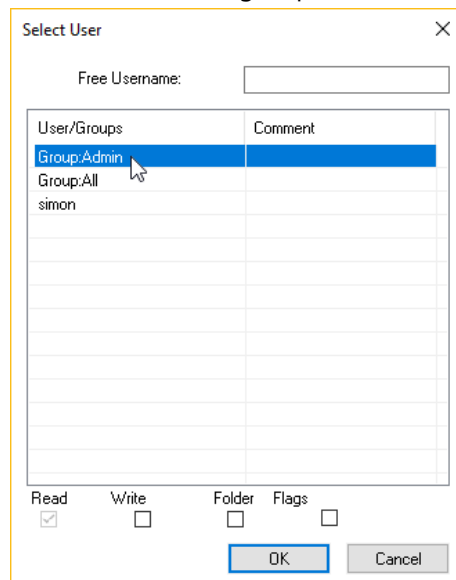
22. Chapter - Sharing Folders

To allow other users to access a folder, the owner must first share it as follows:

1. Open the "Groupware Client > Shares" menu.
2. On the left side (server accounts) click on the folder to be shared.



3. Double-click on the right side (Shares) to open the dialog for a new share. Select the user name or user group with which the folder is to be shared.



4. Use the checkboxes at the bottom of the dialog to select the rights that are to be granted to other users. Close the dialog with "Ok".
5. Click "Save" to add the new rights to the server.

After that, other users can link the shared folders as described in Section 21.2, „Linking Shared Folders“.

We advise against sharing with individual users, but with user groups on the Intra2net system. This simplifies the management of shared folders, especially during user fluctuation and restructuring.

22.1. Rights

The meanings of the various rights are as follows:

Read	The user can see the folder and all of its contents.
Write	The user can create new entries in this folder and change or delete existing ones.
Folder	The user can delete, rename, and create new subfolders within this folder. Additionally, the user gets administration rights to the folder and can change the sharing rights for other users. To delete folders with existing content, the user also needs the "Write" permission.
Flags	The user may change the read, reply, and flagged flags of the existing content.

The set rights normally only apply to the selected folder itself. With the corresponding option, the rights set for the selected folder can also be applied to all subfolders. Not only the currently changed rights are adjusted, but the complete rights set for the selected folder are set for all subfolders exactly the same as for the selected folder.

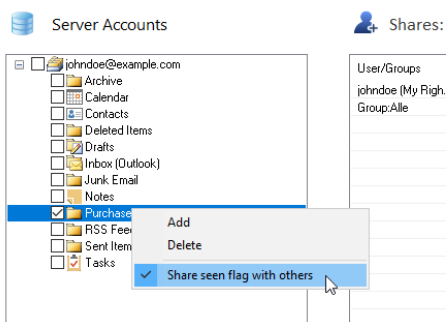
Newly created folders always adopt the rights of their parent folder when they are created.

22.2. Read Status Shared/Individual

The Intra2net system enables the management of the "read" or "unread" status of newly received emails either for all users or for each user with individual access rights to this folder. Which method is more suitable depends on the situation and the reason for sharing an email folder with other users. Therefore, both options can be selected.

If a new share to other users is configured in the menu "Groupware Client > Shares" with the right "Flags", the shared read status is automatically activated.

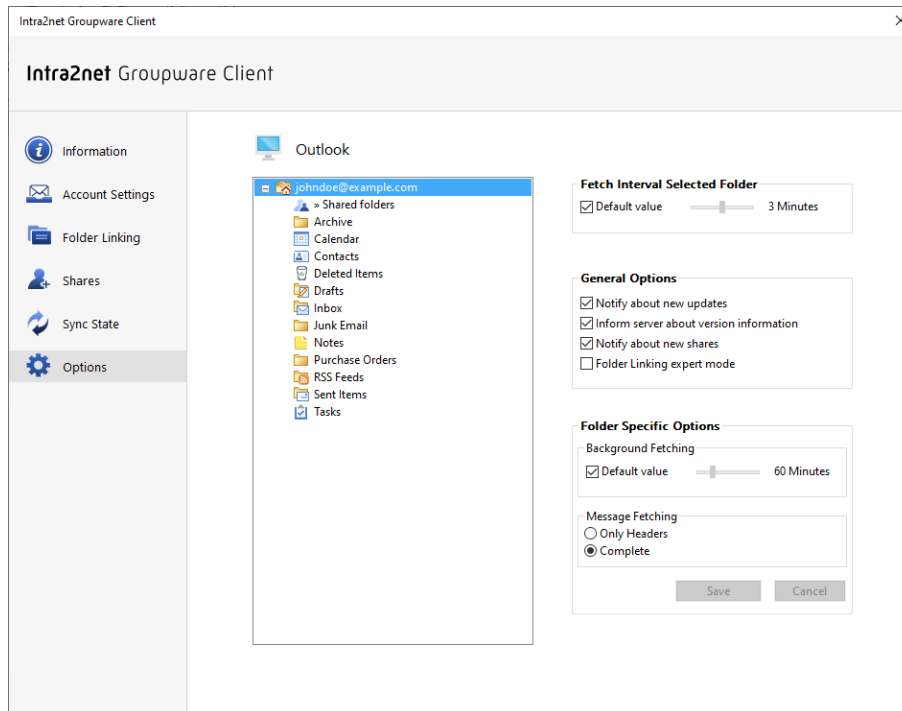
If the read status is to be managed individually for each user, open the context menu of the folder with a right click and deactivate the "Share seen flag with others" option.



23. Chapter - Folder Linking Expert Mode

The expert mode for folder links displays two folder trees in the "Groupware Client > Folder Linking" menu, one for the local Outlook side and one for the server accounts. This allows both finer control of which folders to connect to where, and different modes when dealing with new subfolders.

The expert mode for folder links can be switched on and off via the corresponding option in the "Groupware Client > Options" menu:

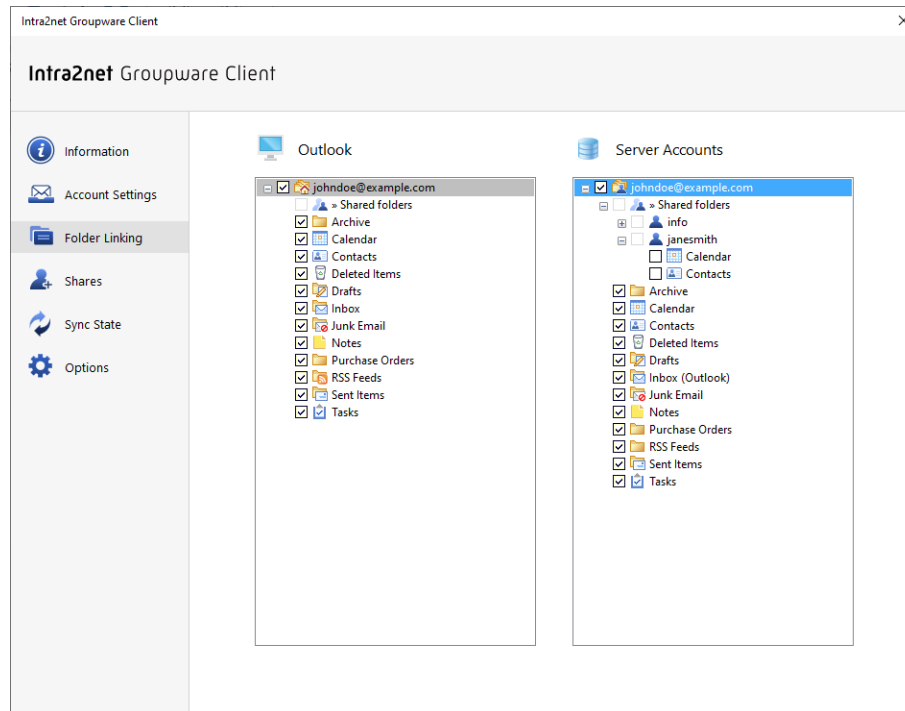


Up to and including Intra2net Groupware Client version 4.0.2 the expert mode for folder linking was always active, only since version 5 there is a choice between the modes.

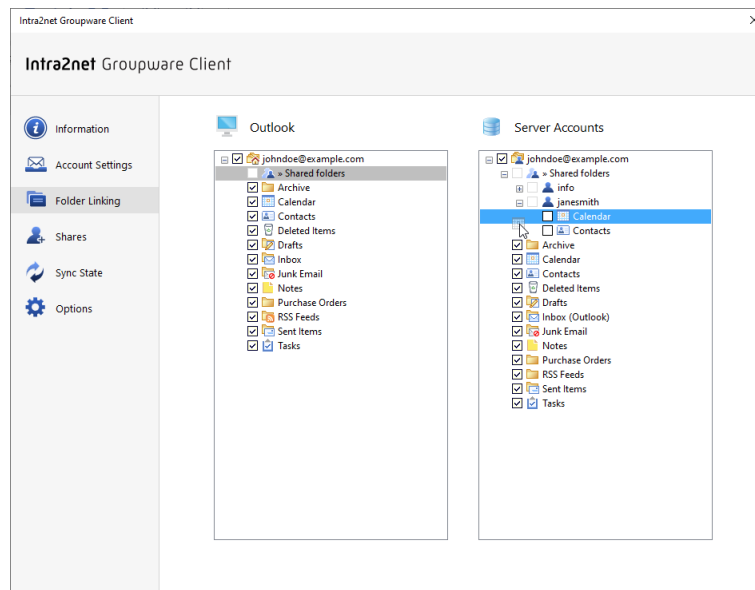
23.1. Linking Shared Folders

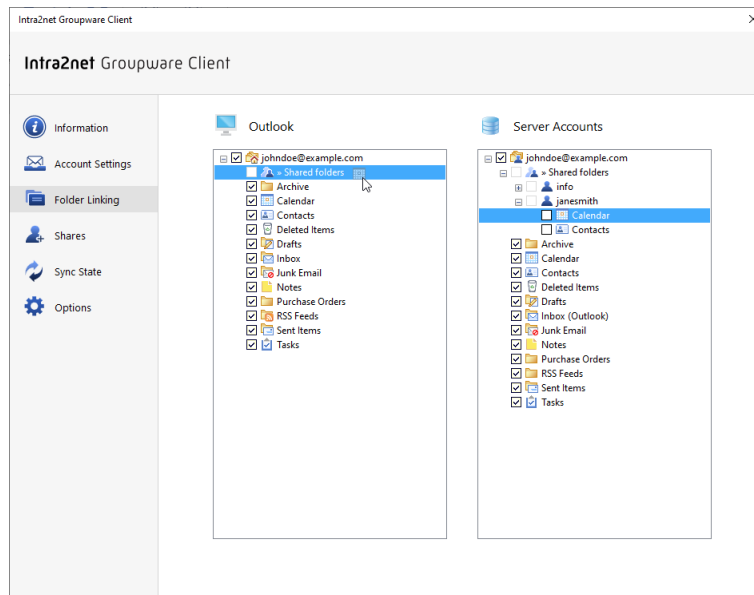
In expert mode, follow the steps below to link folders that other users have shared with you:

1. Go to "Groupware Client > Folder Linking".
2. On the right side (server accounts) the shared folders appear below "» Shared folders".



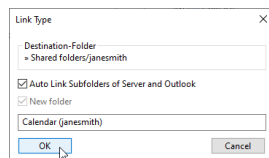
3. Click, and with the mouse button held down, drag the desired folder on the right side to "» Shared folders" on the left side (Outlook). Release the mouse button once it is there.



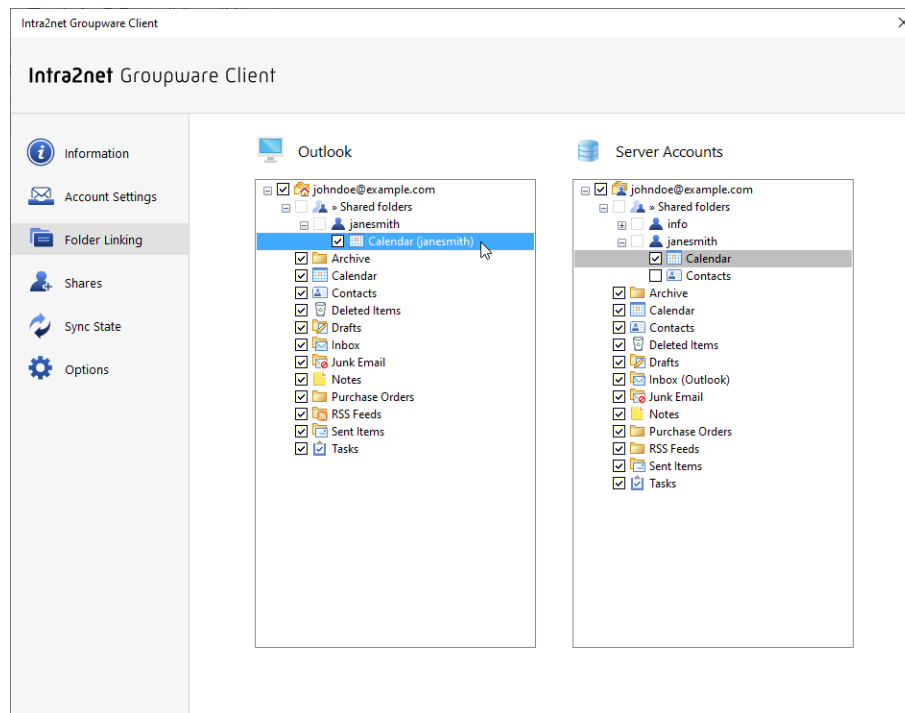


4. A dialog appears asking how the link should be created. By default, the selected folder and all of its shared subfolders are linked. If new subfolders are created or shared on the server at a later stage, they will be automatically linked. Alternatively it is possible to link only the selected folder without subfolders by unchecking this option.

Some folder views in Outlook, such as the calendar view, do not display the folder hierarchy, but only a list of folder names. Therefore, it is recommended to give these folders unique names. The suggested name for a local folder includes the user name of the owner.



5. The linked folder now appears on the left side (Outlook) below "» Shared folders" and the user name.



The difference between expert mode and the standard mode described in the 21. Chapter, „Linking Folders“ is that the shared folders linked in expert mode have the additional option of automatically linking subfolders newly created on the server. In standard mode, you must always link shared folders individually.

Another feature that only the expert mode offers is to give the folders a different name locally than on the server. It is also possible to link folders on another hierarchy level below "»Shared folders".

In the expert mode it is also possible to create the folder link in the same way as in the standard mode. To do this, simply click the checkbox in front of the respective folder name on the "Server Accounts" side instead of using the drag

23.2. Manual folder linking

Normally, the Intra2net Groupware Client automatically links its own folders between the server and Outlook:

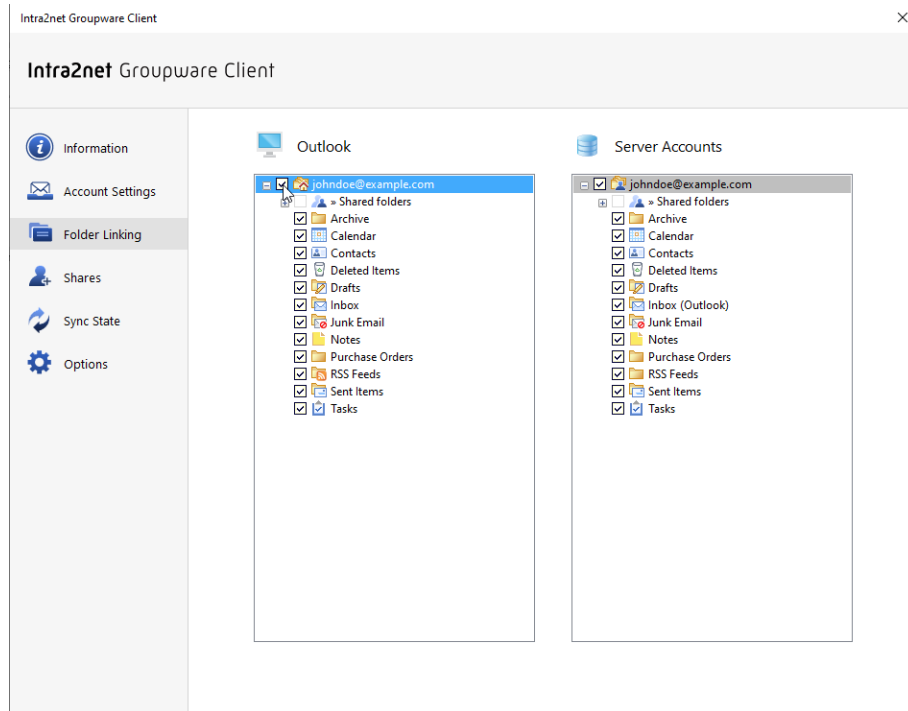
- Folders newly created on the server will automatically appear in Outlook
- Folders created in Outlook are automatically created on the server and linked to it
- Folders deleted locally are also deleted on the server
- Folders deleted on the server are also deleted locally
- Folder names and their hierarchy are identical in Outlook and on the server

The user doesn't have to manually link folders individually, but doesn't have the option to locally reorganize or rename the folder hierarchy in Outlook, differently from the server.

23.2.1. Switching to Manual Linking

To make this possible there is also the option to switch off the automatic mode and to link the folders manually. To do this, proceed as follows:

1. Go to "Groupware Client > Folder Linking".
2. Click the root folder and uncheck the box in front of the name.

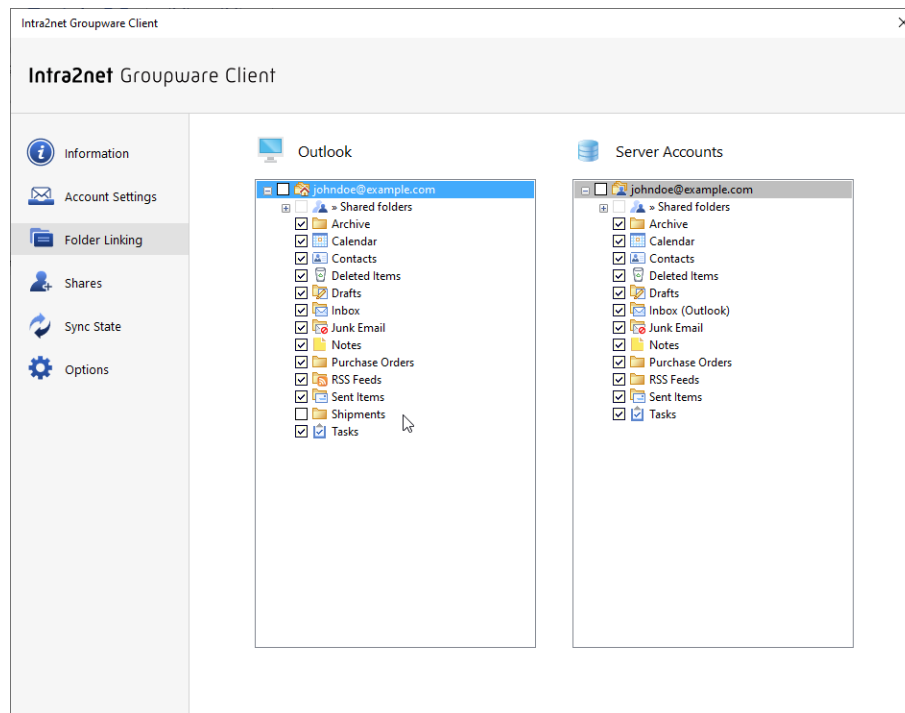


3. You will be asked if you really want to remove the link. Answer with "OK".

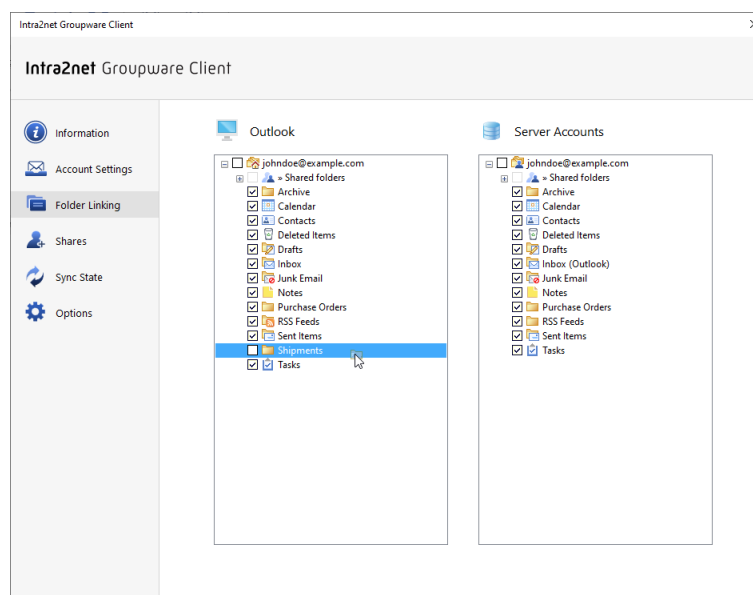
The individual subfolders are still linked at first. Namely, the individual folders on the top folder level are linked using the "All new folders" mode. If new folders are created locally or on the server on the top folder level, they must be linked manually from now on (if desired). In addition, it is now possible to unlink individual folders or to link them at a different location in the folder hierarchy than on the server.

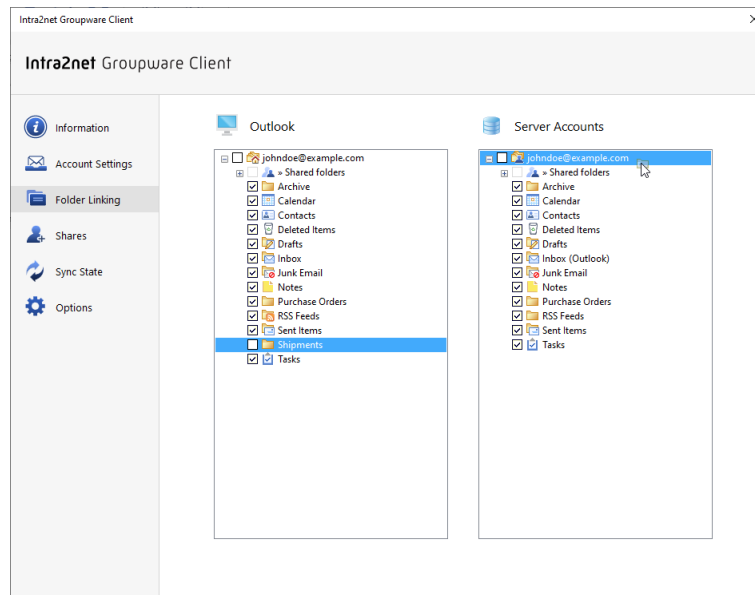
23.2.2. Linking an Individual Folder

1. Go to "Groupware Client > Folder Linking".
2. On the right side, the user account is displayed on the server, and on the left side, the local folder hierarchy in Outlook.



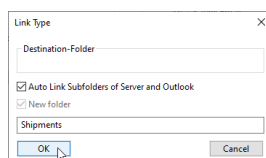
3. Drag the desired folder on the Outlook side, here "Shipments", to the root folder of the account on the right side with the mouse button pressed and release the mouse button there (drag & drop). If the folder to be linked is on the server side, drag it in the other direction.





There will now be a choice of how the link should be configured:

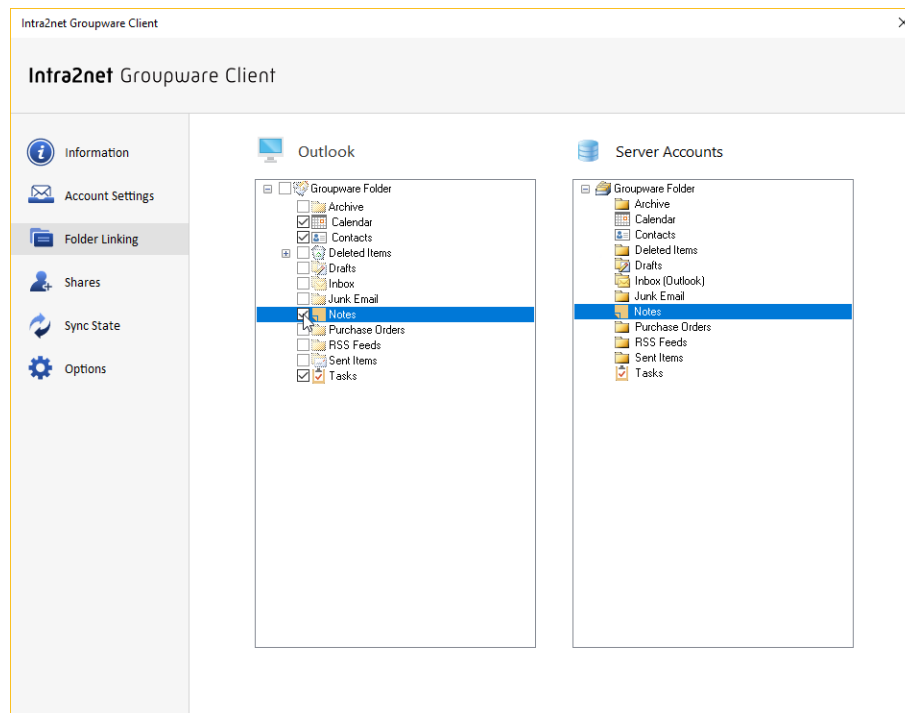
Auto-Link Subfolders	If active, the folder itself and all of its subfolders are linked. If new folders are added or deleted locally in Outlook or on the server, the change is made on the other side, too.
New subfolder	If enabled, a new folder is created inside the previously indicated folder and linked to the server.
Folder name	If a new folder is to be created, the name can be set here. This allows different names for the same folder to be used locally in Outlook and on the server. For example, the <code>Calendar</code> folder of the user <code>john</code> can be called <code>Calendar John</code> locally in Outlook.



23.2.3. Unlinking a folder

To remove the link of a folder, proceed as follows:

1. Go to "Groupware Client > Folder Linking".
2. Click the checkbox in front of the folder name to uncheck it.



3. Confirm that you want to remove the link.

24. Chapter - Additional Features

24.1. Folder Hierarchy and ibx_sub

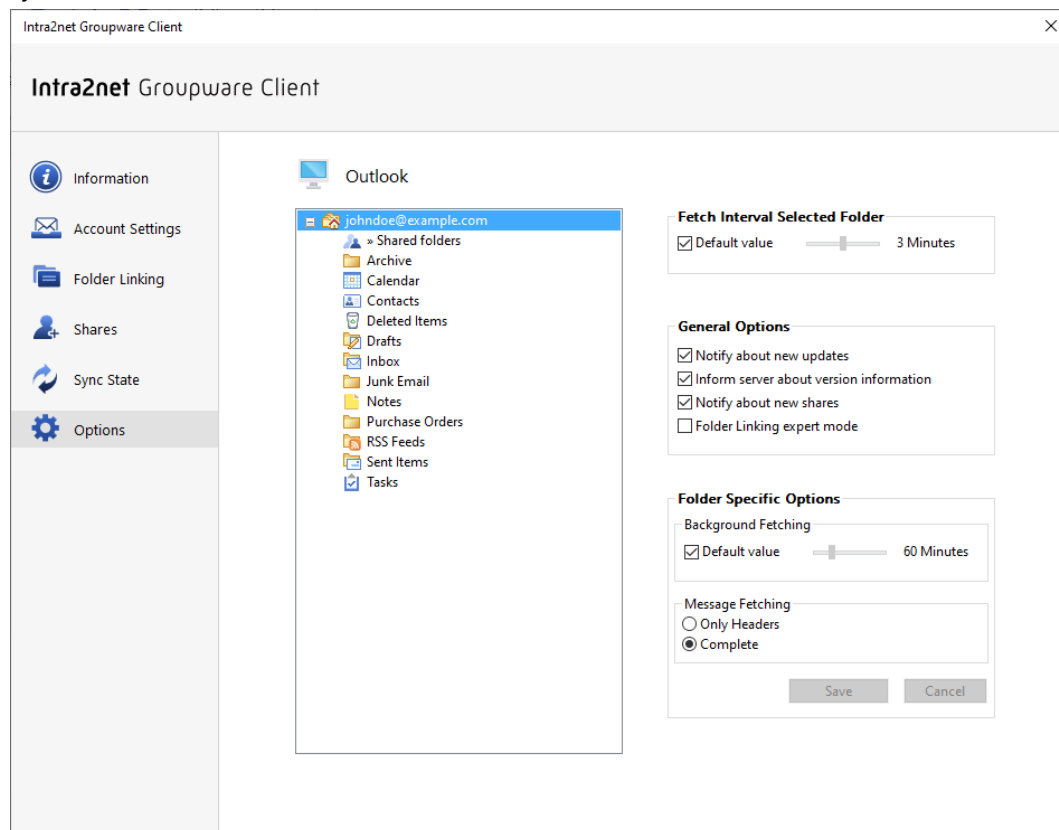
In Outlook, the `Inbox` folder is usually found on the same hierarchy level as `Calendar`, `Contacts`, etc. On the IMAP server, the `Inbox` is the root folder of a user, with all other folders such as `Calendar`, `Contacts` etc. as subfolders of the `Inbox`.

The Groupware Client translates these two different concepts and displays the Outlook folders according to the standard Outlook format.

In Outlook, however, it is possible to create subfolders in the `Inbox`. On the IMAP server, however, there are no differences between subfolders of the `Inbox` and folders at the same level of the `Inbox`. If this happens, the groupware client creates a folder called `ibx_sub` on the IMAP server, and stores all Outlook inbox subfolders inside it.

24.2. Folder Options

In the "Groupware Client > Options" menu, connection options can be set for the email accounts. In particular, it is possible to set the frequency at which individual folders are synchronized with the server.



The folders currently opened or selected in Outlook are updated every 3 minutes by default. This interval can be adjusted globally in the dialog.

In addition, all folders are synchronized with the server in the background at the set interval. If you want to adjust this interval, select the folder, deactivate the control panel "Use default value" and set the desired time. All subfolders of this folder automatically accept the set time, unless you explicitly specify a different value for a subfolder.



Caution

Synchronizing many folders results in significant load on the client and the server. It is therefore important to ensure that only one or very few folders are synchronized at short intervals in the background per user. If all folders are synchronized every few minutes, Outlook can react sluggishly and the server can easily be overloaded by a few users.

The update interval settings here only affect the synchronization of changes on the server to local Outlook. Changes made locally in Outlook are written to the server promptly and without waiting for an interval.



Hint

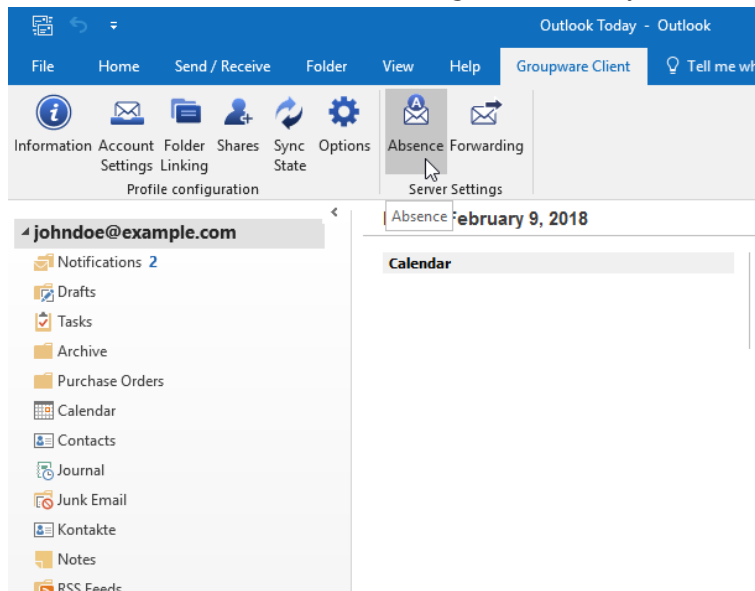
The settings for the update intervals in this menu only affect the contents of the folders, not changes to the folder structure. For folder structure synchronization, see Section 21.1.3, „Update folder list“.

Additional settings for synchronization can be made using the registry. These can be found in Section 30.2, „Advanced Registry Settings“.

24.3. Editing Server-Side Settings

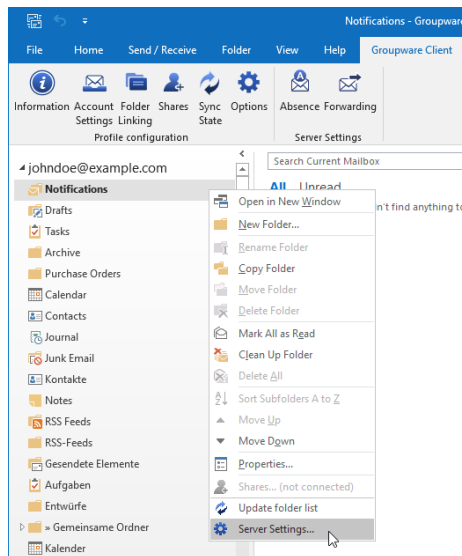
The Groupware Client provides an easy way for users to access their server-side user settings from Outlook. The features such as absence mode, email forwarding, sorting rules and the user-dependent spam filter of the Intra2net system can be configured.

Access is possible through the office menu bar "Groupware Client" and the corresponding entries in the "Server Settings" area. These elements open a web browser which displays the corresponding menu items on the Intra2net system. The session is opened directly with the user's access data, so no login is necessary.



If multiple server accounts (data files) are configured, the user is asked in a dialog for which server settings they want to open.

Alternatively, the server settings can be opened using the context menu of each folder in the folder list (right clicking on the folder name) and then using "Server Settings" option.



For multiple server accounts, the server settings for the account associated with the selected folder are opened.

It is necessary, of course, that the Intra2net system administrator has allowed individual users to configure these settings. This can be set on the server through the "Usermanager > Groups : Administration rights" menu, e.g. in the `ALL` Group, by adding the pages under "Usermanager > Own Profile" to the allowed pages.

In addition, a correct SSL encryption configuration is required for access. For errors with the encryption, proceed as described in Section 20.1.1.1, „Procedure for Certificate Errors“.

24.4. Categories and color assignment

Outlook allows you to assign categories to individual objects (such as emails, appointments or contacts). At first only the names of these categories are stored and synchronized by the Groupware Client to the server and other Outlook instances. In addition, there is a central (=across folders and data files) so-called Master Category List in each Outlook profile. This list can be used to assign colors to the categories.

Because each Outlook profile may have different folders and accounts linked, conflicts between the assigned colors can easily arise. Therefore, the assignment of colors to category names is primarily a local configuration of each Outlook profile.

In order to achieve a mostly uniform color assignment across multiple devices, the Intra2net Groupware Client since version 5.0.2 writes the color assignment to the server for newly created or modified groupware objects. When synchronizing in groupware objects (not emails) with categories and category color assignment from the server, the procedure depends on whether the respective category name already exists in the Master Category List or not. If yes, the already existing category remains unchanged. If no, the category is created in the Master Category List and the color assignment is taken from the server.

This procedure means that the local Master Category List with its color assignment always has priority over changed color assignments on the server. This way, the user can always easily resolve any color conflicts himself in the local Master Category List.

This also means that if there are conflicts between different color assignment data on the server, the final color assignment will depend on the order in which new groupware objects with colored categories are synchronized in.

24.4.1. Recommendation for shared color assignment

In order to achieve a mostly uniform category color assignment for several workstations or Outlook profiles, the following procedure is recommended:

1. Use a shared account, see for example 27. Chapter, „Concept for public folders“.
2. Create a new task folder in it, name e.g. **Color Categories**, and share the folder with all users for reading (see 22. Chapter, „Sharing Folders“).
3. Create a task in this task folder, title e.g. **Standard Categories**.
4. Double-click the task to open it in a separate window. Open the menu of the Master Category List.
5. Create all the desired categories with their respective color assignment in the Master Category List.
6. Assign all shared categories to this one task and save it.
7. All users who are to use the common color assignment now connect the task folder with the standard categories in their Outlook profile, see 21. Chapter, „Linking Folders“.

If some Outlook profiles already have the category names stored in the Standard Categories present in their Master Category List, but have assigned different colors, proceed as described in the next section to reset the color assignment for these Outlook profiles.

24.4.2. Reset local color assignment

With the following steps you can reset the complete Master Category List and color assignment of an Outlook profile and import it fresh from a shared folder (see previous section):

1. Close Outlook and wait until the Outlook process is completely ended.
2. Open the Windows Start menu.
3. Type **outlook.exe /cleancategories** as command and start it with Enter.
4. Outlook starts in a special mode that deletes all entries and color assignments from the Master Category List. The individual groupware objects keep their category assignments (i.e. the category names).
5. Go to "Groupware Client > Folder Linking".
6. If the shared categories folder (see Section 24.4.1, „Recommendation for shared color assignment“) is already connected, remove the connection. Wait a short time until the action is fully processed by Outlook.
7. Reconnect the folder with the shared categories. This will resynchronize the contained data from the server and add the contained categories to the Master Category List.

24.4.3. Changing an existing color assignment

The following describes the process by which an existing category color assignment can be changed uniformly for multiple users network-wide.

Because different color assignments for the same category depend on the order in which new objects are synchronized in (as described above), and the user has little influence on this order, e.g. when setting up a new Outlook profile, all objects to which the respective category is assigned must be modified for a stable color assignment. Changing the color assignment of a category is not considered a change of the respective objects by Outlook and therefore does not trigger a write of the objects with a new color assignment to the server. Therefore the following steps are necessary to change an existing color assignment permanently and for newly created Outlook profiles:

1. Close Outlook on all workstations connected to the Intra2net system and ensure that it remains closed. Also consider home office workstations, mobile devices and similar.
2. Start Outlook on one workstation with an Outlook profile that has write access to the central color categories folder (see Section 24.4.1, „Recommendation for shared color assignment“).
3. Go to the central color categories folder and open the task for the standard categories in a separate window by double-clicking.
4. Open the menu of the Master Category List.
5. Assign the new color to the existing category.
6. Rename the category, for example, by appending a number to the name.
7. Repeat the last two steps for all other categories to which you also want to assign a new color.
8. Exit the category list dialog with "Ok". Wait until Outlook has executed the renaming of the category. The duration for this depends on the number of affected objects and the size of the data files.
9. Open the Master Category List again and rename the category back to its original name. Exit the category list dialog with "Ok" and wait until Outlook is done with rename processing.
10. Wait until the changes of the local objects have been written to the server by the Groupware Client. Use the menu "Groupware Client > Sync-State" for this.
11. Close Outlook on this workstation and make sure it stays closed.



Caution

Make sure that only one workstation has Outlook open at any time. Otherwise, the renamed categories may be mistakenly included in the Master Category Lists there.

1. Perform the steps described in Section 24.4.2, „Reset local color assignment“.
2. Open the menu of the Master Category List.
3. Rename all categories to which a new color is to be assigned, for example by appending a number to the name.
4. Exit the category list dialog with "Ok". Wait until Outlook has executed the renaming of the category. The duration for this depends on the number of affected objects and the size of the data files.
5. Open the Master Category List again and rename the category back to its original name. Exit the category list dialog with "Ok" and wait until Outlook is done with rename processing.
6. Wait until the changes of the local objects have been written to the server by the Groupware Client. Use the menu "Groupware Client > Sync-State" for this.
7. Close Outlook on this workstation and make sure it stays closed.

If the process was completed on the last workstation, the color assignments in all Outlook profiles and in all objects on the server are adjusted uniformly. Now Outlook can be used normally again on all workstations.

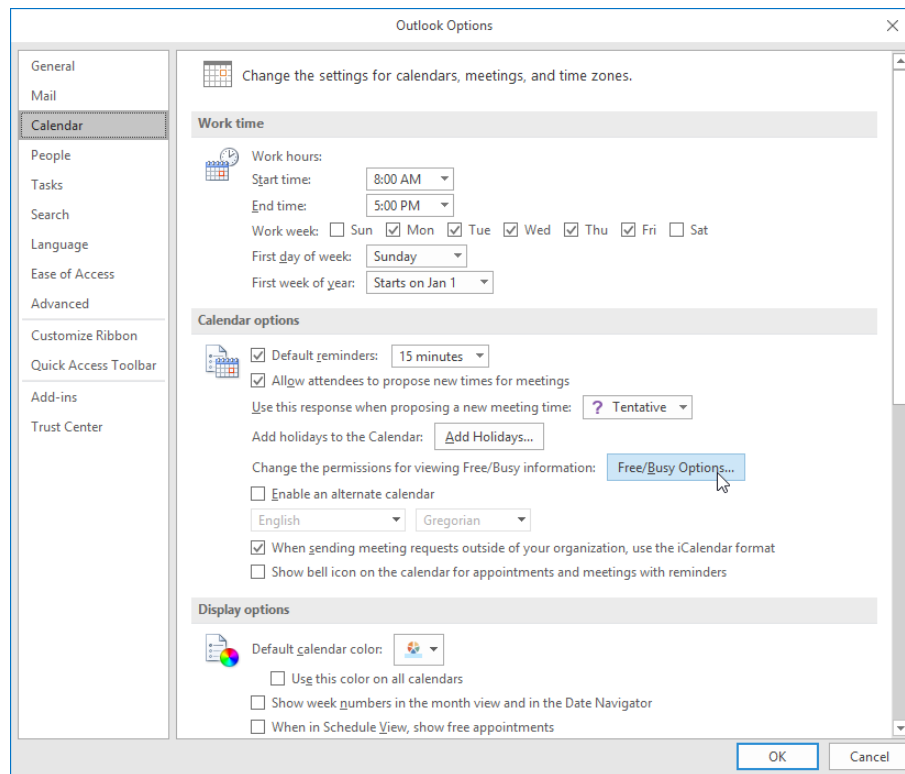
24.5. Use Free/Busy Information

If colleagues have not released their calendars for viewing, it is still possible to determine when they have not entered any other appointments in their calendars, to organize a common appointment. This information is available through the free/busy system.

Before the free/busy data can be used, the correct address must first be specified in Outlook, so it can be retrieved. Proceed as follows:

24.5.1. Outlook 2010 to 2021

1. In Outlook, go to "File" and select "Options".
2. Go to the "Calendar" section.
3. Now click on the "Free/Busy Options" button.

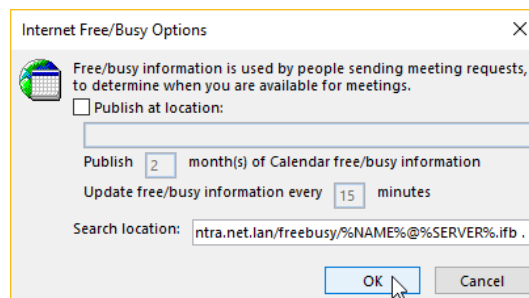


4. Enter the search path into "Search location".

The address is **https://intra.net.lan/freebusy/%NAME%@%SERVER%.ifb**.

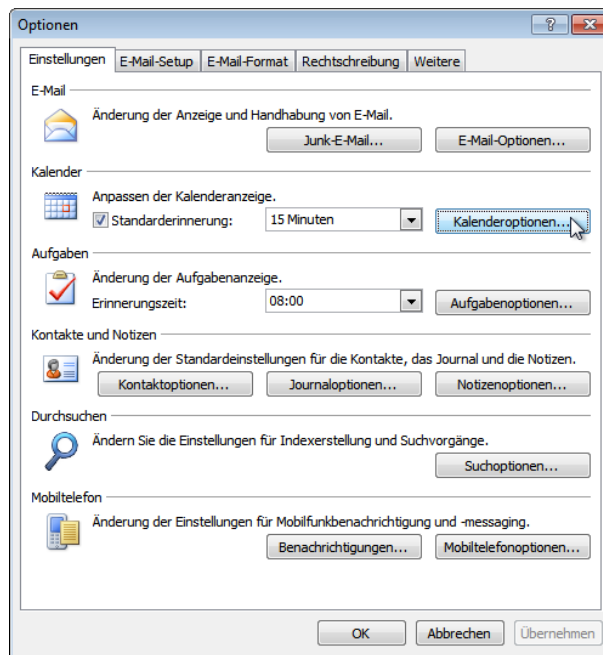
Use the name of the Intra2net system and enter the address as shown here.

Since the Intra2net system automatically generates the free/busy information, the "Publish at location" check box must be unchecked.

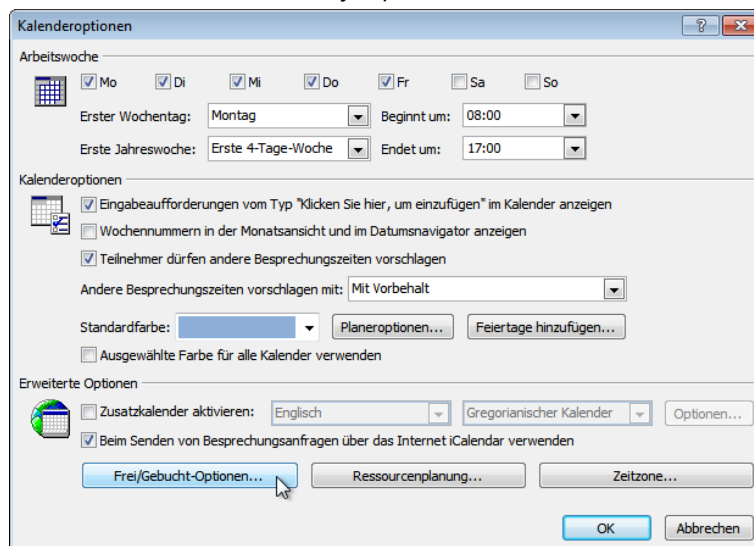


24.5.2. Outlook 2007

1. In Outlook, go to "Extras" and select "Options".
2. Click on the "Calendar Options" button.



3. Now click on the "Free/Busy Options" button.

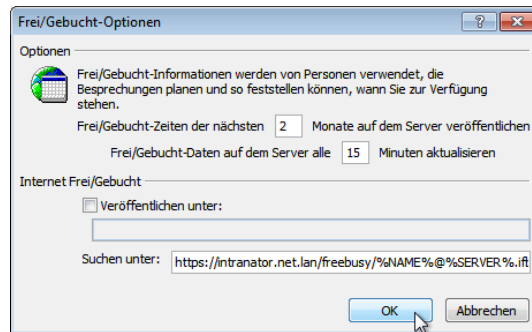


4. Enter the search path into "Search location".

The address is **`https://intra.net.lan/freebusy/%NAME%@%SERVER%.ifb`**.

Use the name of the Intra2net system and enter the address as shown here.

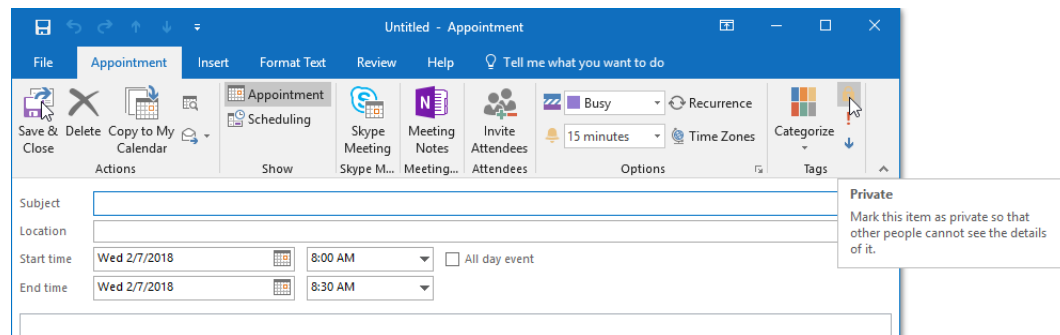
Since the Intra2net system automatically generates the free/busy information, the "Publish at location" check box must be unchecked.



24.6. Marking as Private

Appointments, tasks and contacts can be marked as "private" in Outlook. Regardless of the access rights to the folder, this data is only visible to the person who set the private identifier. The owner of the object is identified by the user login that originally set the state to "private".

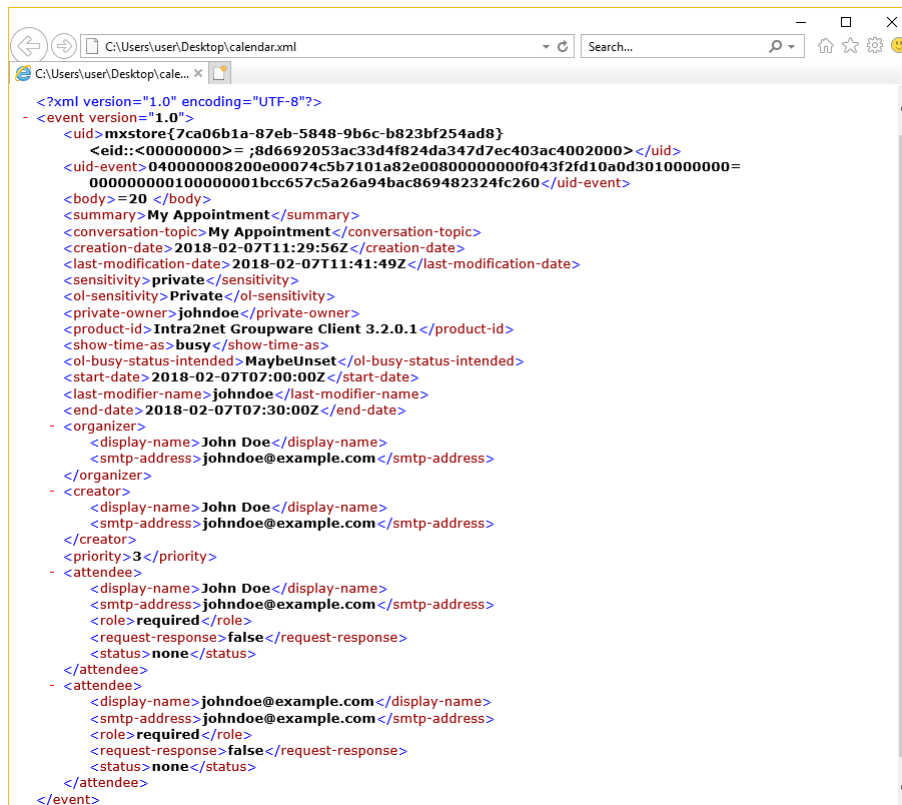
For other users, the data is completely hidden, or for appointments only a placeholder is displayed. See also the settings for CalPrivatePlaceholder in Section 30.2.1, „Store Settings“.



Caution

The private data is only hidden for other users with access rights to the folder, and is not displayed in Outlook. However, this does not mean that others cannot access this data. Marking as private therefore does not meet the usual requirements for security and data protection.

Other users with access rights to the folder can read the data as an XML file via IMAP. The following example shows a private appointment from a calendar that was subscribed to in an email account in Outlook.



As one can see, apart from some not intuitively understandable information, all relevant dates of the appointment are readable in plain text.

As a secure alternative, it is advisable to alternatively create a separate folder for private data, and not to share it.

24.7. Reminders in Shared Folders

Outlook can give reminders of deadlines for appointments and tasks. If a folder is shared by several users, the reminders are handled individually for each user.

Each user can place any number of reminders on each groupware item, and they will appear only on their own due date. The user login is used to identify the user, so the reminders also work if a user works at different PCs.

The only exception is when a user creates a new appointment or task and enables reminders at the same time. In this case, the reminder is made for the creating user, and one for the owner of the folder. This way, for example, a secretary can create an appointment with a reminder for their boss.

A later change to the reminder only affects the user who made the change.

The values **InitialReminderSetting** and **ReminderChangesHandling** in the registry can be used to further change functionality. Details can be found in Section 30.2, „Advanced Registry Settings“.

24.8. User-Defined Fields in Contacts

Outlook allows users to create custom fields for contacts in addition to the predefined fields (Menu bar "Contacts > Show > All fields", select from `User-defined fields in this item`). These can be created by contact folder and then filled with specific content for individual contacts.

The Intra2net Groupware Client can also synchronize these user-defined fields to the server and thus make them usable across different workstations or users. However, a definition file for these fields must be available on all workstations before they can be used for the first time.

The definition file is an XML file, called `userdefined_sync_fields.xml`, and by default it is located in the program folder where the Intra2net Groupware Client is installed. However, the path of this file can be changed in the registry by setting `syncTemplates-FilePath` (see Section 30.2, „Advanced Registry Settings“).

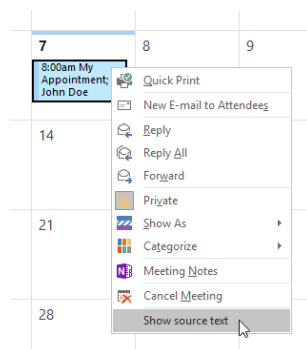
With the Intra2net Groupware Client, an example file is provided as `user-defined_sync_fields_template.xml`, which contains a detailed description and examples of how to create user-defined fields. Copy this template file to `user-defined_sync_fields.xml` and open it with an XML editor (such as Oxygen [<http://www.oxygenxml.com/>], EditiX [<http://www.editix.com/>] or XMLSpy [<http://www.altova.com/xmlspy.html>]). Everything else is described in the sample file.

The user-defined fields can currently only be accessed with the Intra2net Groupware Client. They cannot be edited or displayed in the web groupware or via ActiveSync.

24.9. Showing Item Source Text

To analyze coding problems and other similar matters, it is possible to view the items in the source text. The header of the items is also displayed here.

To display the source text, right-click the item to open the context menu and select "Show source text".



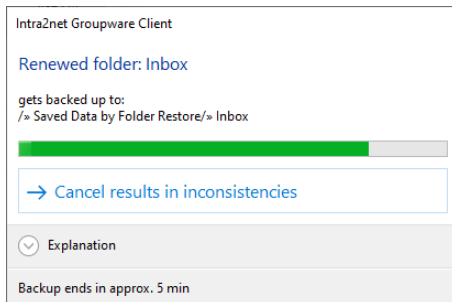
24.10. Backup Folders

If local items are deleted by restoring a backup on the server or linking operations with the server, the Intra2net Groupware Client saves the original versions to special folders. The different types of backup folders for this feature are described below.

24.10.1. Backup Data after Restore

If a folder on the server is deleted and replaced by a new folder with the same name, the Groupware Client recognizes this (using the internal *UIDVALIDITY* identifier of IMAP). This is especially the case if a backup has been restored on the server that replaces the user's previous data.

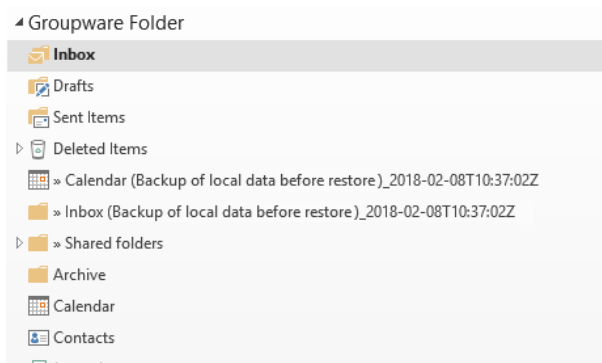
All local items are moved to backup folders. This process must not be interrupted by the user, otherwise inconsistencies will occur in the data file. The user is notified of this with a dialog.



A folder called "Backup of local data before restore" is created in Outlook. Inside this folder are the backup folders with the name of the original folder and a timestamp. The timestamp specifies the time at which the groupware client detected the folder restore on the server and not the time at which the folder restore on the server took place.

Once the local backup folders have been created, the data can be freshly synchronized from the server. To avoid overloading the server, this does not happen automatically for all folders, but only for those opened by the user in Outlook. Alternatively, the user can restart Outlook. In the new Outlook session, the normal behavior of the Groupware Client with synchronization of all folders in the background takes effect again.

The backup folders on the client are not automatically deleted. Therefore, after restoring a backup on the server, we recommend that you wait a few days and then ask users if their data is complete. After that, the backup folders should be manually deleted on all clients.

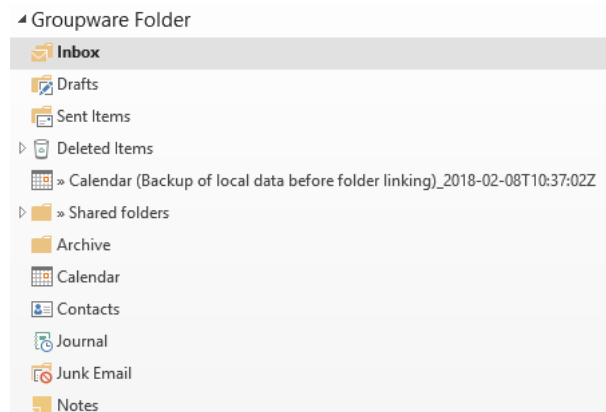


24.10.2. Backup of local data when resetting to automatic mode

If folders are re-linked, a locally existing folder must be empty before it can be connected to a folder on the server. If the local folder is not empty, the user can either abort the link process or delete the local data.

If you switch back from manual link mode to automatic link mode (back from the one described in Section 23.2.1, „Switching to Manual Linking”), this affects a large number of folders. Therefore, in this case, backup folders are created from the locally available data. These folders appear locally on the same hierarchy level as the connected folder. It gets "(backup of local data before folder linking)" and a time stamp attached as identifier.

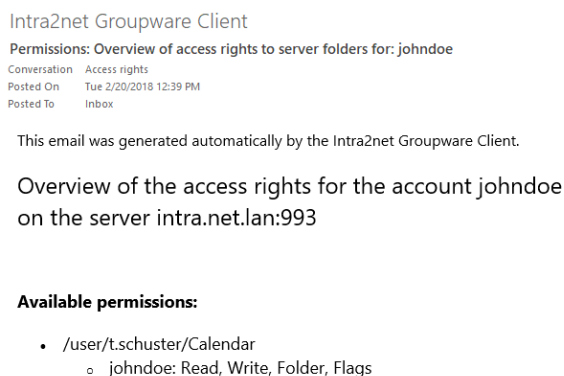
This backup folder contains all of the data that existed in the local folder before the link was made. We recommend that the user manually goes through this backup folder and drags missing data on the server to the folder that is now connected to the server. The backup folder on the client should then be deleted. The backup folder is not automatically deleted on the client.



24.11. Advice to the User

The Groupware Client informs the user about special events, errors etc. by creating emails to the user in the inbox. These emails are identified by the special sender "Intra2net Groupware Client".

For example, such notices are generated when new rights are given to the user:



The notes on new rights can be configured with ACL_ChangeNotification in the registry. See Section 30.2.1, „Store Settings”.

The emails with notes are only stored locally in the Groupware Client and are not synchronized to the server.

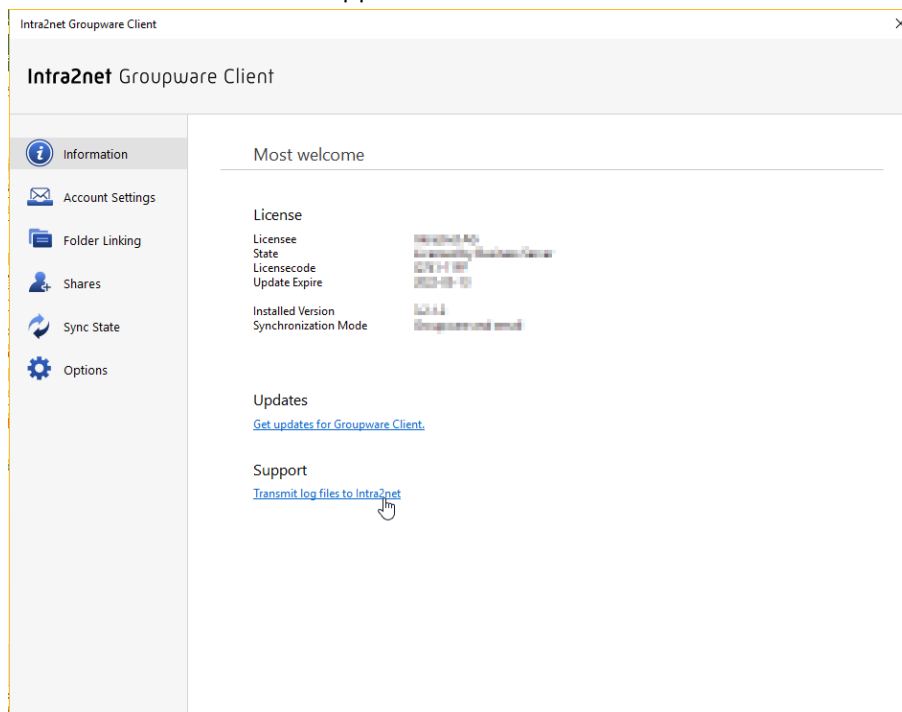
24.12. Log files

By default, the groupware client logs internal details about the user's accounts, shares, data synchronization and user actions. In the event of an error, this data is the basis for reconstructing the events, the possible causes and possibly the recovery of data.

By default, the log files are stored in %LOCALAPPDATA%\Intra2net, which usually points to the hidden directory AppData\Local\Intra2net below the user's profile directory. The files are rotated daily, or if you exceed 170 MB, and kept for 14 days by default. The default values and the scope of the logs can be adjusted via the registry, see Section 30.2, „Advanced Registry Settings“.

24.12.1. Submitting log files to support

If Intra2net Support asks you to send the log files of the groupware client, the easiest way is to use a special function in the menu "Groupware Client > Information". You need the ticket number of the support case.



25. Chapter - Advanced Email Configuration

25.1. Retrieve Emails Completely or Only Headers

Using the "Message Fetching" button in the "Groupware Client > Options" menu, it is possible to specify whether new emails in a folder should be retrieved immediately or only the headers. As soon as the user clicks and opens an email in Outlook with only the headers, the download of the complete content automatically starts in the background.

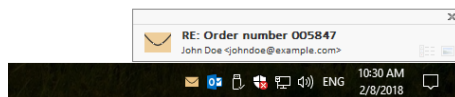
Each email folder allows for individual selection of whether new emails are always downloaded completely or only the headers. The default setting for newly connected folders is "Complete". To change the default setting, adjust the root folder settings.

The advantage of only downloading headers is that they require less space in the data file on the local system. A smaller data file often results in faster response times from Outlook.

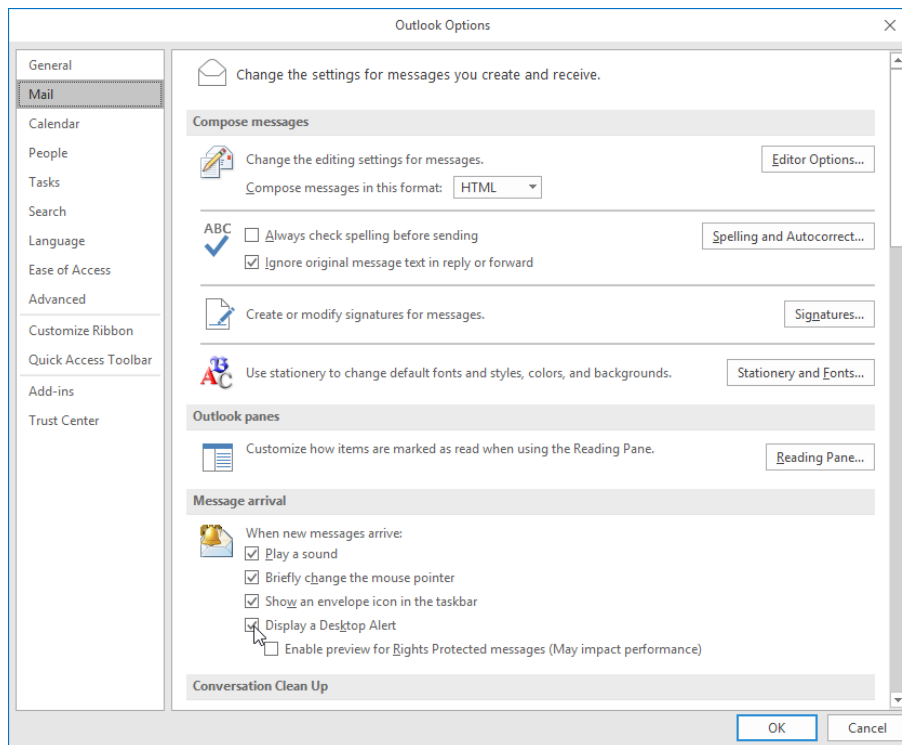
The disadvantage of downloading only as headers is that Outlook cannot search the content of emails that have not yet been downloaded completely. A connection to the Intra2net system is also necessary for reading an email. Moving or copying emails to or from another data file or folder of another server account is only possible once the complete email is locally available.

25.2. Notification of New Emails

The user can be notified with desktop notifications when new emails arrive at one of the Inbox folders. They appear at the bottom right of the screen and display the sender and subject of the newly received emails.



Desktop notifications can be enabled or disabled under "File", "Options", "Mail", in the "Message arrival" section



Desktop notifications display a maximum of 3 new emails. If new emails arrive within 60 seconds of the last desktop notification being displayed, no further desktop notification will be displayed for them, to avoid distracting the user with too many notifications. No notification is displayed for emails that are already marked as read. This also applies to emails that have been on the server for more than 2 hours.

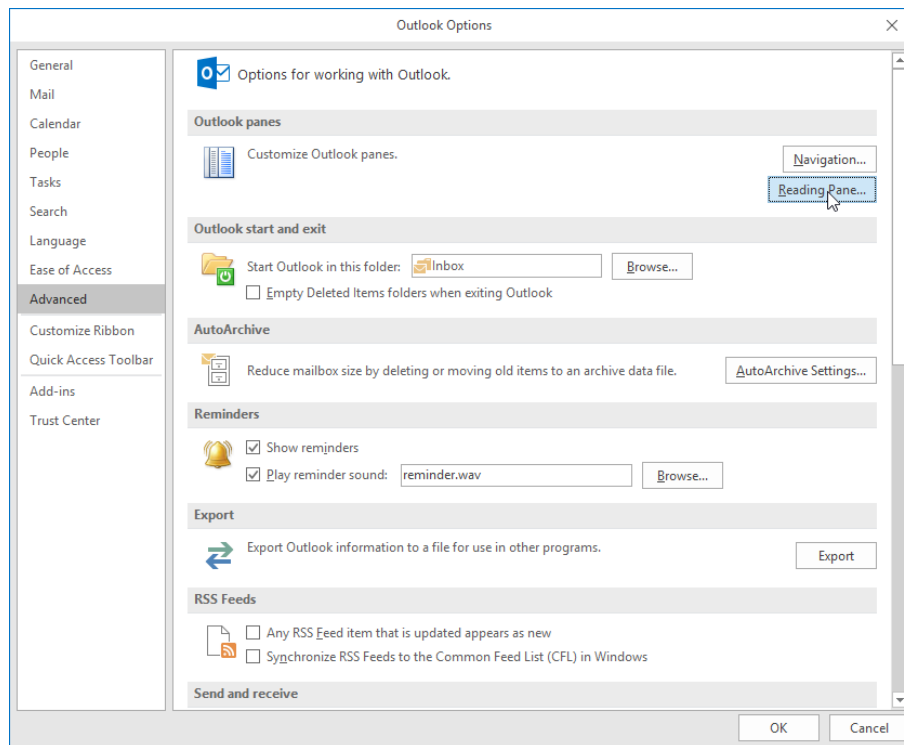
These settings can be adjusted through the registry, see Section 30.2.2, „Addin Settings“.

25.3. Marking Moved Emails as Read

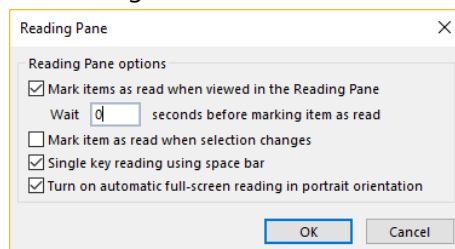
By default, Outlook will mark an email as read once it has been displayed as a preview, and the user has selected another email. However, if the next email is not directly selected, but the currently displayed email is moved to a different folder, the still unread-marked email will be moved. The moved email will then continue to be marked as unread, even if another email is selected.

In order to avoid this scenario, the Read Marker options need to be adjusted as follows:

1. Open "File", "Options", and go to the "Advanced" tab.
2. In "Outlook Panes", open "Reading Pane".



3. Enable "Mark items as read when viewed in the Reading Pane" and select a waiting time of e.g. 0 seconds to immediately mark as read.



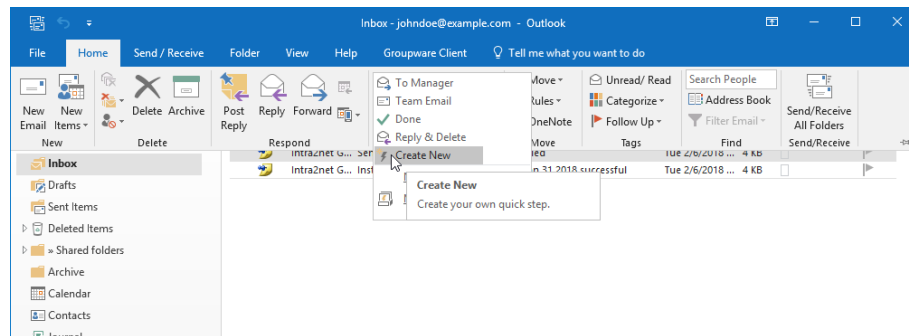
25.4. Email Reminders and Tracking

Outlook provides the ability to define email reminders and create a list of emails to be processed at a later date (tracking feature). This is not possible with the groupware client. In addition, such reminders and tracking information generally cannot be relayed to mobile devices.

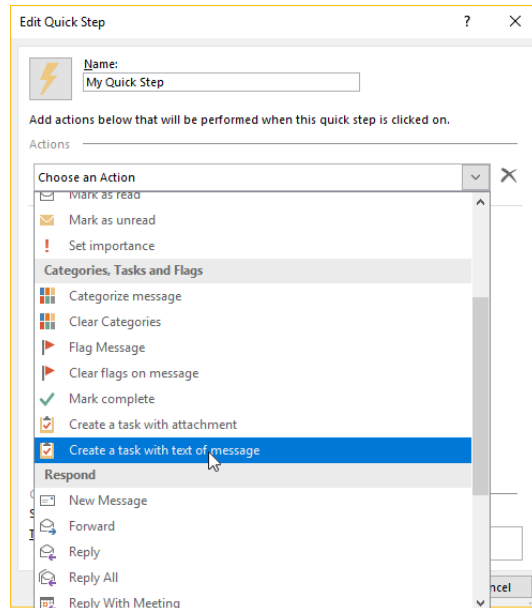
Therefore, we recommend creating a separate task for the email, instead of using the Tracking feature. This can then be used in Outlook, the web groupware, and on devices connected via ActiveSync. If necessary, it can even be shared with and edited by other users, e.g. in case of substitution.

With Outlook 2010 and later, it is possible to automate the creation with "QuickSteps" function. Proceed as follows for the one-time setup:

1. Right click on any existing QuickStep and select "Create New".

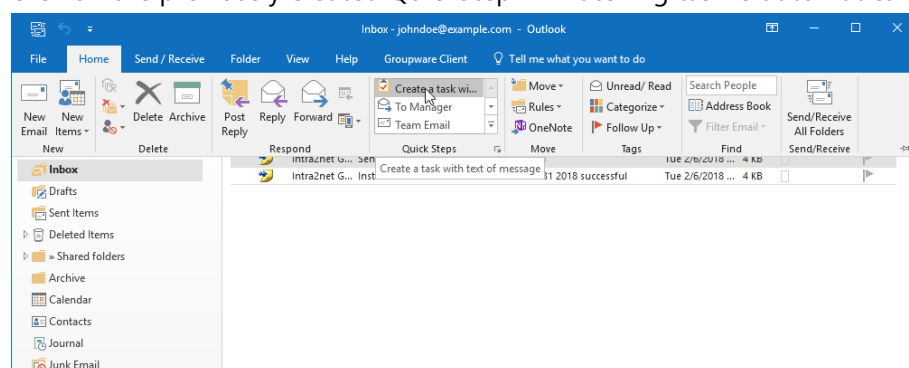


2. Choose "Create a task with text of message".



3. Save the QuickStep by clicking "Finish".

The QuickStep is now set up and ready to use. To do so, open the relevant email and click on the previously created QuickStep. A matching task is automatically created.



25.5. Read receipts

The SMTP standard provides that a sender of an email can request an automatic read confirmation (*Message Disposition Notification* (MDN)) from the recipient. Outlook supports this and offers the possibility to set the handling in the email options. By default, the user is asked whether a read confirmation should be sent or not.

However Intra2net has experienced that Outlook does not fully consider this option and in some cases still sends read confirmations to the sender without being asked. This was mainly observed with regard to moving or deleting emails. Outlook then answered old emails with "Your message has been deleted without being read" without asking the user.

In addition, the groupware client has to delete emails for a correct function and replace them with new versions, e.g. if another user or device has changed the email. This method does not work for emails with read confirmation, since Outlook would ask the user to send the read confirmation each time such a change is made to an email.

Therefore, the Groupware Client removes the request for read receipts from all incoming emails.

If the sending of read confirmations should be absolutely desired, the removal of the read confirmations can be suppressed at the user's own risk by setting the registry value `Md-nAllow`. For more information about the registry, see Section 30.2.1, „Store Settings“.

26. Chapter - Compatibility and Collaboration

26.1. Personal firewalls on the Client

The Intra2net Groupware Client must be able to access the Intra2net system via IMAP/IMAPS, SMTP and HTTP/HTTPS from the Outlook process. Therefore, the corresponding ports must be opened in the firewall of the client.

If the firewall is running in learning mode, please note that HTTP/HTTPS is only required for calendar changes, requests of free/busy lists, and configuration of forwarding and absence automation.

26.2. Virus Scanner on the Client

Virus scanners installed on the client often interfere with the system in an attempt to catch viruses. This can lead to conflicts with the Intra2net Groupware Client.

If there is a problem synchronizing and an anti-virus scanner is running on the client, try disabling IMAP scanning first. New emails first pass through the Intra2net system and its own virus scanner, so there is no additional risk.

Find more detailed information about several products (without guarantee):

Developer	Product	Necessary Procedure
Avast	All Antivirus Products	No change necessary
AVG	Antivirus Business Edition	Disable personal email scanner (for all other email applications)
Avira	All Antivirus Products	Disable scanning of the IMAP protocol, disable Outlook add-in
Eset	NOD32 Antivirus	Disable scanning of the IMAP protocol, disable Outlook add-in
Eset	Endpoint Antivirus	Disturbs network communication even without Outlook add-in and in deactivated state, must be uninstalled
F-Secure	Internet Security	No change necessary
G Data	All Antivirus Products	Disable Outlook Add-in
Kaspersky	Internet Security	Disable Outlook Add-in
McAfee	All Antivirus Products	No change necessary, as it is no longer scanning at IMAP level (McAfee KB52786)
Symantec	Norton AntiVirus	No change necessary, as it is not scanning at IMAP level
TrendMicro	Titanium	No change necessary, as it is not scanning at IMAP level

26.3. Compatibility with PDAs and Mobile Phones

If possible, use the Intra2net system's ActiveSync function to establish a direct connection between the Intra2net system and the mobile device without going through Outlook.

This allows data on the mobile device to be updated while on the move. Furthermore, Outlook will not need an add-in which may cause problems.

The configuration of ActiveSync between the Intra2net system and mobile devices can be found explained in 34. Chapter, „Connecting Mobile Devices using ActiveSync“.

26.4. Other Programs

We recommend that you do not use the Intra2net Groupware Client together with the Microsoft Business Contact Manager, as synchronization problems may occur with certain configurations.

Using programs that synchronize data stored in Outlook with other databases in either direction can lead to undesired results when using the Groupware Client. Typical effects in this context are permanent changes, duplicates, and the loss of changes made in Outlook.

Compatibility with other add-ins or plugins for Outlook is not guaranteed.

26.4.1. Incompatible Addins

The following Outlook add-ins have shown errors:

- Avira Antivirus Premium
- CardScan Microsoft Outlook Add-In
- CodeTwo CatMan
- d.3 Smart Outlook (d.Velop AG)
- Emsisoft Anti-Malware
- Evernote for Outlook Add-In
- G Data AntiVirus
- iTunes Outlook AddIn (Apple)
- Kaspersky Small Office Security
- Nuance PDF Converter Add-In
- Outlook Change Notifier AddIn (Apple)
- Panda Internet Security Antivirus Add-In
- Powerbird
- Skype Meeting Add-In
- TeamViewer Meeting Add-In
- TrendMicro Worry Free Business Security

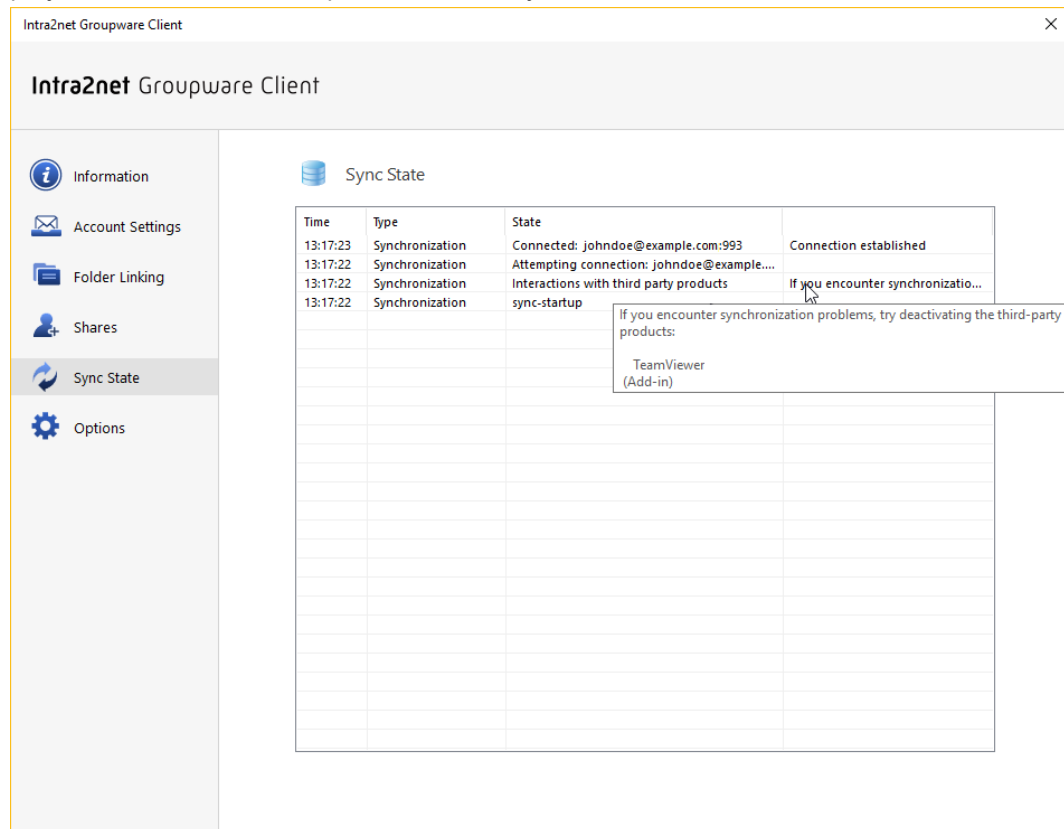
We advise against using these add-ins together with the Groupware Client.

If one or more of these add-ins are installed or active in Outlook, deactivate them under "File", "Options", "Add-Ins" before you set up the Groupware Client.

26.5. Automatic detection of compatibility problems

The groupware client contains a module that tries to automatically detect possible compatibility problems with third-party products. If a possible incompatibility is detected, the user receives a one-time message with the names of the affected programs or add-ins in the inbox.

Additionally, possible compatibility problems and the affected programs are always displayed in the menu "Groupware Client > Sync State".



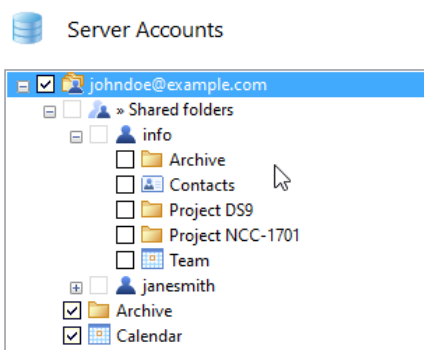
The detection of possible compatibility problems can be deactivated via the registry, see Section 30.2.1, „Store Settings“.

27. Chapter - Concept for public folders

Public folders are email and groupware folders that are not assigned to one person, but are shared by multiple or all users of a company. In the Intra2net system, this concept is implemented by creating an additional, normal user account and folders are shared from this account via user groups.

For example, "info" can be used as the name for a user account used by all users, otherwise names matching the group, such as "sales" or "service".

Within this user account, subfolders with any folder type (email, calendar, contacts, tasks,...) can be created. In addition to a general email mailbox, you can also create a vacation calendar, manage resources such as meeting rooms or service vehicles, maintain customer addresses, maintain employee contact data, and so on.



27.1. Setup

Proceed as follows to set up public folders:

1. Create a new user account on the Intra2net system in the menu " Usermanager > Users". For details see Section 13.2, „User“.
2. If you don't want all users to have equal access rights to the public folders, create one or more user groups in the menu " Usermanager > Groups" and add the appropriate users as members.
3. Create an additional Outlook profile on a PC to manage the public folders. Proceed as described in 19. Chapter, „Setting up a Profile“. Use the access data of the user account that was just created.
4. Start Outlook with the newly created management profile.
5. Create the desired folders in Outlook and share them with the desired user groups as described in 22. Chapter, „Sharing Folders“.
6. Individual users can now link the just shared folders in their Groupware Client as described in Section 21.2, „Linking Shared Folders“.

27.2. Emails

The public folder user account can receive and send email just like any other user account.

To give employees access to incoming emails, you share the inbox of the account and link it among the users.

To enable employees to use the public folder as the sender's address, set up a suitable outgoing mail identity for the employees as described in Section 20.3.2, „Multiple Outgoing Mail Identities“. You should also define the subfolder "Sent items" of the public folder as a folder for sent messages, so that these can also be managed centrally and viewed by all employees.

28. Chapter - Migrating Emails with IMAPCopy

If large amounts of emails are to be transferred from an existing email server to the Intra2net system, IMAPCopy is usually the fastest way. IMAPCopy automatically copies the emails from one IMAP server to another, and can process multiple accounts at once.

This means that the existing email server must be accessible via IMAP protocol. For some groupware servers, such as Tobit David or Microsoft Exchange, the IMAP service may need to be activated first.

IMAPCopy is open source and can be downloaded from the following URL:<http://ardiehl.de/imapcopy/index.html>.



Unpack the program into a separate directory. It is managed by the `ImapCopy.cfg` file. A suitable sample file is included. Open it with a text editor and edit it. Lines starting with `#` are comment lines and are ignored by the program.

Customize the following commands in the file:

SourceServer	The DNS name or IP of the source server from which the emails are to be retrieved
SourcePort	The TCP port used to communicate with the IMAP service on the source server. Usually 143 .
DestServer	The DNS name or IP of the destination server. The name of the Intra2net system.
DestPort	The TCP port for the IMAP service of the destination server. For the Intra2net system it is always 143 .
skipfolder	Folders on the source server that are not to be copied. If necessary, one or more items can be added to prevent deleted emails from being copied. For each folder to be excluded, use a "skipfolder" command in a separate line.
copyfolder	If only certain folders are to be copied, activate this command and specify the folders to be copied in individual "copyfolder" commands. If no "copyfolder" command is specified, all visible folders within <code>INBOX</code> are automatically copied.
DenyFlags	Use the default value " <code>\Recent</code> " because this flag cannot be copied.
Copy	Specify each account to be copied in a "Copy" command and replace the example lines with foo and bar. The 1. parameter is the user's login on the source server The 2. parameter is the password of the user on the source server The 3. parameter is the login of the user on the Intra2net system The 4. parameter is the password of the user on the Intra2net system Several copy commands are processed one after the other.

To run IMAPCopy, open a console with `cmd` and use `cd` to go to the directory where IMAPCopy was unpacked.

First test the basic configuration by entering `imapcopy -t`.

The program progress and any error or success messages are displayed on the console. Only if you have opened IMAPCopy as described in a separate console, you can still see these messages after the program has finished.

The program now checks the availability of the source and target server as well as the logins. If errors are displayed, adjust the configuration file and test it again.

Test the folder structure detection by entering `imapcopy -0`.

The program now tries to import all folders from the source server and create them on the Intra2net system. However, no emails are copied yet. Using the Intra2net system's web groupware, check whether all of the folders have been created correctly. If necessary, adjust the configuration on IMAPCopy.

Now start the actual email transfer by entering `imapcopy`.

29. Chapter - Migration from Microsoft Exchange

To migrate from Microsoft Exchange to the Intra2net Business Server and Groupware Client, there are 2 possibilities:

The first is offline migration, where neither of the two servers can be used during the migration. The migration must be carried out in a single step and cannot be interrupted. This variant is simpler and faster, but can usually only be implemented outside of normal business hours.

Alternatively, there is the migration during operation. This variant is somewhat more complex, but can be implemented during operation and with only very minor restrictions for the users. This moves one user at a time. This means that the migration can be extended over a period of several days.

29.1. Offline Migration

With this method of migration, neither the existing Exchange nor the new Intra2net system can be used for email and groupware, and new emails cannot be received. Therefore, make sure that the relevant users coordinate the date well in advance and schedule enough time.

Requirements:

- Fully functional Microsoft Exchange Server
- Intra2net Business Server in default configuration
- Administrator rights for Exchange Server, Active Directory Domain and Intra2net Business Server
- List of all users and their passwords in the local Active Directory
- Access to the existing Outlook installations of all users
- When fetching emails from an external provider via POP3: List of all logins and passwords for email retrieval.

29.1.1. Migration Step-by-step

1. Set up the Intra2net Business Server to have at least one IP on the LAN, DNS, appropriate local SSL certificate and access to the Internet. It requires a different IP than the former Exchange Server so that both can communicate with each other during migration. The configuration of the individual points is described in the Part 2, „General Functions“.
2. Create an account on the Intra2net system for all users. If required, create user groups. This is especially recommended to make it easier to organize sharing emails and groupware folders at a later stage.
3. Browse each user in Active Directory and take over existing email alias addresses to "Usermanager > Users : Addresses" on the Intra2net system.

4. Deactivate the receipt of any new emails and access via OWA. Do not allow any user to open Outlook. From this moment on, no user can make further changes to the groupware or email data.
5. Create a backup of all emails and groupware data on the Exchange Server.
6. Wait until the backup has been fully created and copy it to another server, for safety reasons.
7. If it is not already done, configure and enable access to emails on the Exchange Server via IMAP protocol.
8. Use IMAPCopy to copy the emails of all users from Exchange to the Intra2net system. A description of how to use IMAPCopy is described in 28. Chapter, „Migrating Emails with IMAPCopy“.
9. Open the Outlook installation of the first user.
10. Create a local Outlook data file that contains all groupware folders (not necessarily the user's email folders). To do this, use the Outlook Import/Export function.
11. Install the Intra2net Groupware Client on the user's PC.
12. Create a new Outlook profile for this user and configure it for use with the Intra2net Groupware Client as described in Section 18.1, „Installing the Program“ and the following sections.
13. Transfer the groupware data from the previously created local Outlook data file as described in Section 20.2.1.2, „Importing to the Groupware Client“.
14. Check if there are users from the local domain in the contacts folders. If so, then the email addresses of these users must be changed from internal Exchange addressing to normal email addresses.
15. Check the Calendar and Task folders whether there are future appointments or open tasks in which other participants from the local domain are invited. These other participants are stored in the form of internal Exchange addressing and must be converted to normal email addresses.
16. Repeat steps 9 to 15 for all users.
17. Migrate the public folders as described in Section 29.2.3, „Shared Folders“.
18. Disable Exchange Server completely, and permanently.
19. Configure how to send and receive new emails in the Intra2net system as described in 14. Chapter, „Email“.

29.2. Migration During Operation

With this variant of the migration, users can continue to work almost as usual during the migration. The users are migrated one by one from Exchange to the Intra2net system.

The only limitation is that the individual user currently being migrated cannot work in Outlook during their migration. However, it is still possible for them to receive emails.

The emails received during the migration can then be used as normal. In addition, during the migration phase, shared resources such as public folders or shared folders cannot be accessed across system boundaries.

Requirements:

- Fully functional Microsoft Exchange Server
- Intra2net Business Server in default configuration
- Administrator rights for Exchange Server, Active Directory Domain and Intra2net Business Server
- List of all users and their passwords in the local Active Directory
- Access to the existing Outlook installations of all users
- When fetching emails from an external provider via POP3: List of all logins and passwords for email retrieval.

29.2.1. Preparing for Migration

1. Set up the Intra2net Business Server to have at least one IP on the LAN, DNS, appropriate local SSL certificate and access to the Internet. It requires a different IP than the former Exchange Server so that both can communicate with each other during migration. The configuration of the individual points is described in the Part 2, „General Functions“.
2. Ensure that on the Intra2net system, under "User manager > Users", *no* accounts have been created yet for normal users.
3. Configure email dispatch via the Intra2net system, see Section 14.1, „Email Relay“.
4. In Exchange, store the Intra2net system as a relay server for sending all emails to the Internet.
5. Configure receiving emails via the Intra2net system and forward the emails to the Exchange. See Section 14.3, „Receive emails using the Intra2net system“ and Section 14.4, „Forwarding of entire domains“.
6. Test the receipt and dispatch of emails with the new configuration.
7. Test sending internal emails from Exchange to the Intra2net system. Use the login as the address and the fully certified local DNS name of the Intra2net system as the domain, e.g. `admin@intra.net.lan`. Check the Intra2net system's web groupware to see if the test email arrived.
8. If it is not already done, configure and enable access to emails on the Exchange Server via IMAP protocol.
9. If one or more users have mobile devices connected to the Exchange Server via ActiveSync, prepare them for ActiveSync use with the Intra2net system as described in 34. Chapter, „Connecting Mobile Devices using ActiveSync“.

10. Configure email archiving on the Intra2net system by going to "Services > Email > Archiving". Archive either in a dedicated archiving system or at least in a separate email account. This will serve as a backup for newly received emails if something goes wrong during the migration.
11. Create a backup of all emails and groupware data on the Exchange Server.
12. Wait until the backup has been fully created and copy it to another server, for safety reasons.

29.2.2. Migrating Individual Users

Perform the following steps for each individual user.

1. Create the user with their access data and group membership on the Intra2net system.
2. Configure the user's email addresses under "User Manager > Users : Addresses". Specifically, select the domains forwarded to the Exchange. From this moment on, new emails from the Internet to this user will arrive at the Intra2net system account and no longer on the Exchange.
3. On Exchange, set up an email forwarding for this user to their account on the Intra2net system. Use the login as the address and the fully certified local DNS name of the Intra2net system as the domain, e.g. `johndoe@intra.net.lan`. From this moment on, local emails to this user will also arrive at the Intra2net system and no longer at the Exchange.
4. During the migration, ensure that this user is no longer allowed to work in Outlook or OWA. Also deactivate all mobile devices that access this account via ActiveSync.
5. Use IMAPCopy to copy the emails of this one user from Exchange to the Intra2net system. The usage of IMAPCopy is described in 28. Chapter, „Migrating Emails with IMAPCopy“.
6. Open the user's Outlook installation.
7. Create a local Outlook data file that contains all groupware folders (not necessarily the email folders). To do this, use the Import/Export function of Outlook.
8. Install the Intra2net Groupware Client on the user's PC.
9. Create a new Outlook profile for this user and configure it for use with the Intra2net Groupware Client as described in Section 18.1, „Installing the Program“ and the following sections.
10. Transfer the groupware data from the previously created local Outlook data file as described in Section 20.2.1.2, „Importing to the Groupware Client“.
11. Check if there are users from the local domain in the contacts folders. If so, then the email addresses of these users must be changed from internal Exchange addressing to normal email addresses.
12. Check the Calendar and Task folders whether there are future appointments or open tasks in which other participants from the local domain are invited. These other

participants are stored in the form of internal Exchange addressing and must be converted to normal email addresses.

13. For this user, reconfigure any existing mobile devices so that they are now using the Intra2net system for ActiveSync.

29.2.3. Shared Folders

1. Open an Outlook installation with an Exchange profile that has full access rights to the shared folders.
2. Create a local Outlook data file that contains all public folders. To do this, use Import/Export on Outlook.
3. Create a general user account on the Intra2net system, such as **info**.
4. Set up a temporary Outlook profile on a PC for use with the Intra2net Groupware Client. Use the newly created user account.
5. Import the previously created data file into this Outlook profile.
6. Share folders with the Groupware Client to groups or individual users as required. See 22. Chapter, „Sharing Folders“.
7. Give at least one user the "Folder" permission for all folders of the account. This user can manage access to the account.
8. Open the "Groupware Client > Sync State" menu and wait for all data to be written to the server.
9. Close Outlook. The newly created Outlook profile is no longer needed and can be deleted.
10. Users who want to access the shared folders can now subscribe to them. The necessary steps are described in Section 21.2, „Linking Shared Folders“.

29.2.4. Final steps

1. Deactivate the domain(s) forwarding to Exchange under "Services > Email > Domains".
2. Disable Exchange Server completely, and permanently.
3. Configure "Services > Email > Archiving" to either change the permanent archiving system or deactivate archiving.

30. Chapter - Reference Information



Hint

The information in this chapter is only valid for the Intra2net Groupware Client. Information about web groupware and activesync can be found under 37. Chapter, „Reference Information“.

30.1. Synchronizable data

The Intra2net Groupware Client synchronizes the following data from Outlook with the server. All settings and data not listed here can be changed locally in Outlook, but cannot be synchronized to the server. They are therefore not visible to other users and are not included in the backup.

30.1.1. Tasks

30.1.1.1. Supported Items

- Subject
- Categories and their color assignment
- Text/Content (text only)
- Creation Date
- Sensitivity and Private Marking
- % Complete
- Status: In Progress,...
- Mileage
- Billing Information
- Total Expense
- Actual Cost
- Assignment
- Owner
- Due date
- Start date
- Reminder
- Expiry
- Organizer
- Creator

- Priority/Importance
- Company
- Recurring tasks except for recurring tasks in which the following task is created in a defined period after completion of the previous task
- Completion date
- Follow Up

30.1.1.2. Unsupported Items

No guarantee of integrity. In case of doubt, only the elements explicitly listed as supported are supported.

- Text/Content (formatted rich text)

30.1.2. Meetings

30.1.2.1. Supported Items

- Subject
- Categories and their color assignment
- Text/Content (text only)
- Sensitivity and Private Marking
- Busy Status / Display as
- Start and end time or full day
- Time Zones for Start
- Organizer
- Creator
- Priority
- Location
- Reminder (with user-specific assignment)
- Attendees marked with "Send meeting to this attendee".
- Recurring appointments

The following exceptions can be used for individual recurring meetings:

- Deleting a single meeting
- Changing subject
- Changing text/contents (text only)

- Changing location
- Changes to date and time

30.1.2.2. Unsupported Items

No guarantee of integrity. In case of doubt, only the elements explicitly listed as supported are supported.

- Text/Content (formatted rich text)
- Confirmation status of individual attendees
- Freely selectable time zones: The current time zone is always used
- Attendees who are not marked with "Send meeting to this attendee".

The following exceptions cannot be used for individual recurring meetings:

- Changing attendees

30.1.3. Notes

30.1.3.1. Supported Items

- Subject
- Categories and their color assignment
- Text/Contents

30.1.4. Contacts

30.1.4.1. Supported Items

- Full Name
- Title
- First Name
- Middle Name
- Last Name
- Suffix
- Initials
- Birthday
- Anniversary
- Spouse/Partner
- Nickname

- Sensitivity and Private Marking
- Company
- Web Page
- FTP-Site
- IM address
- Department
- Office
- Profession
- Position
- Manager
- Assistant
- Children
- Language
- Billing Information
- Hobbies
- Account
- Organizational ID Number
- Government ID Number
- Mileage
- E-Mail 1 to E-Mail 3
- Business Address
- Private Address
- Other Address
- Location
- Mailing Address
- Categories and their color assignment
- Note (text only)
- Business Phone (1 and 2)
- Private Phone (1 and 2)

- Car Phone
- Radio Phone
- Primary Phone
- Mobile Phone
- Pager
- Callback Phone
- Assistant Phone
- Business Phone
- Text Telephone
- Other Phone
- Business Fax
- Private Fax
- Other Fax
- ISDN
- Telex
- User Field 1 to 4
- User defined fields, see Section 24.8, „User-Defined Fields in Contacts“

30.1.4.2. Picture

Contacts can be assigned a picture. The following image formats (MIME types) are supported:

- image/jpeg
- image/png
- image/bmp, image/x-bmp and image/x-ms-bmp
- image/gif
- image/tiff
- image/x-wmf
- image/x-emf
- image/x-icon

Note that Outlook 2010 and older will only display JPG images in the overview, the other image formats will only be displayed in the contact view. From Outlook 2013 onwards, the other image formats will also be displayed in the contact list.

30.1.4.3. Unsupported Items

No guarantee of integrity. In case of doubt, only the elements explicitly listed as supported are supported.

- Internet Free Busy Address
- Certificates for encrypting/signing messages
- Email sending options (email address type, Internet format)
- Business card display options
- File as (save under)
- Note (Rich Text Format)
- Follow Up

30.1.5. Contact Groups

30.1.5.1. Supported Items

- Contact Group Name
- Display name of group members
- Email address of group members
- Contact Group notes (text only)

30.1.5.2. Unsupported Items

No guarantee of integrity. In case of doubt, only the elements explicitly listed as supported are supported.

- Fax number of group members
- Contact Group notes (Rich Text Format)
- Follow Up

30.1.6. Emails

30.1.6.1. Supported Items

- Sender
- Recipient
- CC

- BCC
- Subject
- Sent Time
- Time of Receipt
- Priority
- Web Headers
- Content (text, HTML and rich text format)
- Attachments
- Categories (Excl. Colors)

30.1.6.2. Unsupported Items

No guarantee of integrity. In case of doubt, only the elements explicitly listed as supported are supported.

- Reminders
- Follow Up

30.1.7. All Items

In general, the following items cannot be synchronized with the Intra2net Groupware Client:

- Disabling Auto-Archiving
- Attaching other Outlook items or files (except for emails)
- Linking to contacts

30.2. Advanced Registry Settings

The Intra2net Groupware Client can be further customized with the following adjustments in the Windows registry.

All registry keys can be found below `HKLM\SOFTWARE\Intra2net AG\Intranator Groupware Client`. If a 32-bit Outlook was installed on a 64-bit operating system, they can be found below `HKLM\SOFTWARE\Wow6432Node\Intra2net AG\Intranator Groupware Client` instead.

If the Intra2net Groupware Client was installed for only one user, the corresponding key is under HKCU instead of HKLM.

Most entries are not created automatically during installation. As long as the entries are not created, the standard values listed on the table are used. Create an entry with the name shown on the table with regedit to change the values.

30.2.1. Store Settings

The store settings can be found in the `mxstore_Store` key.

Entry (and data type)	Default Value	Description
SkipPrc (REG_SZ)	SearchProtocolHost.exe	File names of processes whose actions are not logged to avoid unnecessarily increasing the size of the log files. Several entries can be separated by semicolons.
Trace (REG_DWORD)	0x00004800	If normal process tracing is active, the events to be logged are selected. For further information please contact our support.
TraceAttr (REG_DWORD)	0x0000001b	Selects the columns that are output in the trace for a logged event. For further information please contact our support.
TracerDisabled (REG_DWORD)	0	Selects whether only starts and errors are logged (value 1) or also normal processes in operation (value 0).
PathLog (REG_SZ)		The complete path in which the log files are stored. If the entry does not exist, it is created in the %LOCALAPPDATA%\Intra2net directory.
TraceSzMax (REG_DWORD)	170	Maximum size for a log file in megabytes. If this size is exceeded, the file is rotated.
TraceDaysToRemember (REG_DWORD)	14	Maximum number of days that log files are retained.
TrgMin_FldChanged (REG_DWORD)	300	Shortest interval (in seconds), which can be set by the user in update intervals for "Folder changed".
TrgMin_FldTreeChanged (REG_DWORD)	300	Shortest interval (in seconds), which can be set by the user in update intervals for "Folder tree changed".
TrgMin_MailChanged (REG_DWORD)	60	Shortest interval (in seconds) which can be set by the user for "Background fetch" in subfolders.
TrgMin_MailChangedRoot (REG_DWORD)	1800	Shortest interval (in seconds) which can be set by the user in the root folder for "Background fetch".
TrgDefault_FldChanged (REG_DWORD)	3600	Default interval (in seconds) for "Folder changed" if the user has not specified otherwise.
TrgDefault_FldTreeChanged (REG_DWORD)	3600	Default interval (in seconds) for "Folder tree changed" if the user has not specified otherwise.
TrgDefault_MailChanged (REG_DWORD)	3600	Default interval (in seconds) for "Content changed" if the user has not specified otherwise.

Entry (and data type)	Default Value	Description
TrgDefault_Always (REG_DWORD)	0	If 1, the intervals set with the TrgDefault_ entries are always used, regardless of what the user has set. This allows the administrator to specify the update intervals for users.
TrgDefault_Ctx_InFocus (REG_DWORD)	180	Default interval (in seconds) by which the contents of the folder currently open in Outlook is synchronized.
Trigger_Reset (REG_DWORD)	0	If 1, the next time it is started, the trigger settings for all folders are reset to their default values. This value is then reset to 0 in the registry.
CalPrivatePlaceholder_Default (REG_DWORD)	1	<p>If 1, placeholders are displayed for newly created or changed calendar entries marked as private for other users. If 0, calendar entries marked as private are completely hidden from other users.</p> <p>This value is only retrieved and transferred to a new data file with Outlook the first time it is opened. Existing data files are not affected by this setting.</p>
CalPrivatePlaceholder_ResetOnOpen (REG_DWORD)	0	If 1, the CalPrivatePlaceholder_Default setting is applied not only when opening a data file for the first time, but on every start.
MemLoad_SyncOff (REG_DWORD)	90	<p>The threshold value in percent of the total system memory. If more memory is used, synchronization is temporarily deactivated. This will avoid errors caused by running out of memory. A value of more than 100 deactivates this function.</p> <p>This is a protective function that ensures correct functionality. If it is set too high or even deactivated, this can lead to data loss, inconsistencies and program crashes. Therefore, deviating from the default value is strongly discouraged.</p>
IMAP ID: ALLOW Send Id Info To Server (REG_DWORD)	1	If 1, the Groupware Client sends information about the locally installed version and the host via IMAP ID command to the IMAP server and via HTTPS to rss.intra2net.com. The amount of information sent depends on the other IMAP ID: keys.
IMAP ID: Send ONLY Product Version (REG_DWORD)	1	If 1, the groupware client uses the IMAP ID command to only send information about the Groupware Client itself, but not about the host.
IMAP ID: Send ALL Plattform-Information (REG_DWORD)	0	If 1, the groupware client uses the IMAP ID command to send information about the

Entry (and data type)	Default Value	Description
		groupware client, the Outlook version, the operating system used and the hardware specifications of the computer.
ACL_ChangeNotification (REG_DWORD)	1	If 1, the user receives a notification in their Inbox as soon as access rights to folders have changed. 0 disables this function.
ACL_ChangeNotification-Scope (REG_DWORD)	5	<p>Selects the type of changes to access rights the user is notified of. Bit field, therefore add the values for the desired options.</p> <ul style="list-style-type: none"> 1 Notification for other users' folders 2 Notification for own folders 4 Notification only for changes to own rights
ACL_ChangeNotificationView (REG_DWORD)	0	<p>Selects the way in which the user is notified of new access rights.</p> <ul style="list-style-type: none"> 0 Simplified description 1 Complete ACLs as short text 4 Complete IMAP-ACLs as letters (RFC 4314)
KeepOutlookInboxName (REG_DWORD)	0	If 0, a unlinked inbox folder is named <code>Messages</code> . If 1, the folder retains the name <code>Inbox</code> even in disconnected state. When the folder is connected to the server, it is always <code>Inbox</code> regardless of this option.
SyncTemplatesFilePath (REG_SZ)	Groupware Client installation folder	Full directory path of the folder from which the <code>userdefined_sync_fields.xml</code> file is loaded for specifying user-defined fields.
DoLastAuthorTagging (REG_DWORD)	1	If 1, the user name of the most recent editor is stored as a class for each object.
AutoSkipNewRemoteEmail-Folder (REG_DWORD)	1	If 0, new email folders found on the server will be automatically connected when an account is connected 1:1. If 1, only newly detected Groupware folders are automatically connected.
StateSICompletion_Default (REG_DWORD)	0x01	<p>Default mode for downloading new emails.</p> <ul style="list-style-type: none"> 0x01 Only headers 0x07 Entire content <p>The settings can still be configured for each folder using the method described in Section 25.1, „Retrieve Emails Completely or Only Headers“.</p>

Entry (and data type)	Default Value	Description
StateSICompletion_Fixed (REG_DWORD)	0	If 1, only the mode defined by StateSICompletion_Default is used for downloading emails. The user is no longer able to adjust the mode by using the "Options" menu.
UseRemotelcon (REG_DWORD)	0	If 1, emails which were previously only available as headers are marked with a special icon (depicting a phone) in the folder view. This value is only checked when a new email is fetched from the server with headers only. Changing this setting does not affect existing emails.
IconPreferAnsweredOverForwarded (REG_DWORD)	1	If 1, the "Replied" icon is displayed for emails forwarded and answered. If 0, the "Forwarded" icon is displayed.
InitialReminderSetting (REG_SZ)	Creator,Owner	<p>Defines which users are given a reminder when creating a meeting or task.</p> <p>Creator User who creates the appointment Owner Owner of the folder in which the meeting is saved</p> <p>The values are separated by commas and entered without spaces. This setting only applies to the creation of a new meeting or task, not to changing existing ones.</p> <p>If only "Owner" is set and a new meeting with a reminder is created in a shared folder, a reminder is always stored locally in the user's Outlook, in addition to the server-side reminder for the owner of the folder. This is necessary for technical reasons. If it is not desired, the user can remove it after creating the meeting without affecting the reminder for the owner.</p> <p>This value only affects newly created appointments or tasks. Changing this setting does not affect existing appointments or tasks.</p>
ReminderChangesHandling (REG_SZ)	(empty)	<p>Specifies how reminders should be managed in other users' folders.</p> <p>SharesInitFromOwner means that when a meeting or task is fetched from the server for the first time, the folder owner's reminder settings are applied once. After that, the reminder for the local user is handled completely independently of the owner of the folder.</p>

Entry (and data type)	Default Value	Description								
		<p>sharesAsOwner means that the reminders for the local user are always treated exactly the same as for the owner of the folder.</p> <p>This value only affects newly fetched appointments or tasks from the server. Changing this setting does not affect existing appointments or tasks.</p>								
CntMaxFldToAllowAllBack-ground (REG_DWORD)	600	If more folders are connected than the specified threshold value when Outlook is started, only the folders at the top level will be synchronized automatically and periodically, with all others synchronized only when the folder is opened by the user in Outlook. If too many folders are synchronized automatically, the set interval is no longer sufficient to process all folders, causing delays in synchronization.								
PeriodicRecoverDelayMax (REG_DWORD)	0x001b7740 (= 30min)	Interval in milliseconds, in which the default calendar is checked for local changes not yet made on the server.								
SendSyncOutDelayMax (REG_DWORD)	0x001b7740 (= 30min)	Interval in milliseconds, in which the default folder for sent emails of each data file is searched for emails not yet saved on the server.								
RegMailAttrForBackGround (REG_SZ)	Mail,Group-ware,MailBck-Grnd,Group-wareBckGrnd	<p>Controls which folder types are synchronized with the server. Using flags, properties such as read/unread, marked, deleted, etc. of individual items can be assigned. Deactivating this synchronization can improve performance.</p> <table><tr><td>Mail</td><td>Currently selected folders with emails.</td></tr><tr><td>Group-ware</td><td>Currently selected folders with groupware data</td></tr><tr><td>MailBck-Grnd</td><td>Unselected folders with emails.</td></tr><tr><td>Group-wareBck-Grnd</td><td>Unselected folders with groupware data</td></tr></table> <p>Individual values are separated by commas.</p>	Mail	Currently selected folders with emails.	Group-ware	Currently selected folders with groupware data	MailBck-Grnd	Unselected folders with emails.	Group-wareBck-Grnd	Unselected folders with groupware data
Mail	Currently selected folders with emails.									
Group-ware	Currently selected folders with groupware data									
MailBck-Grnd	Unselected folders with emails.									
Group-wareBck-Grnd	Unselected folders with groupware data									
NoAutoIMAPAbol (REG_DWORD)	0	If 1, an IMAP subscription is not created or cancelled when connecting and disconnecting an email folder.								

Entry (and data type)	Default Value	Description
FolderCollisionHandling (REG_SZ)	LikeOL	Controls how name conflicts are handled when renaming or moving folders. Query The user is asked Add The folder is given a number appended to the name LikeOL The folder is given a number appended to the name Merge The contents of the two folders with the same name are merged.
ApplyClassicFolderMove (REG_DWORD)	0	If 1, moving folders is performed locally and transferred to the server as delete and add operations for the individual objects. This is much slower.
MailSourceCacheOff (REG_SZ)	On	Controls how much of the original source of an object read from the server is kept. Omitting this information can save storage space in the data file. On Original source and meta information are retained up to the size limit from MailSourceCacheSzMax MetaOnly The original source and headers are not kept, but meta information like UID and synchronization time is retained Header-Only Metainformation like UID and synchronization time as well as the header part of the original source are retained without size limit Off Original source and meta information are deleted
MailSourceCacheSzMax (REG_DWORD)	16	Maximum size in kilobytes up to which the original source text is kept, see MailSourceCacheOff.
FixDisabledAddIn (REG_DWORD)	1	If 1, the Groupware Client addin (GUI) is automatically activated on startup.
NoWarnOnUnmappedStores (REG_DWORD)	0	If 1, the user will not be warned at startup if there is a Groupware Client data file where no folders are connected to a server.
OnSrvSideFldDel_DelLocalAlways (REG_DWORD)	1	Controls how Outlook is managed when a root folder is deleted on the server side.

Entry (and data type)	Default Value	Description												
		<p>If 0, the root folder on the Outlook side is retained and only the connection is removed.</p> <p>If 1, the root folder is also deleted on the Outlook side. This does not apply to the standard folders of Outlook such as <code>Contacts</code>, <code>Calendar</code> etc., since they cannot be deleted.</p>												
MdnAllow (REG_DWORD)	0	<p>If 1, requests for read receipts (MDNs) are not removed from incoming emails.</p> <p>This value only affects new emails fetched from the server. Changing this setting does not affect existing emails.</p>												
AutoAddToAddressBook (REG_DWORD)	1	<p>If 1, newly linked contact folders are automatically registered as Outlook Address Book.</p>												
NotifyThirdParties (REG_DWORD)	1	<p>If 1, potential compatibility problems with third-party programs or add-ins are reported to the user.</p>												
DisableSyncDialogs (REG_SZ)	(empty)	<p>Permanently disables dialog boxes with specific notes and questions to the user.</p> <table><tr><td>All</td><td>All dialogs disabled</td></tr><tr><td>SlowFolderRenameIndication</td><td>Hint that folder renaming takes longer</td></tr><tr><td>RenameFolderAlsoOnServer</td><td>Ask if a folder should be renamed only locally or also on the server</td></tr><tr><td>MoveHandledAsCopyIndication</td><td>Hint that a copy operation is performed instead of a move</td></tr><tr><td>MergeFolders</td><td>Ask if a folder should be copied or merged with an existing one</td></tr><tr><td>FolderRenewIndication</td><td>Hint about creating a backup copy of folders renewed on the server</td></tr></table> <p>The values of the dialogs to be deactivated are separated by commas and entered without spaces and hyphens.</p>	All	All dialogs disabled	SlowFolderRenameIndication	Hint that folder renaming takes longer	RenameFolderAlsoOnServer	Ask if a folder should be renamed only locally or also on the server	MoveHandledAsCopyIndication	Hint that a copy operation is performed instead of a move	MergeFolders	Ask if a folder should be copied or merged with an existing one	FolderRenewIndication	Hint about creating a backup copy of folders renewed on the server
All	All dialogs disabled													
SlowFolderRenameIndication	Hint that folder renaming takes longer													
RenameFolderAlsoOnServer	Ask if a folder should be renamed only locally or also on the server													
MoveHandledAsCopyIndication	Hint that a copy operation is performed instead of a move													
MergeFolders	Ask if a folder should be copied or merged with an existing one													
FolderRenewIndication	Hint about creating a backup copy of folders renewed on the server													
OnRepair_Profiles (REG_DWORD)	0	<p>If 1, a repair installation of the Groupware Client will repair all Outlook profiles with data files of the Groupware Client of all accessible user accounts. If 0, this repair is</p>												

Entry (and data type)	Default Value	Description
		performed only for the user account that performs the repair installation.
CategoryColorSyncRead (REG_DWORD)	1	If 1, the category color assignment is evaluated when groupware objects are synchronized from the server and possibly transferred to the Master Category List. If 0, the category color assignment stored on the server is ignored.
CategoryColorSyncWrite (REG_DWORD)	1	If 1, the local category color assignment is also transmitted to the server when groupware objects with categories are synchronized out. If 0, only the name of the categories is written, but not the locally used category color assignment.

30.2.2. Addin Settings

The settings for the Outlook addin (GUI) can be found in the `mxstore_GUI` key.

Entry (and data type)	Default Value	Description
Trace (REG_DWORD)	0x00004800	If normal process tracing is active, the events to be logged are selected. For further information please contact our support.
TraceAttr (REG_DWORD)	0x0000001b	Selects the columns that are output in the trace for a logged event. For further information please contact our support.
TracerDisabled (REG_DWORD)	0	Selects whether only starts and errors are logged (value 1) or also normal processes in operation (value 0).
PathLog (REG_SZ)		The complete path in which the log files are stored. If the entry does not exist, it is created in the <code>%LOCALAPPDATA%\Intra2net</code> directory.
TraceSzMax (REG_DWORD)	170	Maximum size for a log file in megabytes. If this size is exceeded, the file is rotated.
TraceDaysToRemember (REG_DWORD)	14	Maximum number of days that log files are retained.
AllowOwnRightsEdit (REG_DWORD)	1	If this is active, a user can edit their own rights to a folder.
AllowShareOwnerRightsEdit (REG_DWORD)	0	If the value is 1, a user can edit the owner's rights to a folder. To do this, the user must have the "Folder" permission for this folder.
ShowAdvancedOptions (REG_DWORD)	1	If this setting is active, the options dialog will be displayed (e.g. for setting the synchronization frequency).
NotifyNewMail (REG_DWORD)	1	At 1, new email notifications are enabled.

Entry (and data type)	Default Value	Description
NotifyNewMailMaxInterval (REG_DWORD)	60	The number of seconds in which no further notification is displayed after a new email notification.
NotifyNewMailMaxItems (REG_DWORD)	3	Maximum number of emails displayed in a new email notification.
NotifyNewMailTimeOn-MouseOverMs (REG_DWORD)	1000	Time in milliseconds after which a new email notification closes when the mouse pointer is in the notification area.
NotifyNewMailInitialDelay (REG_DWORD)	5	Waiting time in seconds until a notification is displayed after a new email has been received.
NotifyNewMailMaxAge (REG_DWORD)	120	Maximum age in minutes for unread emails to be displayed as new email notifications. The time of receipt on the server is used to calculate this age.
SyncStateFetchInterval (REG_DWORD)	5	Frequency in seconds in which the display in the Sync status menu is refreshed.
UpdateCheckEnabled (REG_DWORD)	1	At 1, a check is made when the Groupware Client is started to see whether a new version is available. The check is done via HTTPS to rss.intra2net.com , maximum once per day.
EnableIncellEditClose (REG_DWORD)	1	At 1 directly edited items in the overview screen are forced to close when quitting which allows them to be synchronized to the server.
OlReceiveRulesEnabled (REG_DWORD)	0	The value 1 activates the client-side sort rules. This only makes sense in exceptional cases and involves risks such as duplicates. Instead, use server-side sort rules.
DfltLinkMode (REG_SZ)	OlHide,SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted	Controls the folder view in the "Folder Linking" dialog. The value "OlHide,SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted" corresponds to expert mode off, "SrvOwnAuto,SrvShareTree,SrvOwnTree,SrvOwnRooted" corresponds to expert mode on.

30.3. Data Formats

All groupware items are stored on the IMAP server as individual emails. The groupware data is coded XML and stored as an attachment in the email.

The XML format used is based on the Kolab Storage Format Version 2.0, the specification of which can be found at <https://www.intra2net.com/en/download/manuals/kolabformat-2.0.pdf>.

Additionally, the Intra2net Groupware Client stores application specific data as email headers. Their names begin with `x-mxstore` and `x-sync`. The format of these headers may change at any time without notice. These headers should therefore not be interpreted by other software.

Part 4. Web-Groupware and ActiveSync

31. Chapter - Introduction to Web Groupware

Web groupware enables you to access email and groupware data such as calendars, tasks, contacts and notes using a standard web browser.

It can be accessed on the interface of the Intra2net system using the "Groupware" menu. When accessed from the Internet without using "Remote Administration via HTTPS" (Menu " Usermanager > Groups : Administration rights"), it opens directly after login.

31.1. The Display Modes

The web groupware can be used in different display modes. These are optimized for different browsers and end devices:

Dynamic	For current browsers. High ease of use due to AJAX and dynamic background updating.
Classic	Maximum compatibility with simple or older browsers. Does not offer all functions of the dynamic display mode.
Smartphone	Optimized for smartphones and tablets with touch control. Clear presentation even on small screens. Addresses and calendar entries can currently only be viewed.

When logging on to the Intra2net system it is possible to choose which display mode is to be used. By default, the system automatically determines the most suitable display mode using browser recognition (the "Automatic" setting).

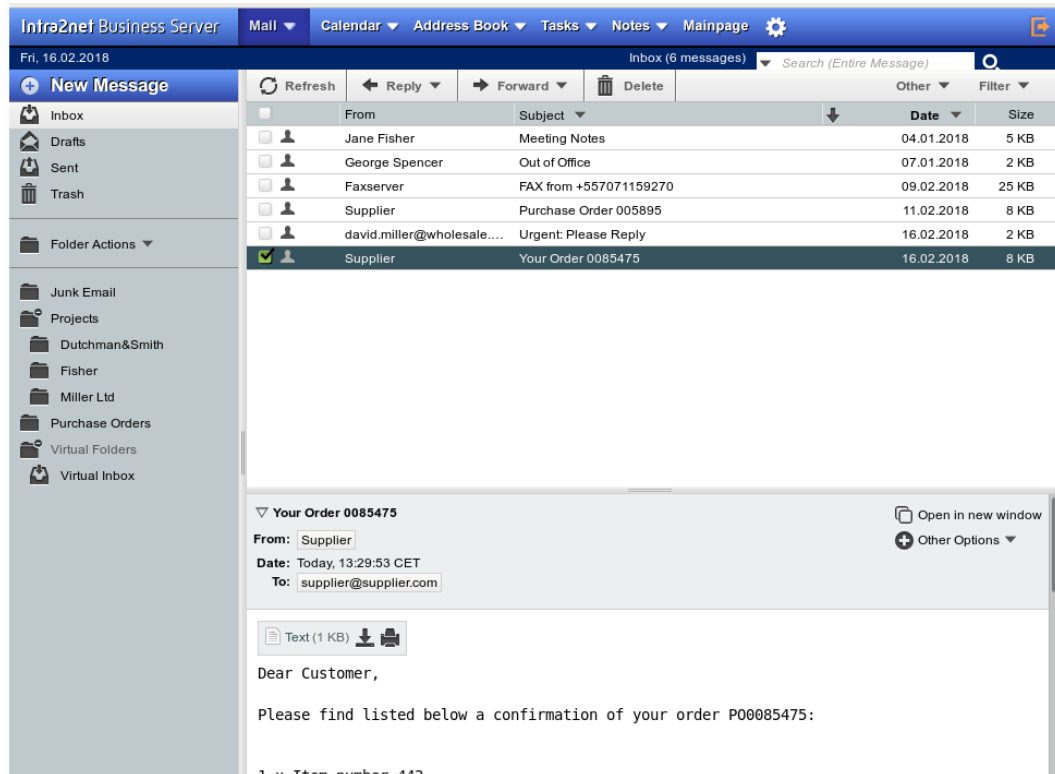
The following documentation refers to the dynamic mode.

32. Chapter - Email

32.1. Reading and Editing Emails

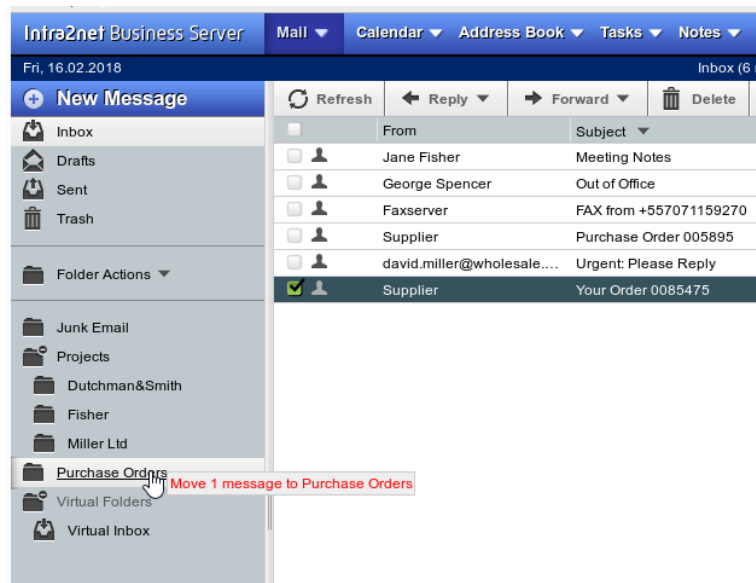
32.1.1. Displaying Emails

"Webmail" provides the facility to read, write and edit emails in the web groupware.



In the email list of the active folder, the individual emails can be right-clicked. A context menu opens which offers functions such as deleting, forwarding and marking emails.

Emails can be dragged and dropped from the email list to another folder.



32.1.2. Deleted Emails

Emails are moved to the recycle bin by the delete command.

If a deleted email should be restored, simply drag and drop it back to the correct folder from the Recycle Bin.

The system can automatically clear the recycle bin after a set period (Usermanager > Users : Groupware). By default, this happens every 30 days. Alternatively, the entire recycle bin can be cleaned up manually using the "Empty" command in the recycle bin context menu (right-click the folder name).

Some email clients (e.g. Mozilla Thunderbird and Outlook 2003) do not move deleted emails to the Recycle Bin, but leave them in the original folder and mark them for deletion. Depending on the program, the emails are then deleted automatically when the program is closed or only upon manual command (*IMAP Expunge*).

Refresh			Other ▾	Filter ▾
	From	Subject ▾		
	George Spencer	Out of Office	Date ▾	Size
	Faxserver	FAX from +557071159270	16.02.2018	2 KB
	Supplier	Purchase Order 005895	16.02.2018	2 KB
	david.miller@wholesale....	Urgent: Please Reply	16.02.2018	2 KB
	Supplier	Your Order 0085475	16.02.2018	2 KB

The marked emails can be permanently deleted or hidden with the Web Groupware. These functions can be found in the "Other" menu.

	Refresh		Reply		Forward		Delete		Other	Filter
	From		Subject						Date	Size
	George Spencer		Out of Office						16.02.2018	2 KB
	Faxserver		FAX from +557071159270						16.02.2018	2 KB
	Supplier		Purchase Order 005895						16.02.2018	2 KB
	david.miller@wholesale....		Urgent: Please Reply						16.02.2018	2 KB
	Supplier		Your Order 0085475						16.02.2018	2 KB

Reply

Forward

Mark as...

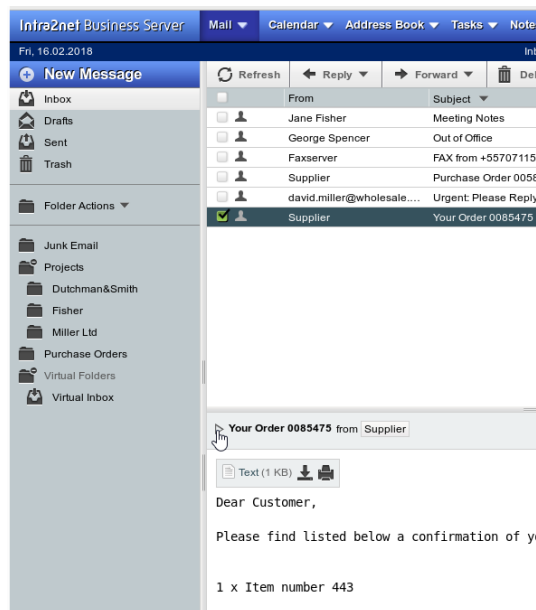
Delete

32.1.3. Exporting Emails

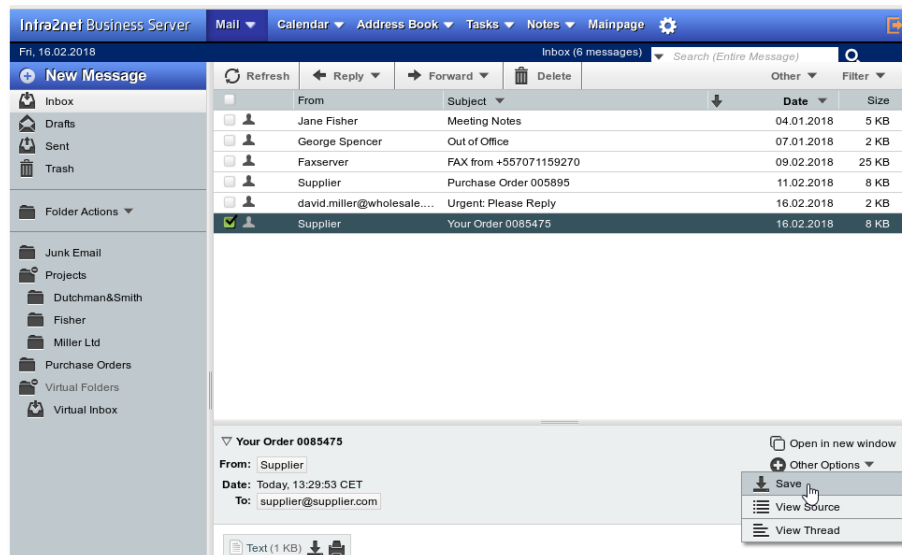
In order to be able to process individual emails on other programs or to analyze them more precisely for troubleshooting purposes, it is possible to export emails in RFC822 format (sometimes also referred to as .EML).

Proceed as follows:

1. Open the relevant email
2. Expand the details with the arrow



3. Select the menu "More functions" on the right hand side, and menu option "Save". It is now possible to select the appropriate target directory in your browser.



4. To forward the exported email again by email, e.g. for error analysis, it is best to compress the .EML file with a compression program such as WinZip. This ensures that the email is not accidentally changed during transmission.

32.2. Sending Emails

32.2.1. New Message

Click on the "New message" button in the upper left corner and a window for composing a new email will open.

When starting to type a name in the "To", "Cc" or "Bcc" fields, all available address books are automatically searched for this name in the background. Contacts found will then be offered as a selection dialog.

Alternatively, it is possible to click "To" to add matching recipients from the address books.

The screenshot shows an email composition window. At the top, there are buttons for 'Send', 'Check Spelling', and 'Save as Draft'. The 'From' field is populated with 'John Doe <john.doe@mycompany.com>'. The 'To' field is empty, and a hand cursor is pointing at it. Below the 'To' field are buttons for 'Add Cc', 'Add Bcc', and 'Add Attachment'. The 'Subject' field is empty. On the right side, there are options for 'HTML composition', 'Save in Sent', 'Priority: Normal', and 'Other Options'. Below the email fields is an 'Address Book' sidebar. It has a 'Find' field and a 'from' dropdown set to 'Contacts'. A search button is present. The address book list shows three entries: 'Fisher, Jane' <jane.fisher@example.com>, 'Intra2net' <info@intra2net.com>, and 'Smith, Matt' <matt@smiths.com>. The 'Smith, Matt' entry is selected. To the right of the list are buttons for 'To >>', 'Cc >>', and 'Bcc >>'. A 'Remove' button is at the bottom right of the address book panel.

32.2.2. Append Signatures

It is possible to define a signature, which is automatically appended when a new email is sent.

Each user can configure their signature under "Usermanager > Own Profile > Groupware". To access this menu, the web groupware must first be exited via the "Mainpage" button. The administrator can configure the signatures of all users using the "Usermanager > Users : Groupware" menu.

The screenshot shows the 'Own profile' settings page. On the left is a sidebar menu with options: 'Mainpage', 'Usermanager' (expanded), 'Overview', 'Users', 'Groups', 'Import/Export', 'Own profile' (selected), 'Settings', 'Forwarding', 'Vacation', 'Sorting', 'Spamfilter', 'Groupware', 'Network', 'Services', 'System', 'Information', and 'Groupware'. The main content area is titled 'Own profile' and contains two sections: 'Default folders' and 'Webmail settings'. The 'Default folders' section has dropdown menus for 'Calendar' (INBOX/Calendar), 'Contacts' (INBOX/Contacts), 'Tasks' (INBOX/Tasks), 'Notes' (INBOX/Notes), 'Drafts' (INBOX/Drafts), 'Sent emails' (INBOX/Sent Items), and 'Trash' (INBOX/Deleted Items). Below these is a 'Delete messages from trash after' field set to '30' days, with a 'Save settings' button. The 'Webmail settings' section has a 'Messages per page' field set to '25', a 'Default sender' dropdown set to 'John Doe <john.doe@mycompany.com>', and a 'Signature' text area containing the following text: 'John Doe', 'Test Engineer', 'My Company Ltd', '123 Main St.', 'Anytown 12345', and 'Phone: 01234-56789'.



Hint

The signature is not displayed in the email editor. However, it will be automatically attached to the email once it is sent.

32.3. Managing Folders

32.3.1. Folder Hierarchy

The list of all email folders is displayed on the left side of the screen. The user's root folder (called "INBOX" in IMAP) is displayed at the top as `Inbox`. The folders for drafts, sent emails and recycle bin are displayed below. These are always displayed with the names `drafts`, `sent` and `trash`, regardless of how they are actually named.

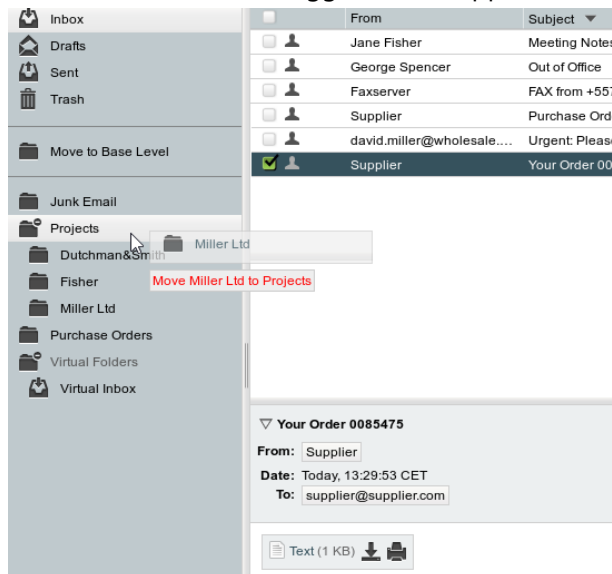
The actual name of these folders can be configured in the "User Manager > Own Profile > Groupware" menu or by the administrator in the "Usermanager > Users : Groupware" menu.

All other subfolders of the user are displayed below "Folder Actions" in alphabetical order.

32.3.2. Organizing Folders

The folder names in the folder list can be right-clicked. A context menu opens with options to delete, rename or create subfolders.

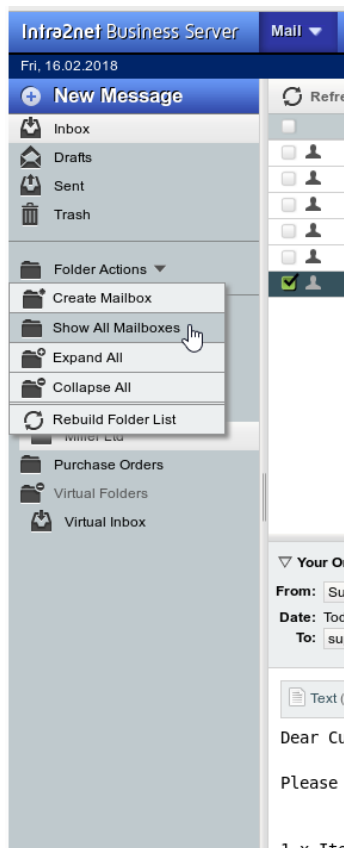
Entire folders can be dragged and dropped into the folder hierarchy.



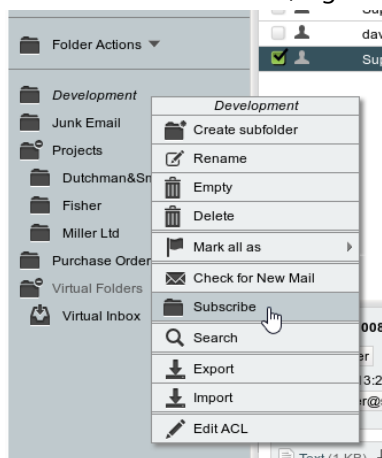
32.3.3. Subscribing to Folders

The Webmail system normally only displays the subscribed folders, all other folders are hidden.

In order to subscribe to a folder, first switch to the view of all folders. To do this, use the "Folder Actions > Show All Mailboxes". Now the folders that are not subscribed to will also be displayed, which are shown in italics.



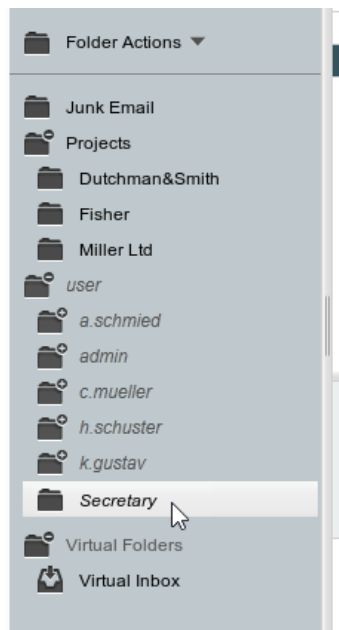
To subscribe to a folder, right click the folder and select "Subscribe".



If all needed folders have been subscribed to, "Folder Actions > Hide Unsubscribed" can be used to hide them again.

The list of subscribed folders is stored on the IMAP server. Most email programs access this server-side subscription list. For example, a folder only needs to be subscribed to once and is then displayed in all email programs and devices used.

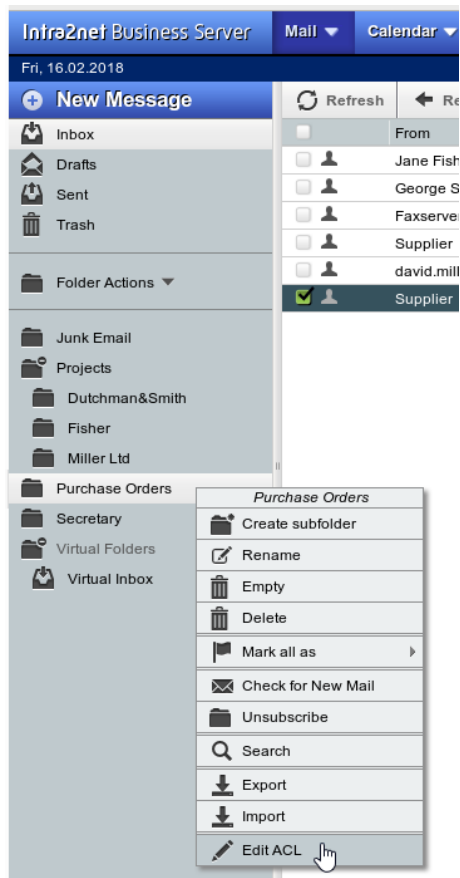
If another user has shared one of their email folders with you, this can be found in the `user` hierarchy and underneath the user name. If another user has shared their inbox, it is the same as the user name itself; no subfolder `Inbox` is displayed.



Shared folders of other users are hidden after sharing and must be subscribed to as described above before they are displayed permanently.

32.3.4. Sharing Folders

To share folders with other users, right-click on the folder name in the folder list and open "Edit ACL".



A window opens in which the access rights to this folder can be edited in detail.

Other user names can be entered in the left column under "User". After entering the user name, the IMAP ACLs can either be controlled individually using the check boxes, or frequently used rights combinations can be selected from the templates.

If a folder is to be shared not only for one user but also for an entire user group, use **group:** as the user name and then the name of the user group on the Intra2net system (e.g. **group:All**).

The screenshot shows the Intra2net Business Server interface. The top navigation bar includes links for Mail, Calendar, Address Book, Tasks, Notes, and Mainpage. Below this, the 'Preferences for Mail' section is visible, with options to 'Show Advanced Preferences' and 'Edit Preferences for:'. The main content area is titled 'Share Mailboxes' and contains a table titled 'Current access to Purchase Orders'. The table has columns for 'User', 'List', 'Read', 'Mark (Seen)', 'Mark (Other)', 'Insert', 'Post', 'Administer', 'Create Subfolders/Rename Mailbox', 'Delete/Rename Mailbox', 'Delete', and 'Purge'. Two users are listed: 'john.doe' and 'jane.fisher'. A dropdown menu is open for 'jane.fisher', showing a list of templates: 'None', 'Read', 'Post', 'Append', 'Write', 'Delete', and 'All'. The 'Write' template is selected.

User	List	Read	Mark (Seen)	Mark (Other)	Insert	Post	Administer	Create Subfolders/Rename Mailbox	Delete/Rename Mailbox	Delete	Purge
john.doe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
jane.fisher	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

33. Chapter - Address Book



Hint

This chapter, as well as others about calendars and tasks, are still in progress and will be published soon.

34. Chapter - Connecting Mobile Devices using ActiveSync

34.1. Introduction

ActiveSync is a protocol developed by Microsoft to synchronize groupware data between a server and mobile devices such as smartphones and tablets. It can now also be used by Office programs such as Outlook 2013.

Most mobile devices contain an interface for synchronization of emails, contacts, appointments and tasks via ActiveSync. Since the protocol was first offered by the Microsoft Exchange Server, it can often be found on devices under the keywords such as "Microsoft Exchange Server", "Exchange Server ActiveSync" or similar.

ActiveSync can be used with all Intra2net licenses that include the Mail Server function.

34.2. Server Settings

In order to connect devices to the Intra2net system via ActiveSync, the following basic configurations must first be made or checked on the server:

1. Check how the Intra2net system is connected to the Internet. To do this, check the type of active provider in the "Network > Provider > Profile" menu. If it is a (DSL) dial-up line, everything is fine and you can proceed to the next step.

If it is a router provider type, check whether this router allocates an unchanged official IP to the Intra2net system or whether it assigns an IP from a private address range via NAT. In the latter case, port forwarding for TCP port 443 (https) to the IP of the Intra2net system must be configured on the router.

2. Check the firewall ruleset for incoming connections from the Internet. It can be found in the "Network > Provider > Profiles : Firewall" menu for the active provider and can be examined with the magnifying glass icon. It must have "Incoming HTTPS connections active" enabled.
3. The Intra2net system must be contactable by the mobile device via a DNS name on the Internet.

If the Intra2net system has a static IP, set up a DNS entry in your own official domain for it. The system is then accessible under a name such as `intra.clientname.de` or `mail.example.com`. This can normally be set up free of charge and promptly by the webspace provider who manages your domain.

If the Intra2net system is assigned a different IP for each Internet dial-in, a DynDNS service must be set up for addressing. See Section 10.13, „DynDNS“.

A static IP cannot be used directly and without DNS names, since certification authorities are not allowed to issue certificates on IPs.

4. Access to ActiveSync takes place exclusively via HTTPS. For the encryption a suitable certificate is required, which has been issued by an external certification authority for the external DNS name (see above). Proceed as described in Section 9.5, „Using an External Certificate Authority“ to set up this certificate.

We strongly advise against trying to establish the ActiveSync connection with a self-signed certificate. For many devices this requires a more complex configuration and/or compromises the security of the connection. Setting up a certificate from an external certificate authority, on the other hand, is simple, fast, free and secure.

5. Test whether access to HTTPS from the Internet works and whether the certificates are correctly configured. Use the menu "System > Diagnosis > External HTTPS".
6. Check the quality of the passwords for all users who will be using ActiveSync. The passwords should be sufficiently long (at least 8 digits), comprising letters, numbers and special characters, if necessary. They should also not consist of, to a large extent, a word or characteristic names of a common language.
7. Before a user can use ActiveSync, the "Access groupware data via ActiveSync" (under menu "Usermanager > Groups : Rights") must be enabled in a user group the user belongs to.



Tip

We recommend to set up a separate user group specifically designed for ActiveSync and to include only users with verified password quality (see above).

8. ActiveSync only transfers data from a single folder for each item type. For this reason, each user in the "Usermanager > Users : Groupware" menu should have their default folders to be set to be transferred via ActiveSync.
9. Configure the individual devices as described in the following chapters.

34.3. Special Features and Tips

34.3.1. Deleting Emails on the Server

If an email account is used with an email client via IMAP simultaneously with the ActiveSync mobile device, which does not represent the deletion of emails by moving them to a recycle bin, but rather by deletion marks, the emails deleted by the client are only deleted on the ActiveSync device at the time of the final deletion (expunge command).

Applicable email clients include Mozilla Thunderbird and Microsoft Outlook 2003.

34.3.2. Synchronization Steps

If the mobile device reports to the Intra2net system for synchronization, it is notified of all changes since the last synchronization and then updates its data. Changes made on the mobile device are also transferred to the Intra2net system.

For technical reasons, however, some changes require two synchronization steps for complete transfer. There must be a time interval of at least 4 minutes between these steps. This is especially important for synchronization intervals of several hours. In case of doubt, use manual synchronization twice in a row at 4-minute intervals on the mobile device. At the end of this period all data will be up to date.

34.3.3. Manage and Resynchronize Devices

On the Intra2net system, the "Usermanager > Users : Groupware" menu displays a list of all devices connected to the corresponding user account. This is also available for each user under "User manager > Own profile > Groupware".

The "Reset" button cancels the synchronization state of a device on the server. The next time the device reports for synchronization, all data is transferred again. This helps to solve synchronization or data consistency problems. This is also automatically triggered when a backup of the Intra2net system is restored.

34.3.4. Synchronize Multiple Calendars or Contact Lists

An ActiveSync connection transfers only one folder for each groupware item type (appointment, address, task, etc.). In some cases, however, in addition to the private address book, a company-wide address book is also required.

This can be done by setting up additional ActiveSync connections. Since the folders to be transferred are set per user account in the "User Manager > Users : Groupware" menu, a different user account must be used for each of these connections.

For example, if a company-wide address book is to be transferred, a general user such as `info`, where the desired address book is also stored, can be used. There is no limit to how many ActiveSync connections can be connected in parallel to one user account.

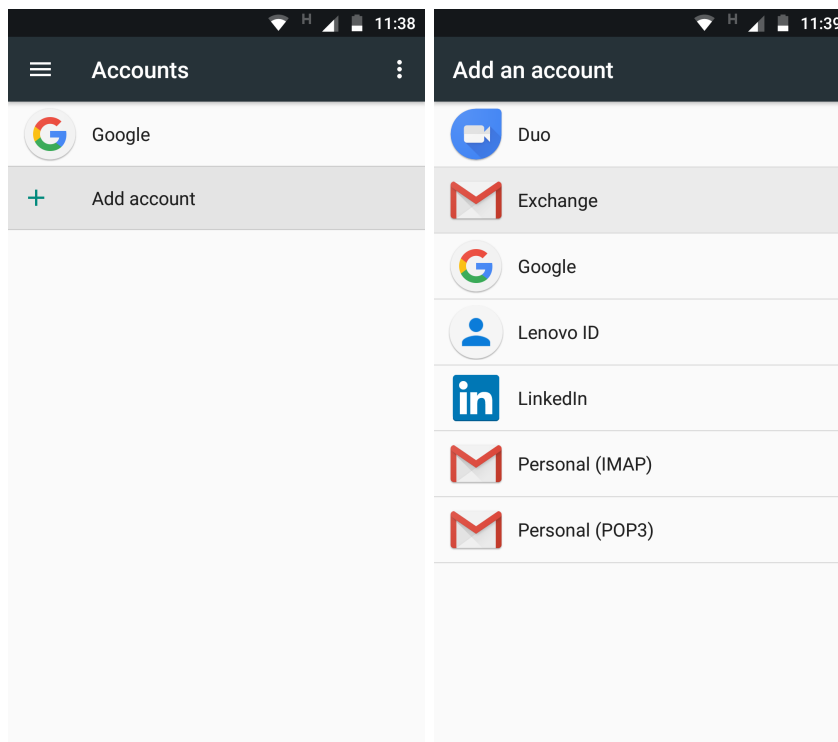
If calendars or task lists are included in this way, reminder settings always apply to the entire user account. If this is shared by multiple users, the reminders will also appear for all users.

35. Chapter - ActiveSync with Android Devices

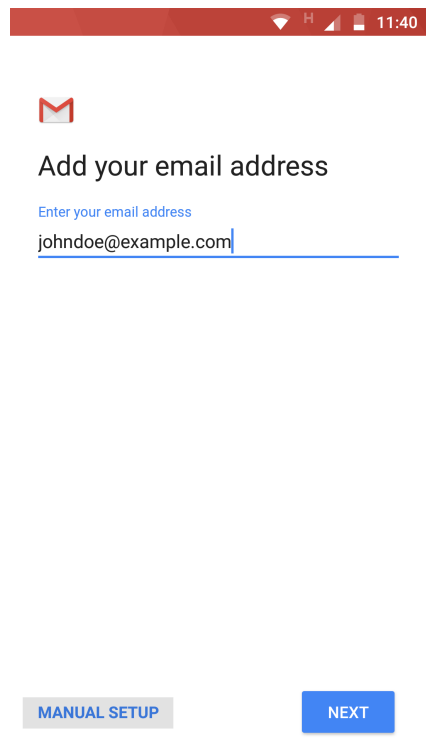
Before configuring the device, the Intra2net system must be prepared for connection. Perform the steps described in Section 34.2, „Server Settings“.

The configuration procedure of the device is as follows:


1. First of all, make sure that your login details remain confidential. The necessary steps are described in Section 51.1, „Preparing the Device“.
2. On the Android device, open "Settings", navigate to the "Accounts" tab, and select "Add an account". The type of account to be added is "Exchange".



3. Enter your email address. Then choose "Manual Setup".



11:40



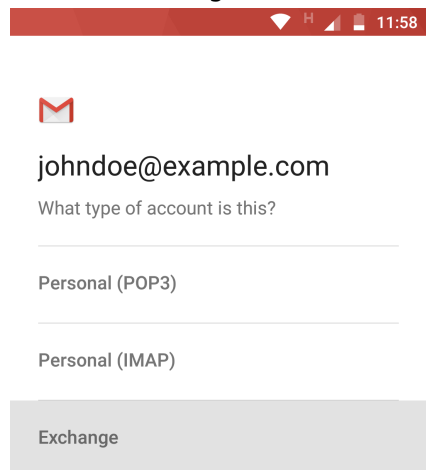
Add your email address

[Enter your email address](#)


johndoe@example.com

MANUAL SETUP NEXT

4. Choose "Exchange" as the account type.



11:58



johndoe@example.com

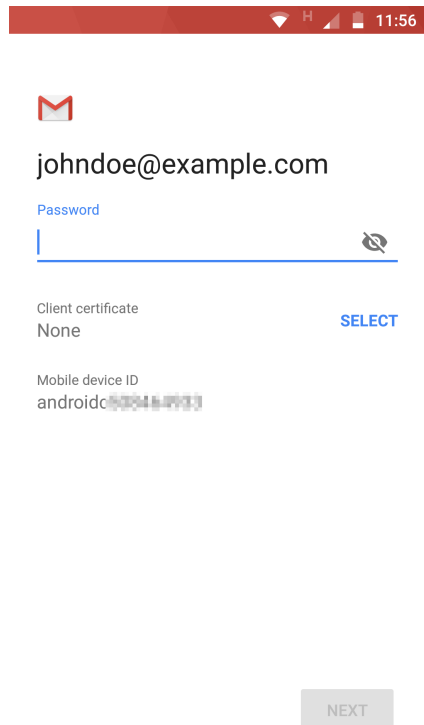
What type of account is this?

Personal (POP3)


Personal (IMAP)

Exchange

5. Enter the user's password on the Intra2net system.



11:56



johndoe@example.com

Password

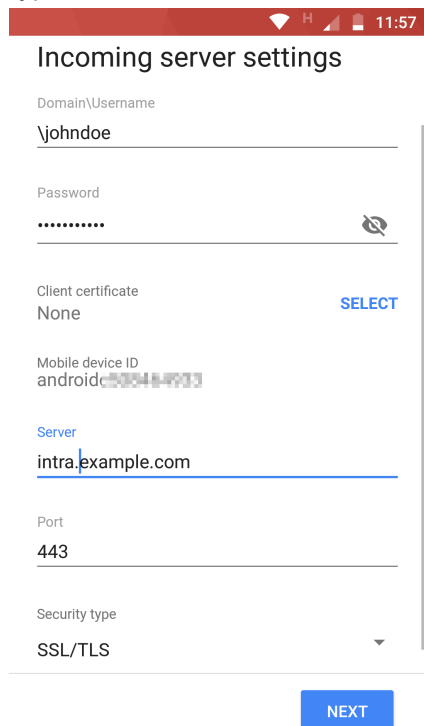
Client certificate
None [SELECT](#)

Mobile device ID
android:505464903

NEXT

6. Fill in under "Domain/Username" a \ (Backslash) directly followed by the username on the Intra2net system. Usernames on the Intra2net system consist exclusively of lower case letters, so enter only lower case letters here.

Enter the external DNS name of the Intra2net system in the "Server" field. The security type must be "SSL/TLS".



11:57

Incoming server settings

Domain/Username
\\johndoe

Password
.....

Client certificate
None [SELECT](#)

Mobile device ID
android:505464903

Server
intra.example.com

Port
443

Security type
SSL/TLS

NEXT

7. No message about a certificate error should appear. If one appears, stop here and check the steps described in Section 34.2, „Server Settings“.

8. Next, you configure how often data is to be synchronized between server and mobile device.

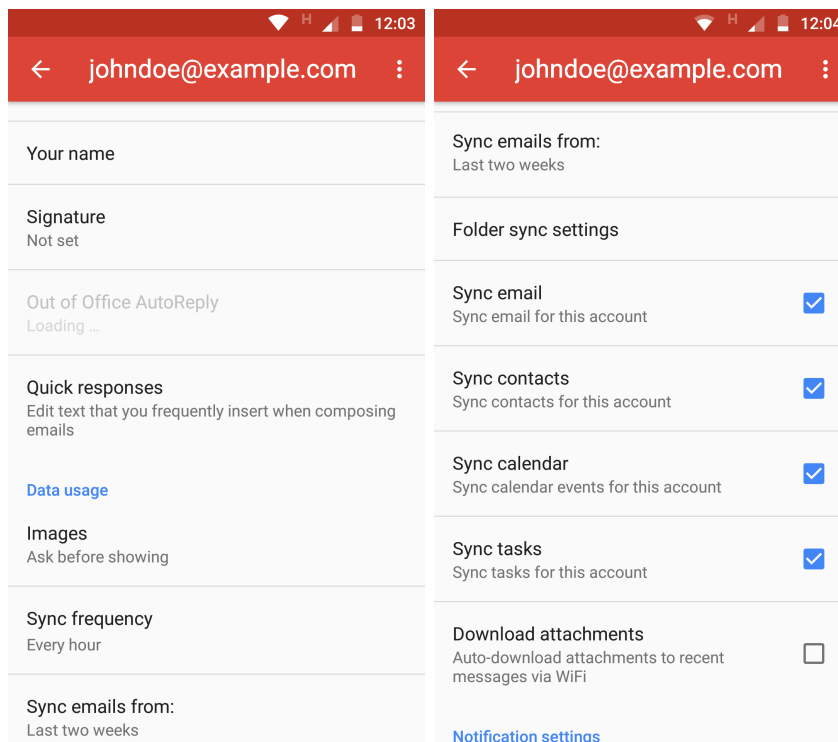


Tip

We recommend setting the synchronize frequency to 15 minutes or longer and advise against using "Push". In push mode, a wireless connection is constantly active and the device cannot make use of energy saving modes. This significantly reduces the battery life. In addition, we have observed transfer errors in some devices using push mode, which resulted in duplication of emails and appointments.

In addition, it can be configured that only the emails and calendar entries of a certain period of time are synchronized. This saves data traffic volume, storage space on the mobile device and prevents slowing applications running on the mobile device.

In the lower part of the dialogue it is possible to select which types of items should be synchronized.



The new account is now available for selection in email, contacts and appointments/tasks in the appropriate applications. For new items to be added, choose between different accounts set up on the device.

All relevant applications also offer the facility to manually trigger data synchronization. This option is usually preferable to using a very short synchronization interval.

36. Chapter - ActiveSync with Apple iOS Devices

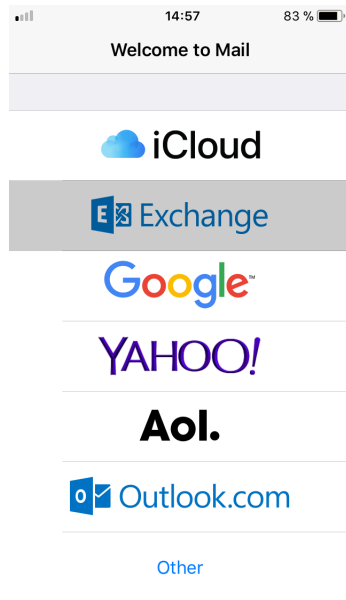
Before configuring the device, the Intra2net system must be prepared for connection. Perform the steps described in Section 34.2, „Server Settings“.

The configuration procedure of the device is as follows:

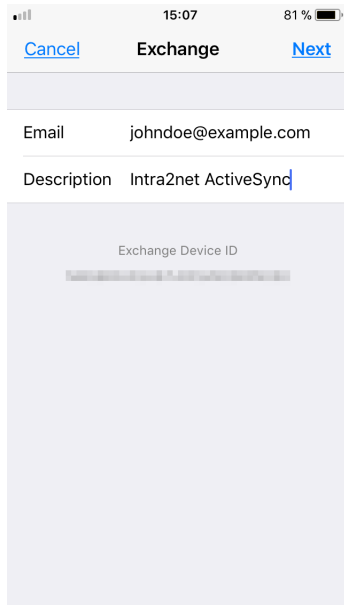
1. Open "Settings", Submenu "Accounts & Passwords" and select "Add Account".



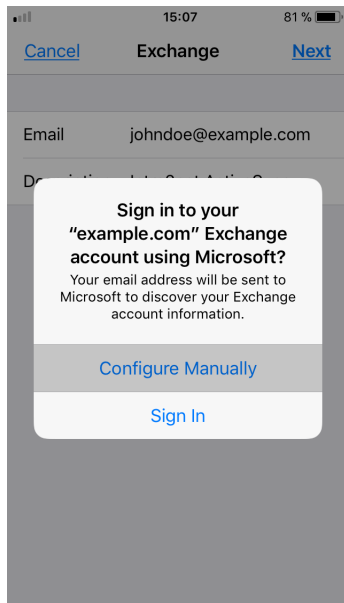
2. The type of account to be added is "Exchange".



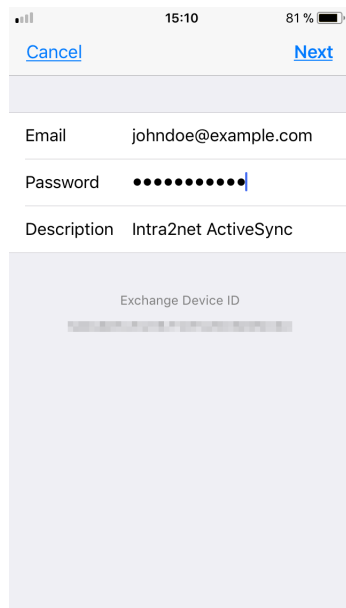
3. Enter the email address and a name of the account for the iOS device.



4. Select "Configure Manually".



5. Enter the user account password for the Intra2net system.



15:10 81 %

[Cancel](#) [Next](#)

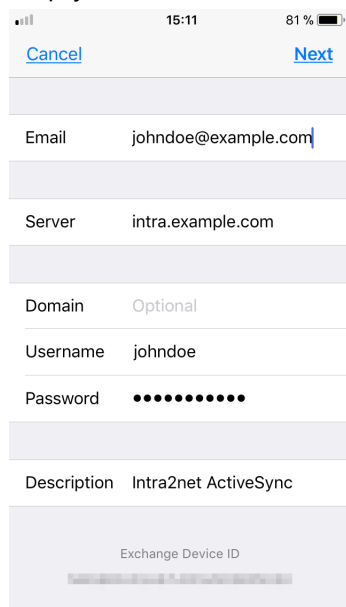
Email johndoe@example.com

Password ●●●●●●●●

Description Intra2net ActiveSync

Exchange Device ID

6. Enter the external DNS name of the Intra2net system in the "Server" field. Enter the user name (login) of the account on the Intra2net system. Leave the field "Domain" empty.



15:11 81 %

[Cancel](#) [Next](#)

Email johndoe@example.com

Server intra.example.com

Domain Optional

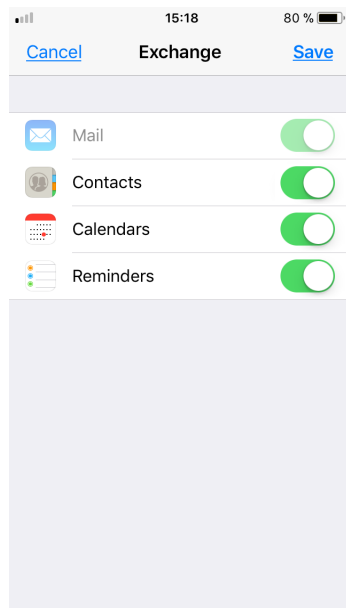
Username johndoe

Password ●●●●●●●●

Description Intra2net ActiveSync

Exchange Device ID

7. No security warning or certificate error message should appear. If one appears, stop here and check the steps described in Section 34.2, „Server Settings“.
8. Select which types of data you want to synchronize.

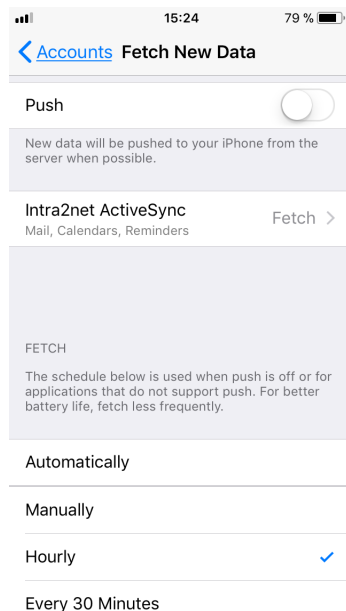


9. Finally, open the "Fetch New Data" menu and set how often the data should be synchronized.



Tip

We recommend setting the synchronize frequency to 15 minutes or longer and advise against using "Push". In push mode, a wireless connection is constantly active and the device cannot make use of energy saving modes. This significantly reduces the battery life.



The new account is now available for selection in email, contacts and appointments/tasks in the appropriate applications. For new items to be added, choose between different accounts set up on the device.

It is also normally possible to manually trigger data synchronization. This option is usually preferable to using a very short synchronization interval.

37. Chapter - Reference Information



Hint

The information in this chapter is only valid for Webgroupware and Activesync. Information about the Intra2net Groupware Client can be found in 30. Chapter, „Reference Information“.

The Webgroupware and the ActiveSync interface do not support all fields that can be sent by ActiveSync or the Intra2net Groupware Client. Therefore, the data stored in these fields cannot be displayed, used or edited in the webgroupware or via ActiveSync. In addition, the data stored in it can be lost when you change other fields of the same object.

The following is not supported by the Webgroupware and Activesync:

- Pictures of contacts
- Appointment and task series with the recurrence type "work week" and recurrence type monthly when the last day of the week is specified (for example, "last Monday of each month").
- Exceptions in series of appointments and tasks in which more is changed than the complete omission of an element of the series
- Color representation of categories: Categories are only displayed as text
- Processing incoming task assignments by email
- Contact Groups
- Reminders and tagging for emails
- Attach other elements or files to groupware items (not emails, attachments are of course possible here)
- Linking of groupware objects to each other, e.g. with contacts
- Groupware objects marked as private are no longer displayed to the owner in some special cases
- Telephone numbers in the "Company Main Phone" field. Use "Business phone" instead.

For Activesync, the restriction still applies that only one folder is transferred for each groupware object type (appointment, address, task,...). This restriction can be mitigated by setting up additional accounts, see Section 34.3.4, „Synchronize Multiple Calendars or Contact Lists“.

Further information will be available soon. If you need more detailed information to support individual data types or functions, please contact the Intra2net sales department.

Part 5. Firewall

38. Chapter - Selecting Firewall Rulesets

The firewall of the Intra2net system consists of individual, separate firewall rulesets. These rulesets can be assigned to individual objects such as clients or networks. When creating a new object, an existing firewall ruleset can be applied again. Additionally, the most important, basic rules are supplied pre-installed. This considerably simplifies configuration.

38.1. Rulesets on LAN

Each client, IP range, routing, network and VPN can be assigned one firewall ruleset using the respective menu (e.g. "Network > Intranet > Clients").

Since clients or IP ranges are always located in a network or routing at the same time, 2 firewall rulesets are assigned to them. In this case, only the rule assigned to the client or IP range is valid, the rule assigned to the network or routing is not used. These only apply to IPs from the network for which no client or IP range is configured.



Caution

The source of a packet alone determines which firewall ruleset is used.

Therefore, a ruleset for a client contains rules for accessing other local networks as well as the Internet, VPNs, etc. Anything that comes from a client is checked against the ruleset assigned to the client.

In a group of rights (e.g. for a client) you will not only find the firewall ruleset but also settings for the proxy profile, as well as DNS and email relaying. The firewall ruleset has priority over these settings. This means that only if the firewall ruleset allows access to the proxy, the proxy profile configuration will apply.

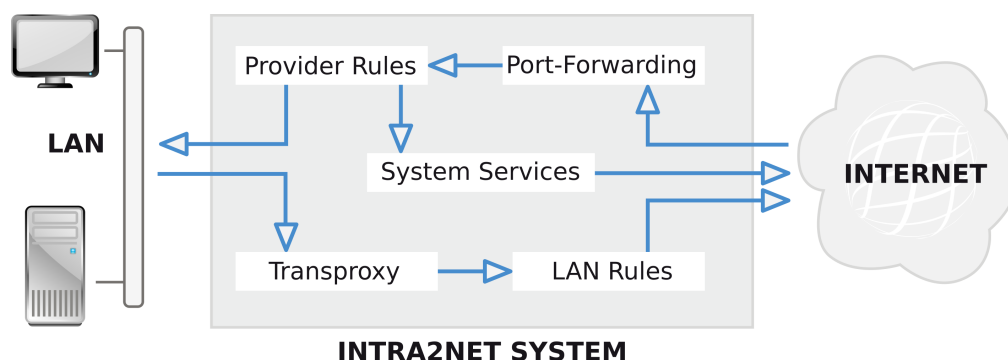
38.2. Rulesets for the Internet

Under "Network > Provider > Profiles : Firewall", a firewall ruleset is assigned to each provider. The firewall ruleset assigned to the active Internet provider decides which packets from the Internet may and may not be allowed onto the local networks.

Again, only the firewall ruleset assigned to the source of the packets (i.e. Internet and thus provider) decides whether the packets are allowed through or not.

38.3. Packet Routes Through the Firewall

38.3.1. Packet Routes on the LAN and Internet



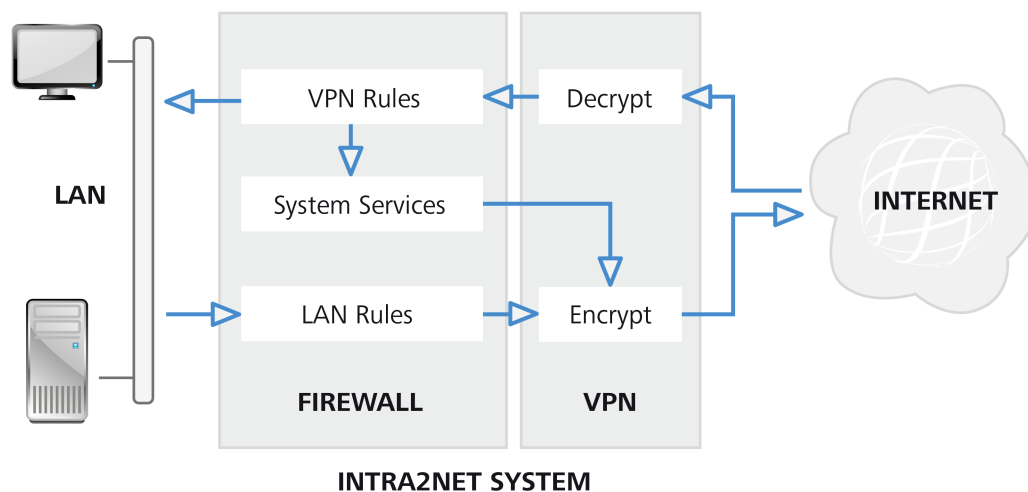
The route of the packets can be summarized quite easily:

- The rulesets used always depend on the source of the packets.
- Rules that modify packets are always performed first. This includes NAT, port forwarding, static NAT and transparent proxy. All following rules will only see the already modified packets.
- The connections of the Intra2net system itself cannot be restricted.

38.3.2. Packet Routes for VPN Connections

With VPNs, the packets are checked by the firewall before encryption and after decryption.

Packets coming from the VPN are checked after decryption by the ruleset assigned to the VPN. Only this ruleset decides whether the packets are allowed through.



39. Chapter - Firewall Profile

Easy Rulesets

There are three different classes of firewall rulesets: Simple firewall profiles, full rulesets and provider profiles. Rules of all three types are managed together in "Network > Firewall > Rules".

For standard scenarios, no complex firewall rulesets are required on the Intra2net system, but the most important settings can be made easily using the firewall profiles.

If one of these firewall profiles is no longer sufficient for its intended purpose, it can be converted to a complete ruleset by clicking "Convert" and then extended accordingly.

39.1. General Basic LAN Rules

All firewall computer profiles are based on the basic LAN or basic LAN and local area networks ruleset. These contain basic rights for access to the Intra2net system itself, but do not permit any access to the Internet or to emails.

"Basic LAN" allows access to the following services of the Intra2net system:

- DNS
- Web Interface via HTTPS
- Windows Share (SMB) for backups
- ICMP Basic Services (e.g. Ping)
- SSH for access to the system console of the Intra2net system

"Basic LAN and local networks" also allows full access to all other local networks and routings connected to the Intra2net system. Which of the two rulesets "Basic LAN" or "Basic LAN and local networks" is used is determined by the setting "Allow access to local networks".

"Basic LAN and local networks" or the "Allow access to local networks" option should therefore never be used for de-militarized zones (DMZ).

39.2. Client Profiles

The "Access right" option allows you to set basic access rights. "No Access" corresponds to the right of "Basic LAN" or "Basic LAN and Local Networks". In addition to "Basic LAN", "Email only" allows access via the email protocols SMTP, POP3(S) and IMAP(S). In addition to "Basic LAN", "VPN only" allows access to VPN networks connected via the Intra2net system. Access to these VPN networks is then possible with all protocols.

The "Proxy webaccess" option decides how the HTTP and FTP proxy on the Intra2net system can be used. "Free access" allows access to the proxy port, but does not force it. Only when the user has entered the proxy in the browser is it used. "Force proxy use" ensures that direct access to HTTP servers on the Internet is prevented. The user is therefore obliged to enter the proxy in the browser. "Transparent proxy" redirects all ac-

cesses to HTTP servers invisibly to the proxy of the Intra2net system. This means that there is no need to reconfigure any specific settings on the browser.

Using the "Additional services" option, additional ports (such as HBCI) can be enabled for Internet access.

The option "Allow mail transfer only via the Intra2net system" ensures that the email protocols are limited to the Intra2net system. This prevents email programs from accessing mail servers directly on the Internet and thus ensures that all emails must be sent via the Intra2net system. This is useful, for example, to ensure that the email virus scanner or an archiving function cannot be bypassed.

39.3. Provider profile

Provider profiles have a very simple structure. Each of the services that are typically accessed from outside the Intra2net system can be enabled separately.

The provider profiles only cover access to the Intra2net system itself and port forwarding. If a de-militarized zone (DMZ) is used, a full ruleset must be configured.

40. Chapter - Full Rulesets

Full firewall rulesets allow full functionality of the firewall, and therefore can be more complicated to configure than the firewall profiles.

40.1. Components

To avoid overloading the firewall configuration interface with IP addresses and port numbers, we combine IPs, networks etc. into network groups or protocols, and port numbers and port ranges into services. These are compiled centrally and can then be used in all firewall rules. In addition to this, the most important services are already pre-defined in the basic configuration.

40.1.1. Services

Under "Network > Firewall > Services", protocols and port numbers can be combined under a service name. This makes them usable in firewall rules.

A service consists of freely entered ports and protocols ("Custom service") as well as of other, pre-configured services ("Used services"). This means that services can be composed of multiple other services. This is particularly useful if a protocol consists of multiple sub-protocols. A good example of this is FTP, which consists of the FTP control connection and the FTP data connection.

With the protocols TCP and UDP, both source and target ports can be specified. Both are not limited to individual ports, but can also configure complete port ranges (e.g. target ports 5000 to 5050 for remote maintenance of the Intra2net support).



Hint

Please note that with TCP, only the target ports are typically defined and the source port can be freely selected by the client. Therefore, normally only the target port is entered in the Intra2net system.

40.1.2. Netgroups

Under "Network > Firewall > Netgroups" IPs, IP networks and IP ranges can be combined as a netgroup. This makes them usable in firewall rules. All clients, network areas, routings etc. which you have entered in the Intra2net system in the corresponding menus, are directly available as network objects in the firewall and do not have to be configured as a netgroup first.

As with services, a netgroup can contain other netgroups.

Individual IPs are entered under "Custom Client/subnet" with the netmask 255.255.255.255. If you would like to configure a network range that can also be represented as an IP network (e.g. IPs from 192.168.1.0 to 192.168.1.255), it is recommended to enter this as an IP network with the appropriate netmask (in the example IP 192.168.1.0 with netmask 255.255.255.0). This leads internally to more streamlined and faster firewall rules.

40.1.3. Netgroups with DNS hostnames

Netgroups can not only contain IP-based objects, as described in the previous section, but also DNS hostnames.

The Intra2net system constantly updates the DNS hostnames entered automatically in the background and adjusts the firewall ruleset if necessary. If a DNS hostname resolves to several IP addresses, all of them added to the netgroup.

In the "Information > System > DNS netgroups" menu, you can see an overview of all IP addresses currently resolved for the DNS hostnames. If required, a DNS hostname can be manually re-resolved via the "Renew" link.

Some service providers use groups of constantly rotating IP addresses, e.g. for load balancing. To handle these, the Intra2net system keeps an IP address in the list for 24 hours longer, even if it is currently no longer included in the DNS resolution. This function is called *Extended Hold* and the affected IP addresses are marked with "(EH)" in the overview.

40.1.4. Automatic Objects

The Intra2net system combines known objects into automatic objects. Some of these objects also depend on the current state, e.g. the current Internet IP. These can be used directly in firewall rules and do not require any further configuration.

List of Automatic Objects:

Object	Description
Clients and ranges	All clients and ranges defined in the Intra2net system. For DHCP ranges, this only affects the assigned IPs.
DHCP Ranges	All DHCP ranges (including unoccupied IPs).
Remote VPN networks	The networks behind the currently active VPN peers. For "LAN to Host" connections, this is the VPN peer station itself.
IP of the system in the LAN	IP addresses of the Intra2net system in all its networks of the type "LAN with NAT" and "LAN without NAT".
All Local Networks	All networks ("LAN with NAT" and "LAN without NAT") and routings.
Broadcast IPs of all local networks	Broadcast IPs of all local networks.
Current Internet IP	Current IP address of the Intra2net system on the Internet. If the system is offline, this condition no longer applies.
Internet	Everything outside the local networks and VPNs.

40.2. Rulesets

40.2.1. Default Settings

For each ruleset, specify whether it can be used for local area networks and VPNs or for access via the Internet (provider). This distinction is an additional protection, so that you cannot accidentally define a rule with full access for connections from the Internet, for example.

Almost all protocols expect a response to a sent IP packet. With TCP, for example, data can only flow once the peer has confirmed the connection. Therefore, for almost all protocols not only the outward movement of the packets in the firewall must be allowed, but also the way back for the reply packets must be opened.

So that every rule does not have to be entered in two or more places, the Intra2net system can automatically assign each reply packet to the corresponding connection (Stateful Firewall). The "Automatic response rule" option lets these response packets pass through the firewall automatically. Only in very few exceptions does it make sense to do without the automatic response rule.

40.2.2. Passing Through the Ruleset

A ruleset is processed from top to bottom. If all conditions of a rule apply ("Match"), the action of the rule is executed. For most actions, the run for this packet is completed, later rules have no effect (the first rule applies).

If no rule applies to a ruleset, the packet is rejected (implicit deny). This is visualized by the unchangeable rule at the end of the ruleset. If a packet is forwarded to another ruleset and no rule applies there, the packet is referred back to the original ruleset. The "Deny" rule displayed in the forwarded ruleset does not apply to the return step.

40.2.3. Linking Rule Criteria

If different criteria of a rule are activated (e.g. source, service and connection status), all of these criteria must apply to the packet to execute the action. If no criteria are entered for a rule, the action is always executed.

Multiple options can be set for the criteria "source", "destination" and "service". It is sufficient if one of them applies (logical OR linkage).

Example:



Source	Service	Applies to
Client1	Ping	No
Client1	HTTP	Yes
Client1	FTP	Yes
Client2	HTTP	Yes
Client2	FTP	Yes

Objects can also be inserted into a rule with "Not". The action is executed if this object does not appear in the packet. If multiple objects are set with "Not", none of them may occur (and-link).

If objects with "Not" and normal objects in a condition are used together, at least one of the normal objects must apply (or link), but none of the objects with "Not" (and link).

Example:



Source	Applies to
Client1	No
Client2	No
Client3	Yes
Clients from the Internet	No

40.2.4. The Actions

The Actions at a Glance:

Action	Description
Accept	Let packet through.
Deny	Discard packet, the sender does not receive an explicit error message (must wait for timeout).
Reject	Reject packet, send an error message to the sender (ICMP Port unreachable).
Nothing	Do nothing, packet goes through the other rules. The log option is still executed.
Forward to	Forwarding to another ruleset; forwarding is only possible to complete rulesets of the same type.
Return	Return to original ruleset. If no forwarding was used, this is equivalent to "Deny".
Transproxy	Redirection to the HTTP proxy of the Intra2net system (only for type "LAN and VPN"). Rules for the transparent proxy must always be at the beginning of a ruleset.

We recommend using "Reject" to block packets from the LAN. The advantage compared to "Deny" is that the user immediately receives an error message and does not have to wait for a timeout.

For packets from the Internet (in a provider rule) we recommend "Deny", because the immediate feedback from "Reject" accelerates and simplifies a portscan from the Internet considerably.

40.2.5. Extra Options

The "Extra" tab contains further information.

40.2.5.1. Time Profiles

Time profiles can be defined under Network > Firewall > Times. These time profiles can then be added as a condition for each rule. The condition only applies within the defined time profile; only then can the action be executed.

40.2.5.2. Logging

Logging is not a condition, but rather like another action: If logging is active and all conditions apply, then the packet data plus the logging text specified in the rules is logged in the messages log file.

40.2.5.3. Limitation

Limits can be configured separately for action and logging. A limit for an action means that the action will not be executed if the limit is exceeded. A limitation for the log means that the packet is not logged if the limit is exceeded.

It is possible to limit the number of packets per time unit. The limit can be exceeded at short notice via the peak value. If the peak value was used in a time unit, it is only available again in the following time units if the limit was not used in a time unit.

40.2.5.4. Packet Size

A condition that applies when the packet has a size within the specified range.

40.2.5.5. Connection Status

The Intra2net system uses a stateful firewall. This means that it assigns each packet to a connection and can remember the state for each of these connections. This data can be accessed using the connection status condition.

New	First packet that establishes a new connection
Invalid	The packet either requires an already present connection that does not exist, or does not match an existing connection status
Established	The packet belongs to an existing connection
Belongs to	The connection of this packet logically belongs to another, already existing connection (e.g. packets from ftp-data belong to ftp-control)
Port Forwarding	The connection of the packet is forwarded via port forwarding
Static NAT	The connection of the packet is forwarded via static NAT

40.2.5.6. TCP Flags

This condition is normally not needed, the connection status offers more possibilities.

40.2.6. Special Features of Provider Rulesets

Some servers (especially public FTP servers) try to determine user data using the ident protocol when establishing a connection. To do this, the server establishes a connection to TCP port 113 of the calling client. Because of NAT, this call normally ends up in the Intra2net system and is blocked by the provider rule.

However, most of these servers are waiting for a timeout or an error message from the ident before they allow a login. Therefore, it has proven to be useful to insert a "reject" for the ident protocol into each provider rule.

41. Chapter - Additional Functions

41.1. Checking MAC Addresses

Under "Network > Firewall > Settings" the MAC address check can be activated. The MAC addresses of individual clients are entered under "Network > Intranet > Clients". Then every incoming packet is checked to see if it really comes from the MAC belonging to the IP. It also ensures that a MAC uses only the stored IP address.

If a client does not have a MAC, the MAC check ignores the IP address of that client. Also with IP ranges, no MACs can be stored or checked.

If IP and MAC do not match, any access is denied and logged with the identifier "BADMAC" in the messages log file.

41.2. Preventing LAN spoofing

In all instances, the Intra2net system ensures that local IP addresses can only access the Intra2net system using the appropriate LAN interfaces. If a packet with a source address comes in from one of the local networks via the Internet, it is rejected immediately.

The "Prevent spoofing of IP addresses in the local network" option can also be used to ensure that, in the case of multiple routings in the local network, the packets are not allowed to arrive at the Intra2net system via any LAN interfaces, but only via those selected using the gateway routing IP.

41.3. Blocking IPs After Too Many Login Errors

If this option is activated, the Intra2net system counts the login errors of each IP on all available protocols. If the threshold of 10 login errors is exceeded within 5 minutes, the IP will be blocked for 5 minutes for every further attempt to access any services. If multiple attempts are made, the blocking time is added up.

The access attempts of blocked IPs are logged with the identifier "BLOCKED_IP" in the messages log file.

41.4. Firewall Emergency Mode

In the event that you lock yourself out with the firewall: In the command line menu (see Section 6.4, „Firewall Emergency Mode“) the "Firewall emergency mode" can be activated. This allows access to the local network and browsing the Internet. The emergency mode is automatically deactivated the next time the firewall is changed.

If the emergency mode is active, a message is displayed on the main page.

42. Chapter - Case Studies and Examples

42.1. Example 1: Extending a Simple Client Profile

The following simple client profile is provided:

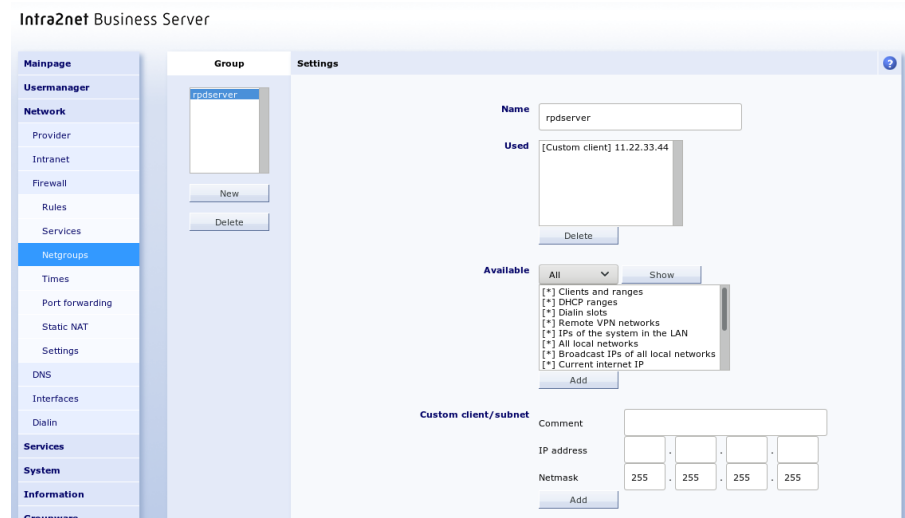
- Access authorisation: WWW/FTP/E-Mail/News
- Access to local networks not allowed
- no additional services allowed
- Web access via proxy: Forced Proxy
- Email transfer only via Intra2net system: active

Create this client profile. Then convert it into a complete firewall ruleset and add a rule that allows access to a server on the Internet with IP 11.22.33.44 via RDP protocol.

Create a client with the name "R10" and the IP 192.168.1.10 and assign this firewall ruleset to it.

42.1.1. Sample Solution

Creating a network group for the client 11.22.33.44 under Network > Firewall > Netgroups



Firewall Ruleset

Name

Usable for LAN, dialin and VPN

Automatic answer rule ☒

#	Source	Destination	Service	Action	Comment	Extra
01	all	IPs of the system in the LAN, Current internet IP	ntp, http-proxy, email, hylafax	Accept	Intranator services	↑ ↓ 🗑
02	all	Internet	http, nntp, https, nntp, ping, ftp	Accept	Internet	↑ ↓ 🗑
03	all	Remote VPN networks	all	Accept	Remote VPN networks	↑ ↓ 🗑
04	all	rdpserver	rdp	Accept	RDP on 11.22.33.44	↑ ↓ 🗑
05	all	all	all	Redirect	Basic LAN	↑ ↓ 🗑
	all	all	all	Deny		📄 🛡

Assign the new firewall ruleset to the client R10

Intra2net Business Server

Mainpage

Usermanager

Network

Provider

Intranet

Overview

Clients

Ranges

Import/Export

DHCP

Routing

Firewall

DNS

Interfaces

Dialin

Services

System

Information

Groupware

Client

r10

New

Delete

Settings

Name

Aliases

Comment

IP address

MAC address

Firewall ruleset Example 1

Proxy profile [Free access]

Email relaying allowed ☒

DNS requests for the Internet allowed ☒

42.2. Example 2: Port Forwarding Only Accessible from an External IP

- Set up port forwarding for port 3389 to client R10.
- Configure the firewall to allow port forwarding from a single IP (33.44.55.66) only.
- It should be possible to access HTTPS, SMTP and SMTP submissions, but not to other services, from anywhere.
- Create a firewall ruleset and assign it to the default provider.

42.3. Example 3: Separate Guest Network

The Intra2net system is connected to two local networks, one of which is used for the staff and the other for guests. Staff and guest networks should be strictly separated from each other.

In Detail:

- The employee network uses 192.168.1.0/24, the guest network uses 192.168.5.0/24. Each of the two networks uses a separate interface of the Intra2net system.
- Full access to the Internet from the guest network is permitted. Access to the Intra2net system is only allowed for DNS. Access to the employee network must not be possible under any circumstances.
- The Intra2net system is DHCP server, but only for the guest network. Set up a DHCP pool for the guest network and make sure that guests are assigned the correct firewall ruleset for a DHCP request.

42.3.1. Sample Solution

Intra2net Business Server

The screenshot displays the Intra2net Business Server web interface, specifically the 'Ruleset' and 'Interface' configuration pages.

Ruleset Configuration:

- Name:** Guest
- Usable for:** LAN, dialin and VPN
- Automatic answer rule:** ☒
- Rules Table:**

#	Source	Destination	Service	Action	Comment	Extra
01	all	IPs of the system in the LAN	dns	Accept	DNS on System	⬆ ⬇ ⬇
02	all	Internet	all	Accept	Full access to Internet	⬆ ⬇ ⬇
03	all	all	all	Reject	Reject everything else	⬆ ⬇ ⬇
	all	all	all	Deny		⬆ ⬇ ⬇
- Show IP addresses:** Move rule 01 to position End. Add new rule at position End.
- Queue changes:** [Button]

Interface Configuration:

- Name:** eth2
- Comment:** Guest
- MAC address:** 52:54:00:95:82:85
- Type:** LAN with NAT
- IP address:** 192 . 168 . 5 . 254
- Netmask:** 255 . 255 . 255 . 0
- Rewrite addresses of other networks (NAT):** ☐
- Firewall ruleset:** Guest
- Proxy profile:** [Free access]
- Email relaying allowed:** ☐
- DNS requests for the Internet allowed:** ☒
- Queue changes:** [Button]

Mainpage

- Usermanager
- Network
 - Provider
 - Intranet
 - Overview
 - Clients
 - Ranges
 - Import/Export
 - DHCP**
 - Routing
 - Firewall
 - DNS
 - Interfaces
 - Dialin
- Services
- System

Settings

DHCP active ☒

DNS server 1 . . .

DNS server 2 . . .

WINS server . . .

Different standard gateway . . .

NTP server

Assign IP address for (lease time) 24 hours

Deactivate DHCP server for eth0 (192.168.1.254)

Mainpage

- Usermanager
- Network
 - Provider
 - Intranet
 - Overview
 - Clients
 - Ranges**
 - Import/Export
 - DHCP
 - Routing
 - Firewall
 - DNS
 - Interfaces
 - Dialin
- Services
- System
- Information
- Groupware

Range

DHCP: Guest-Pool

Settings

Name Guest-Pool

Comment

Range from 192 . 168 . 5 . 1

Range to 192 . 168 . 5 . 253

Use as DHCP pool ☒

Firewall ruleset Guest

Proxy profile [Free access]

Email relaying allowed ☐

DNS requests for the Internet allowed ☒

DHCP pool informations

Total IP count	253
Used	0
Free	253
Free IPs	192.168.5.1-192.168.5.253
Used IPs	none

42.4. Example 4: Restricted Access from the VPN

A user should connect to the Intra2net system for remote maintenance of a server from a VPN client. Using this connection, it should only be able to address a specific service on a server.

- The target client for remote maintenance has the name "testserver" and the IP 192.168.1nn. 100.
- Create a new firewall ruleset that only allows access to this server using the HTTP service.
- For addressing, access to the DNS of the Intra2net system is also required. All unauthorized accesses should be rejected with Reject.
- Activate this firewall configuration for an existing VPN dial-up connection.

- Establish the VPN connection and use a web browser to test whether the server can be accessed via HTTP. A test page should be displayed.
- Open the program "zenmap GUI", which is part of the portscanner suite Nmap. To test the firewall ruleset, perform an "Intense Scan" on the target server. Only the HTTP service must be available.
- Perform an "Intense Scan" on the IP of the Intra2net system in the VPN network, i. e. 192.168.1nn. 254. Only the DNS service may be accessible.

42.5. Example 5: Web Server in the DMZ

Scenario:

- A web server is located in a DMZ (De-Militarized Zone) and has an official IP (LAN without NAT). Classic routing is used (see Section 10.7.1, „Classic Routing“).
- The router of the provider has the IP 88.89.90.1, the external IP of the Intra2net system is 88.89.90.2 (network mask 255.255.255.252).
- The DMZ uses the network 88.89.90.4/255.255.255.252 (30 bit network with 4 IPs), the Intra2net system has the IP 88.89.90.5, the web server 88.89.90.6
- Access to TCP ports 80 and 443 (predefined services http and https) of the web server is permitted from the Internet.
- The clients from the LAN have full access to the web server
- The clients from the LAN may only access the Internet via the proxy, email is only possible via the Intra2net system
- The web server only has access to TCP port 3306 of a database server (IP 192.168.1.40) in the LAN.
- The web server may use the DNS and SMTP services of the Intra2net system.

42.5.1. Sample Solution

The clients in the LAN are assigned a firewall profile for clients, see previous task. For full access to the web server it is necessary to check "Access to local networks allowed".

Rules for the DMZ

Name <input type="text" value="DMZ"/>						
Usable for <input type="text" value="LAN, dialin and VPN"/>						
Automatic answer rule <input checked="" type="checkbox"/>						
#	Source	Destination	Service	Action	Comment	Extra
01	all	database	mysql	Accept	Database access	⬆️⬆️⬆️
02	all	IPs of the system in the LAN	smtp, dns	Accept	Email dispatch and DNS	⬆️⬆️⬆️
	all	all		Deny		⬆️⬆️⬆️

Provider Rule

Name

Usable for LAN, dialin and VPN ▼

Automatic answer rule ☒

#	Source	Destination	Service	Action	Comment	Extra
01	all	all	ident	Reject	Reject ident service	⬆️⬆️⬆️
02	all	Current internet IP	icmp-basis	Accept	External services	⬆️⬆️⬆️
03	all	webserver	http, https	Accept	External access to webserver	⬆️⬆️⬆️
	all	all	all	Deny		⬆️⬆️⬆️

Part 6. IPSec VPN

43. Chapter - IPsec Basics

43.1. IPsec

IPsec is a standard for securely connecting local networks over the Internet. IPsec creates virtual private networks (VPN) for this purpose.

IPsec works on the IP level. This means that no changes (such as encryption modules) are required in the programs used. That is why it is also compatible with all TCP/IP based network programs.

IPsec can connect local networks or individual clients with private network addresses over the Internet. For this purpose, the original IP packets are encrypted and packed into new packets. The packets are unpacked, decrypted, checked and forwarded to the recipient.

However, before an encrypted connection can be established, the two connection partners must be sure that the other party is the same person they claim to be (authentication). There are two procedures for this. One is called Pre-Shared Key (PSK) or Shared Secret. Both sides know a common password. The other method uses public-key cryptography.

43.2. Public-Key Cryptography

Public-key cryptography is based on a mathematical technique in which a key pair is generated from a private key and a corresponding public key. Messages encrypted with the public key can only be decrypted with the corresponding private key. If someone only has the public key, they can only encrypt, not decrypt.

As a result, public keys can easily be exchanged on insecure channels (e.g. by email).

The only danger is that an attacker might have swapped the key (man-in-the-middle attack). In order to be absolutely sure, the signatures (also known as fingerprint) of the keys can be compared on the phone, for example, after the key exchange.

43.3. Certificates

Certificates are available as an extension to the concept of public and private keys. In this case, the public key is digitally signed by a certification authority (abbreviated CA), digitally. For larger systems, this enables a remote system to use the digital signature to determine whether a key is valid without the key itself being installed beforehand.

For the Intra2net system, such a certification body generally has few advantages, but the Intra2net system consistently uses the certificate standard X.509. This standard has become established in practice instead of simple public/private key pairs.

In order to simplify the operation, the Intra2net system normally generates self-signed certificates, where the holder (called a subject) is also the certificate issuer. Therefore, no additional steps for the use of certificates are necessary. Of course however, external certification bodies can also be used.

43.4. IPsec connections

An IPsec connection is established in two phases using the Internet Key Exchange (IKE) protocol.

Phase 1: First, a secure connection is established (called ISAKMP SA or IKE SA). This connection is established via UDP port 500. If the system detects that one side is behind a NAT router, it switches to UDP port 4500. There are two connection setup modes: Main Mode and Aggressive Mode. Aggressive mode speeds up the connection setup by a few tenths of a second, but is easier to crack. The Intra2net system therefore only supports the more secure Main Mode.

Phase 2: The previously established secure connection is now used to negotiate the actual connection data and session keys (Quick Mode). If this is successful, a IPSec SA is configured and can then be used to transmit encrypted data.

For security reasons, both phases of the connection have a limited service life and are therefore updated regularly.

For security reasons, and to simplify routing, each side of the connection verifies that only the packets coming through the connection are those that were previously configured. It is therefore important that identical values for the start and destination network of a tunnel are given on both sides.

In order to be able to configure security policies very narrowly, it is possible to establish any number of different IPSec connections between two clients.

43.5. Algorithms

Both sides agree on the cryptographic algorithms to be used for encryption and data signing. The algorithms are separately adjustable for each phase. In the Intra2net system, encryption profiles with algorithms can be configured in the Services > VPN > Encryption menu.

An encryption method consists of an algorithm for encryption, for hashing (signature) and a Diffie Hellman group for establishing a secure connection. Most algorithms are offered in different lengths. The length is given in bits and the algorithm is stronger the more bits are used. However, the number of bits also increases the required amount of processing.

A list of possible methods is configured for both phases. This list is offered in the set order of the peer, which then uses the uppermost method it supports.

The use of Perfect Forward Secrecy (PFS) in phase 2 is also configured on the Intra2net system using the encryption profiles. If a PFS group is specified on the Intra2net system, it is used when establishing a connection. If the other side establishes the connection, the Intra2net system accepts the configured set and any stronger groups. If the PFS group is set to `NO`, connections are established without PFS. If the other side establishes the connection, connections with and without PFS are accepted.

From a contemporary point of view, all offered algorithms offer sufficient strength. The Intra2net system does not even offer any more proposed algorithms like simple DES with 64 bit. However, some possible vulnerabilities of MD5 and SHA have been discussed recently in cryptographic research. We therefore recommend to switch to one of the stronger SHA2 variants (256,384 and 512 bit) as soon as possible.

43.6. Limitations

During the development of IPSec, it was a prerequisite that no information be sent unencrypted or to unauthorized peers. Unfortunately, this also introduces some limitations associated with dynamic IP addresses:

All information is transmitted in encrypted form, including the identification of a station. Since dynamic IPs cannot decide which key to use for decryption based on the IP address or the identifier, all of these peers must use the same key.

Fortunately, this restriction only applies to the pre-shared key procedure; when using public key procedures, each peer can have its own key. By separating public and private keys, this is possible without endangering data. We therefore recommend that you only use the Public Key method.

43.7. Compatibility with Other IPSec Peers

IPSec is standardized and the Intra2net system can establish connections with all standard compliant peers. However, the IPSec standard allows a wide selection of functions, some of which have to be configured or implemented identically on both sides. Therefore, we cannot guarantee overall compatibility.

Many basic devices (e.g. small routers) only support authentication with pre-shared keys. Due to the limitations described in the previous section, we can only advise doing so if both sides have static IP addresses.

If no static IP addresses are available, a router that supports Public Key should be used. The configuration of some of these routers is described in the following chapters.

44. Chapter - Key Management

For public-key encryption procedures, secret keys must be generated on each side before the connection is established and the corresponding public keys must be exchanged with the peer.

For this purpose, key management is available on the Intra2net system.

44.1. Own Keys

In the menu System > Keys > Own keys you can create your own key pairs from public and private keys.

The keys are created according to the X.509 standard. The majority of IPSec systems support this key type. It has a more complex structure and is used not only for IPSec but also for SSL/TLS (e.g. HTTPS) and the encryption of emails (S/MIME).

The security of the encryption depends, among other things, on the key length in bits. The Intra2net system supports a key length of 1024 to 4096 bits. The longer the key, the more secure the connection is. Some peers may not support all key lengths or might be overloaded by keys that are too long. We recommend using 2048 bits.

Owner data for X.509 keys can be a country code (2 digits), state, city, company name, department name, computer name and email address. Either a computer name or an email address must be entered, the rest of the data is voluntary.



Caution

The owner data of a key must be unique. Therefore, the owner data may only be entered once on this device and on all devices connected via VPN.

For security reasons, the validity period of an X.509 key is limited. After the expiry of the validity period, the key is no longer accepted and must be renewed. Extending the validity is not possible.

To send the public key to the peer, it can be saved to a file with Export certificate.

If multiple VPNs are set up on the Intra2net system, you do not have to create a separate key for each connection: you can use an Own Key for all VPNs. You only need the public key from each of the peers.

44.1.1. Certificate Authorities (CAs)

In order to simplify the operation, the Intra2net system normally generates self-signed certificates, where the holder (Subject) is also the certificate issuer.

If you want to use a CA instead, create a normal key first. You can export a certificate request under the tab CA. This certificate request is signed by the CA and can then be imported back into the Intra2net system as a certificate.

Some VPN peers do not accept self-signed keys, but request keys that have been signed by a CA. To facilitate compatibility with such peers, there is the "Sign key with other key" option.

If you are dealing with such a peer, proceed as follows:

1. Create your own new key. This certificate is only used indirectly for signing, so call it **server-ca** for example.
2. Export this certificate and import it on the other side as a trusted Root CA.
3. Now create your own key on the Intra2net system. This will be used later by the system for the VPN.
4. Use the "Sign key with another key" option to sign this key with the CA key created previously.

44.2. Foreign Keys

In order for the Intra2net system to establish a connection, it must first know the public key of the peer. From the peer, export, send, and import it to the Intra2net system.

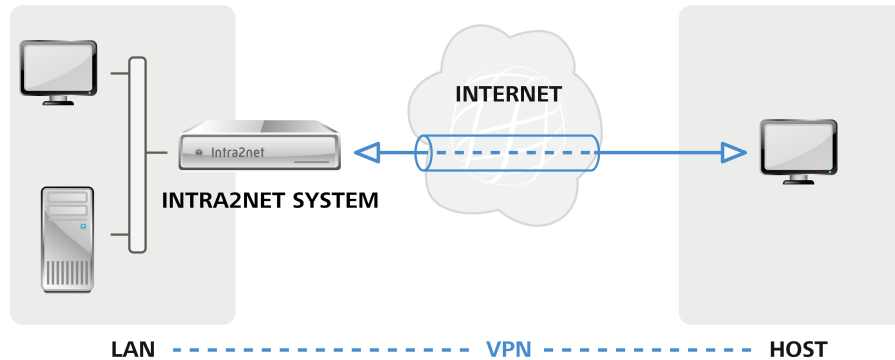
To import, go to the System > Keys > Foreign keys page, input a name and set the key type. Now open the key in a text editor, select and copy it to the clipboard. Now you can paste it into the Copy & Paste field.

If you have transferred the keys over the Internet, you can compare the signatures (also called fingerprint) of the keys over the phone. Otherwise, an attacker could have swapped the key undetected, thus subverting the encryption (a *Man-in-the-middle* attack). For compatibility reasons, the Intra2net system supports the two most common fingerprint methods, MD5 and SHA1, it is sufficient for comparing one of the two fingerprints.

45. Chapter - Connecting Individual PCs

45.1. Method

To connect a single client to the company network, you can install an IPSec VPN client software on the client and use it to establish a VPN connection.



Such individual clients are usually located behind routers that mask their local network via NAT. With portable devices, the IP in the local network also changes with every change of location or dial-in process. This is not a problem in itself, but VPN clients can't simply use the IP in the current local network for the VPN, but access a pre-defined virtual IP. This is defined in the Intra2net system and on the client once during setup and is valid from then on permanently for this one client.

If the local network in which the client is currently located uses the same IP network as the company network with which you want to establish a VPN connection, the IPs can no longer be uniquely assigned and the connection fails.

For most of the supported clients the Intra2net system can automatically prepare suitable configuration files which only need to be imported into the client. A manual configuration is always possible, too.

45.2. Preparing the configuration on the Intra2net system

45.2.1. Create certificate

The Intra2net system requires its own private key with a X.509 certificate to accept VPN connections from clients. This single key can easily be used for all VPN connections. Technically it would be possible to use this key also for SSL/TLS connections. However, certificates used for this purpose typically have a short validity period, which is why a dedicated key is usually the better choice for VPN connections.

Some VPN clients require a CA signed certificate, so we recommend setting up a CA signed certificate as described below from the very beginning.

1. The Intra2net system should be addressable for the VPN clients via a DNS name on the Internet.

If the Intra2net system has a static IP, set up a DNS entry for it in your own official domain. The system can then be reached under a name such as `intra.company.com` or `mail.example.com`. This can normally be set up free of charge and promptly by the web space provider that hosts the domain.

If the Intra2net system is assigned a different IP for each Internet dial-up, a DynDNS service must be set up for addressing. See Section 10.13, „DynDNS“.

A static IP cannot be used directly with some VPN clients without a DNS name. In addition, changing the IP when changing providers is costly. We therefore recommend to use only DNS names and no IPs for addressing.

2. Go to the menu "Network > DNS > Settings" and enter this externally accessible DNS name in the field "Full hostname for connections from the Internet".
3. Go to the menu "System > Keys > Own keys" and create a new, self-signed certificate.
4. Name the key **VPN-CA** or similar and also enter this as computer name. Enter *NOT* the DNS hostname of the Intra2net system as host name. We recommend a validity period of 5 years. Let the key be generated.

The screenshot shows the 'Step 2 of 2: Enter key details' form in the Intra2net Administrator interface. The left sidebar contains a navigation menu with the following items: Mainpage, Usermanager, Network, Services, System, Update, Backup, Diagnosis, Shutdown, ISDN, Web interface, Keys, Own keys (highlighted), Foreign keys, Hardware, Remote support, Queue, Information, and Groupware. The main form area contains the following fields and options:

- Name:** VPN-CA
- Algorithm:** SHA2_256
- Key size:** 2048
- Country code (C):** (empty)
- State (ST):** (empty)
- City (L):** (empty)
- Company/organization (O):** (empty)
- Department (OU):** (empty)
- Computer name (CN):** vpn-ca
- Email (Email):** (empty)
- Additional computer name (subjectAltName):**
 - Type: None
 - Name: (empty)
 - Add button
- Period of validity:** 5 years
- Create key** button

5. Create another new self-signed certificate. Give the key the name "VPN" and then append the external DNS host name of your Intra2net system, e.g. **VPN myintra.dyndns.org**. Enter the external DNS host name under "Computer name (CN)". To prevent ID conflicts with certificates used for TLS, enter for example **VPN** under "Department (OU)". Create the key.

The screenshot shows the 'Step 2 of 2: Enter key details' form in the Intra2net Administrator. The left sidebar contains a navigation menu with categories: Mainpage, Usermanager, Network, Services, System, and Information. Under 'System', 'Keys' is selected, and 'Own keys' is highlighted. The main form area contains the following fields and options:

- Name:** VPN myintra.dyndns.org
- Algorithm:** SHA2_256
- Key size:** 2048
- Country code (C):** (empty)
- State (ST):** (empty)
- City (L):** (empty)
- Company/organization (O):** (empty)
- Department (OU):** VPN
- Computer name (CN):** myintra.dyndns.org
- Email (Email):** (empty)
- Additional computer name (subjectAltName):** Type: None, Name: (empty), Add button
- Period of validity:** 5 years
- Create key:** (button)

6. Change to the tab "CA" for the just created key. Sign this key with the previously generated VPN-CA key.

The screenshot shows the 'CA' tab for a key in the Intra2net Administrator. The left sidebar is the same as in the previous screenshot. The main form area is divided into two tabs: 'Key' and 'CA'. The 'CA' tab is selected. The 'Key' tab shows a list of keys: intra.net.lan, VPN myintra.dyndns.org, and VPN-CA. Below the list are buttons for 'New', 'Delete', and 'Import key'. The 'CA' tab contains the following sections:

- Export:** Export certificate request (text area)
- Copy & paste certificate import:** (text area)
- Copy & paste certificate chain (optional):** (text area)
- Import:** (button)
- Sign key:** Sign key with other key (dropdown menu showing 'VPN-CA'), Sign button

7. Go to the menu "Services > VPN > Settings" and configure the just created and signed server certificate as default.

The screenshot shows the 'Settings' page for VPN connections in the Intra2net Administrator. The left sidebar contains a navigation menu with the following items: Mainpage, Usermanager, Network, Services, Email, Emailfilter, Proxy, Fax, DynDNS, VPN, Connections, Encryption, Settings (highlighted), Time sync, Monitoring, System, Information, and Groupware. The main content area is titled 'Settings' and contains the following configuration options:

- NAT Traversal:** ☒
- Send own certificate unsolicited:** ☐
- Don't send greeting message to client:** ☐
- WINS server for "Assign IP (mode-config)" mode:** [] . [] . [] . []
- Default settings for new connections:**
 - Server certificate:** VPN myintra.dyndns.org
 - Server address:** ☒ Full hostname for connections from the Internet
Current value: myintra.dyndns.org
☐ Custom []
 - Validity period for automatically generated keys:** 5 years
 - Firewall ruleset:** Basis LAN
 - Proxy profile:** [Free access]
 - Encryption profile:** Standard (ohne PFS)
 - Base IP address for single devices:** 192 . 168 . 40 . 1
- Save settings** button

45.2.2. Default settings for new connections

In the menu "Services > VPN > Settings" you can define the default settings for newly created VPN connections. The settings stored there apply to both IPsec and WireGuard connections.

Server certificate and server address must be configured as described in Section 45.2.1, „Create certificate“.

Select a firewall ruleset that allows the needed access to the local network that is desired for VPN clients.

Each VPN client is assigned an individual, virtual IP for the VPN connection. This IP must lie outside of all local networks, routings and other VPN connections. Enter the IP for the first VPN client under "Base IP address for single devices". All other VPN clients will receive consecutive IPs.

45.3. Automatic configuration for clients on the Intra2net system

For most VPN client programs, the Intra2net system can generate ready-to-use configuration files directly from the VPN configuration on the Intra2net system. These files only have to be imported on the client. Proceed as follows:

1. Go to the menu "Services > VPN > Connections" and create a new connection. Select the type "IPsec: Single device".
2. Select the VPN client software. If the type is to be changed later, the connection configuration must be created again.
3. Give the connection a meaningful name, e.g. the name of the employee or device that is to connect. If an employee has several devices that should be able to establish VPN connections, you need a separate connection configuration for each device.

4. Select the local network to which the VPN client should establish the connection.

With most client types you have the choice here whether only the packets into a designated network should run through the VPN tunnel, or whether all connections from the client, to the local networks and the Internet, should run through the VPN tunnel and the Intra2net system. For the latter, select "Local Network" the option "All (0.0.0.0/0.0.0.0)", for all other cases the desired network.

5. For connections from iOS and Android clients, you must select a user account that will be used for XAUTH login. The user must be in a group that has the permission "VPN authentication via XAUTH".
6. Next, enter the password to be used to protect the private key.
7. The connection is then automatically created and the appropriate configuration file is provided for the client. Save this file and transfer it to the client.
8. Import the configuration file on the client. The steps required for this are explained in the following chapters.

If necessary, you can re-export the configuration for the client later using the "Download" link.

The password for the client's private key, which must be entered by most clients each time a connection is established, is not stored on the Intra2net system. If you want to change the password, you simply need to re-export the configuration for the client.

45.4. Manual configuration on the Intra2net system

45.4.1. Prerequisites

First of all, you must ensure that each side has its own key as well as the public key or the certificate of the other. It is recommended to create a separate key for VPNs on each system.

If you set up multiple VPNs on the Intra2net system, you do not have to create a separate key for each connection: you can use a separate key for all VPNs. Of course, only the public key is required from each of the peers.

It is therefore best to create a certificate for VPNs as described in Section 45.2.1, „Create certificate“.

Further details on key management can be found in 44. Chapter, „Key Management“.

A connection configured on the Intra2net system applies to the connection between a client and a network behind the Intra2net system. If you want to access multiple networks behind the Intra2net system from the one client, multiple connections can be easily configured. Make sure that you always use the same combination of keys and certificates for each of these connections.

45.4.2. Default Settings

You can configure VPN connections in the Services > VPN > Connections menu.

To manually configure a new connection, select "IPSec: Site-to-site or custom configuration".

Set the options for the peer. The peer is not usually known on individual clients. Therefore, set it to "Dynamic IP (Road Warrior)".

The encryption algorithms used can be selected using the encryption profile; for details see Section 43.5, „Algorithms“. It is important that the settings for Perfect Forward Secrecy (PSF) are identical on both sides.

Encapsulation controls how the packets for the VPN tunnel are packed. With ESP, encryption and authentication are encapsulated. ESP+AH uses separate encryption and authentication. ESP+AH cannot be routed through NAT, so it is strongly recommended to use ESP for individual clients. This setting must be identical on both sides of the connection.

45.4.3. Authentication

Some client programs offer the option of verifying a user's login and password in addition to authentication using a pre-shared key (PSK) or certificates. This is done using the *Extended Authentication (XAUTH)* protocol. If this is to be used by clients, activate the option "XAUTH server mode".

45.4.4. Configuring the Tunnel

On the "Tunnel" page, you can configure which network is connected to which virtual client IP via this VPN connection.

The "Local network" option selects the network to be connected on the Intra2net system side. With the option "Local networks" select one of the networks directly connected or routed to the Intra2net system.

If you want all client traffic to run through the Intra2net system and thus also benefit from the firewall and proxy server, select the "All (0.0.0.0/0.0.0.0)" option for "Local network".

For "Network on remote side", select "Custom net". Select a previously unused IP that is not located on one of the networks of the Intra2net system or client. This is the virtual IP that you must also enter into the client. Always use 255.255.255.255 as the netmask.

Most VPN clients can have their virtual IP and related DNS servers automatically assigned via the *Mode Config* protocol extension. If your client supports this (e.g. Shrew Soft, NCP or iPhone, see the description of the individual clients), set the "Remote network" option to "Assign IP (mode-config)" and enter the IP that the client should get. As a DNS server, the Intra2net system automatically transmits its own IP.

If "Local network" has been set to a network containing addresses that are not located in local or other VPN networks, the client can access the Internet via the VPN. This applies in particular to the setting "Everything". Since the virtual IP usually originates from a private address range, it can be rewritten to the external address of the Intra2net system (NAT) via the "Rewrite remote addresses for Internet access (NAT)" option. This NAT is only active when accessing the Internet, accesses to the local network continue to be made with the virtual IP.

Further options for address conversion (NAT) are explained in 57. Chapter, „Solving IP Address Conflicts in VPNs Through NAT“.

45.4.5. Rights

This menu defines the rights of the VPN client. This applies to all packets coming from the VPN client. A description of the rights options can be found under Section 8.3, „Access Rights of a Network Object“.

Intra2net Business Server

The screenshot shows the 'Step 4 of 5: Configure rights' configuration page. On the left is a navigation menu with categories: Mainpage, Usermanager, Network, Services, and System. Under 'Services', options include Email, Emailfilter, Proxy, Fax, DynDNS, VPN, Connections (highlighted), Encryption, and Settings. The main content area contains the following settings:

- Firewall ruleset:** A dropdown menu set to 'Vollzugriff'.
- Proxy profile:** A dropdown menu set to '[Free access]'.
- Email relaying allowed:** A checkbox that is checked.
- DNS requests for the Internet allowed:** A checkbox that is checked.
- Save settings:** A button at the bottom right.

45.4.6. Activation

This menu is used to configure when the connection is established and when existing sessions are to be extended. With VPN clients, the Intra2net system cannot initiate the connection itself. Therefore, set the start to "Passive / manual" and use the default values for the remaining options.

Intra2net Business Server

The screenshot shows the 'Step 5 of 5: Select activation type' configuration page. The navigation menu on the left is similar to the previous page, but includes additional options under the 'System' category: Time sync, Monitoring, and System. The main content area contains the following settings:

- Start:** Two radio buttons; 'Passive / manual' is selected, and 'Always' is unselected.
- Connect retries:** A text input field containing the value '3'.
- Lifetime IKE / phase 1:** A text input field containing '480' followed by the unit 'minutes'.
- Lifetime IPSec SA / phase 2:** A text input field containing '60' followed by the unit 'minutes'.
- Offline detection every:** A text input field followed by the unit 'seconds'.
- Save settings:** A button at the bottom right.

46. Chapter - VPN with the NCP Secure Entry Windows Client

The NCP Secure Entry Windows Client is sold through several distributors. A 30-day trial version can be downloaded from the Homepage of NCP [<https://www.ncp-e.com>].

46.1. Import

Prepare the Intra2net system for a connection with VPN clients first as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that the complete configuration for the client can be generated by the Intra2net system as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“.

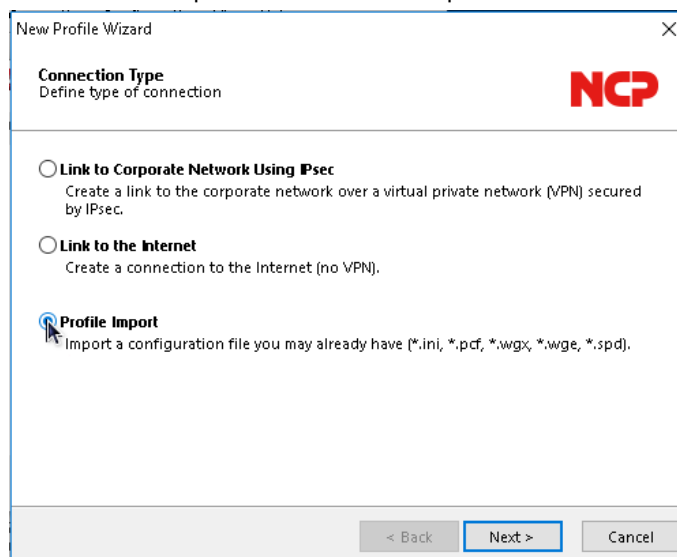
Transfer the generated configuration file to the client PC, e.g. via USB stick or a remote maintenance program. To simplify the installation, the ZIP file contains a batch file and a PowerShell script. Since these are blocked by many email filters, we recommend not to send the file by email.

Then proceed as follows on the client PC to import the configuration:

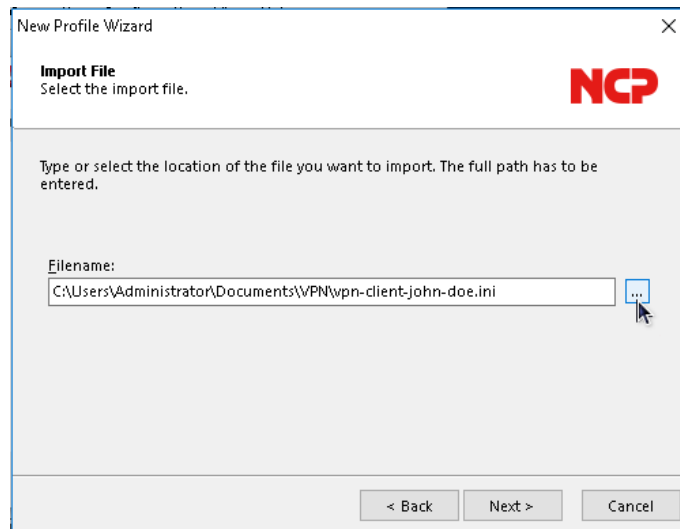
1. The configuration consists of several individual files and is transferred packed as a ZIP file. Open the ZIP file in Windows Explorer and extract all contained files into a new directory.
2. The unzipped files contain the batch file `install-ncp-certs.bat`. Start it with a double click to install the certificates.

This will copy the certificate files to subdirectories of `C:\ProgramData\NCP\Secure-Client`, the private key for the client to `certs`, the public key of the Intra2net system to `cacerts`.

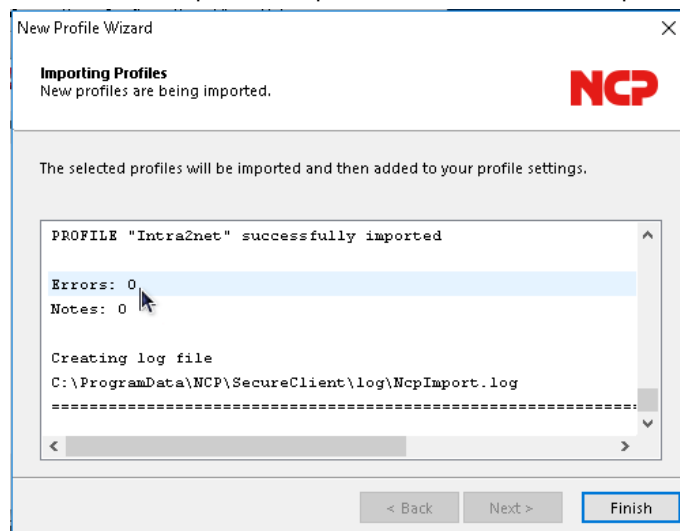
3. Start the NCP Secure Entry Client and open the menu "Configuration > Profiles".
4. Click "Add / Import" and "Profile Import".



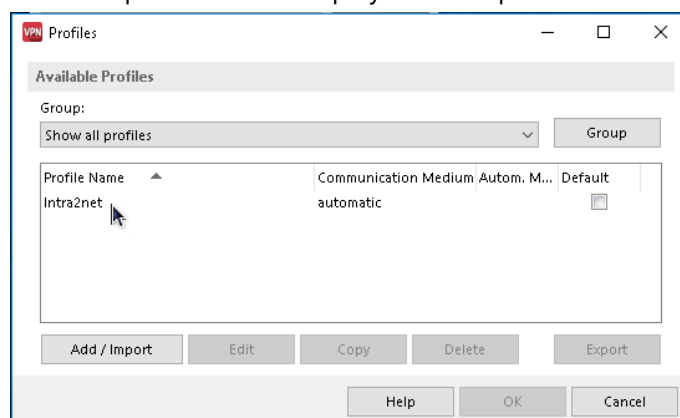
5. Click on "Next" and select the previously unzipped INI file.



6. Confirm the import. The profile should now be imported without errors.

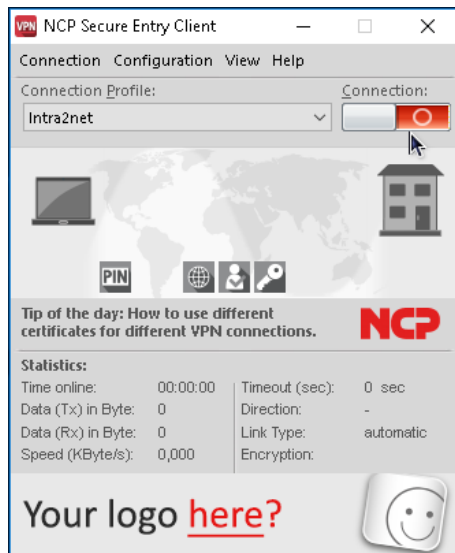


7. The new profile is now displayed in the profile overview and can be used.

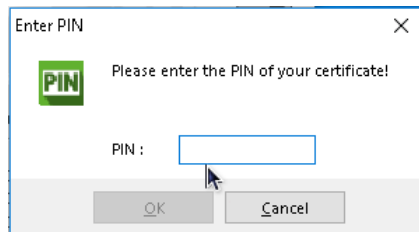


46.2. Establish connection

You can establish the connection by flipping the switch symbol in the NCP client.

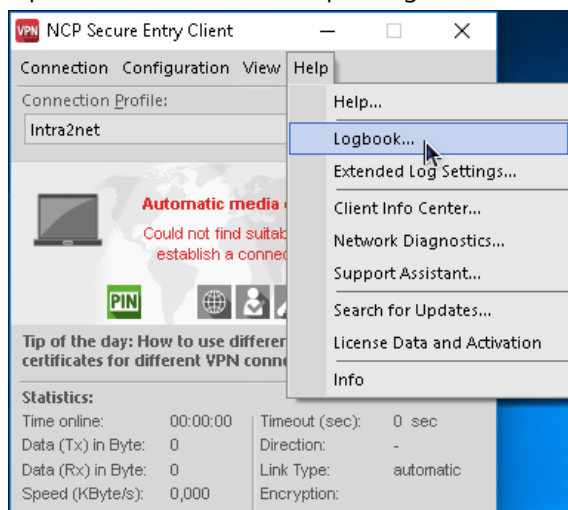


To establish the connection, the password that protects the private key must be entered. This password was set when creating the connection on the Intra2net system.

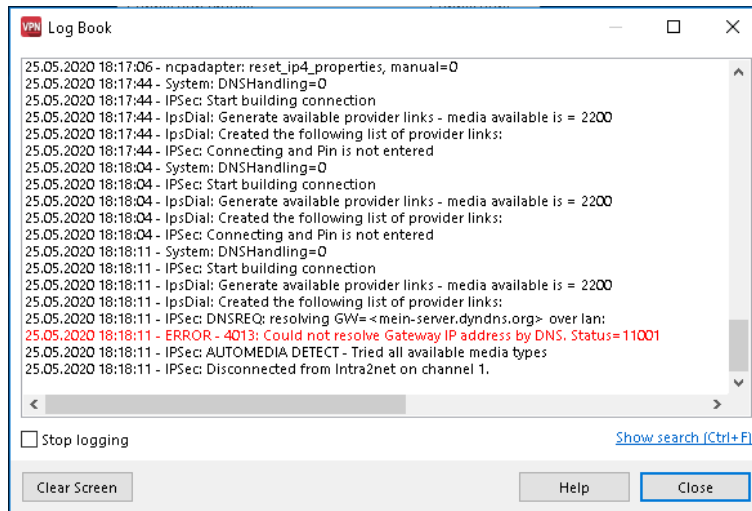


46.3. Connection protocols

To analyze errors in the connection establishment, the logbook of the client is useful. Open it via the menu "Help > Logbook".



You can transfer the content via the clipboard to an editor, save it there and then send it as a file to the support.

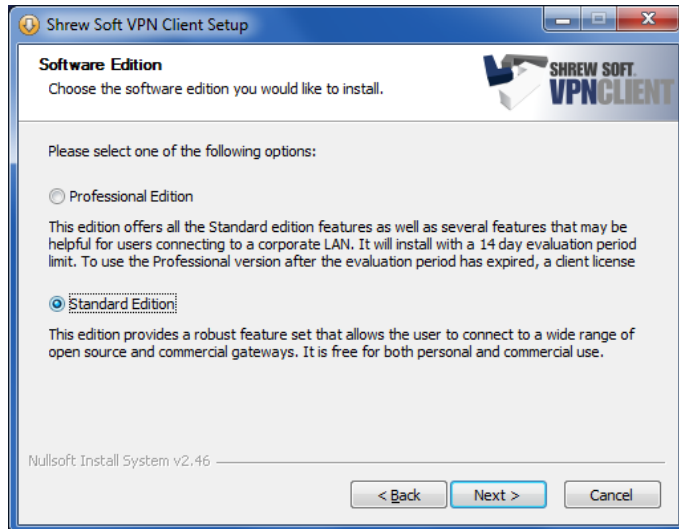


47. Chapter - VPN with the Shrew Soft VPN Client

The Shrew Soft VPN Client for Windows is a free VPN client for Windows 10, 8, 7, Vista and XP. It runs on 32 bit and 64 bit platforms.

You can download the latest version from this URL: <https://www.shrew.net/download/vpn>

During installation, select "Standard Edition". This contains all functions necessary for the connection to the Intra2net system.



47.1. Import

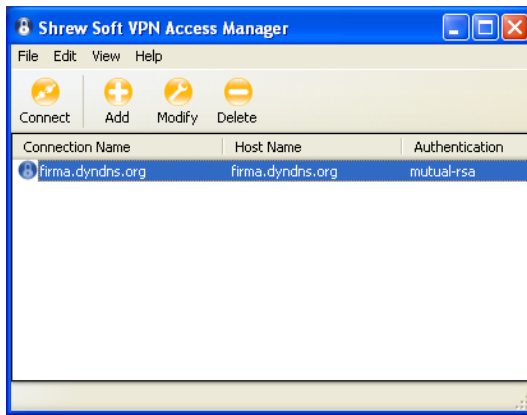
Prepare the Intra2net system for a connection with VPN clients first as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that the complete configuration for the client can be generated by the Intra2net system as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“.

Transfer the newly created configuration file to the client PC, e.g. as an email attachment. Provide the user with the password that protects the private key in another way, e.g. personally on site. For security reasons, do not send this password by email.

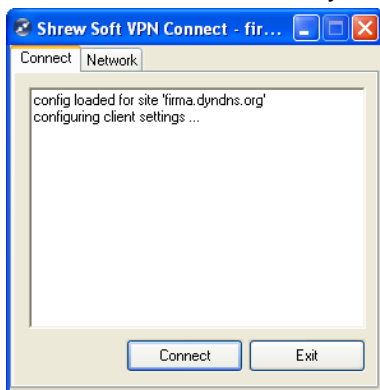
Start the VPN Access Manager and go to the menu "File > Import". Select the file created by the Intra2net system with the extension `.vpn` and import it.

47.2. Establishing Connection

1. Open the newly imported connection in the main menu of the Access Manager by double-clicking it or by clicking "Connect".



2. Establish the connection by clicking "Connect".

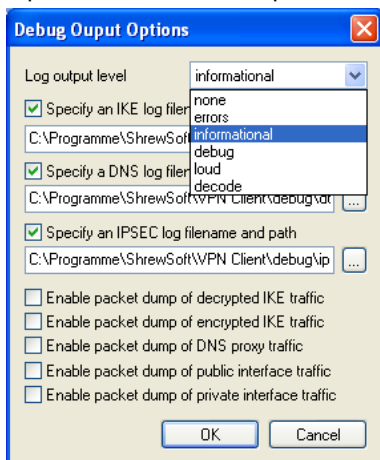


3. You will now be asked for the password for your own key which has been configured on the Intra2net system. Enter it and the connection will be established.

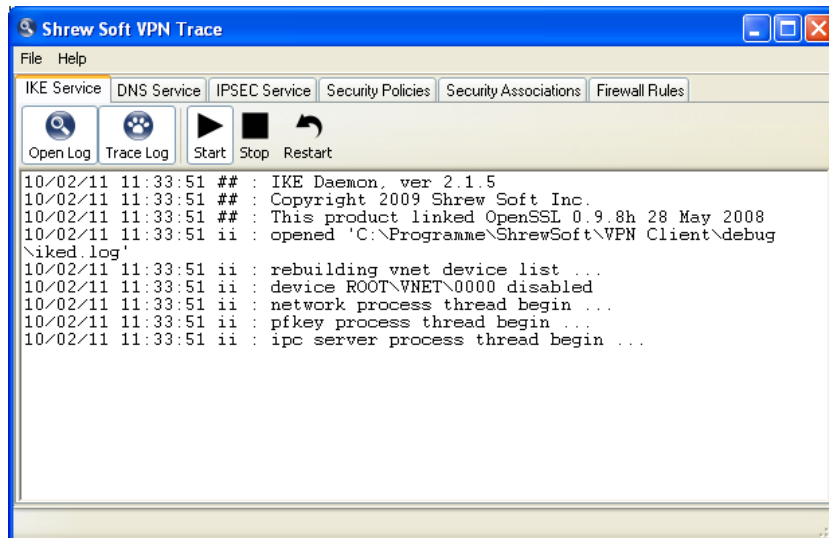
47.3. Connection Protocols

The client's connection protocols can be used to analyze errors in the connection setup.

1. Start Trace Utility, you can find it in the program folder of the Shrew Soft VPN client.
2. Open menu "File", "Options". Set "Log output level" to **informational**.



3. Restart the IKE service with the new trace option by clicking "Restart". Now open the log by clicking "Open Log".



48. Chapter - VPN with Mac OS X

48.1. Installation

Mac OS X already includes a fully functional IPSec stack. However, there is no configuration interface. The free IPSecuritas software provides an interface.

It can be downloaded and installed from <http://www.lobotomo.com/products/IPSecuritas/>.

48.2. Generating Certificates

IPSecuritas cannot generate certificates itself. Therefore the OpenSSL program will be used for this purpose.

1. Open a Unix terminal (Programs > Utilities > Terminal).
2. Enter the following command in one line:

```
openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -outform PEM -  
keyform PEM -keyout private_key.pem -out newcert.pem
```

3. The key pair is calculated and the system will request the certificate data. The entered values are not relevant in this function, they only have to be unique on all systems connected by VPN. Do not use special characters such as accents or umlauts.

```
Generating a 2048 bit RSA private key  
.....  
.....+++.....  
writing new private key to 'private_key.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [GB]:DE  
State or Province Name (full name) [Berkshire]:BW  
Locality Name (eg, city) [Newbury]:Tuebingen  
Organization Name (eg, company) [My Company Ltd]:Intra2net  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:MyComputerName  
Email Address []:
```

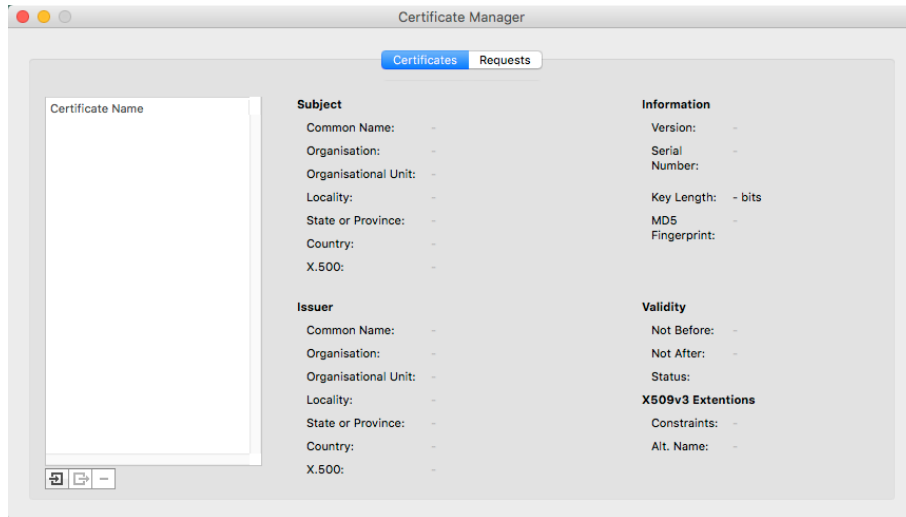
4. The certificate is now valid for 2 years (730 days) and is located in `newcert.pem`. The private key is in the `private_key.pem` file. It is possible to change the validity period using the `-days` parameter in the command line.
5. Current versions of IPSecuritas read the private key only in PKCS 12 format. The following command on the command line converts the key pair created in step 2 appropriately:

```
openssl pkcs12 -export -in newcert.pem -inkey private_key.pem -out new-  
cert.p12
```

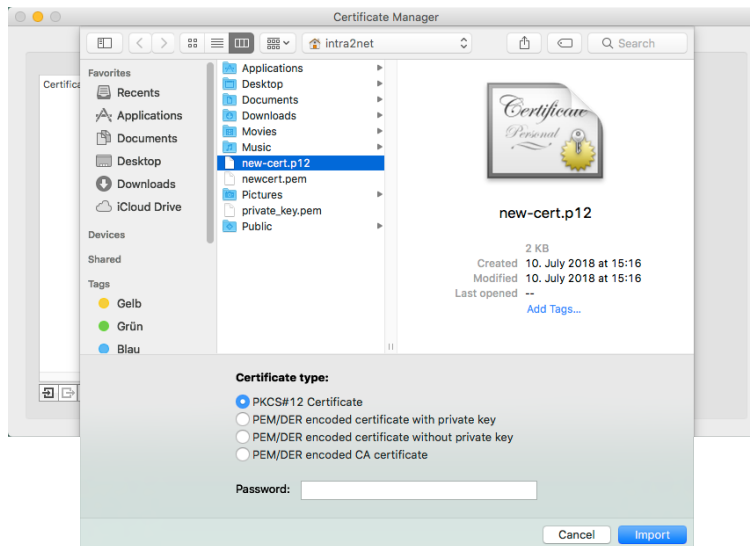
At this point, you must enter a password with which the private key is secured. This password is needed again later when importing to IPSecuritas. The result is saved under the file name `newcert.p12`.

48.3. Importing Certificates

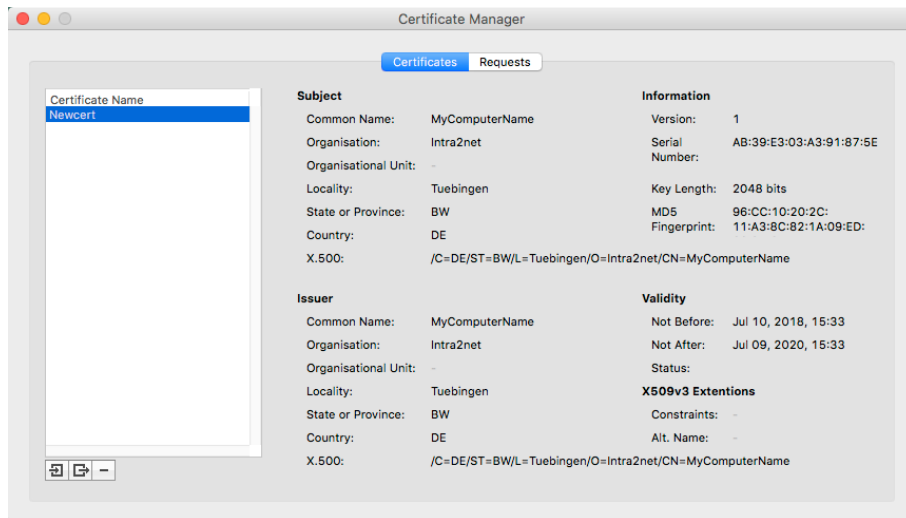
1. Start IPSecuritas, and navigate to "Certificates", "Certificates Manager".



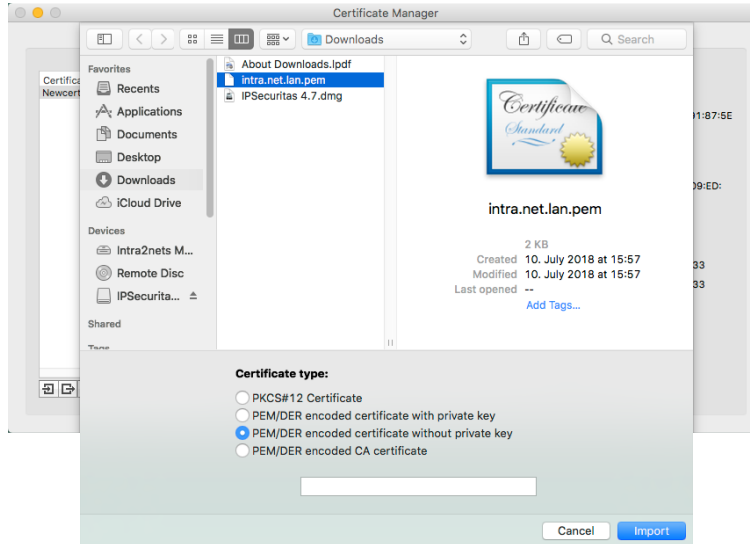
2. Click the "Import" icon in the lower left corner.
3. Select the PKCS 12 file (in the example `newcert.p12`) and set the type to "PKCS#12 Certificate". Enter the password used during creation in the corresponding field.



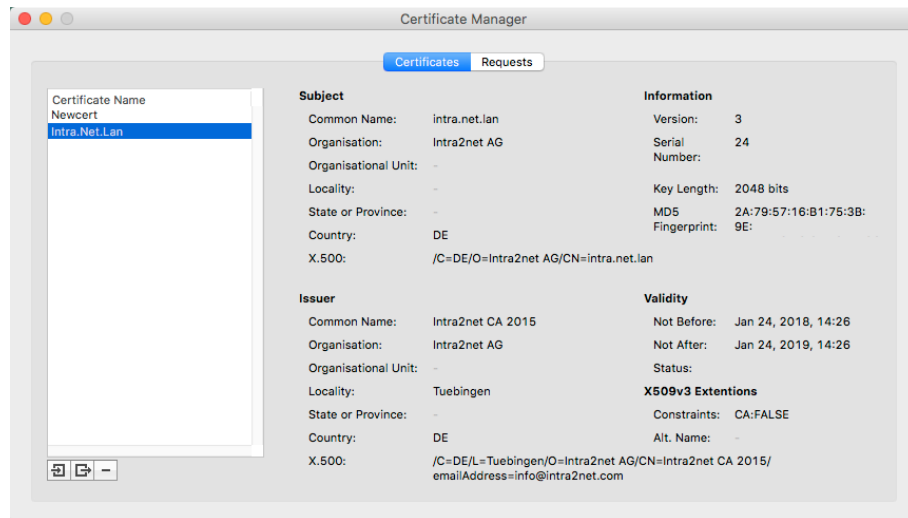
4. The imported certificate is displayed in the Certificate Manager.



5. Open the own certificate (e.g. `newcert.pem`) in a text editor, and copy the content to the clipboard. Open the "System > Keys > Foreign Keys" menu on the Intra2net system and create a new key. Enter a name for the key (e.g. that of the user) and copy the certificate data from the clipboard into the "Copy & paste certificate" field.
6. Open the System "> Keys > Own Keys : Data" menu on the Intra2net system. Select the desired certificate and export it to a .pem file using the "Export Certificate" option.
7. Select the "Certificates Manager" inside IPSecuritas, and the "Import" function again. Import the newly saved certificate file from the Intra2net system and set the type to "PEM/DER encoded certificate without private key".

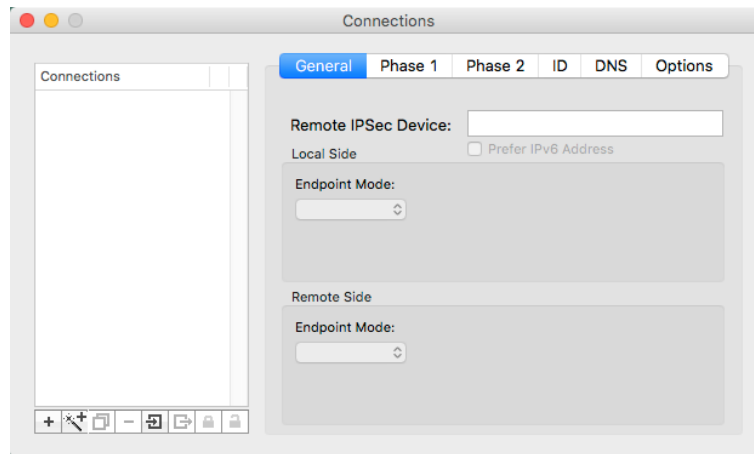


8. The imported certificate is displayed in the Certificate Manager.

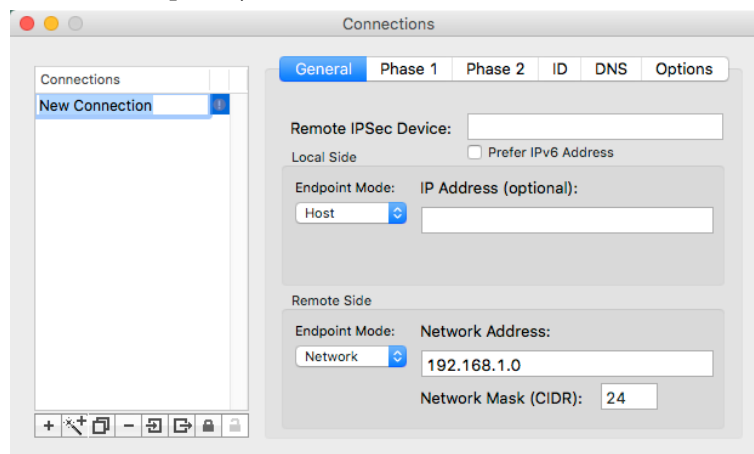


48.4. Configuring Connections

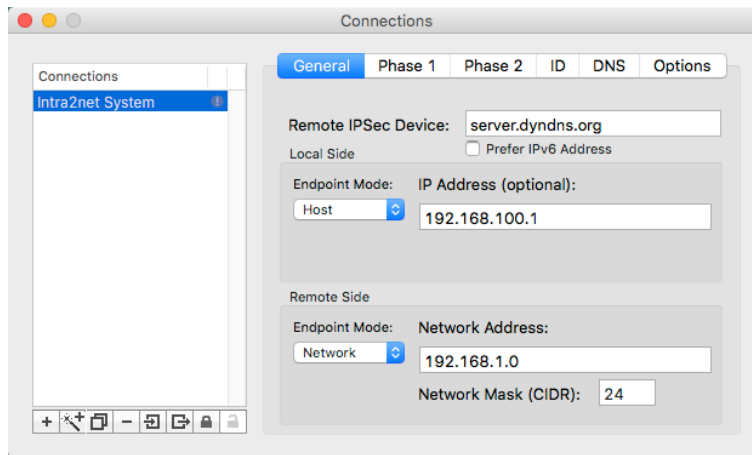
1. In IPSecuritas, open the "Connections", "Edit connections" menu.



2. Create a new connection using the "New" button and give it a name (in this example **Intra2net system**).

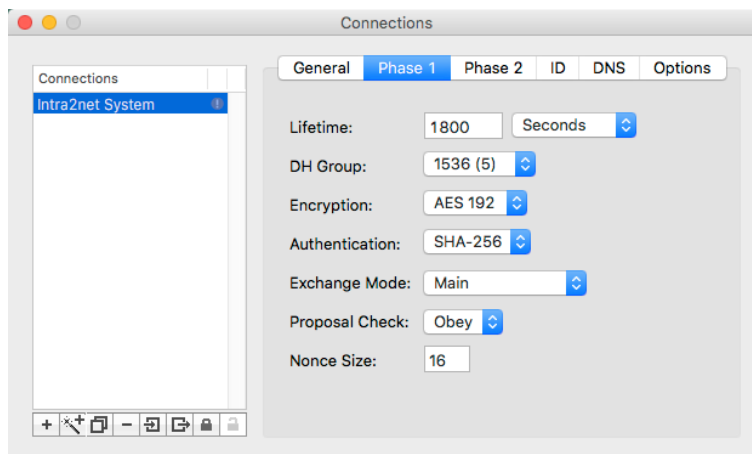


3. In the "General" menu, under "Remote IPSec Device" enter the DNS name of the remote side or if necessary the external IP address of the Intra2net system.



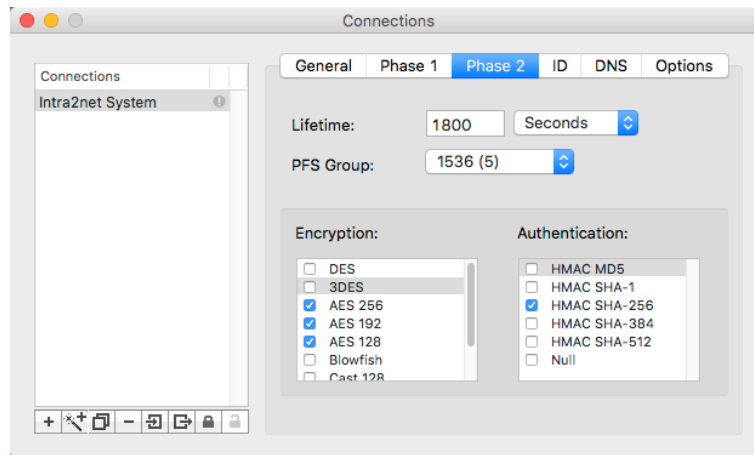
4. On "Local Side", set "Endpoint Mode" to "Host" and enter the virtual IP that the Mac client should use for the VPN. Contrary to the field description, the IP is *not* optional, even if you selected "mode-cfg" in the configuration on the Intra2net system. The IP must be the same as specified there.
5. With "Remote Side" set "Endpoint Mode" to "Network" and enter the address of the network behind the Intra2net system. The netmask is entered in CIDR notation; **24** (bit) corresponds to **255.255.255.0**.
6. From the "Phase 1" menu, it is possible to configure the encryption parameters for phase 1. These must match the encryption profile selected on the Intra2net system.

For the default settings, set the "DH Group" to **1536 (5)**, "Encryption" to **AES 192** and "Authentication" to **SHA-256**.

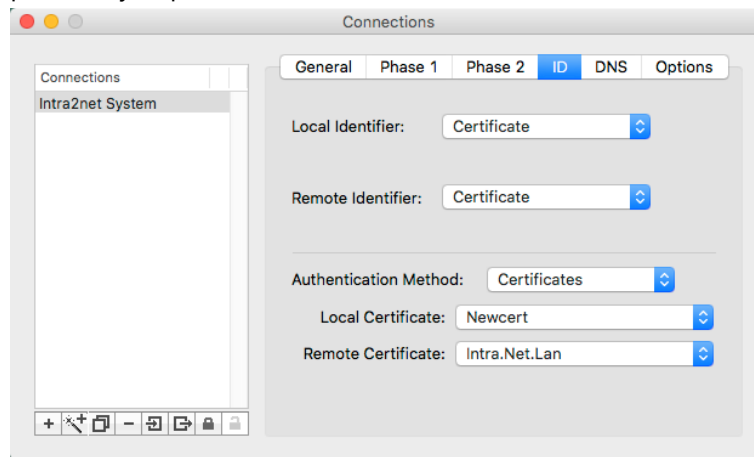


7. From the "Phase 2" menu, it is possible to configure the encryption parameters for phase 2. These must match the encryption profile selected on the Intra2net system.

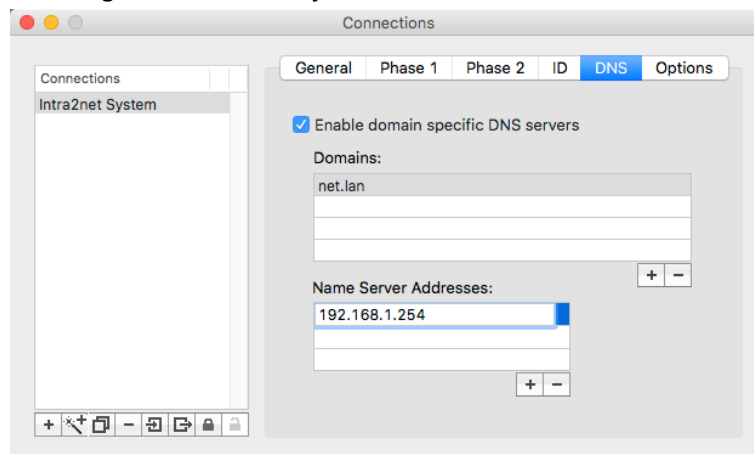
In the default settings, set the "PFS Group" to "1536 (5)" and activate only the AES encryption methods under "Encryption". Under "Authentication" enable "HMAC SHA-256" only.



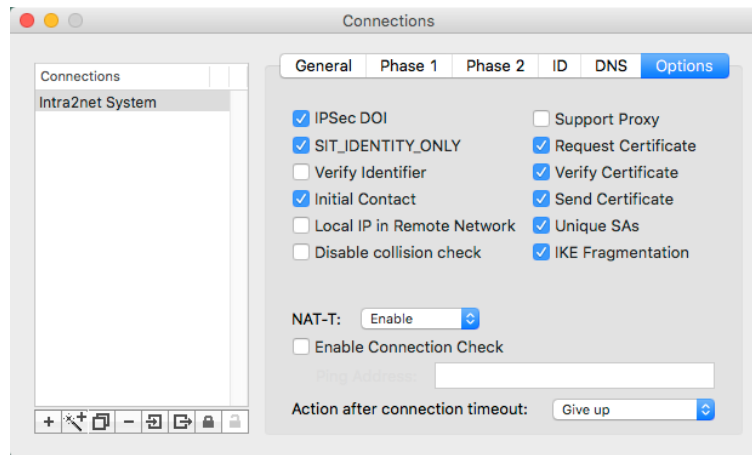
8. In the "ID" menu, under "Local Identifier" and "Remote Identifier", set "Certificate" for each item. Select "Certificates" as the "Authentication Method" and enter the two previously imported certificates.



9. In the "DNS" menu it is possible to have a specific domain resolved by a server in the VPN (e.g. the Intra2net system).



10. In the "Options" menu, set the various options as shown here.



11. The connection can now be established in the main window by clicking "Start".



48.5. Intra2net System

On the Intra2net system, the connection must also be configured correctly. For VPN clients, this is described in 45. Chapter, „Connecting Individual PCs“.

49. Chapter - VPN with the NCP Secure Entry macOS Client

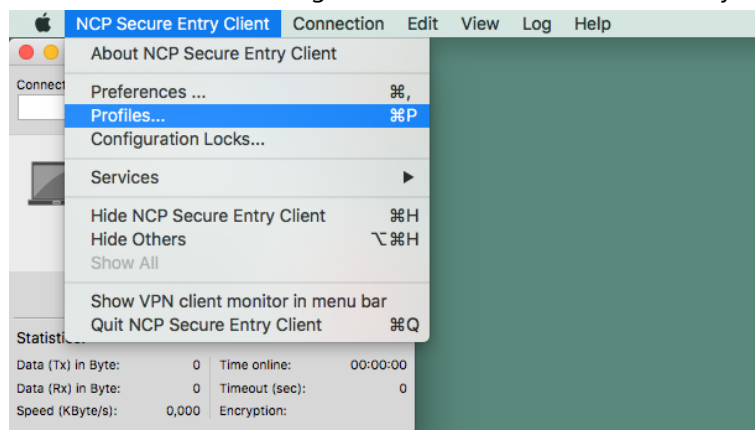
The NCP Secure Entry macOS Client is sold through several distributors. A 30-day trial version can be downloaded from the homepage of NCP [<https://www.ncp-e.com>].

Prepare the Intra2net system for a connection with VPN clients first as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that the complete configuration for the client can be generated by the Intra2net system as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“.

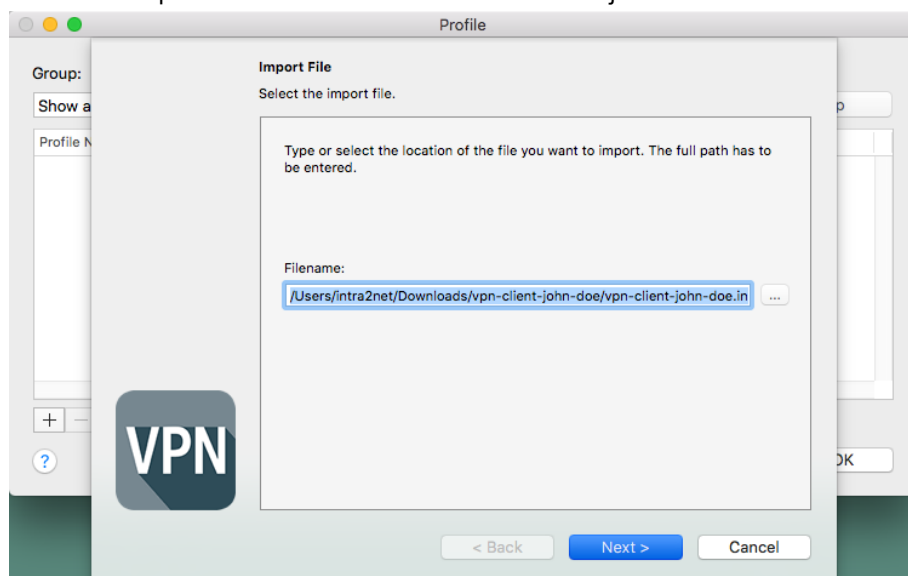
Transfer the configuration file thus created to the macOS device, e.g. as an email attachment. Give the user the password that protects the private key in another way, e.g. personally on site. For security reasons, do not send this password by email.

Then proceed as follows on the macOS device to import the configuration:

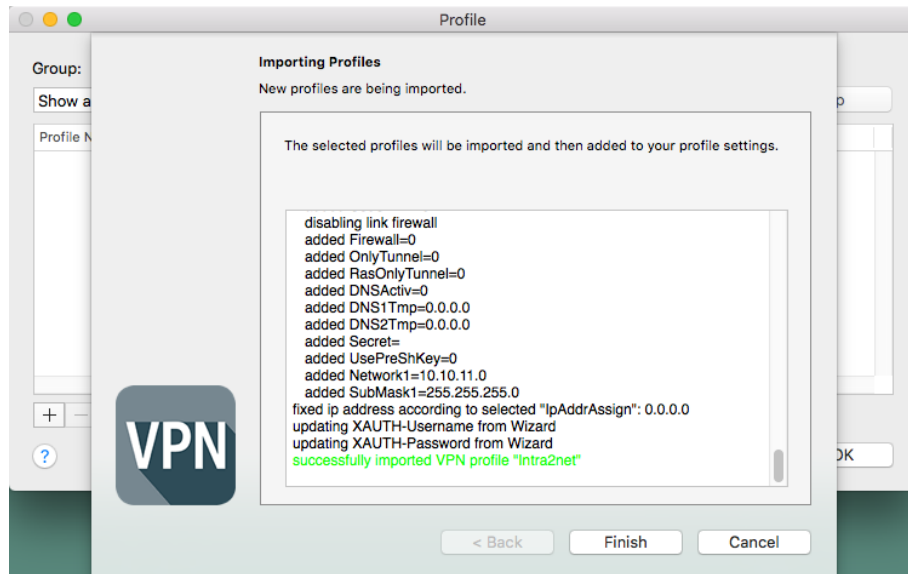
1. The configuration consists of several individual files and is transferred packed as a ZIP file. Open the ZIP file in the file manager of macOS and unpack all contained files into a directory.
2. Start the VPN client and go to the menu "NCP Secure Entry Client > Profiles".



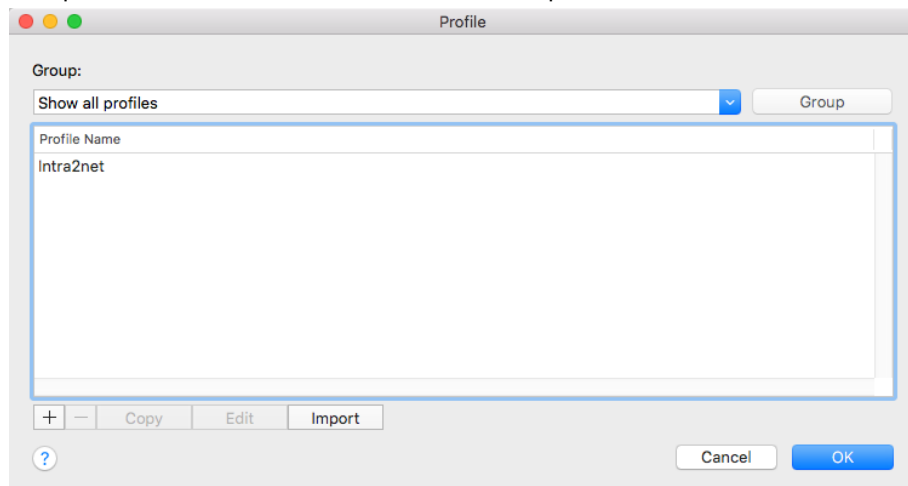
3. Click on "Import" and select the INI file that was just extracted.



4. Click on "Next" to import the profile. The profile should import successfully.



5. The profile overview now contains the new profile.



6. Next, the file with the certificate of the Intra2net system must be copied. This was contained in the previously unzipped ZIP file and has the external DNS host name of the Intra2net system with the extension `.pem` as file name.

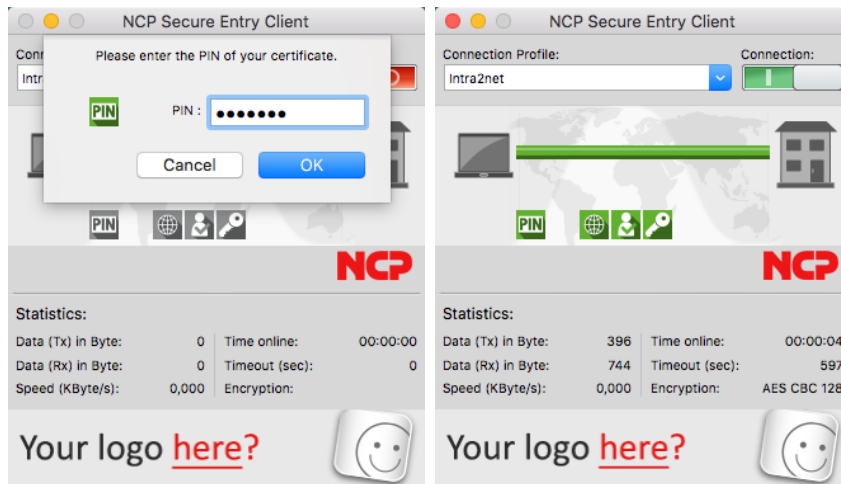
Copy them with the macOS file manager into the directory `Library/Application Support/NCP/Secure Client/cacerts`.

7. Next, the file with the private key for the client must be copied. This was contained in the previously unpacked ZIP file and has the name of the connection with the extension `.p12`.

Copy them into the directory `Library/Application Support/NCP/Secure Client/certs`.

You can now establish the connection by flipping the switch symbol in the NCP client.

To establish the connection, the password that protects the private key must be entered. This password was configured when the connection was created on the Intra2net system.



50. Chapter - VPN with the Apple iOS devices

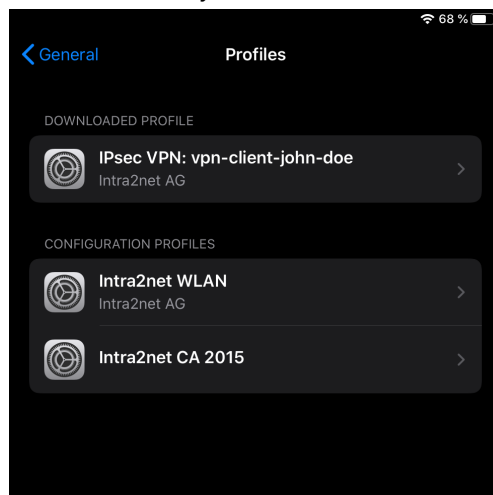
iOS comes with an integrated VPN client that can be used to connect to the Intra2net system.

First prepare the Intra2net system for a connection with VPN clients as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that the complete configuration for the client can be created by the Intra2net system as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“.

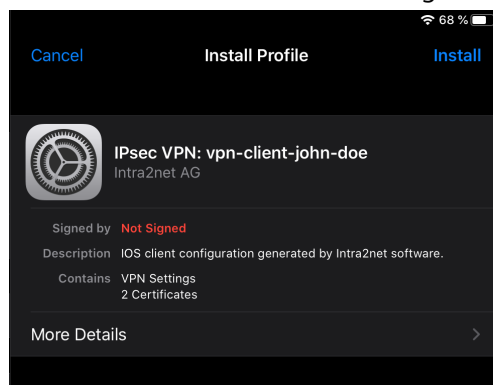
Transfer the configuration file created in this way (extension `.mobileconfig`) to the iOS device, e.g. as an email attachment. Give the user the password that is used to protect the private key in another way, e.g. personally on site. For security reasons, do not send this password by email.

Then proceed as follows on the iOS device to import the configuration:

1. Click on the configuration file (extension `.mobileconfig`), e.g. in the email client. It is then loaded as a profile in the iOS device, but is not yet installed.
2. Open the menu "Settings > General > Profiles". The VPN connection is displayed as loaded but not yet installed.

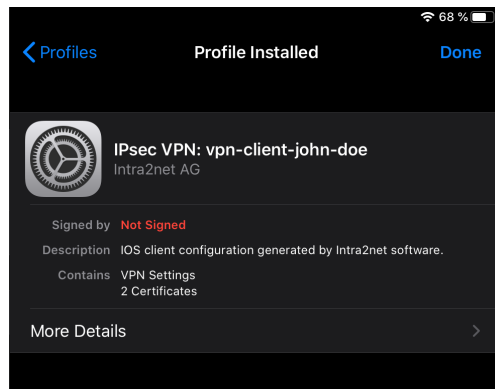


3. Click on the VPN connection and go to "Install".

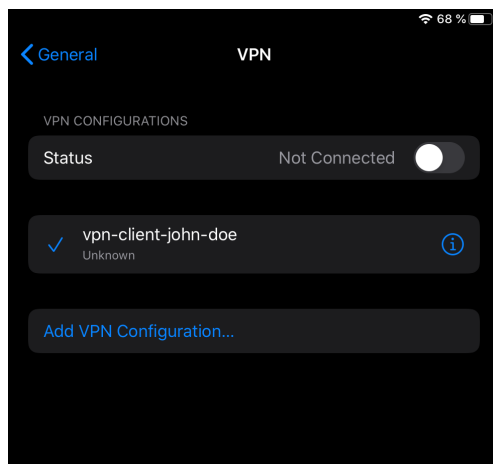


4. You must enter the iOS device password to install a new profile. You will then see security warnings. Select "Install" again and confirm the installation.

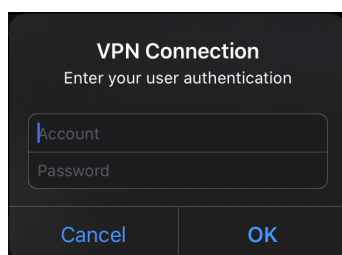
5. You must now enter the password that protects the private key once. This password was set when the connection was created on the Intra2net system.
6. The profile was successfully installed. Complete the process with "Done".



To establish the connection, open the menu "Settings > General > VPN" and then flip the switch to connect.



You must now enter the login and password of the user on the Intra2net system to establish the connection.



51. Chapter - VPN with Android

Devices with Android Version 4 (Ice Cream Sandwich) or later, contain everything necessary to establish VPN connections with the Intra2net system. Additional software, root rights and similar are not required.

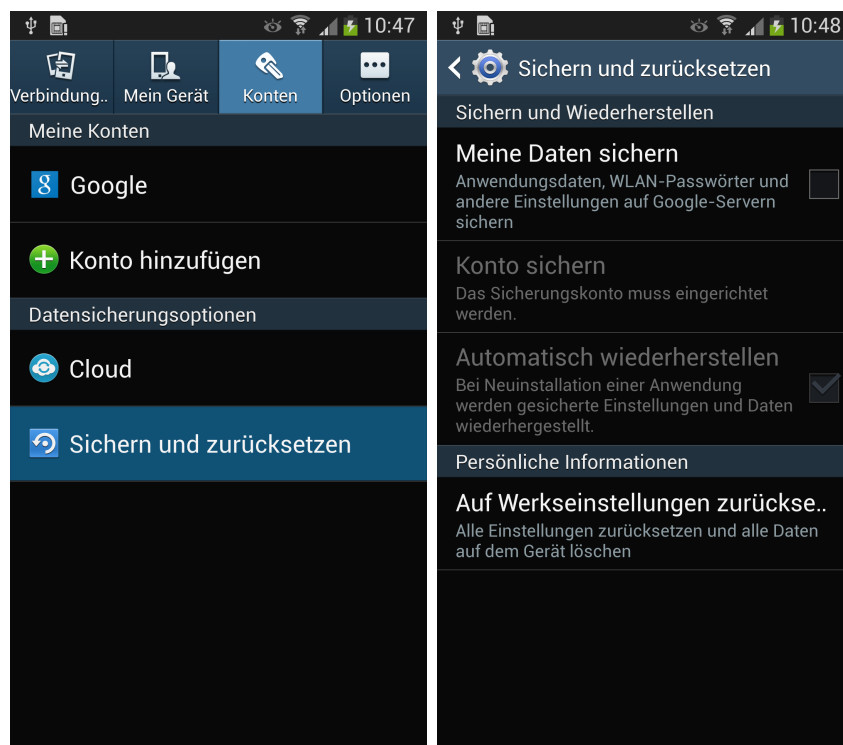
Devices with Android are provided by many different manufacturers. Every manufacturer has the ability to modify the original Google Android on their devices. For this reason, we cannot guarantee the functionality of all devices. In addition, the details of how to operate it may differ from those described here. These instructions and images were produced using a Samsung Galaxy S4.

Initial setup requires a PC with a USB connection to the Android device.

51.1. Preparing the Device

Before setting up the VPN connection, check whether the login data remains hidden or not. Go to "Settings", tab "Accounts", and "Backup and reset".

The setting "Backup my data" should be disabled. If this setting is active, the login data is uploaded to Google and stored there unencrypted. Anyone who knows the password to the Google Account associated with the device can retrieve it. Google and any third parties authorized by Google are equally entitled to do so.



Hint

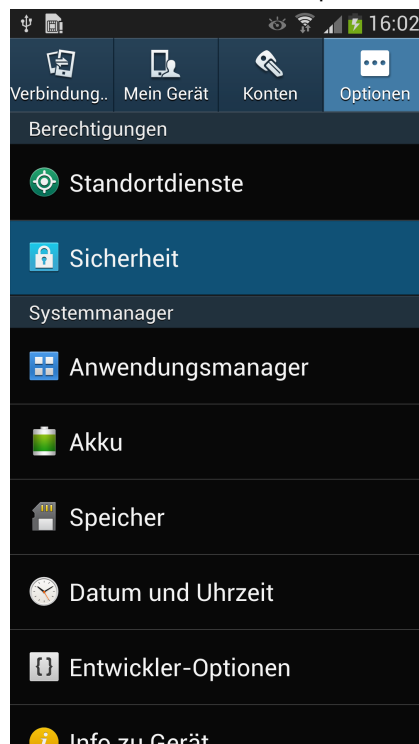
If the setting was previously active, all access data stored on the device (including email accounts, WLANs, social media, etc.) must be regarded as compromised and should be changed immediately. It can be assumed that the data will continue to be stored by Google, even if the upload of new data has been deactivated.

51.2. Connection on the Intra2net System

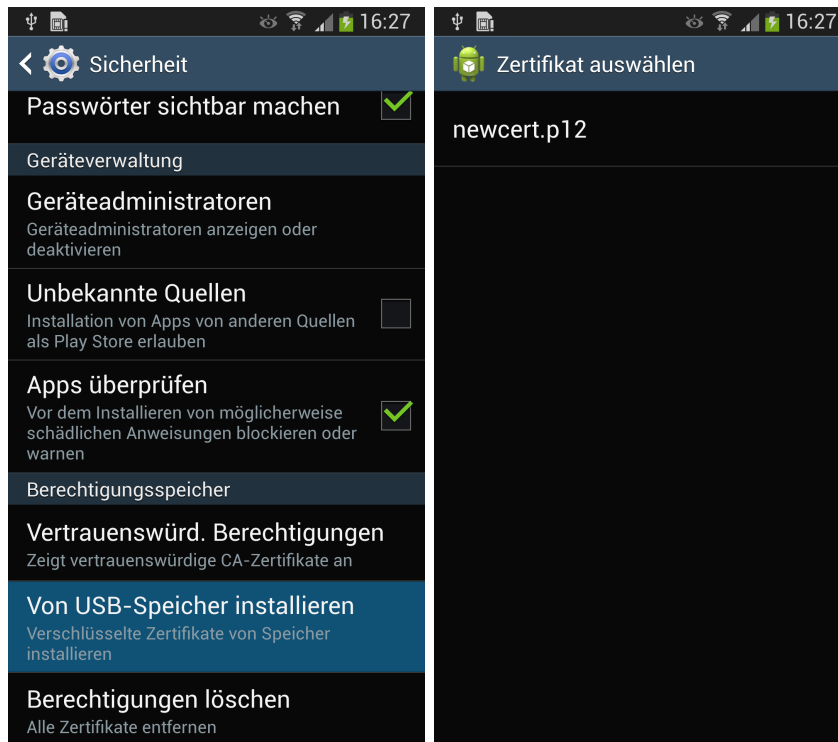
First prepare the Intra2net system for a connection with VPN clients as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that, the connection can be prepared as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“. In doing so, select "Native Android" as the VPN client type.

51.3. Certificates

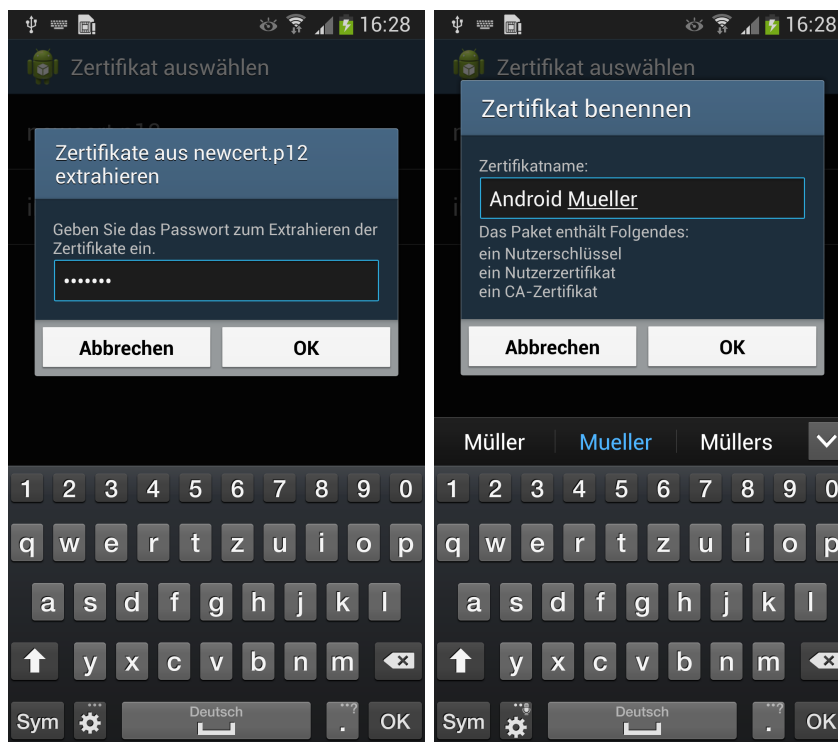
1. When creating the connection on the Intra2net system, a file with the private key for the Android client (extension .p12) is created and exported.
2. Now connect the Android device to your computer via USB. Many devices have different connection modes to choose from. Select a mode in which you can exchange files between PC and Android device, such as Media Device (MTP) or drive. If there are any uncertainties, consult the manual of your Android device regarding data exchange between a PC and the device.
3. Now copy (e.g. with Windows Explorer) the previously exported .p12 file to the Android device.
4. Disconnect the PC and Android device properly using the remove hardware feature in the Windows taskbar.
5. On the Android device, open "Settings", then "Options", and "Security".



6. Under the "Credential storage" category, and select "Install from device storage".

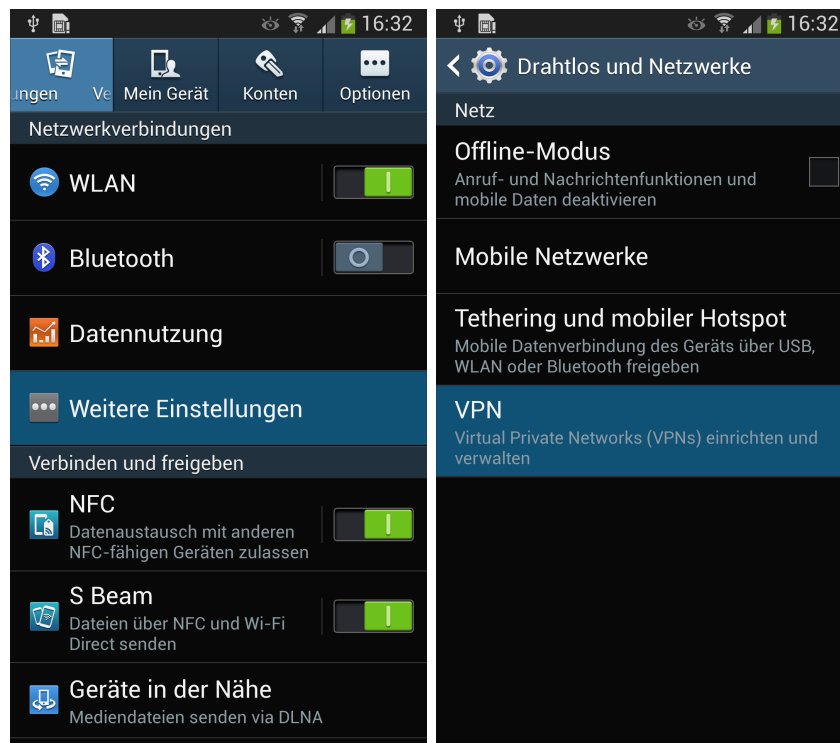


7. Click the private key (filename `newcert.p12`) to import it. You will be asked for the password assigned on the Intra2net system and will then be given the option to assign a suitable name for the certificate.

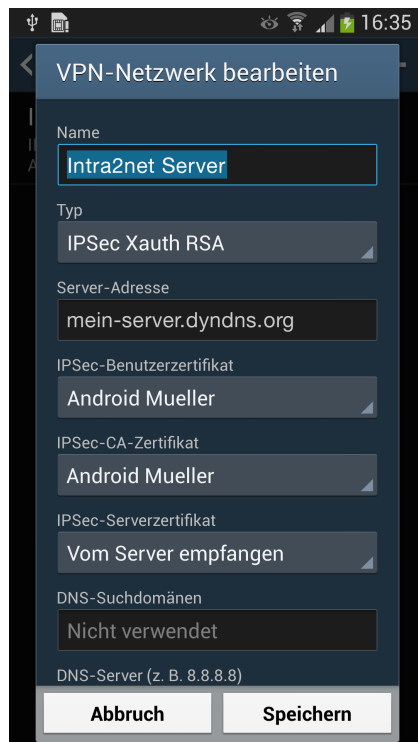


51.4. Connecting with Android

1. On the Android device, open "Settings", go to the "Connections" tab, and open "More Networks". In the following menu, select "VPN".



2. Add a new VPN and assign a suitable name for the connection.
3. Select "IPSec Xauth RSA" as the VPN type.
4. "Server address" is the externally accessible, official DNS name of your Intra2net system (better) or, if necessary, its external, static IP.
5. Now select the "IPSec user certificate", which you have just imported from the PC.
6. For "IPSec-CA-Certificate" select the previously imported certificate.
7. The "IPSec server certificate" can be set to (received from the server).



VPN-Netzwerk bearbeiten

Name
Intra2net Server

Typ
IPSec Xauth RSA

Server-Adresse
mein-server.dyndns.org

IPSec-Benutzerzertifikat
Android Mueller

IPSec-CA-Zertifikat
Android Mueller

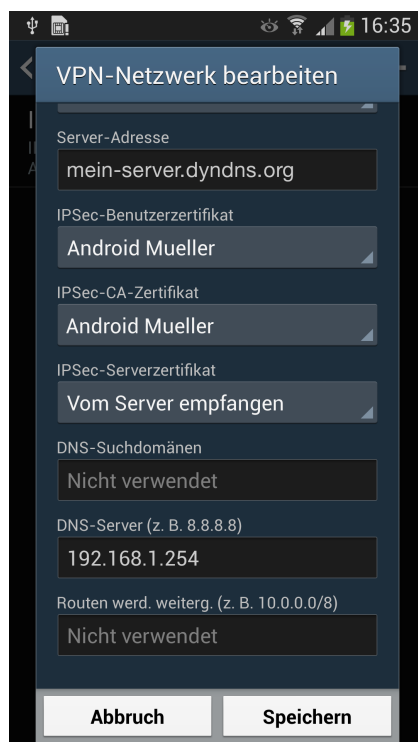
IPSec-Serverzertifikat
Vom Server empfangen

DNS-Suchdomänen
Nicht verwendet

DNS-Server (z. B. 8.8.8.8)

Abbruch Speichern

8. Open "Show advanced options".
9. For "DNS-Server" enter the internal IP of the Intra2net system.



VPN-Netzwerk bearbeiten

Server-Adresse
mein-server.dyndns.org

IPSec-Benutzerzertifikat
Android Mueller

IPSec-CA-Zertifikat
Android Mueller

IPSec-Serverzertifikat
Vom Server empfangen

DNS-Suchdomänen
Nicht verwendet

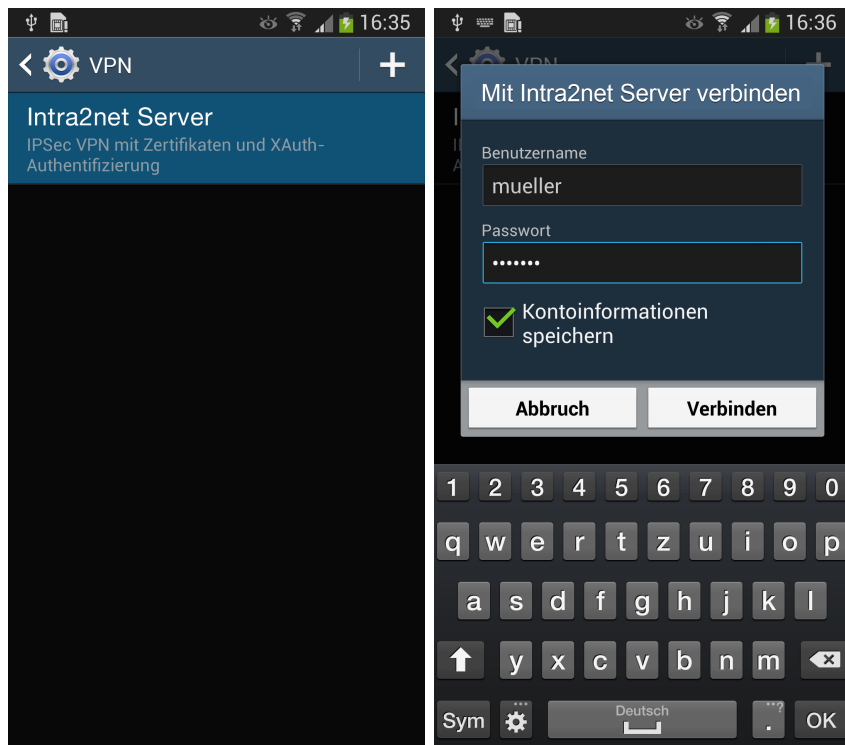
DNS-Server (z. B. 8.8.8.8)
192.168.1.254

Routen werd. weiterg. (z. B. 10.0.0.0/8)
Nicht verwendet

Abbruch Speichern

10. Save the connection.
11. Clicking on the name of the connection prompts you to enter your user name and password. Enter the login data as stored on the Intra2net system in the user manager.

The user must be on the Intra2net system, in a user group that has the right to log on to the VPN with XAUTH.



12. If the connection was established successfully, a key icon is displayed in the top left corner of the status bar.

51.5. Simplify Connection Setup

The connection is always established using the VPN menu. To make this easier to access, proceed as follows:

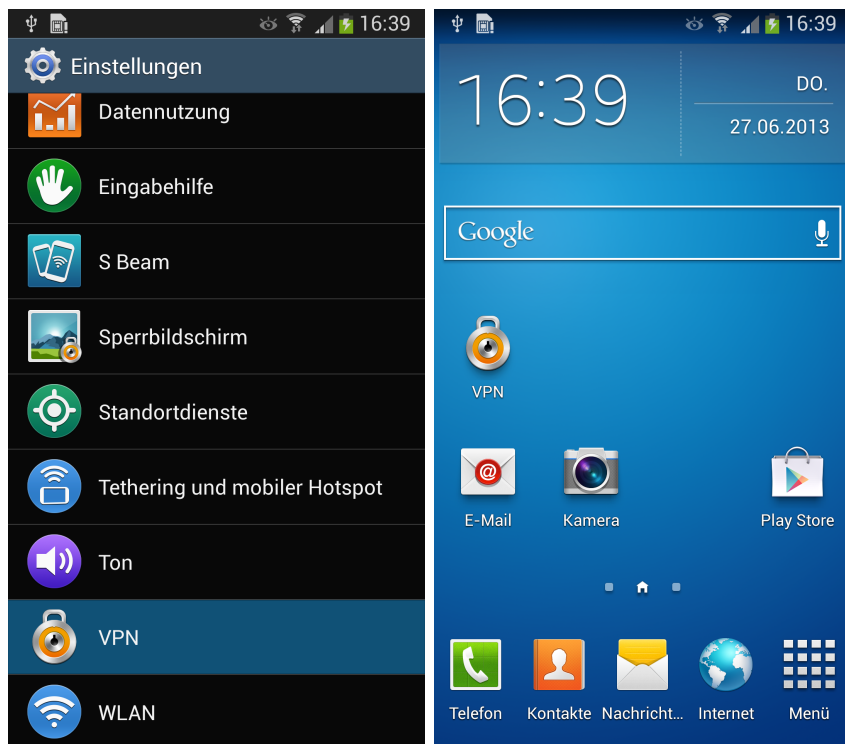
1. Go to the home screen and select "Add Apps and Widgets".



2. Open the "Widgets" tab and search for "Settings". Press and hold your finger on the settings until the home screen is displayed. Drag the settings widget to a free space and let go.



3. Now select "VPN". The VPN menu is now accessible directly from the main screen.



52. Chapter - VPN with the NCP Secure Android Client Premium

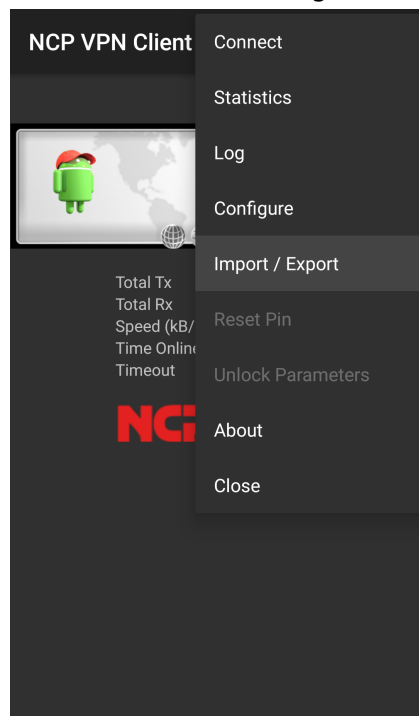
The NCP Secure Android Client Premium can be purchased through the Google Play Store.

Prepare the Intra2net system for a connection with VPN clients first as described in Section 45.2, „Preparing the configuration on the Intra2net system“. After that the complete configuration for the client can be generated by the Intra2net system as described in Section 45.3, „Automatic configuration for clients on the Intra2net system“.

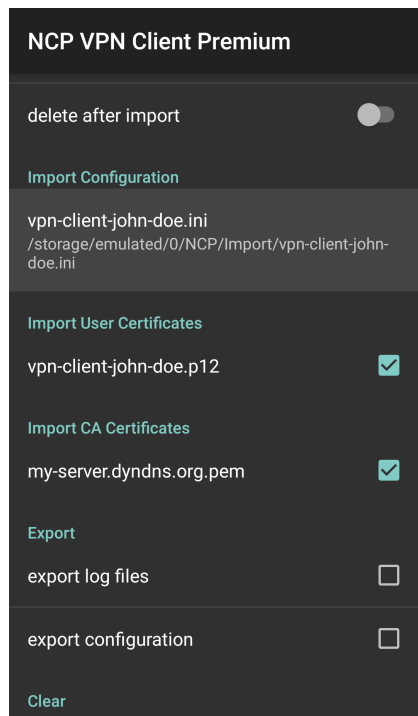
Transfer the configuration file thus created to the Android device, e.g. as an email attachment. Give the user the password that protects the private key in another way, e.g. personally on site. For security reasons, do not send this password by email.

Proceed as follows on the Android device to import the configuration:

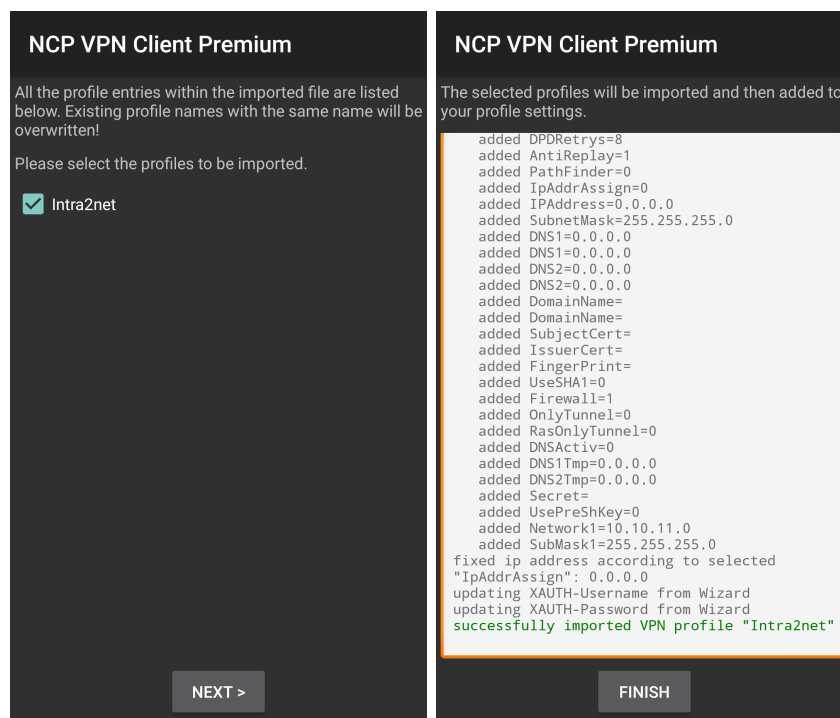
1. The configuration consists of several individual files and is transferred packed as a ZIP file. Open the ZIP file in the file manager of Android, select all contained files and unpack them into the directory `NCP/Import` on the internal memory of the device.
2. Start the VPN client and go to the menu "Import / Export".



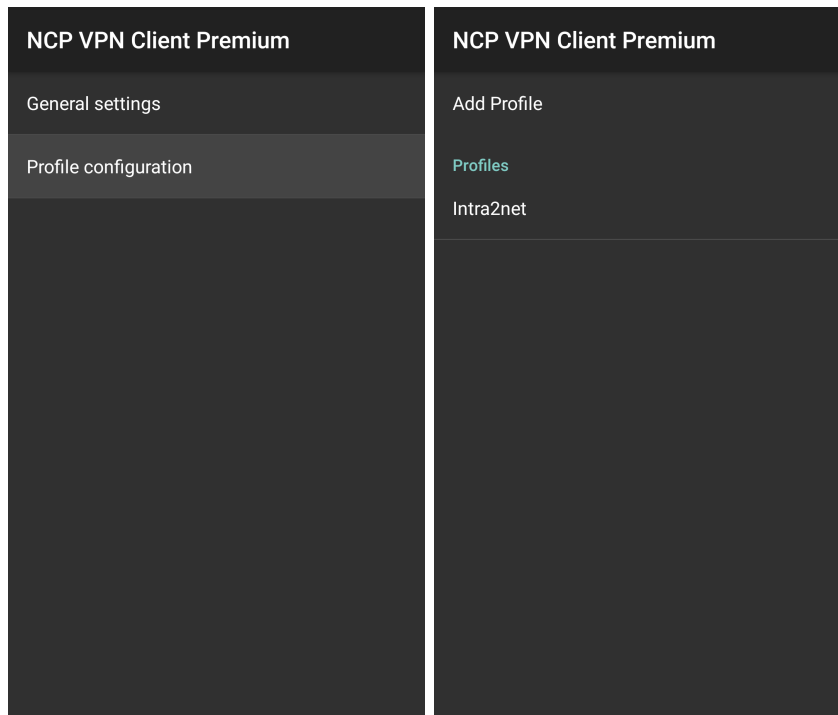
3. Under "Import Configuration", select the INI file you just extracted and start the import.



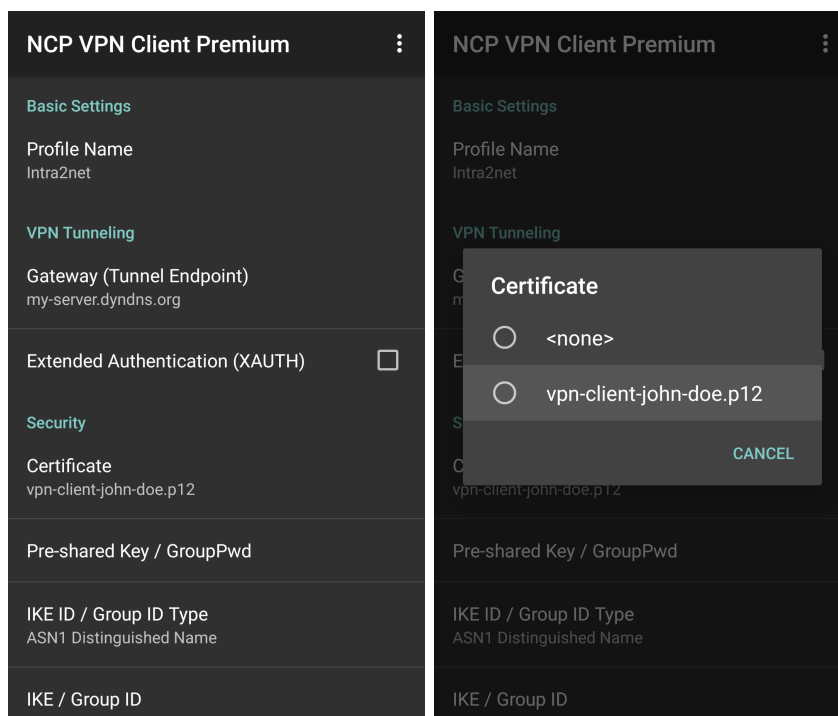
4. Confirm that the profile is to be imported. The profile should be imported successfully.



5. Go to the menu "Configure > Profile configuration" and open the profile "Intra2net".



6. Open the menu item "Certificate" and confirm the use of the imported key for this connection.



7. Save the connection profile.

NCP VPN Client Save

Basic Settings Revert

Profile Name
Intra2net

VPN Tunneling

Gateway (Tunnel Endpoint)
my-server.dyndns.org

Extended Authentication (XAUTH) ☐

Security

Certificate
vpn-client-john-doe.p12

Pre-shared Key / GroupPwd

IKE ID / Group ID Type
ASN1 Distinguished Name

IKE / Group ID

You can now establish the connection by flipping the switch symbol in the VPN client.

To establish the connection, the password that protects the private key must be entered. This password was configured when the connection was created on the Intra2net system.

NCP VPN Client Premium

Intra2net

Total Tx 0 Byte
Total Rx 0 Byte
Speed (kB/s) 0,000
Time Online 0 sec.
Timeout 0 sec.

NCP ☐

NCP VPN Client Premium

Please enter PIN for profile "Intra2net":

.....

☐ Show PIN

OK CANCEL

1 2 3 4 5 6 7 8 9 0

@ # \$ % & - + ()

= \ < * " ' : ; ! ?

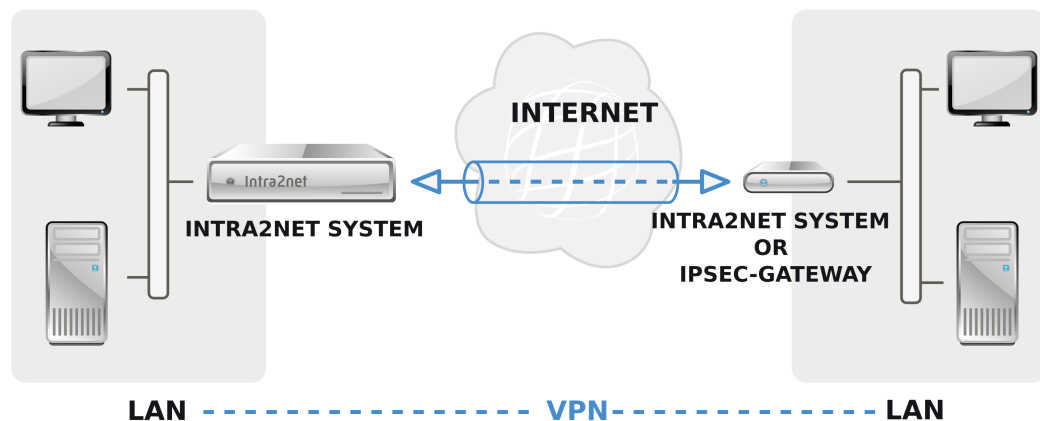
ABC , _ English / .

53. Chapter - Connecting Complete Networks

53.1. Method

If multiple clients on a remote network are to be connected to a network behind the Intra2net system (e.g. in a branch office), it is generally more practical to establish a VPN between the two networks instead of setting up a single VPN for each of the clients.

The VPN is then established between the Intra2net system and an IPsec gateway ahead of the other network. This IPsec gateway can be an Intra2net system, but it can also be another compatible product.



Networks can also be connected to private IPs via a VPN tunnel. However, the IPs continue to be used for addressing. This means that you cannot connect networks with identical or overlapping network areas via VPN.

Make sure that the Intra2net system and the IPsec gateway on the remote station get an official IP and are not behind a router that uses NAT. Although VPN behind a NAT router is possible, it can cause difficulties if both sides are behind NAT routers.

It is not necessary to use dedicated IPs. Dynamic IPs with DynDNS can be used on one or both sides without difficulty.

If the connection on one side is disconnected regularly (e.g. by forcibly disconnecting DSL), it should be ensured that the connection can be re-established from both sides and not only from one.

A connection configured on the Intra2net system is valid for the connection from a network on the side of the peer and a network behind the Intra2net system. If you want to connect multiple networks, you can configure a separate connection for each network combination. Make sure that you always use the same combination of keys and certificates for each of these connections.

53.2. Configuration on the Intra2net System

53.2.1. Prerequisites

First of all, you must ensure that each side has its own key and the public key of the other. It is recommended that you create a dedicated key for VPNs only on each system.

If you set up multiple VPNs on the Intra2net system, you do not have to create a separate key for each connection: You can use a single key for all VPNs. Of course you will still need the public key from each of the peers.

Further details on key management can be found in 44. Chapter, „Key Management“.

53.2.2. Default Settings

You can configure VPN connections in the Services > VPN > Connections menu. Create a new connection and select the type "IPSec: Site-to-site or custom configuration".

On the first page, set the remote side. The remote side is the official IP under which the Intra2net system can reach the IPSec gateway on the peer's side of the connection. Do not confuse this with the IP that the peer has in its own network (typically from a private network area).

If the peer has a static IP, it is advisable to enter this IP and not the DNS name, which might also exist. If the peer is not accessible from the Intra2net system or has no DynDNS name (e.g. because it is located in a UMTS network and cannot be reached behind NAT), you can enter "Dynamic IP (Road Warrior)" as the type. However, this setting is intended for individual clients and not so much for permanently active connections between networks.

The encryption algorithms used can be selected via the encryption profile; for details see Section 43.5, „Algorithms“. It is important that the setting for Perfect Forward Secrecy (PSF) is identical on both sides.

Encapsulation controls how the packets for the VPN tunnel are packed. With ESP, encryption and authentication are encapsulated. With ESP+AH, encryption and authentication are carried out separately. ESP+AH cannot be conducted through NAT, so ESP is widely accepted. This setting must be identical on both sides of the connection.

53.2.3. Authentication

Select your own key and the key of the remote side.

For the reasons mentioned in Section 43.6, „Limitations“ we advise against authenticating connections using a pre-shared key (PSK). If you still want to use it, you must choose the IPSec IDs of both sides in addition to the common key. If both sides have static IPs, you can use the IPs directly as IPSec IDs. For dynamic IPs, it is recommended to enter email addresses as IPSec IDs.

53.2.4. Configuring the Tunnel

On the "Tunnel" page, you can configure which networks are connected to each other by this VPN connection.

The "Local network" option selects the network to be connected on the side of the Intra2net system. With the "Local networks" option, select one of the networks directly connected or routed to the Intra2net system.

For "Remote network" select the "Custom net" type and enter IP and netmask of the network behind the IPSec Gateway on the peer's side.

The options for address conversion (NAT) are explained in 57. Chapter, „Solving IP Address Conflicts in VPNs Through NAT“.

53.2.5. Rights

In this menu the rights of the VPN network on the peer's side are defined. This applies to all packets coming from the VPN network. A description of the rights options can be found under Section 8.3, „Access Rights of a Network Object“.

53.2.6. Activation

This menu is used to configure when the connection is established and when existing sessions are to be extended.

For passive or manual start, the Intra2net system waits until either the peer establishes the connection or a user establishes the connection manually through the mainpage. If the connection is always running, the Intra2net system will continuously try to establish the connection and keep it open.

The number of setup attempts only affects the manual setup on the mainpage. This option has no impact when used in conjunction with "Always".

The lifespan of the two phases indicates how many minutes after a connection should be re-authenticated and new session keys negotiated. The time for phase 1 should be greater than the time for phase 2, these values do not have to match the settings of the peer.

If a value is entered for "Offline detection", the Intra2net system sends a packet to the other side at a minimum of the specified number of times. If no response is received on multiple occasions, the connection is dropped and re-established. This function uses the IPSec default dead-peer detection (DPD).

54. Chapter - VPN with ZyXEL ZyWALL USG

54.1. Overview

This guide applies to the ZyXEL ZyWALL USG product range. These support VPNs with X.509 certificates and are not limited to pre-shared key authentication. Thusbypassing the restrictions described under Section 43.6, „Limitations“.

The router supports self-signed certificates as well as being able to produce them itself. This significantly reduces setup time.

The Intra2net system can of course also support connections with other routers. However, this router is described in more detail as it is relatively inexpensive and readily available compared to other routers with X.509 certificate support.

54.2. Preparation

The router verifies the validity period of the certificate during authentication. For this reason, the system time must always be correct in order to establish a VPN connection.

The router updates its time using NTP protocol. This can be checked and configured under "Configuration > System > Date/Time". Open the menu and set the correct time zone and Daylight Saving settings. Use the "Sync Now" button to test if the NTP synchronization is fully functioning.

ZyXEL ZyWALL USG 20

Welcome admin | [Logout](#) | [Help](#) | [About](#) | [Site Map](#) | [Object Reference](#) | [Console](#) | [CLI](#)

CONFIGURATION

- Quick Setup
- Licensing
- Network
- Auth. Policy
- Firewall
- VPN
- BWM
- Anti-X
- Object
- System
 - Host Name
 - Date/Time**
 - Console Speed
 - DNS
 - WWW
 - SSH
 - TELNET
 - FTP
 - SNMP
 - Vantage CNM
 - Language
- Log & Report

Date/Time

Current Time and Date

Current Time: 11:58:48 GMT+01:00
Current Date: 2011-03-14

Time and Date Setup

☐ Manual

New Time (hh:mm:ss): 11 : 58 : 19
New Date (yyyy-mm-dd): 2011-03-14

☒ Get from Time Server

Time Server Address*: 0.pool.ntp.org [Sync Now](#)

*Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels

☒ Enable Daylight Saving

Start Date: Last Sunday of March at 02:00

End Date: Last Sunday of October at 03:00

Offset: 1 hours

[Apply](#) [Reset](#)

54.3. Certificate

1. Go to "Configuration > Object > Certificates". You can create a new certificate using "Add".

- Enter a name for the new certificate, enter a host domain name for the ZyWALL (doesn't need to actually exist) and create a self-signed certificate with 2048 bit RSA.

- Certificate creation takes up to 5 minutes.
- Open the detailed data of the certificate using "Edit".

#	Name	SELF	CN	Issuer	Valid From	Valid To
1	default	SELF	CN=usg20_404A03752A6E	CN=usg20_404A03752A6E	2010-01-01 00:01:06 GMT	2029-12-27 00:01:06 GMT
2	zywall-aussens	SELF	CN=zywall-aussenstelle	CN=zywall-aussenstelle	2011-03-14 12:32:17 GMT	2014-03-13 12:32:17 GMT

- Copy the certificate in PEM format to the clipboard.

Edit My Certificates

Configuration

Name:

Certification Path

Certificate Information

Type:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	1300105937
Subject:	CN=zywall-aussenstelle
Issuer:	CN=zywall-aussenstelle
Signature Algorithm:	rsa-pkcs1-sha1
Valid From:	2011-03-14 12:32:17 GMT
Valid To:	2014-03-13 12:32:17 GMT
Key Algorithm:	rsaEncryption (2048 bits)
Subject Alternative Name:	zywall-aussenstelle
Key Usage:	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint:	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint:	13:94:b5:9d:db:e0:8d:5b:f5:f2:53:5f:8c:cf:db:e3
SHA1 Fingerprint:	bd:19:d6:40:60:a2:26:35:dc:6d:6f:46:a8:c5:15:6c:28:76:f7:87

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDADCCAeigAwIBAgIETX4K0TANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDEExN
eXdhbGwtYXVzc2Vuc3RlbGxlMB4XDTE0MDMxMzE0MDM0MDMxMzE0MDMxMzE0
N1owHjEcmBoGA1UEAxMTenI3YWxsLWFlc3NlbnN0ZWxsZTCwCAS1wDQYJKoZIhvcN
-----
```

Export Certificate Only

OK Cancel

- Paste the certificate from the clipboard into the Intra2net system under "System > Keys > Foreign keys".

Intra2net Business Server

Einstellungen

Name Zywall Aussenstelle

Schlüsseltyp ☐ RSA ☒ X.509

Copy & Paste Schlüssel

```

MIowHJECMB8oGA1UEAXMTenI3YWxsLWFlc3NidhN0ZWxsZlCCASjWDQYJKoZIhvc
AQEBBQADggEPADCCAQoCggEBANQnIKBe3vutpknP5WhxizUctw4RAgmsUrsEwy
e4VwILbCB6FMzCTJOlt7eJ55ObkzSZ+I7ASxRTYTq27IS96S0TTLp/cJyokM6s+H
xxYdd9pWEOGF1V5vgfQ0aUV1zMKwR0PWr27+aWqnIOE1YH3PAQYGo2BxuDLW2I
bLptIY7oLRoJPismWC4PwDq+Y0L5d81FpT+vO39ErgH8frWn0gxwt2QSEKX3IZ5n
yhHXc0nEhN/2Tn4tN665NLJWUue83WuURts8GB3NSf6CsOKbmv7V1DJsqBVKSY
qqqaAYS0uYco6oppttVassna1vB2dzO3Fct0YJ1s1H0rtx8CAwEAANgMEQwDgYD
VR0PAQH/BAQDAgKkMB4GA1UdEQQXMBWCE3p5d2FsbC1hdXNzZW5zdGVsbGU
VR0TAQH/BAQwBgEB/wIBATANBgkqhkiG9w0BAQUFAAOCAQEAY2ZGpR6AQedKd
mieuR11F4Y0ETPKhkfnm1mh+fjIDQy9sPimV65RL6ukZmokHIAhJRCI8JAayH4S
o5EDbSKJq4QxWTWGqLsn/LdZx6KL5iGU0leI0ytTeUr4BTOQqkEhwjSes92Cpnb
FjBM7KDt6vL4+Uctxy5WBRWwnOgeHYfB5aY8hu/W3Z1w+oUszJOAZzaEPqc0K
y/YX42df/a7ynpTWfGHI8aHTpC9RR3FA0BC9Im0SvgaFxmMxtFTDIP80Gyn6NQdJ
qihu12ZZjkvt3R1P8GwQ0bCdU4RPeGF72q5Yv92ZxwkyKTZ3fjb3tLlpWytjRiX
nGgJZg==
-----END X509 CERTIFICATE-----

```

Einstellungen speichern

- Under IPsec ID, select just the DNS host name, not the certificate holder ("/CN=" etc.).

Intra2net Business Server

Schlüssel

Einstellungen

Name Zywall Aussenstelle

Schlüsseltyp X.509

IPsec ID zywall-aussenstelle

Schlüssellänge /CN=zywall-aussenstelle

Fingerprint (MD5) 1394 8390 0B8E 8D5B F3FZ 535F 8CCF DBE3

Fingerprint (SHA1) BD19 D640 60A2 2635 DC6D 6F46 A8C5 156C 2876 F787

Inhaber (Subject) /CN=zywall-aussenstelle

Aussteller/CA (Issuer) /CN=zywall-aussenstelle

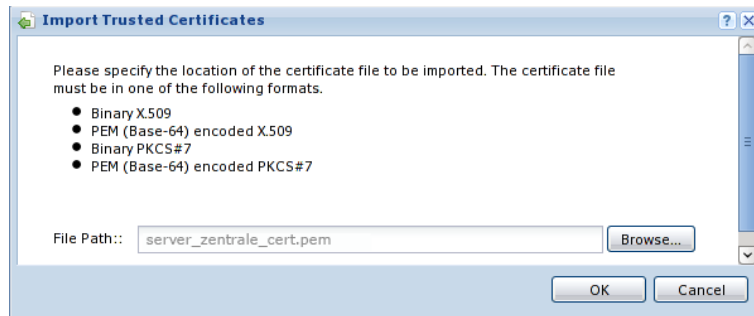
Gültig von 14.03.2011 13:32

Gültig bis 13.03.2014 13:32

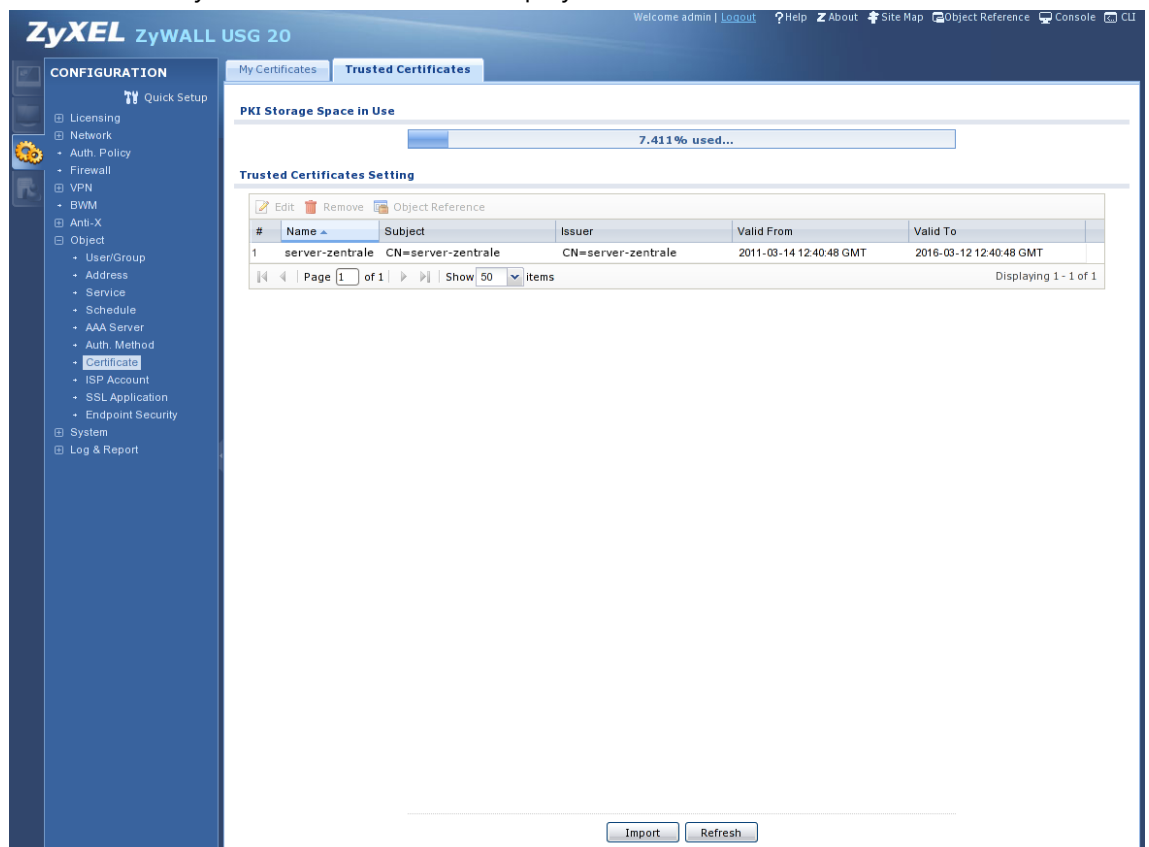
Einstellungen speichern

- Export your own certificate from the Intra2net system as a .pem file (Under "System > Keys > Own keys", Data tab).
- Import the Intra2net system certificate into ZyWALL, under the menu "Configuration > Object > Certificate", tab Trusted Certificates. Click "Import" below.

10. Select the directory in which you have saved the certificate of the Intra2net system.



11. The Intra2net system certificate is now displayed as a Trusted Certificate.



54.4. Connection

54.4.1. IKE / Phase 1

1. Open "Configuration > VPN > IPSec VPN" VPN Gateway tab. Create a new IKE connection to a peer with "Add".
2. Click "Show Advanced Settings" to see all of the necessary fields.
3. Enter the IP or DNS name of the Intra2net system as the peer gateway address. Even if the Intra2net system uses a dynamic IP with DynDNS, you must select "Static Address".
4. Specify the authentication on certificates and select the previously created certificate for the ZyWALL.

5. Select AES128 and SHA1 as Proposal, the matching "Key Group" is DH2.
6. If the Zywall or Intra2net system is located behind a NAT router, you need to enable "NAT Traversal".

Add VPN Gateway

Hide Advanced Settings

General Settings

☒ Enable
VPN Gateway Name: Zentrale

Gateway Settings

My Address

☒ Interface: wan1 (DHCP client -- 172.16.2.113/255.255.0.0)
☐ Domain Name / IP

Peer Gateway Address

☒ Static Address
Primary: zentrale.dyndns.org
Secondary: 0.0.0.0
☐ Dynamic Address

Authentication

☐ Pre-Shared Key
☒ Certificate: zywall-aussenstelle (See My Certificates)
Local ID Type: DNS
Content: zywall-aussenstelle
Peer ID Type: Any
Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)
Negotiation Mode: Main
Proposal:

#	Encryption	Authentication
1	AES128	SHA1

Key Group: DH2
☐ NAT Traversal
☒ Dead Peer Detection (DPD)

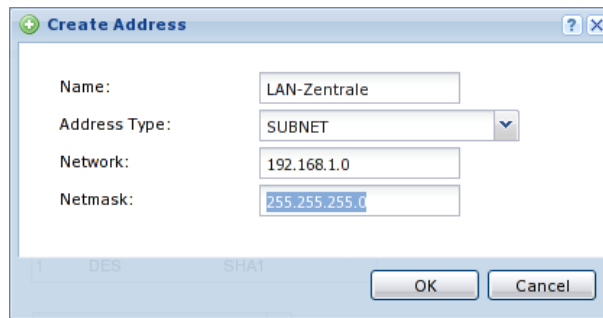
Extended Authentication

☐ Enable Extended Authentication
☒ Server Mode: default
☐ Client Mode
User Name:

OK Cancel

54.4.2. IPSec / Phase 2

1. Go to "Configuration > VPN > IPSec VPN" VPN Connection tab. Create a new IPSec connection with "Add".
2. Create a network object for the network of the peer. Use the "Create new Object > Address" menu. Use SUBNET as type and enter the network address and netmask.



Create Address

Name: LAN-Zentrale

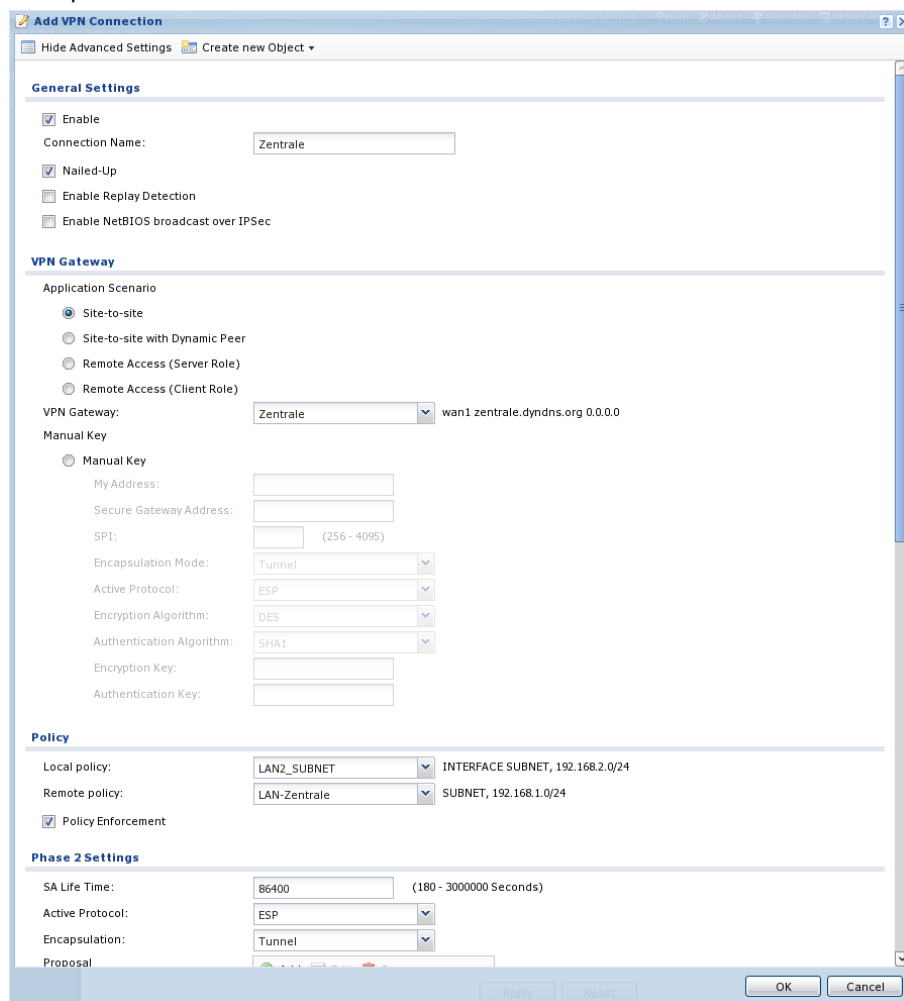
Address Type: SUBNET

Network: 192.168.1.0

Netmask: 255.255.255.0

OK Cancel

3. Click "Show Advanced Settings" to see all of the necessary fields.
4. Set the connection to Nailed Up so that ZyWALL keeps the connection open automatically.
5. Select Site-to-site and select the newly created IKE connection to the Intra2net system as gateway.
6. Select the network to be connected behind the Zywall as "Local policy". As "Remote Policy" select the network object you just created with the network of the Intra2net system.
7. Activate "Policy Enforcement" to ensure that the connection is secure against network manipulation.



Add VPN Connection

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: Zentrale

☒ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: Zentrale wan1 zentrale.dyndns.org 0.0.0.0

Manual Key

☐ Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

Policy

Local policy: LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24

Remote policy: LAN-Zentrale SUBNET, 192.168.1.0/24

☒ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

Apply Reset OK Cancel

8. Select "Proposal" AES128 and SHA1, set " Perfect Forward Secrecy (PFS)" to DH2.

Add VPN Connection

Hide Advanced Settings Create new Object

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	AES128	SHA1

Perfect Forward Secrecy (PFS): DH2

Connectivity Check

☒ Enable Connectivity Check

Check Method: icmp

Check Period: 5 (5-30 Seconds)

Check Timeout: 5 (1-10 Seconds)

Check Fail Tolerance: (1-10)

☐ Check This Address Domain Name or IP Address

☒ Check the First and Last IP Address in the Remote Policy

☐ Log

Inbound/Outbound traffic NAT

Outbound Traffic

☐ Source NAT

Source: Please select one ...

Destination: Please select one ...

SNAT: Please select one ...

Inbound Traffic

☐ Source NAT

Source: Please select one ...

Destination: Please select one ...

SNAT: Please select one ...

☐ Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port Start	Original Port End	Mapped Port Start	Mapped Port End
No data to display							

Page 1 of 1 Show 50 items

Apply Reset OK Cancel

The connection is now configured and should be established in the background.

ZyXEL ZyWALL USG 20

Welcome admin | Logout ? Help ? About ? Site Map ? Object Reference ? Console ? CLI

CONFIGURATION

Quick Setup

- Licensing
- Network
- Auth. Policy
- Firewall
- VPN
 - IPSec VPN
 - SSL VPN
- BWM
- Anti-X
- Object
- System
- Log & Report

VPN Connection VPN Gateway

Global Setting

☒ Use Policy Route to control dynamic IPsec rules

☐ Ignore "Don't Fragment" setting in packet header

Configuration

#	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1	🟡	Zentrale	Zentrale	TUNNEL	AES128/SHA1	LAN2_SUBNET/LAN-Zer

Page 1 of 1 Show 50 items

Displaying 1 - 1 of 1

Apply Reset

54.5. Intra2net System

On the Intra2net system, the connection must also be configured accordingly. For VPN routers, this is described in 53. Chapter, „Connecting Complete Networks“.

54.6. Logs

ZyWALL logs all VPN events. These protocols can be viewed in the "Monitor > Log" menu. For phase 1 events, select `IKE` as the display filter, and `IPSec` for phase 2.

The screenshot shows the ZyXEL ZyWALL USG 20 web interface. The left sidebar contains the 'MONITOR' menu with options: System Status, VPN Monitor (selected), Anti-X Statistics, and Log. The main area is titled 'View Log' and includes a 'Show Filter' button. Below this, the 'Logs' section has a 'Display:' dropdown set to 'IKE'. There are buttons for 'Email Log Now', 'Refresh', and 'Clear Log'. A table of logs is displayed with columns: #, Time, Prior, Categ, Message, Source, Destination, and Note. The logs show various IKE events, including cookie pair generation, tunnel establishment, and rekeying. A red box highlights the 'Destination' column for log entry 15, showing the IP address 172.16.2.113.500.

#	Time	Prior	Categ	Message	Source	Destination	Note
3	2011-03-14 14:17:58	info	IKE	Recv:[HASH][DEL]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
4	2011-03-14 14:17:58	info	IKE	The cookie pair is : 0xeb1b43faef447338 / 0x932d547e21aa6cd3	172.16.1.147.500	172.16.2.113.500	IKE_LOG
5	2011-03-14 14:17:58	info	IKE	Send:[HASH][DEL]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
6	2011-03-14 14:17:58	info	IKE	Tunnel [Zentrale:Zentrale:0xc4366098] is disconnected	172.16.2.113.500	172.16.1.147.500	IKE_LOG
7	2011-03-14 14:17:58	info	IKE	The cookie pair is : 0x932d547e21aa6cd3 / 0xeb1b43faef447338 [count=2]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
9	2011-03-14 14:17:29	info	IKE	Tunnel [Zentrale:Zentrale:0xc4366098] rekey successfully	172.16.2.113.500	172.16.1.147.500	IKE_LOG
10	2011-03-14 14:17:29	info	IKE	[ESP aes-cbc hmac-sha1-96][SPI 0xcc409b00][0xc4366098][PFS DH2][Lifetime 3600]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
11	2011-03-14 14:17:29	info	IKE	[Responder:172.16.2.113][Initiator:172.16.1.147][Policy: ipv4(192.168.2.0-192.168.2.255)-ipv6(192.168.2.0-192.168.2.255)]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
12	2011-03-14 14:17:29	info	IKE	Recv:[HASH]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
13	2011-03-14 14:17:29	info	IKE	Send:[ID][CERT][SIG]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
14	2011-03-14 14:17:26	info	IKE	Recv:[ID][CERT][SIG]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
15	2011-03-14 14:17:26	info	IKE	Tunnel [Zentrale:Zentrale:0xc4366098] built successfully	172.16.2.113.500	172.16.1.147.500	IKE_LOG
16	2011-03-14 14:17:26	info	IKE	[ESP aes-cbc hmac-sha1-96][SPI 0xcc409b00][0xc4366098][PFS DH2][Lifetime 3600]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
17	2011-03-14 14:17:26	info	IKE	[Initiator:172.16.2.113][Responder:172.16.1.147][Policy: ipv4(192.168.2.0-192.168.2.255)-ipv6(192.168.2.0-192.168.2.255)]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
18	2011-03-14 14:17:26	info	IKE	Send:[HASH]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
19	2011-03-14 14:17:26	info	IKE	Recv:[HASH][SA][NONCE][KE][ID][ID] [count=2]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
20	2011-03-14 14:17:26	info	IKE	Recv:[KE][NONCE]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
21	2011-03-14 14:17:26	info	IKE	Send:[HASH][SA][NONCE][KE][ID][ID] [count=2]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
22	2011-03-14 14:17:26	info	IKE	Phase 1 IKE SA process done [count=2]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
23	2011-03-14 14:17:26	info	IKE	Recv:[ID][CERT][SIG]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
24	2011-03-14 14:17:26	info	IKE	Send:[SA][VD][VD][VD][VD][VD]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
25	2011-03-14 14:17:26	info	IKE	The cookie pair is : 0x932d547e21aa6cd3 / 0xeb1b43faef447338 [count=3]	172.16.2.113.500	172.16.1.147.500	IKE_LOG

55. Chapter - VPN with Lancom Routers

55.1. Overview

VPN-capable routers from Lancom with LCOS version 6 and higher can establish connections with certificates and are compatible with the Intra2net system. This manual was written for version 8.84. However, experience has shown that the VPN configuration is not changing significantly over most versions.

55.2. Certificate for the Lancom device

1. Download the "Tool to create certificates" (makecert) from the Intra2net system under Information > Download, and unpack it into a directory on your computer.
2. Lancom routers cannot create its own certificates. This is therefore done by makecacert on a PC. Start the makecacert.bat batch file

```
C:\makecert>makecacert
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -config
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

3. Now enter the router data. For some fields there is a default value in square brackets. If you want to use it, just press Return. Do not use umlauts or other special characters, as otherwise problems may occur. The "common name" (or "computer name" on the Intra2net system) must be unique and must not be reused for other clients or for a CA.



Tip

It is recommended to enter as little data as possible here (e.g. only the common name), as these must be entered again identically when configuring the connection.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:lancom
Email Address []:
```

```
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem
-out newcert.p12
Loading 'screen' into random state - done
```

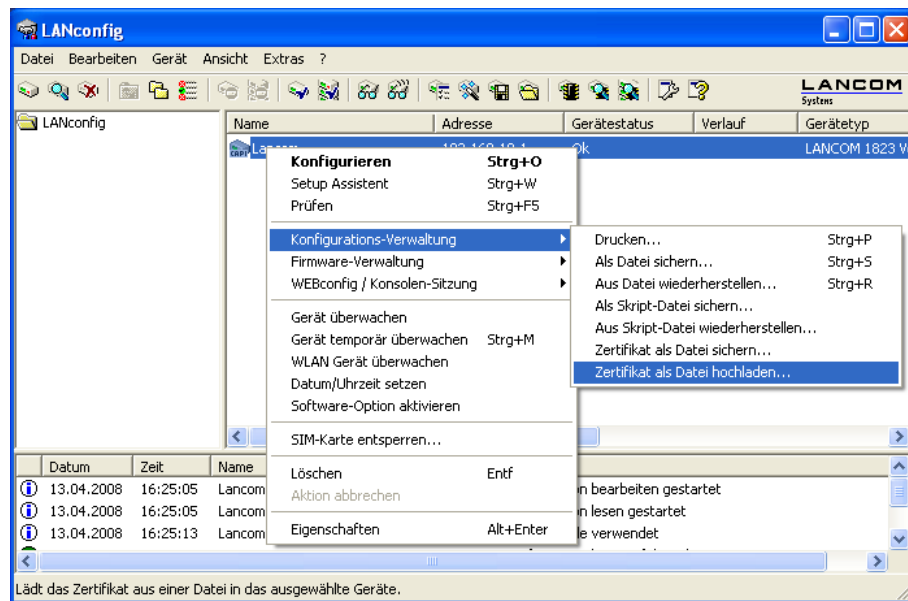
4. Select an export password that protects the key file on the way to the router. The password must be at least 3 characters long.

Enter Export Password:

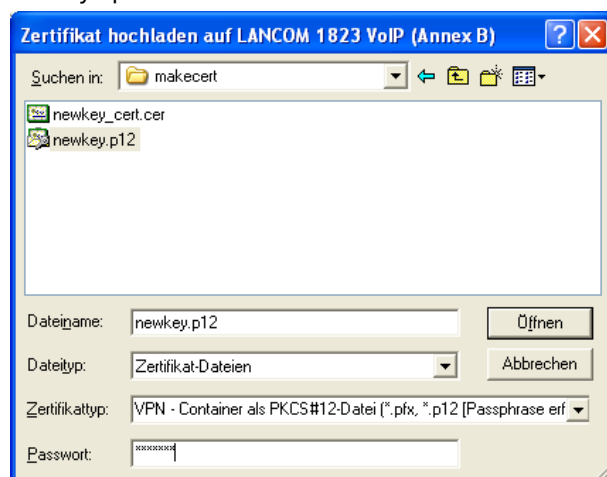
Verifying password - Enter Export Password:

```
C:\makecert>del privatekey.pem
```

5. Start the LANconfig program to configure the router. The router must be recognized by LANconfig.
6. Open the context menu "Configuration Management", and submenu "Upload Certificate or File".



7. Select the `newkey.p12` file you just created with the `makecert` program. Set the certificate type to "VPN - Container as PKCS#12 file" and enter the export password previously specified.

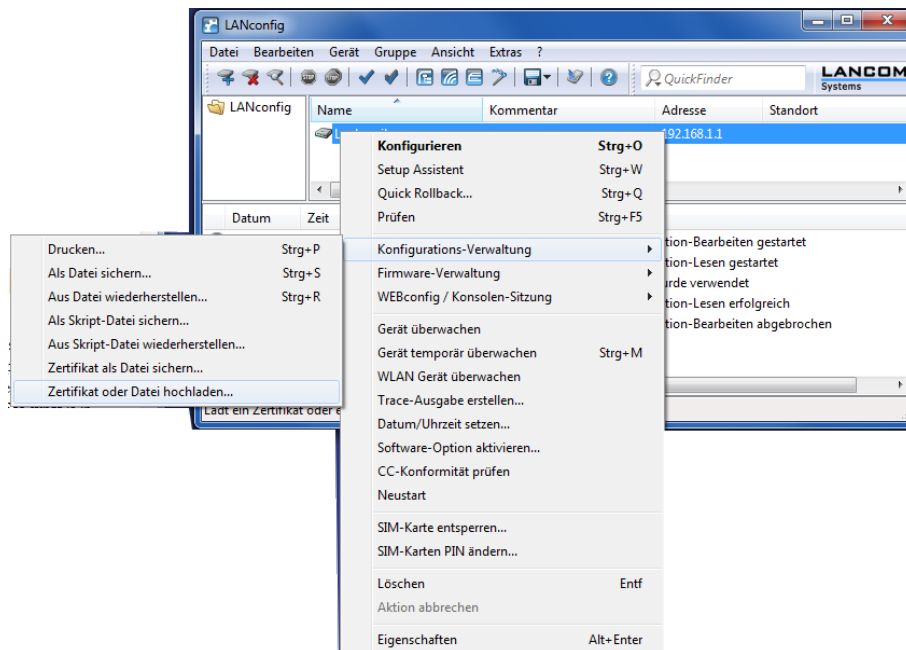


8. Open the certificate file (`newkey_cert.cer`) with a text editor (e.g. Wordpad) and copy the entire contents of the file to the clipboard. In the Intra2net system open the menu System > Keys > Foreign keys and create a new key. Enter a name for the key (e.g. the

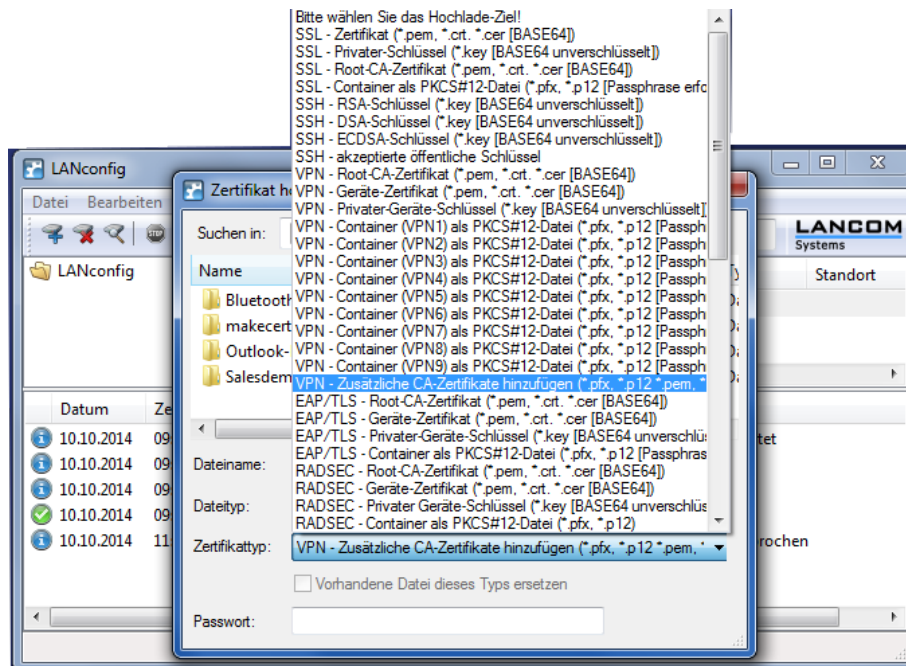
name of the router) and then paste the certificate data from the clipboard into the field "Copy & paste certificate".

55.3. Certificate for the Intra2net System

1. The Lancom router requires a special configuration of the Intra2net system certificate. Since version 8 of the LCOS firmware, self-signed keys have not been accepted, only certificates signed by an independent CA. The following shows how such a key can be generated and signed on the Intra2net system.
2. Firstly, the certificate must be created for the CA: In the Intra2net system, open System > Keys > Own Keys : Data. Click on the menu item "New" to start key creation. The certificate is only used to sign the actual encryption certificates, so we call it **server-ca** (to be entered in the "Name" and "Host name (CN)" fields).
3. This CA certificate must now be given to the Lancom router. To do this, export it from the Intra2net system using the "as .pem" option. Then in LANconfig, open the context menu "Configuration Administration" of the relevant device. Select the option "Upload certificate or file".



Select the .pem file just created and upload it as the certificate type "VPN - Add additional CA certificates".

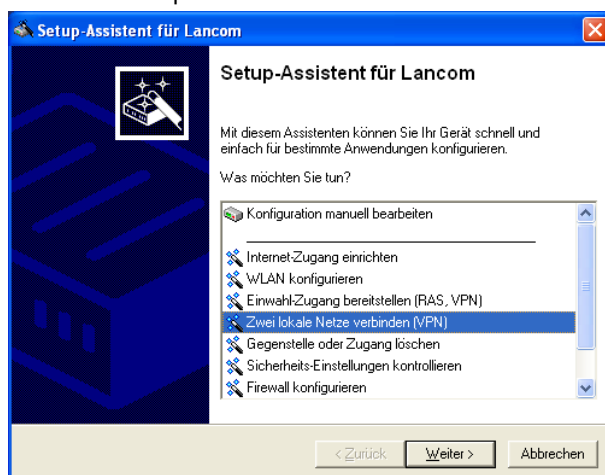


4. Now return to the Intra2net system under System > Keys > Own Keys : Data. Create another key as the foundation for the VPN certificate. Please note that the value in the "Computer Name (CN)" field (i.e. the "Common Name" of an SSL certificate) is later entered into the Lancom router exactly, without tolerance for deviations. Therefore, make sure that you do not make any typos at this point!
5. Now go to the System > Keys > Own Keys : CA menu on the Intra2net system and select the recently created VPN key. In the "Sign keys with other key" section, select the CA key created in the previous steps (**server-ca**) and then click "Sign".

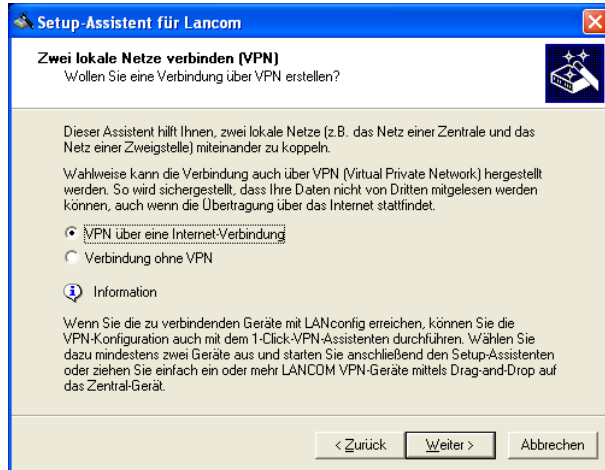
Now check the value "Issuer/CA" under System > Keys > Own Keys : Data. The data specified when the CA certificate was created should be summarized in this field. (If you follow the above example, this field contains the string **CN=server-ca**. The key can now be used to establish a VPN connection.

55.4. Connecting

1. Start the setup wizard and select "Connect two local networks (VPN)".



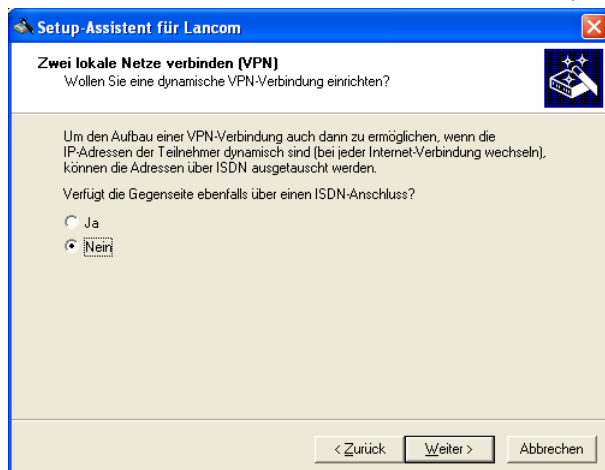
- The VPN connection should run over an Internet connection.



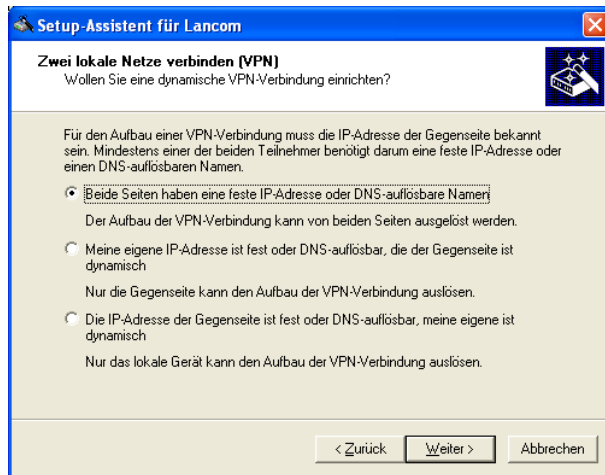
- The VPN type must be left at IPSec.



- Do not use an ISDN connection, as a Lancom protocol is used instead.

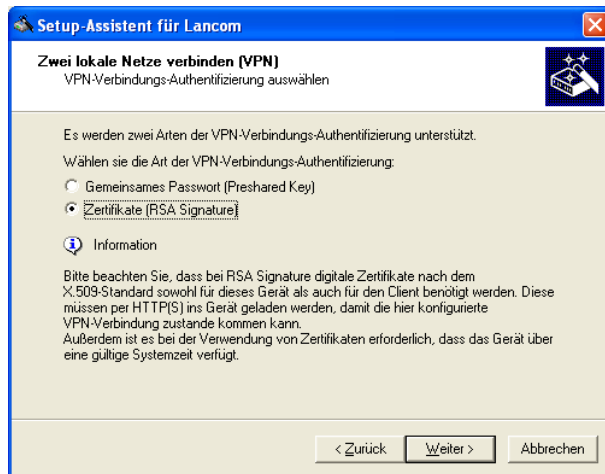


- The connection is established via static IP addresses or DynDNS names.

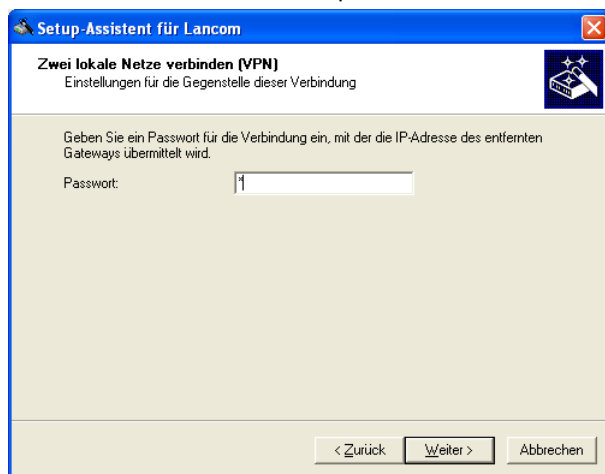


6. Give a name to both your own side and to the peer side. The name is not relevant for the connection, it just needs to be unique.

7. Use certificates (RSA) to authenticate the connection.

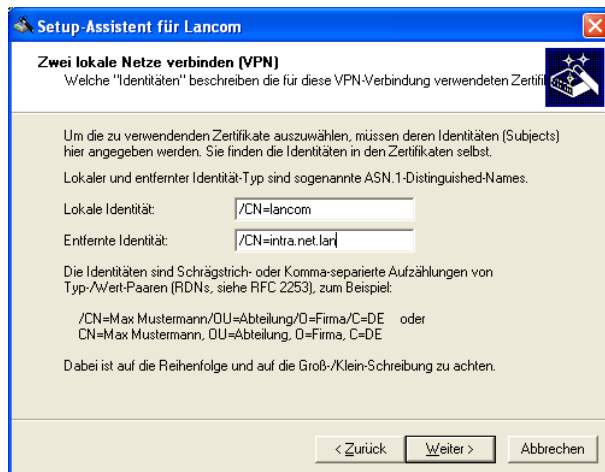


8. Enter a password of your choice. This password is not required as it would only be used for the Lancom ISDN protocol which is not used here.

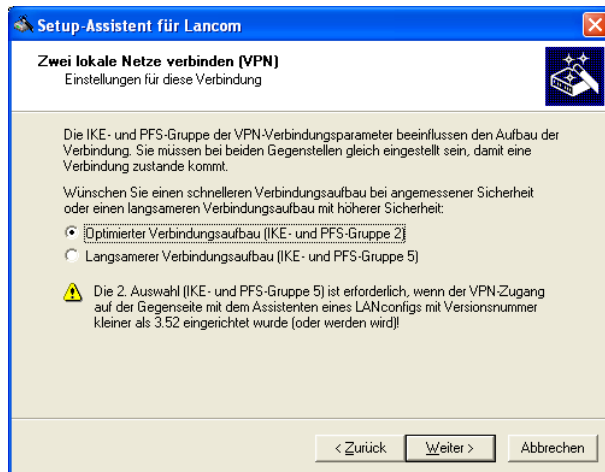


9. Enter the identity (= owner) of the certificates for your own (Lancom) and remote (Intra2net System) side. The data for the Distinguished Names can be found e.g. on the Intra2net system under System > Keys > Own or Foreign Keys, respectively in the field

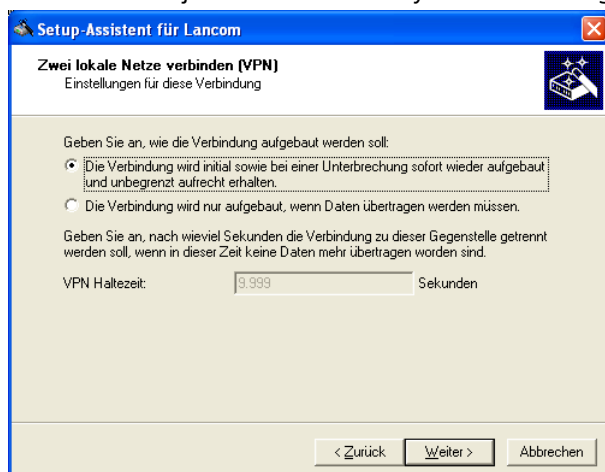
"Owner (Subject)". The individual data groups must be entered in the reverse order as shown in the Intra2net system.



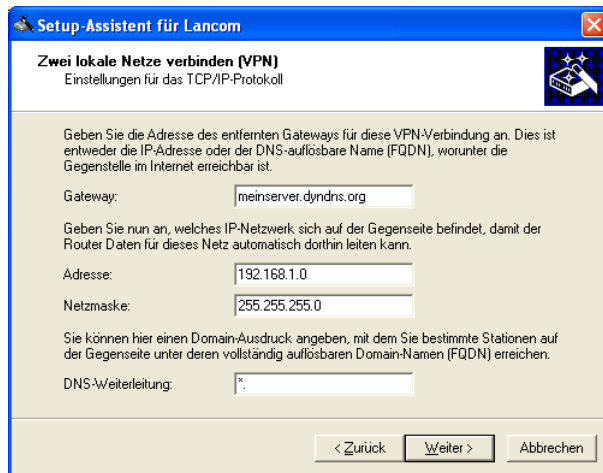
10. Use the optimized connection setup (IKE and PFS group 2).



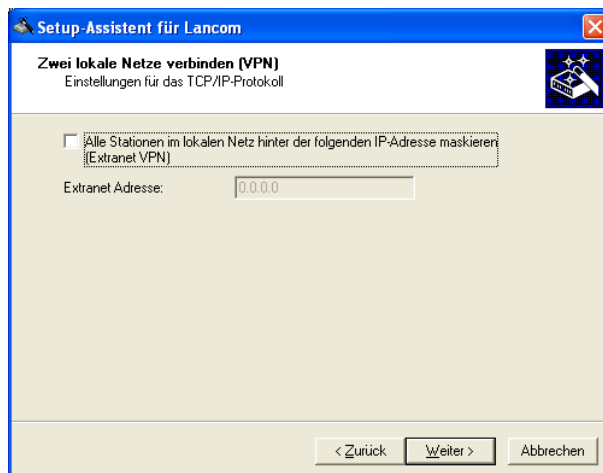
11. You can either leave the connection open at all times, or start it only when necessary. It is best to adjust the Intra2net system accordingly.



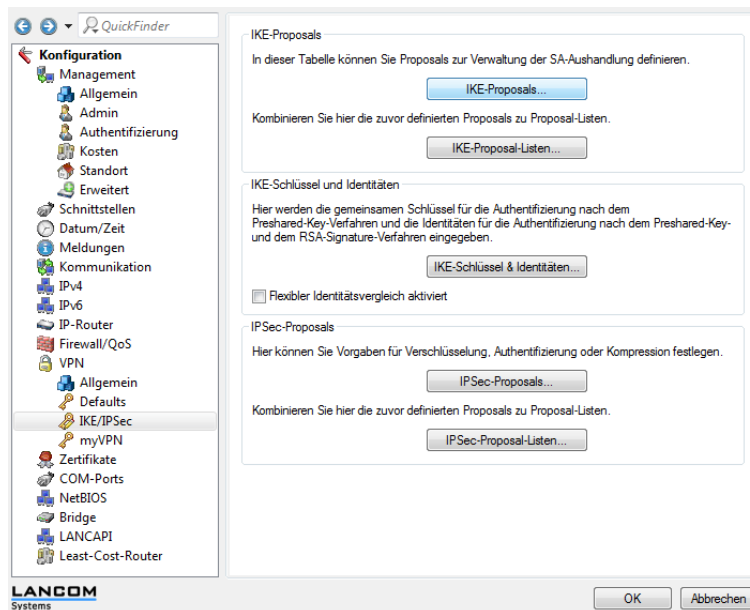
12. Enter the static IP or the DynDNS name of the Intra2net system as "Gateway" (in the example **myserver.dyndns.org**). Then enter the IP and netmask of the network behind the Intra2net system, in the example **192.168.1.0 / 255.255.255.0**.



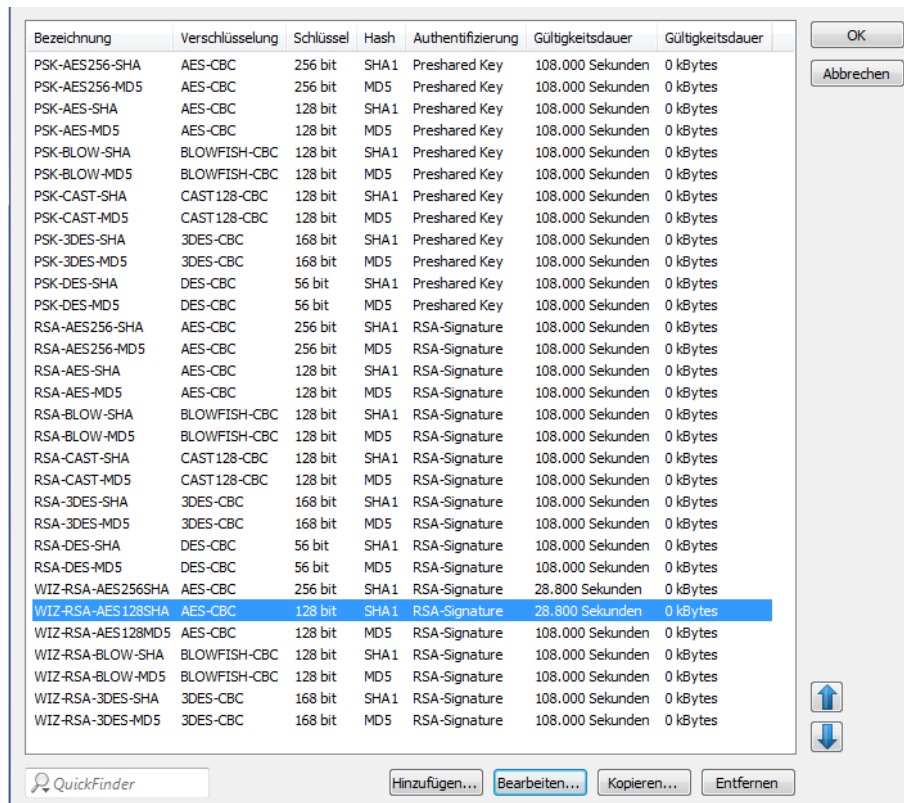
13. The Lancom router can transfer all IPs of its own network to a single address via NAT. This may be beneficial if the same network area is used on both sides. Leave this function disabled if in doubt.



14. In any case, deactivate the NetBIOS option. It is based on a proprietary Lancom protocol and prevents the connection from being established. It is usually no longer needed because modern Windows file servers use CIFS over IP.
15. Close the wizard and start configuring the router without the wizard. Go to "VPN"-Settings, "IKE-Param." tab and click "IKE-Proposals".



16 Edit the IKE proposal with the name "WIZ-RSA-AES128SHA".



17. Enter a value that is less than 86400 for the validity period, as this is the maximum value that the Intra2net system accepts. It is recommended to use 28800 here. This corresponds to the standard lifetime for IKE/Phase 1 of 480 minutes in the Intra2net system.

The screenshot shows a configuration window with the following fields and options:

- Bezeichnung:** WIZ-RSA-AES128SHA
- Verschlüsselung:** AES-CBC
- Schlüssel-Länge:** 128 bit
- Hash:** SHA1
- Authentifizierung:** RSA-Signature
- Text:** Hier können Sie die Gültigkeitsdauern der mit diesem Proposal ausgehandelten Verbindungen definieren.
- Gültigkeitsdauer:** 28.800 Sekunden, 0 kBytes
- Buttons:** OK, Abbrechen

55.5. Intra2net System

On the Intra2net system, the connection must also be configured correctly. For VPN routers, this is described in 53. Chapter, „Connecting Complete Networks“.

55.6. Deleting Certificates

If a previously installed certificate has the same ID as a new certificate, conflicts may occur. In this case the previous certificate must be deleted. VPN connections can be deleted from the Lancom router on the configuration interface when no longer required. Certificates cannot be deleted using the normal interface.

One possibility is to save the configuration, reset the router completely and then restore the configuration. In this case, however, all certificates are deleted.

The other way is by using the command line via Telnet or SSH. Go to the certificate directory with `cd /Status/File-System/Contents`. Display the contents of the directory with the `ls` command. Various certificates are displayed, such as `vpn_rootcert`, `vpn_add_cas` and `vpn_pkcs12`. You can use the `del vpn_add_cas` command for example, to delete the certificate of the peer.

56. Chapter - VPN with Linux

56.1. Overview

To establish a VPN connection with a Linux peer, one of the two software packages `openswan` or `strongswan` is required. For most current versions, one of the packages should be pre-installed or available through the package manager. The documentation for that version should explain how to check whether one of the packages is already installed, and if necessary, how to install it.

56.2. Generating Certificates

1. Open a terminal / command line and log in as the root user. Normally, this is done using the `su` command.
2. Enter the following command in one line:

```
openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -outform PEM -
keyform PEM -keyout /etc/ipsec.d/private_key.pem -out /etc/ipsec.d/cert.pem
```

3. The key pair is calculated and the system will request the certificate data. The entered values are not relevant in this function, they only have to be unique on all systems connected by VPN. We advise against using special characters such as accents or umlauts.

```
Generating a 2048 bit RSA private key
.....
.....+++.....
writing new private key to 'private_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:DE
State or Province Name (full name) [Berkshire]:BW
Locality Name (eg, city) [Newbury]:Tuebingen
Organization Name (eg, company) [My Company Ltd]:Intra2net
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:MyComputerName
Email Address []:
```

4. The certificate is now valid for 2 years (730 days) and is located in the `/etc/ipsec.d/cert.pem` file. The private key is in the `/etc/ipsec.d/private_key.pem` file. To modify the validity period, use the `-days` parameter in the command line.
5. Open the `/etc/ipsec.d/cert.pem` file, copy the content to the clipboard and import it into the Intra2net system under System > Key > Foreign keys.
6. In the Intra2net system, navigate to System > Keys > Own Keys : Data. Select the appropriate certificate and export it to a file using the "Export certificate" menu item. Save it to the Linux computer, e.g. to `/etc/ipsec.d/intra2netserver.pem`.

56.3. Configuring Connections

1. Display the content of the `/etc/ipsec.conf` file. It should contain the line `include /etc/ipsec.d/*.conf`. It must not begin with the `#` character, otherwise it will be commented out.
2. Display the content of the `/etc/ipsec.secrets` file. It should contain the line `include /etc/ipsec.d/*.secrets`. It also should not begin with the `#` character.
3. Select a name for the connection. It should not contain any special characters or spaces. In this example `intra2netserver` is used.
4. Create a file called `/etc/ipsec.d/intra2netserver.conf` (or your connection name) and open it in a text editor (e.g. nano or vi).
5. The configuration file starts with the line `conn intra2netserver` (or your connection name). It is important that all subsequent lines must be indented with spaces or tabs. Blank lines are not allowed, or with at least one (indented) `#` character must be used, as with comments.
6. Enter the information for the connection as in the following example:

```
conn intra2netserver
    auto=start
    keyingtries=0
    type=tunnel
    auth=esp
    authby=rsasig
    ike=aes128-sha-modp1024!
    esp=aes128-sha1!
    pfs=yes
    ikelifetime=480m
    keylife=60m
    rekey=yes
    #
    # left: our side
    left=%defaultroute
    leftid="/C=DE/ST=BW/L=Tuebingen/O=Intra2net/CN=MeinRechnerName"
    lefttrsasigkey=%cert
    leftcert=/etc/ipsec.d/cert.pem
    leftsubnet=192.168.10.0/24
    leftfirewall=yes
    #
    # right: intra2net system side
    right=mein-server.dyndns.org
    rightid="/CN=intra.net.lan"
    righttrsasigkey=%cert
    rightcert=/etc/ipsec.d/intra2netserver.pem
    rightsubnet=192.168.1.0/24
```

The meanings of the entries are briefly explained below. Entries beginning with `left` represent the local side, those beginning with `right` represent the remote side (in this case the Intra2net system). All entries that are not explained separately should be accepted as they appear.

auto	With add , the connection is only loaded, with start , the connection is established automatically.
------	---

keyingtries	How often the connection should be attempted until it is aborted due to an error. 0 represents unlimited.
ike	Encryption algorithm for phase 1: The combination used must be specified in the encryption profile of the Intra2net system.
esp	Encryption algorithm for phase 2: The combination used must be specified in the encryption profile of the Intra2net system.
pfs	Enables/Disables Perfect Forward Secrecy
ikelifetime	Lifetime of phase 1 (IKE)
keylife	Lifetime of phase 2 (IPSec)
left/right	IP address or DNS name. For the local side %defaultroute . If there is a static IP, always enter the IP and not an available DNS name.
leftid/rightid	IPSec-Id of the corresponding side in quotation marks. Enter the certificate owner data as shown in the key menu of the Intra2net system.
leftcert/rightcert	File name of the corresponding side's certificate
leftsubnet/rightsubnet	Network with a netmask on the corresponding side. If only the external IP is to be connected via VPN on the Linux (left) side, omit the leftsubnet parameter and set the "network on remote side" to "external IP" on the Intra2net system.
leftfirewall	yes will automatically attempt to open the local firewall for the VPN connection. This only works if the firewall has not been heavily modified.

7. Create a file called `/etc/ipsec.d/intra2netserver.secrets` (or your connection name) and open it in a text editor (e.g. nano or vi).
8. The file must reference the file name of the private key:


```
: RSA /etc/ipsec.d/private_key.pem
```
9. In most cases, it will be necessary to tell the IPSec service to restart in order to reload the configuration files. This is typically done by using `/etc/init.d/ipsec restart`.
10. If the connection is set to start automatically, it will now be established in the background. If it is to be started manually, it can be done with `ipsec auto --up intra2net-server` (or your connection name).

Connection setup protocols can be found in one of the system's log files using `pluto` service identifier. In most cases `/var/log/secure`, for current versions.

56.4. Intra2net System

The connection must also be configured accordingly on the Intra2net system. For VPN routers, this is described in 53. Chapter, „Connecting Complete Networks“.

57. Chapter - Solving IP Address Conflicts in VPNs Through NAT

57.1. The Problem

All IP communication is based on the assumption that IP addresses are uniquely assigned and that no two clients or networks use the same IPs. However, since IPv4 addresses are scarce, addresses from the 192.168.0.0/16, 172.16.0.0/12 and 10.0.0.0/8 ranges are normally used in local networks for this purpose. Since everyone can freely choose their addresses from these areas, conflicts can easily occur.

If two networks with the same or overlapping IPs are to be connected via VPN, the IPs are no longer unique and the VPN will not function.

To solve this problem, the Intra2net system offers the facility to rewrite IPs at input and output from the VPN (Network Address Translation, NAT). This means that the peer can always be reached via a different network range. The addressing is once again unique and the conflict is resolved.

57.2. Configuration

For each VPN connection, you can define individual settings for address changes in the Tunnel tab, under Services > VPN > Connections.

Rewrite local IPs	<p>The local network of the Intra2net system is rewritten to another IP area, which is transmitted to the peer. It must therefore be registered on the peer as a network behind the Intra2net system.</p> <p>The "on free IP" option combines the selected local network into a single IP, from the perspective of the peer. Therefore, connections within the VPN can only be initiated from the local network, not from the peer.</p> <p>The "1:1 on free net" option rewrites the selected local network to the perspective of the peer. The 1:1-NAT indicates that the 1st IP of the real network is rewritten to the first of the NAT network, the 2nd IP to the 2nd, and so on.</p>
Rewrite remote IPs 1:1 to network	<p>If active, the peer's network can be reached using the network specified here (see "Peer Network"). This definition is only valid for the local network of the Intra2net system and is not visible from the peer. Only the network specified under "Peer Network" is sent to the peer during connection setup.</p>
Rewrite remote addresses for Internet access (NAT)	See Section 45.4.4, „Configuring the Tunnel“

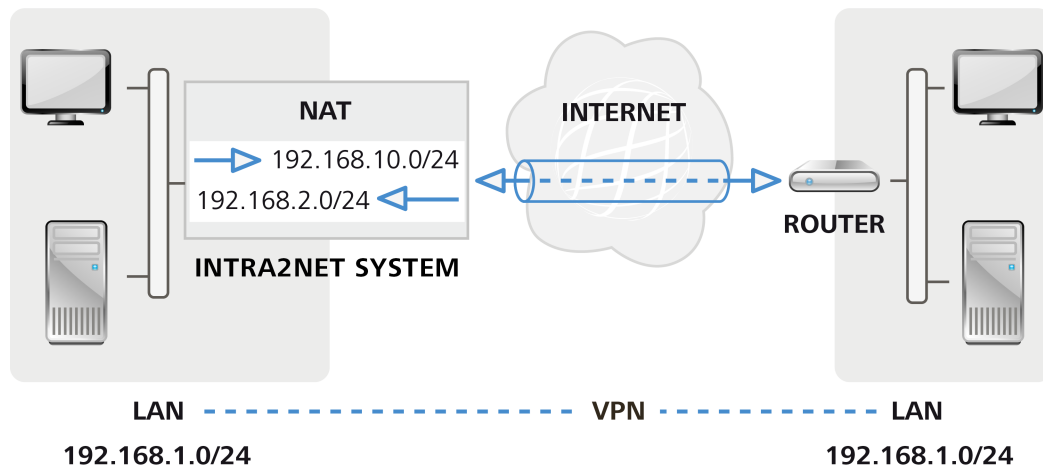
57.3. Same IPs on LAN and Peer

The local network of the Intra2net system and the peer use an identical or at least overlapping network area. In this example it is 192.168.1.0/24.

To resolve the address conflict, the local network of the peer is rewritten to 192.168.10.0/24. If a client from the LAN of the Intra2net system wants to reach the peer, it must address the corresponding IP in the network 192.168.10.0/24 instead of 192.168.1.0/24.

At the same time, the LAN of the Intra2net system can be reached by the peer on 192.168.2.0/24.

Both address conversions take place on the Intra2net system, the peer does not participate. If an Intra2net system is used on both sides of the VPN, the address conversion may only be set on one side.



57.3.1. Implementation

Intra2net Business Server

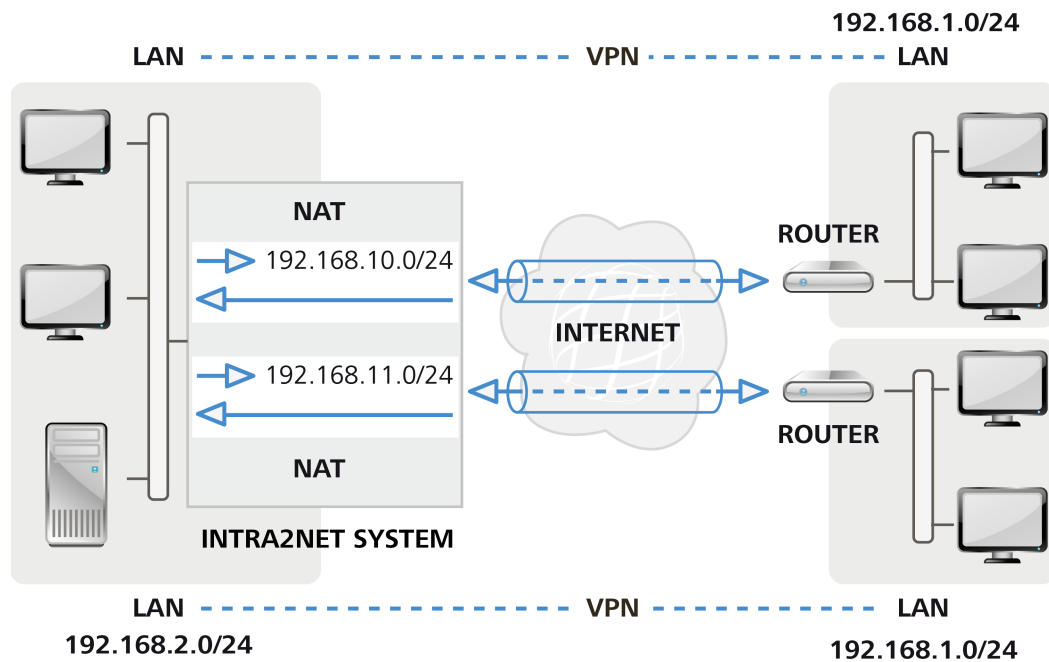
The screenshot shows the Intra2net Business Server configuration interface. The left sidebar contains a menu with options: Mainpage, Usermanager, Network, Services (Email, Emailfilter, Proxy, Fax, DynDNS, VPN), Connections, Encryption, Settings, Time sync, Monitoring, System, Information, and Groupware. The main content area is divided into tabs: Connection, Settings, Authentication, Tunnel, Rights, and Activation. The 'Tunnel' tab is selected, showing the 'Local network' and 'Remote network (sent to peer)' settings. The 'Local network' is set to 'Local networks' with a dropdown menu showing '192.168.1.0 / 255.255.255.0'. The 'Remote network (sent to peer)' is set to 'Custom net' with a dropdown menu showing '192.168.1.0 / 255.255.255.0'. The 'Address translation (NAT)' section is expanded, showing 'Rewrite local IPs (sent to peer)' set to '1:1 to network' with a dropdown menu showing '192.168.2.0 / 255.255.255.0'. The 'Rewrite remote IPs 1:1 to network' checkbox is checked. The 'Rewrite remote addresses for internet access (NAT)' checkbox is unchecked. A 'Save settings' button is at the bottom right.

57.4. Multiple Peers with the Same IPs

VPNs to multiple peers should be set up simultaneously from an Intra2net system. For example, for remote maintenance of various customers or locations. Multiple peers use the same IP network, in this example 192.168.1.0/24.

If the LAN of the Intra2net system does not overlap with any network of the peers, it is not necessary to rewrite the local IPs of the Intra2net system.

For each VPN connection to one of the peers, the peer network is rewritten to another network (in the example 192.168.10.0/24 and 192.168.11.0/24). This means that each of these peers can be addressed by unique IPs.



57.4.1. Implementation

Intra2net Business Server

Mainpage Usermanager Network Services Email Emailfilter Proxy Fax DynDNS VPN **Connections** Encryption Settings Time sync Monitoring System Information Groupware

Connection Settings Authentication Tunnel Rights Activation

Customer A Customer B

New Delete Copy

Local network

☐ Current internet IP or IPs of the system in the LAN

☒ Local networks 192.168.2.0 / 255.255.255.0

☐ Custom net

Netmask

Everything (0.0.0.0/0.0.0.0)

Remote network (sent to peer)

☐ External IP

☒ Custom net

192 168 1 0

Netmask

255 255 255 0

☐ Assign IP (mode-config)

Address translation (NAT)

Rewrite local IPs (sent to peer)

☒ unmodified

☐ to one IP

☐ 1:1 to network

Rewrite remote IPs 1:1 to network

☒ 192 168 10 0

Rewrite remote addresses for internet access (NAT)

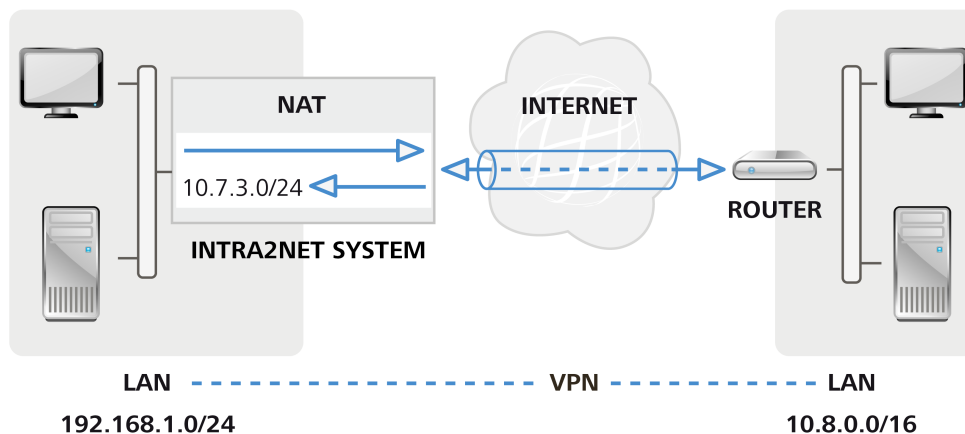
☐

Save settings

57.5. Local IPs Defined by Service Provider for Remote Maintenance

A service provider should be able to remotely maintain certain systems on the LAN. For this purpose, a VPN is established between the service provider's network (10.8.0.0/16 in the example) and the LAN. To avoid conflicts with the service provider, the service provider specifies a certain network area for the LAN, in this case 10.7.3.0/24.

However, the local network is already configured to another network, in the example 192.168.1.0/24, so that the local network does not have to be completely converted, the local network is rewritten to the specified IPs for this one VPN connection.



57.5.1. Implementation

Intra2net Business Server

The screenshot displays the Intra2net Business Server web interface. The sidebar on the left contains the following navigation links: Mainpage, Usermanager, Network, Services (Email, Emailfilter, Proxy, Fax, DynDNS, VPN), Connections (Encryption, Settings, Time sync, Monitoring), System, Information, and Groupware. The 'Connections' link is highlighted.

The main content area has tabs for Connection, Settings, Authentication, Tunnel, Rights, and Activation. The 'Tunnel' tab is selected. The 'Connection' sub-tab is active, showing a list of connections with a 'Branch' column and buttons for 'New', 'Delete', and 'Copy'.

The 'Local network' section has three radio buttons: 'Current internet IP or IPs of the system in the LAN', 'Local networks' (selected), and 'Custom net'. The 'Local networks' option shows a dropdown menu with the value '192.168.1.0 / 255.255.255.0'. The 'Custom net' option has input fields for IP and Netmask.

The 'Remote network (sent to peer)' section has three radio buttons: 'External IP', 'Custom net' (selected), and 'Assign IP (mode-config)'. The 'Custom net' option shows input fields for IP and Netmask.

The 'Address translation (NAT)' section has two radio buttons: 'unmodified' and 'to one IP'. The 'to one IP' option is selected, showing input fields for IP and Netmask. The '1:1 to network' option is also selected, showing input fields for IP and Netmask.

The 'Rewrite remote IPs 1:1 to network' section has a checkbox that is unchecked.

The 'Rewrite remote addresses for internet access (NAT)' section has a checkbox that is unchecked.

A 'Save settings' button is located at the bottom right of the configuration area.

58. Chapter - Error Diagnosis

58.1. Reading Logs

Unfortunately, we are not aware of an IPSec system that issues easy-to-understand error messages to the user. Therefore, as soon as an error occurs within a VPN connection, you have to analyze the log files and deduce the error from them. In many cases, the actual error is only logged on one side of the connection, the other side only receives a general error message such as "INVALID_ID". For this reason, it is often necessary to analyze the log files of both sides.

On the Intra2net system, the log data of the IPSec connections can be found in the messages log file (Information > System > Logfiles) and are marked by date and time with "pluto". Where to find the log files on other devices should be documented in their manual. Often, logging of IPSec events must also be activated before data is actually collected.

The first step in analyzing an error is to determine which phase of the connection the error occurs in.

58.2. The Protocol Format of the Intra2net System

An example of a line from a system log file:

```
Nov  5 10:54:40 intra pluto[2332]: "C2"[1] 192.168.1.200 #1:
    responding to Main Mode from unknown peer 192.168.1.200
```

Nov 5 10:54:40	Date and time of the event
intra	Hostname of the Intra2net System
pluto[2332]	ID and process ID of the IPSec service
C2	Identification of the connection; is not always correct at first. The more data the system receives, the more accurate it becomes. The list of connection identifiers can be found under Information > System > VPN.
192.168.1.200	The IP of the peer. Only displayed for the connection type "Dynamic IP"
responding to ...	Notification

58.3. Error in Phase 1

Errors in phase 1 usually mean an incorrect authentication configuration (e.g. incorrectly configured certificates or a different IPSec ID used) or in rare cases, incorrectly configured encryption algorithms.

At the beginning of each connection, the peers typically exchange information about their capabilities and recognize whether the connection is NAT:

```
packet from 192.168.1.200:500: received Vendor ID payload [draft-ietf-
ipsec-nat-t-ike-00]
packet from 192.168.1.200:500: received Vendor ID payload [draft-ietf-
ipsec-nat-t-ike-02_n]
responding to Main Mode from unknown peer 192.168.1.200
ignoring Vendor ID payload [47bbe7c993f1fc13b4e6d0db565c68e50102010...]
```

```
ignoring Vendor ID payload [da8e937880010000]
received Vendor ID payload [Dead Peer Detection]
received Vendor ID payload [XAUTH]
NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike-02/03: no NAT detected
ignoring informational payload, type IPSEC_REPLAY_STATUS
ignoring informational payload, type IPSEC_INITIAL_CONTACT
```

Then the one who initiates the connection sends their certificate:

```
Peer ID is ID_DER_ASN1_DN: 'CN=client1'
```

The system checks whether the certificate is trustworthy via certification authorities. Since the Intra2net system does not use this function, it always fails:

```
issuer cacert not found
X.509 certificate rejected
```

Next, the system checks whether the certificate is known. In this example, this fails because a different certificate is configured:

```
no RSA public key known for 'CN=client1'
```

The Intra2net system therefore sends a short error message to the peer:

```
sending encrypted notification INVALID_KEY_INFORMATION to 192.168.1.200:500
```

If the Intra2net system establishes a connection on its own, we get much less information in case of the same error:

```
we have a cert and are sending it
ignoring informational payload, type INVALID_CERTIFICATE
```

In this case, the log of the peer should be examined in more detail, where more detailed information can be found.

If the peer tries to establish a connection with an incorrect authentication method, or if no connection is expected from this peer IP, the following is logged:

```
initial Main Mode message received on 192.168.1.254:500 but no connection
has been authorized with policy=PUBKEY
```

Instead of "policy=PUBKEY" it is possible to get "policy=PSK" or "policy=XAUTHR-SASIG+XAUTHSERV" if the other party has chosen a corresponding authentication. Check the authentication methods set, the IP of the peer and the tunnel configuration, as the latter affects the IPs that are expected to connect.

If the peer wants to establish the connection with an unauthorized encryption algorithm (in this example a simple DES), the following is logged:

```
OAKLEY_DES_CBC is not supported. Attribute OAKLEY_ENCRYPTION_ALGORITHM
```

The peer can propose multiple algorithms. If there are no acceptable ones, the Intra2net system logs this and sends a corresponding message to the peer:

```
no acceptable Oakley Transform
sending notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

In this case, the encryption profile on the Intra2net system or on the opposite side must be adapted in such a way that at least one algorithm combination is allowed on both sides.

If everything is configured correctly, phase 1 will be completed successfully:

```
sent MR3, ISAKMP SA established
```

58.4. Error in Phase 2

In phase 2, the data for the IP tunnels is negotiated. If an error occurs here, it is mostly due to incorrect IP addresses for the tunnel. However, there may not be suitable encryption algorithms here either.

Unsuitable IP addresses are logged as follows:

```
cannot respond to IPsec SA request because no connection is known for
192.168.2.0/24===192.168.1.254[CN=server-vpn]...192.168.1.200[CN=client1]
```

192.168.2.0/24	Network behind the Intra2net system with which the peer wants to establish the connection
192.168.1.254	IP of the Intra2net system that received the connection
[CN=server-vpn]	IPSec-ID of the Intra2net System
192.168.1.200	IP of the peer
[CN=client1]	IPSec-ID of the peer

In this case, the client forgot to configure the virtual IP. This can be seen from the fact that no network is specified behind the IP address of the client. Therefore, the client wants to connect to their real IP instead of the virtual IP (which often fails due to NAT).

An attempt to connect to an incorrect virtual IP (in this case 192.168.2.78) would look like this:

```
cannot respond to IPsec SA request because no connection is known for
192.168.2.0/24===192.168.1.254[CN=server-vpn]...
192.168.1.200[CN=client1]===192.168.2.78/32
```

If the peer wants to establish a connection without PFS (Perfect Forward Secrecy), but if it is activated on the Intra2net system, it looks like this in the logs:

```
we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
sending encrypted notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

The encryption algorithms must also match in phase 2. If this is not the case (in the example, the client wants to encrypt with simple DES), it looks like this:

```
IPSec Transform [ESP_DES (64), AUTH_ALGORITHM_HMAC_SHA1] refused due
to insecure key_len and enc. alg. not listed in "esp" string
no acceptable Proposal in IPsec SA
sending encrypted notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

A successful connection setup, on the other hand, is logged as follows:

```
IPsec SA established
```

Part 7. WireGuard VPN

59. Chapter - WireGuard basics

59.1. The WireGuard protocol

WireGuard is a VPN protocol that was developed with the aim of significantly reducing the complexity of VPNs. This simplification goes so far that functions offered by other VPN protocols are omitted.

An important part of this is that only one set of cryptographic algorithms defined in the protocol is used. There is therefore no negotiation of algorithms when establishing a connection. This simplifies the connection setup and prevents downgrade attacks. X25519 ECDH is used for the key exchange, ChaCha20 for the encryption of the user data and Poly1305 for the authentication of the user data.

As X25519 ECDH could possibly be successfully attacked by quantum computers in the future, WireGuard has an additional layer of protection. For this purpose, the key negotiation is additionally symmetrically encrypted with an identical key (pre-shared key) stored on both sides. According to current knowledge, quantum computers offer no advantage over the symmetric encryption used here.

Encrypting user data using ChaCha20-Poly1305 is less computationally intensive than the AES-GCM often used with other protocols. WireGuard therefore often achieves a higher data throughput than IPSec with AES, for example. However, as many CPUs have acceleration for AES in hardware, but not for ChaCha20-Poly1305, this does not apply in all cases.

Compared to other VPN protocols, establishing a WireGuard connection is particularly lean and fast. Only one UDP packet needs to be sent to and from the other side. This is the so-called handshake. It implements the complete authentication and negotiation of session keys used for the user data.

The UDP packets for the handshake are smaller than 1259 bytes and therefore pass through the vast majority of Internet connections without fragmentation. As some routers and NAT implementations have difficulties with fragmented UDP packets, the absence of UDP fragmentation is an important advantage.

The handshake is only performed if user data actually needs to be transferred or if the so-called keepalive is activated in the configuration. The keepalive keeps the connection open in order to be able to deal with NAT routers in the connection path, for example. The handshake is performed approximately every 2 minutes if user data is constantly being transferred. This is much more frequent than is usual for establishing a connection with other VPN protocols such as IPSec.

As the connection is established so quickly, WireGuard can dispense with more complex management of the connection status. WireGuard only remembers whether the last successful handshake took place within the permitted time frame and starts a new one in good time if a data transfer is pending.

Both the handshakes and the user data are transmitted as UDP packets. The UDP port numbers are used jointly for both. The UDP port numbers are basically freely selectable and can be different on both sides. The port number 51820 is often used for WireGuard. However, Intra2net has observed conflicts with other routers using WireGuard as well as with source ports for outgoing packets of other connections and therefore recommends

port 800 for VPN routers and firewalls as well as random port numbers above 1024 for VPN clients.

WireGuard does not require the connection to be set to a specific remote IP. An IP or a DNS hostname can be stored to which the connection is always re-established. However, if the remote peer with valid keys logs in from a different IP via a handshake, this is accepted and the connection continues with the other IP from this moment on. This is useful, for example, for mobile clients that switch between WLAN and mobile communications or for switching to a fallback Internet line.

The WireGuard handshake does not exchange any information about the IP networks to be connected. The configuration only stores which source addresses may be used from a specific remote site (*AllowedIPs*). Each side blocks incoming IP packets that do not match this configuration. However, this is independent of the handshakes and it is not possible to deduce a correct configuration of the IP networks from successful handshakes.

WireGuard has established a common file format for the transfer of configuration data and keys ("wg-quick" format) and can be used across manufacturers. It can also be displayed as a QR code and photographed with the camera of mobile devices. As a result, the VPN configuration can be transferred to mobile devices particularly easily and securely.

59.2. Customization by Intra2net

Intra2net has made some customizations to WireGuard in order to improve its function. These adjustments do not affect the protocol on the line, Intra2net systems are therefore compatible with other WireGuard remote sites.

Connection status: A clear connection status is maintained and logged for each WireGuard connection. Whether a connection is online or offline is displayed on the mainpage. Each connection setup can be traced in the system logs for documentation and testing purposes.

The keepalive function should be activated in order to be able to reliably recognize the connection status. If no successful handshake is established for a connection after a maximum of 180 seconds plus the set keepalive time, it is listed as offline.

Detailed logs: Not only the online/offline status change is logged, but also setup attempts with incorrect keys, non-responding remote sites, changes of IP addresses or port numbers and packets from incorrect IP addresses within the tunnel. This data is useful for troubleshooting as well as for documentation and testing purposes.

Connection establishment independent of keepalive: In the normal implementation of WireGuard, a configured keepalive means that a connection is always attempted. Keepalive is useful for connections to VPN clients, but in times when the client is not running, the constant connection attempts and their error messages are irritating. Therefore, the Intra2net system separates the basic activation of a connection from the keepalive as soon as the connection is online.

Continuous DNS resolution: If a DNS hostname is configured as a WireGuard remote peer, the Intra2net system updates its DNS resolution every minute. This means that dynamic IPs with DynDNS or fallback Internet lines can also be used as remote sites without any problems. Nevertheless, an existing WireGuard connection is not interrupted when the DNS resolution changes. The newly resolved IP is only used to establish a new connec-

tion if handshakes to the currently used IP address are unsuccessful and the connection therefore goes offline.

Definition of local IP networks: WireGuard only provides for the configuration of the remote site networks (*AllowedIPs*, see above). This makes the configuration of fine-grained access rights more difficult, as additional firewall rulesets would have to be configured manually for the local networks. The Intra2net system provides for the IP networks involved to be configured for both the local side and the remote side. The firewall automatically restricts access to the configured networks. This configuration data also enables the preparation of complete WireGuard configuration files for the remote site.

It is not necessary to configure each individual pair of source and destination networks separately, as is the case with IPSec. Simply listing all local IP networks and those of the remote site is sufficient to connect all these networks with each other.

59.3. Comparison with IPSec

With WireGuard, the cryptographic algorithms used are firmly anchored in the protocol, whereas with IPSec they are negotiated dynamically between the remote sites each time a connection is established. WireGuard is therefore simpler and faster, but IPSec allows step-by-step evolution and adaptation of the cryptography without having to fundamentally change the protocol. Older remote sites can remain connected via IPSec without any changes, allowing a slow, uninterrupted migration. Should the cryptographic algorithms defined in WireGuard one day no longer be considered sufficient, a hard break and a fundamentally new and incompatible protocol would be necessary.

IPSec is set to UDP port 500 for the connection setup. However, this port can be used flexibly for all connections, connection and protocol variants and several individual keys. This makes it easier to set up port forwarding, for example. WireGuard requires a separate port number for each private key. However, this port number can be freely selected.

By negotiating the protocol variants and algorithms, IPSec requires the exchange of several packets to establish a connection. This is therefore slower and requires larger UDP packets which may then have to be fragmented. WireGuard uses just one packet to establish a connection and this packet is small enough that it does not normally need to be fragmented. This increases the speed and functionality of WireGuard on limited Internet access.

As IPSec establishes a unique connection at the beginning and this normally only needs to be repeated over a period of several hours, the private keys required for authentication can be stored on external devices such as smartcards or USB tokens and never needs to be stored in the RAM of the client PC. This enables full multi-factor authentication with real read protection of the private keys. Even if the private key is stored on the client PC, IPSec clients usually encrypt it with a special password and request this before each connection is established. For the transmission of private keys to clients, most clients use PKCS#12, which protects the key for transmission with a password.

With WireGuard, the handshake with authentication takes place approximately every 2 minutes. It is not intended or realistic to store the private keys on external hardware for this purpose. The established exchange format for WireGuard configurations ("wg-quick format") does not provide for the private key to be secured with a password. Most clients for WireGuard also do not provide for this to be added subsequently for the local storage of the keys and rely on any functions provided by the operating system.

IPSec uses standardized X.509 certificates and can therefore be easily connected to existing certification authorities and infrastructure. WireGuard uses its own key format, which is used exclusively for WireGuard.

The X.509 certificates used with IPSec have an expiration date that is set when they are created. This allows regular verification of authorization and the use of appropriate cryptographic standards to be defined and ensured from the outset. A regular change of keys limits the damage in the event of key loss that is not immediately detected or access by unauthorized persons. The keys used with WireGuard have no expiration date and the user must implement their own processes to ensure that the above points are checked at the correct time interval. For WireGuard keys, the Intra2net system displays the time at which a key was created or imported to support such processes.

With IPSec, the source and target networks to be connected are compared at the beginning when the connection is established between the remote sites. A connection is only established if they are exactly identical. Configuration errors are therefore immediately apparent when the connection is established and it is ensured on an additional level to the firewall that only the desired networks are connected. However, as each pair of source and target networks must be configured individually, configuration can be more complex.

With WireGuard, the IP networks are not part of the connection setup and are not compared between the two sides. A configuration error at this point is therefore not noticed when the connection is established and may first have to be identified by comparing the settings and protocols on both sides. However, it is easier to create and adapt the configuration as no pairs of source and target networks need to be defined.

IPSec does not have an established file format for the exchange of configuration data. The common formats PEM and PKCS#12 are used for authentication. However, the details of the certificates required by different remote sites, such as Subject-CN vs. SubjectAlternativeName, chain of trust or CRL, differ. This complicates the configuration of IPSec connections between different remote sites and requires detailed knowledge of the respective products from the administrators. The lack of a common exchange format for configuration data makes communication more difficult, especially if the remote sites are operated and managed by different organizations.

WireGuard has established a manufacturer-independent format for the exchange of configuration data and keys. This can at least be imported by most WireGuard clients and simplifies the configuration considerably.

In most cases, IPSec uses AES to encrypt the user data. Although this is more computationally intensive, it is supported by many CPU models with special hardware acceleration. The ChaCha20-Poly1305 from WireGuard is simpler, but is implemented purely in software. Which of the two methods ultimately delivers the higher data throughput is therefore heavily dependent on the specific CPU, mainboard and network cards used and is difficult to predict without specific tests.

IPSec has been established on the market for many years and therefore has broad, manufacturer-independent and mutually compatible support for router and firewall products. WireGuard is a newer VPN standard and is therefore not yet so widespread, especially with firewall products. However, where WireGuard is supported, we have not yet observed any compatibility problems between different implementations. Here it is helpful to have one cryptography standard only.

Free client programs are available for WireGuard for all common platforms. For IPSec, only paid client programs are recommended for some platforms.

The conclusion is that both standards have their individual strengths and justification for their existence. It should be decided individually for each application which of the two protocols is more suitable.

60. Chapter - Preparing the configuration on the Intra2net system

Below you will find a description of the steps you need to take before you can use WireGuard.

60.1. Own key and interface

WireGuard requires a pair of private and public keys on each remote site involved. This is then linked to a virtual WireGuard interface.

1. Go to the menu "System > Key > Own keys" and create a new key of the type "WireGuard "Curve 25519" private key".
2. Go to the menu "Services > VPN > WireGuard interfaces" and create a new virtual interface. Assign the custom key you have just created.

Each WireGuard interface requires its own UDP port number via which it can be addressed externally. These port numbers can be freely selected. However, it is recommended to assign port numbers from 800 upwards to the Intra2net system, as conflicts with other WireGuard-capable routers and with source ports for other outgoing UDP connections such as DNS have been observed with the port number 51820 often used with other systems.

Each WireGuard interface requires an IP address in order to communicate. The Intra2net system can reuse the IP addresses of other interfaces in order to avoid possible IP conflicts with other networks. To do this, select the interface to which most VPN remote sites are subsequently connected. For example, the primary local network.

The interfaces whose IPs are not used here can also be connected without any problems via WireGuard. However, connections originating from the Intra2net system itself and entering the VPN connection use this IP as the source address. In order for these connections to function, the source address must therefore be accepted by the VPN remote side. If a connection has already been configured for the network of this IP anyway, no further steps are necessary.



Hint

It is highly recommended to create only one WireGuard interface for all VPN connections.

Although you can easily create several WireGuard interfaces, these occupy limited resources in the system. Therefore, this should only be done when really necessary and should be examined critically.

60.2. External address and firewall

1. The Intra2net system should be addressable for the VPN clients via a DNS name on the Internet.

If the Intra2net system has a fixed IP, set up a DNS entry for it in your own official domain. The system can then be accessed under a name such as **intra.company.com** or **mail.example.com**. This can normally be set up free of charge and quickly by the web space provider who manages the domain.

If the Intra2net system is assigned a different IP each time it dials into the Internet, a DynDNS service must be set up for addressing. See Section 10.13, „DynDNS“.

Although it is possible to use a fixed IP for WireGuard directly and without a DNS entry, the DNS entry is clearly recommended. This is because changing the IP when changing provider or contract would otherwise be time-consuming. In addition, other TLS-based services of the Intra2net system require a certificate, which certification authorities only issue for DNS hostnames. This can then also be used for the VPN.

2. Go to the menu "Network > DNS > Settings" and enter this externally accessible DNS name in the field "Full hostname for connections from the Internet".
3. Check how the Intra2net system is connected to the Internet. To do this, check the type of active provider in the "Network > Provider > Profiles" menu. If it is a (DSL) dial-up line, everything is fine and you can proceed to the next step.

If it is a provider type with a router, check whether this router assigns an unchanged official IP to the Intra2net system or whether it assigns an IP from a private address range via NAT. In the latter case, port forwarding must be configured on the router for the UDP port of the WireGuard interface (see Section 60.1, „Own key and interface“) to the IP of the Intra2net system.

4. Check the firewall ruleset for incoming connections from the Internet. It is selected in the "Network > Provider > Profiles : Firewall" menu for the active provider and can be examined using the magnifying glass icon. In it, "VPN connections" must be activated. If a complete firewall ruleset is used, access to the predefined service "WireGuard interfaces" must be permitted.

60.3. Default settings for new connections

In the "Services > VPN > Settings" menu, you can define the default settings for newly created VPN connections. The settings stored there apply to both IPsec and WireGuard connections.

For the server address, it is recommended to use the full hostname for connections from the Internet.

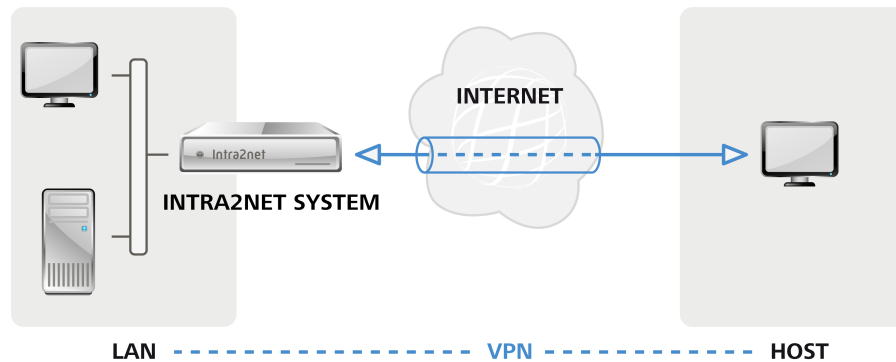
Select a firewall ruleset that allows the access to the local network that is usually desired for VPN clients.

Each VPN client is assigned an individual, virtual IP for the VPN connection. This must be outside all local networks, routings and other VPN connections. Enter the IP for the first VPN client under "Base IP address for single devices". All other VPN clients are assigned consecutive IPs.

61. Chapter - Connect individual PCs

61.1. Concept

To connect a single computer to the company network, you can install WireGuard VPN client software on the computer and use it to establish a VPN connection.



Such individual computers are usually located behind routers that mask their local network using NAT. In the case of mobile computers, the IP in the local network also changes with every change of location or dial-up process. This is not a problem in itself, but this is why VPN clients cannot simply use their IP in the current local network for the VPN, but fall back on a previously defined virtual IP. This is configured once in the Intra2net system and in the client during setup and is then permanently valid for this one client.

If the local network in which the client is currently located uses the same IP network as the company network with which you want to establish the VPN connection, the IPs can no longer be clearly assigned and the connection will fail.

For most supported clients, the Intra2net system can automatically prepare suitable configuration files that only need to be imported into the client. However, manual configuration is also always possible.

61.2. Automatic configuration for clients on the Intra2net system

For most VPN client programs, the Intra2net system can generate ready-made configuration files directly from the VPN configuration on the Intra2net system. These only need to be imported on the client. To do this, proceed as follows:

1. Make sure that the preparatory steps have all been carried out as described in 60. Chapter, „Preparing the configuration on the Intra2net system“.
2. Go to the menu "Services > VPN > Connections" and create a new connection. Select the type "WireGuard: Single device".
3. Give the connection a meaningful name, e.g. the name of the employee or device that is to connect. If an employee has several devices that should be able to establish VPN connections, you need a separate connection configuration for each device.
4. Select the local networks to which the VPN client should establish the connection.

Here you can choose whether only the packets to configured networks should run through the VPN tunnel or whether all connections from the client to the local net-

works and the Internet should run through the VPN tunnel and the Intra2net system. For the latter, select the "Local networks" option "All (0.0.0.0/0.0.0.0)", for all other cases select the relevant networks.

5. The system then automatically creates a key for the client, the connection configuration and the appropriate configuration file for the client. You can either download the configuration file for the client as a file and transfer it to the client or take a photo of the displayed QR code with the client.

If required, you can also export the configuration for the client again later using the "Download" link or display the QR code.



Caution

The configuration file and the QR code contain the private key for the client and the pre-shared key for the connection. You should therefore ensure that access is strictly controlled and that the file is only transmitted in encrypted form.

62. Chapter - WireGuard clients

62.1. Installation

The WireGuard VPN client program can be downloaded for the various platforms from <https://www.wireguard.com/install/>. You will also find links to the app stores of the respective platforms as well as the commands required for installation on the respective platform.



62.2. Configuration

Create a configuration file on the Intra2net system as described in Section 61.2, „Automatic configuration for clients on the Intra2net system“ and transfer it to the client.

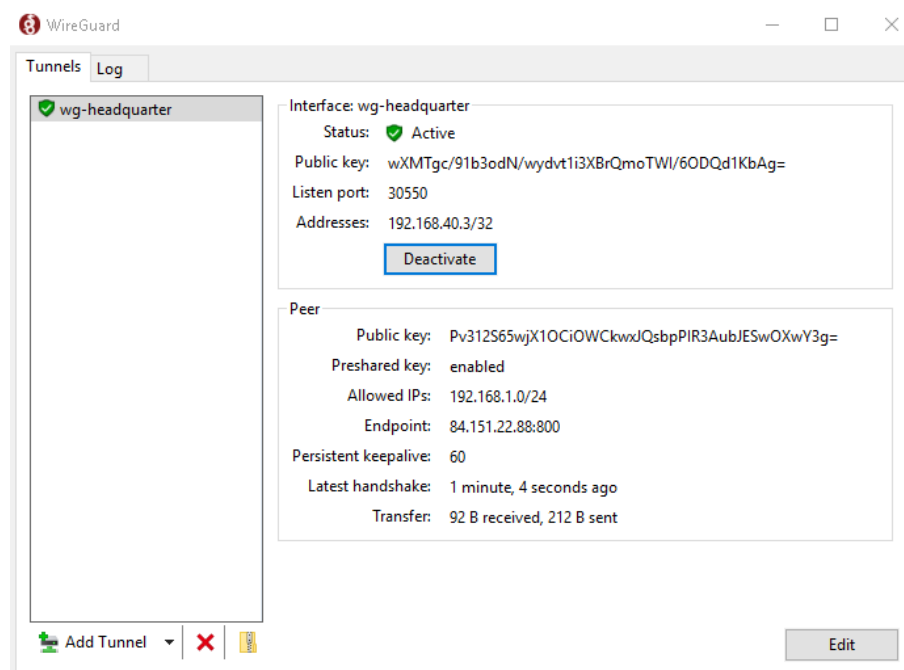
Make sure that you strictly control access to the file and only transfer the file in encrypted form as it contains private keys.

Import the file on the client using the "Import tunnel(s) from file" button.

For client devices with a camera, you can alternatively photograph the QR code directly from the screen.

62.3. Operating the client

The available connections are displayed on the left-hand side. Click on "Activate" to start the respective connection.



Hint

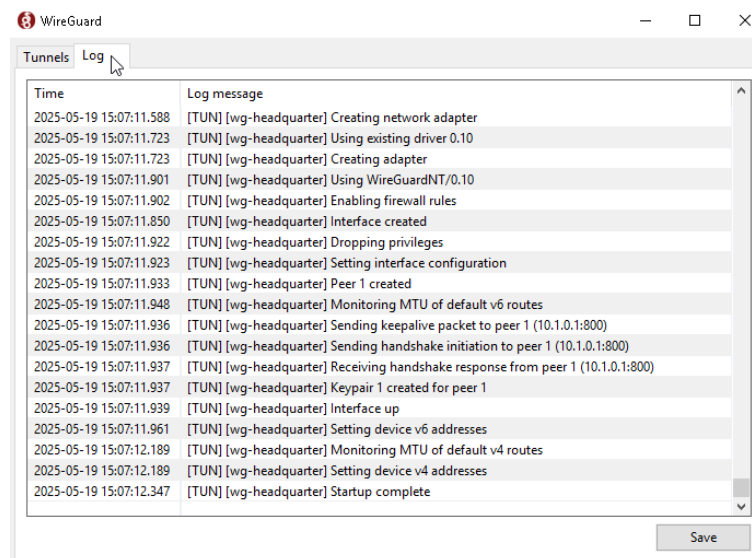
Please note that the "Status: Active" does *not* mean that a connection has been successfully established. It only means that the client is trying to establish a connection if required.

Even if the display of the transferred data volume increases in both directions, this does not allow any conclusions to be drawn about an actual connection. This is because incomplete handshake attempts and their responses also count towards the amount of data transferred.

You can only tell whether a connection has actually been established or not by the "Lastest handshake" display. If a successful handshake is displayed there within the last 3 minutes, it can be assumed that a connection has actually been established.

62.3.1. Log files

The "Log" tab can be used to view a detailed log of the connection progress and export it if required. This is helpful for troubleshooting.



62.3.2. DNS name resolution

62.3.2.1. Remote site/endpoint

If the full hostname for connections from the Internet of the Intra2net system is configured as the remote site/endpoint as recommended, the WireGuard client resolves this DNS name once when the connection is activated.

If the IP address behind the DNS hostname changes, e.g. for a dynamic IP with DynDNS, the VPN connection must be briefly deactivated in the client and then reactivated in order to update the name resolution.

62.3.2.2. DNS hostnames in the VPN network

When creating the VPN configuration, the Intra2net system adds its own IP within the VPN network as a DNS server. This is then added by the client as an additional DNS server in the system when the connection is established. DNS queries are then sent through the VPN tunnel according to the normal logic of the client operating system.

Make sure that DNS queries in the VPN tunnel always use the full domain, e.g. `intra.net.lan` instead of just `intra`, because there is no domain stored in the VPN client that could be automatically appended.

In the event of DNS problems, check whether the Intra2net system is correctly integrated into the domain in the company network. See Section 8.4, „Domain and DNS“.

62.4. Special features of the Windows client

62.4.1. Protection of private keys

The WireGuard client for Windows uses the Microsoft Data Protection API (DPAPI) to protect the configuration and keys. These are always stored encrypted with the DPAPI on the hard disk, usually in `C:\Program Files\WireGuard\Data\Configuration`. The user's password or a random value stored in the Microsoft account is used for encryption via DPAPI. If Active Directory is used, a duplicate key is also stored there.

The protection of the VPN configuration is therefore closely linked to the Windows login. Measures to improve security should therefore start with the Windows login. Other programs running with the rights of the respective user can gain access to the VPN configuration. However, access is not possible without a valid user login.

62.4.2. Usage without administrator rights

For full use of the WireGuard client, the rights of the administrator group are required under Windows. It is possible to set up the WireGuard VPN once as an administrator and then prepare it for other users without administrator rights. These other users require membership of the Windows user group `Network Configuration Operators` (S-1-5-32-556) to be able to use WireGuard.

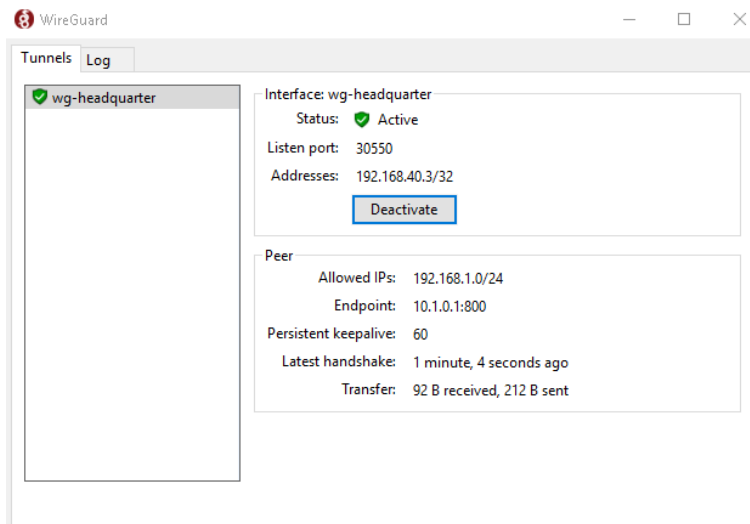
Proceed as follows and in this order to set up access:

1. Open Windows User Management and add the desired user(s) to the `Network Configuration Operators` group (S-1-5-32-556).
2. Open a command prompt (`cmd.exe`) as administrator and execute the following command to enable access in the WireGuard client:

```
reg add HKLM\Software\WireGuard /v LimitedOperatorUI /t REG_DWORD /d 1 /f
```

3. Configure the desired VPN connection in the WireGuard client once as a user with administrator rights.

Users without administrator rights now see a variant of the WireGuard client with reduced options and can use it to establish and disconnect the connections previously stored by the administrator. The menu items for importing or editing connections are not available.



62.4.3. Routing for the network Everything (0.0.0.0/0.0.0.0)

The WireGuard client for Windows allows the default gateway to be set in the VPN tunnel. This is implemented when configuring the tunnel on the Intra2net system via the option "All (0.0.0.0/0.0.0.0)" at the item "Local networks".

All data traffic, including that destined for the Internet, then first flows through the VPN tunnel to the Intra2net system. This is recommended if the client does not have a trustworthy Internet connection, e.g. a public WLAN hotspot. However, the Internet line of the Intra2net system is more heavily loaded, as the data traffic from the client to the Internet now has to be transmitted twice.

In this context, the WireGuard client for Windows also has another function, the blocking of data traffic outside the VPN tunnel. With a few exceptions, this function blocks all packets that do not enter the VPN tunnel. This applies in particular to data traffic in the local network at the client's location. For example, access to network printers, NAS drives and similar at the client's location.

You can specify whether these packets should be allowed or blocked when creating the connection on the Intra2net system. It can also be changed later when editing the VPN tunnel on the Windows client.

The Windows Filtering Platform (WFP) is used for blocking. This is not to be confused with the Windows Firewall and is located one level deeper in the system independently of the Windows Firewall. Therefore, these filters are not visible in the Windows Firewall or can be influenced by it.

63. Chapter - Connection to other Intra2net systems

Proceed as follows to establish a VPN connection between two Intra2net systems:

1. Make sure that the preparatory steps have all been carried out as described in the 60. Chapter, „Preparing the configuration on the Intra2net system“ on *both systems*.
2. On the second Intra2net system, open the menu "System > Keys > Own keys" and copy the public part of the WireGuard key to the clipboard. On the first Intra2net system, go to the menu "System > Keys > Foreign keys", click "New", paste the key from the clipboard and save.
3. On the first system, open the menu "Services > VPN > Connections" and create a new connection. Select the type "WireGuard: Site-to-site or custom configuration" and in the next step "Intra2net system".
4. Enter the external DNS hostname of the remote site and the UDP port number of the WireGuard interface there. Select the previously imported public key of the remote site.
5. Next, select the nets to be connected on both sides.
6. Configure the rights for incoming connections from the remote site. In particular, ensure that you do not select a firewall ruleset that is too permissive and only allow the connections that are actually required. If in doubt, create a dedicated firewall ruleset for this VPN connection.
7. The last step is to configure activation. A passively/manually started connection remains offline for the time being and is then started when required. This can be done via the mainpage, via an IP packet to be sent from this side or via a handshake from the other side.

If the connection is always started, the Intra2net system constantly tries to establish the connection and keep it open. For the latter in particular, a keepalive should also be configured, which keeps a connection online once it has been opened.

8. Export the connection configuration by clicking on "Download" and transfer it to the other side. The configuration contains the pre-shared key and should therefore only be transferred in encrypted form.
9. On the second system, open the menu "Services > VPN > Connections" and create a new connection. Select the type "WireGuard: Site-to-site import".
10. Paste the previously exported configuration file and save.

If the VPN connection is to be permanently connected, we recommend configuring the connection so that it can be established from both sides. This increases stability and ensures that the connection is re-established more quickly in the event of an interruption.

64. Chapter - Connection with other routers and firewalls

Proceed as follows to establish a site-to-site connection with other routers.

1. Make sure that the preparatory steps have all been carried out as described in the 60. Chapter, „Preparing the configuration on the Intra2net system“.
2. Check whether the other router or firewall already has any other WireGuard VPN connection, or at least its own WireGuard key.

Depending on the result, continue with one of the following two sections.

64.1. Remote site without own key

The following steps create the connection configuration and a suitable key pair for the remote site on the Intra2net system:

1. Open the menu "Services > VPN > Connections" on the Intra2net system and create a new connection. Select the type "WireGuard: Site-to-Site or custom configuration" and in the next step "Other device without any existing WireGuard VPN connections".
2. Enter the external DNS hostname of the remote site and the UDP port number of the remote WireGuard interface.
3. Select the nets to be connected on both sides.
4. Configure the rights for incoming connections from the remote site. Take particular care not to select a firewall ruleset that is too permissive and only allow the connections that are actually required. If in doubt, create a dedicated firewall ruleset for this VPN connection.
5. The last step is to configure activation. A passively/manually started connection remains offline for the time being and is then started when required. This can be done via the mainpage, via an IP packet to be sent from this side or via a handshake from the other side.

If the connection is always started, the Intra2net system constantly tries to establish the connection and keep it open. For the latter in particular, a keepalive should also be configured, which keeps a connection online once it has been opened.

6. Export the connection configuration by clicking on "Download". This is a complete configuration for a WireGuard interface including a private key. Transfer this to the other site.

The configuration contains the private key and pre-shared key and should therefore only be transmitted in encrypted form.

7. Import the configuration file on the other router or firewall.

Under Linux, the file is normally stored as `/etc/wireguard/wg0.conf`.

Depending on the product, you may also have to configure the data from the configuration file via individual items in a user interface. If in doubt, consult the product documentation.

If the VPN connection is to be permanently connected, we recommend configuring the connection so that it can be established from both sides. This increases stability and ensures that the connection is re-established more quickly in the event of an interruption.

64.2. Remote site with existing own key

1. Display the public key of a WireGuard interface on the other router or firewall. This can often be viewed in a menu for the WireGuard interfaces or the WireGuard status. The command `wg` can be used on the Linux command line. Make sure that you export the public key and not the private key. If in doubt, consult the product documentation.

Copy the public key to the clipboard.

2. On the Intra2net system, open the menu "System > Key > Foreign keys", click on "New", paste the key from the clipboard and save.
3. Open the menu "Services > VPN > Connections" on the Intra2net system and create a new connection. Select the type "WireGuard: Site-to-site or custom configuration" and in the next step "Another device with existing WireGuard VPN connections".
4. Enter the external DNS hostname of the remote site and the UDP port number of the WireGuard interface there. Select the previously imported public key of the remote site.
5. Select the nets to be connected on both sides.
6. Configure the rights for incoming connections from the remote site. Take particular care not to select a firewall ruleset that is too permissive and only allow the connections that are actually required. If in doubt, create a dedicated firewall ruleset for this VPN connection.
7. The last step is to configure activation. A passively/manually started connection remains offline for the time being and is then started when required. This can be done via the mainpage, via an IP packet to be sent from this side or via a handshake from the other side.

If the connection is always started, the Intra2net system constantly tries to establish the connection and keep it open. For the latter in particular, a keepalive should also be configured, which keeps a connection online once it has been opened.

8. Export the connection configuration by clicking on "Download" and transfer it to the other side. The configuration contains the pre-shared key and should therefore only be transferred in encrypted form.
9. Add the previously exported configuration file to the existing configuration of the other router or firewall.

If the device allows you to edit the configuration in `wg-quick` format, add the new connection as another "[peer]" section at the end of the existing file. Under Linux, you will normally find the files in the `/etc/wireguard/` directory. If there are files for several interfaces, make sure to edit the one from which you previously exported the public key.

Depending on the product, you may also have to configure the data from the configuration file via individual items in a user interface. If in doubt, consult the product documentation.

If the VPN connection is to be permanently connected, we recommend configuring the connection so that it can be established from both sides. This increases stability and ensures that the connection is re-established more quickly in the event of an interruption.

65. Chapter - Connection with AVM FRITZ!Boxes

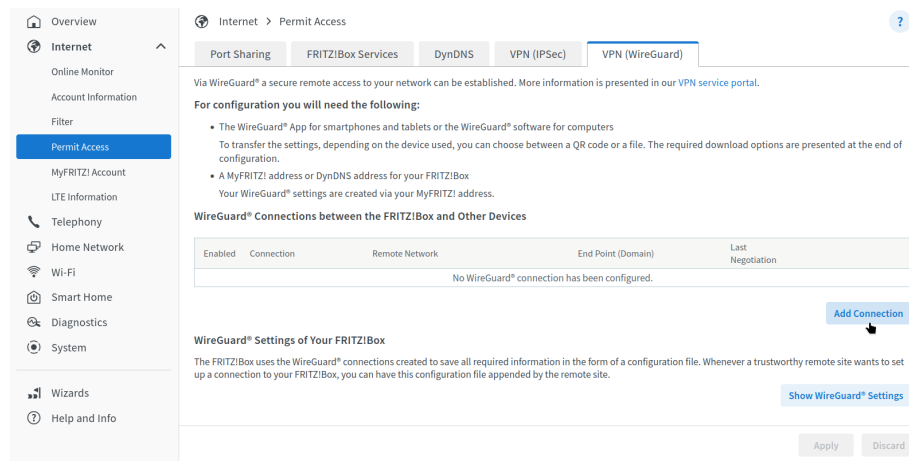
Proceed as follows to set up a site-to-site connection with an AVM FRITZ!Box.

1. Make sure that the preparatory steps have all been carried out as described in the 60. Chapter, „Preparing the configuration on the Intra2net system“.
2. Check whether the AVM FRITZ!Box already has any other WireGuard VPN connection. To do this, open the menu "Internet > Permit Access > VPN (WireGuard)".

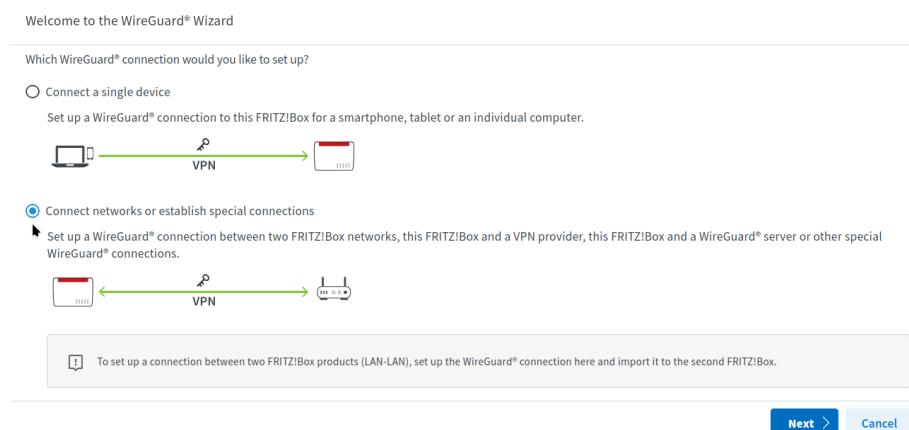
Depending on the result, continue with one of the following two sections.

65.1. AVM FRITZ!Box without previous connection

1. Carry out the steps described in Section 64.1, „Remote site without own key“ on the Intra2net system.
2. Open the menu "Internet > Permit Access > VPN (WireGuard)" on the AVM FRITZ!Box and click on "Add Connection".



3. Select "Connect networks or establish special connections"



4. Select "Yes" when asked whether the connection has already been established on the remote site.

Specify User-defined Settings

Has this WireGuard® connection already been set up at the remote connection? ☒ Yes ☐ No

[< Back](#) [Next >](#) [Cancel](#)

5. Give the connection a name and select the configuration file previously exported from the Intra2net system. Click on "Finish".

Import the Settings of an Existing WireGuard® Connection

Assign a unique name for the WireGuard® connection; you can then find it under this name in the Overview.

Name of the WireGuard® connection

Select the file from which the WireGuard settings are to be imported.

[Browse...](#) wg-8-fritzbox.conf

Advanced Settings for Network Traffic

☐ Send all IPv4 network traffic via the VPN connection
Enable this option if this FRITZ!Box should send all IPv4 web requests over the VPN connection to the WireGuard® remote site.

☐ Allow NetBIOS over this connection
NetBIOS allows a name to be registered for devices throughout the network. This is especially important for sharing files and printers in Microsoft Windows.

☐ Only certain devices in the home network are to be accessible over this WireGuard® connection:

Click on "Finish" to apply the selected settings.

[< Back](#) [Finish](#) [Cancel](#)

6. The connection will be imported.

It has been observed that this can sometimes lead to internal errors on the FRITZ!Box. In this case, repeat the import. If it still does not work after 2 attempts, restart the FRITZ!Box (menu "System > Backup > Restart").

7. Display the WireGuard settings of the FRITZ!Box.

Internet > Permit Access [?](#)

[Port Sharing](#) [FRITZ!Box Services](#) [DynDNS](#) [VPN \(IPSec\)](#) [VPN \(WireGuard\)](#)

Via WireGuard® a secure remote access to your network can be established. More information is presented in our [VPN service portal](#).

WireGuard® Connections between the FRITZ!Box and Other Devices

Enabled	Connection	Remote Network	End Point (Domain)	Last Negotiation
WireGuard® network connection				
<input checked="" type="checkbox"/>	Headquarter	192.168.1.0/24	(headquarter.example.com:800)	Edit Delete

[Add Connection](#)

WireGuard® Settings of Your FRITZ!Box

The FRITZ!Box uses the WireGuard® connections created to save all required information in the form of a configuration file. Whenever a trustworthy remote site wants to set up a connection to your FRITZ!Box, you can have this configuration file appended by the remote site.

[Show WireGuard® Settings](#)

8. The FRITZ!Box always automatically selects a random UDP port number for WireGuard when the first connection is created. Look it up under the item "ListenPort".

WireGuard® Settings of Your FRITZ!Box

The settings file contains confidential information about your FRITZ!Box and the access information for all configured WireGuard® remote sites. For this reason, use the settings file only on remote sites you trust. Passing on the settings file to third parties can lead to abuse.

Settings

Public key	MwH2gJFh3uuOsz+wVkyxK2r3RsJrevrtbWvNvjBZ1Y=	
Web address of your FRITZ!Box	g1iaho35bug1uiiw.myfritz.net:55760	
IPv4 Address	192.168.178.1	
IPv4 subnet mask	255.255.255.0	

```

[Interface]
PrivateKey = 8bRo4Hu89KPIDZDNvIMCdWCIENQFQkdAq4sclrOox84=
ListenPort = 55760
Address = 192.168.178.1/24
DNS = 192.168.178.1
DNS = fritz.box,192.168.111.1

[Peer]
PublicKey = xBLnruNEczBM1Z4ByFd1opA8wKKEP0nfwwms5LC89AM=
PresharedKey = axGdv1h9trA9IXm+m5RibTZD9X+qX62x1edPBpE3zyo=

```

[Download Configuration File](#)

[Close](#)

- On the Intra2net system, go to the menu "Services > VPN > Connections", select the connection to the FRITZ!Box and enter the port number read from the FRITZ!Box under "Remote port (UDP)".

In some cases, it was observed that the FRITZ!Box only activated a newly set up WireGuard connection after a restart, although it was shown in the connection list. In the event of connection problems, we therefore recommend restarting the FRITZ!Box (menu "System > Backup > Restart").

If the VPN connection is to be connected permanently, it is recommended to configure the connection so that it can be established from both sides. This increases stability and ensures that the connection is re-established more quickly in the event of an interruption.

65.2. AVM FRITZ!Box with other VPN connection

Proceed as follows on an AVM FRITZ!Box with an existing VPN connection to another remote site:

- Open the menu "Internet > Permit Access > VPN (WireGuard)" on the AVM FRITZ!Box and click on "Show WireGuard Settings".

Internet > Permit Access

Port Sharing FRITZ!Box Services DynDNS VPN (IPSec) **VPN (WireGuard)**

Via WireGuard® a secure remote access to your network can be established. More information is presented in our [VPN service portal](#).

WireGuard® Connections between the FRITZ!Box and Other Devices

Enabled	Connection	Remote Network	End Point (Domain)	Last Negotiation
<input checked="" type="checkbox"/>	Headquarter	192.168.1.0/24	(headquarter.example.com:800)	

[Add Connection](#)

WireGuard® Settings of Your FRITZ!Box

The FRITZ!Box uses the WireGuard® connections created to save all required information in the form of a configuration file. Whenever a trustworthy remote site wants to set up a connection to your FRITZ!Box, you can have this configuration file appended by the remote site.

[Show WireGuard® Settings](#)

- The existing public key of the FRITZ!Box is displayed. Copy it to the clipboard.

WireGuard® Settings of Your FRITZ!Box

Use these information to set up a connection to this FRITZ!Box on a trustworthy remote site.

The settings file contains confidential information about your FRITZ!Box and the access information for all configured WireGuard® remote sites. For this reason, use the settings file only on remote sites you trust. Passing on the settings file to third parties can lead to abuse.

Settings

Public key: [Copy](#)

Web address of your FRITZ!Box: [Copy](#)

IPv4 Address: [Copy](#)

IPv4 subnet mask: [Copy](#)

```
[Interface]
PrivateKey = 8bRo4Hu89KPIDZDNvIMCdWCiENQFQkdAq4sclrOox84=
ListenPort = 55760
Address = 192.168.178.1/24
DNS = 192.168.178.1
DNS = fritz.box,192.168.111.1

[Peer]
PublicKey = xBLnruNEczBM1Z4ByFd1opA8wKKEP0nfwwms5LC89AM=
PresharedKey = axGdv1h9trA9IXm+m5RiBTZD9X+qX62x1edPBpE3zyo=
```

[Download Configuration File](#) [Close](#)


- Carry out the steps described in Section 64.2, „Remote site with existing own key“ on the Intra2net system.
- Open the menu "Internet > Permit Access > VPN (WireGuard)" on the AVM FRITZ!Box and click on "Add Connection".
- Select "Connect networks or establish special connections"

Welcome to the WireGuard® Wizard

Which WireGuard® connection would you like to set up?


☐ Connect a single device


Set up a WireGuard® connection to this FRITZ!Box for a smartphone, tablet or an individual computer.



☒ Connect networks or establish special connections

Set up a WireGuard® connection between two FRITZ!Box networks, this FRITZ!Box and a VPN provider, this FRITZ!Box and a WireGuard® server or other special WireGuard® connections.



 To set up a connection between two FRITZ!Box products (LAN-LAN), set up the WireGuard® connection here and import it to the second FRITZ!Box.

- Select "Yes" when asked whether the connection has already been established on the remote site.

Specify User-defined Settings

Has this WireGuard® connection already been set up at the remote connection? ☒ Yes ☐ No

- Give the connection a name and select the configuration file previously exported from the Intra2net system. Click on "Finish".

Import the Settings of an Existing WireGuard® Connection

Assign a unique name for the WireGuard® connection; you can then find it under this name in the Overview.

Name of the WireGuard® connection

Select the file from which the WireGuard settings are to be imported.

wg-8-fritzbox.conf

Advanced Settings for Network Traffic

☐ Send all IPv4 network traffic via the VPN connection
Enable this option if this FRITZ!Box should send all IPv4 web requests over the VPN connection to the WireGuard® remote site.

☐ Allow NetBIOS over this connection
NetBIOS allows a name to be registered for devices throughout the network. This is especially important for sharing files and printers in Microsoft Windows.

☐ Only certain devices in the home network are to be accessible over this WireGuard® connection:

Click on "Finish" to apply the selected settings.

- The connection will be imported.

It has been observed that this can sometimes lead to internal errors on the FRITZ!Box. In this case, repeat the import. If it still does not work after 2 attempts, restart the FRITZ!Box (menu "System > Backup > Restart").

In some cases, it has been observed that the FRITZ!Box only activated a newly set up WireGuard connection after a restart, although it is shown in the connection list. In the event of connection problems, we therefore recommend restarting the FRITZ!Box (menu "System > Backup > Restart").

If the VPN connection is to be connected permanently, it is recommended to configure the connection so that it can be established from both sides. This increases stability and ensures that the connection is re-established more quickly in the event of an interruption.

66. Chapter - Status and error diagnosis

66.1. Mainpage

All VPN connections that are currently online are displayed in the status area on the mainpage. Connections that should always be online (activation "Always") but cannot be established are explicitly listed as `Offline`. This applies to both WireGuard and IPsec connections.

The VPNs can be controlled directly using the "Connect VPN" and "Disconnect VPN" buttons.

Please note that "Disconnect VPN" only disconnects the connection on the local side, as the WireGuard protocol does not provide the ability to inform the remote site of a disconnection. The remote party can continue to re-establish the connection on its own initiative. If you want to prevent this, the connection must be deactivated in the "Services > VPN > Connections" menu.

66.2. VPN status

A detailed overview of the current status of all VPN connections can be obtained via the menu "Information > System > VPN".

All configured WireGuard connections are listed below the respective WireGuard interface. Details such as the current connection status, the IP of the remote station and the last successful handshake are displayed.

In contrast to the VPN clients, the Intra2net system only displays the status "Online" if a successful handshake has actually taken place within the last 3 minutes (plus any keepalive interval).

Information
?

VPN Status:

*** WireGuard connections ***

Interface wg-main (wg800):
 Port: 800
 Public Key: xBLnruNEczBM1Z4ByFd1opA8wKKEP0nfwwms5LC89AM=
 Address: 192.168.1.1/32

Peer Zentrale:
 Endpoint (configured): 84.151.22.88:800 (zentrale.example.com)
 Endpoint (in use): 84.151.22.88:800
 State: online (last handshake 34s ago)
 Activation: always
 Keepalive: 60
 Public Key: +cO9V6mUY0PIAjB/6qgO2XpRFy3hUBIamIN2Mxk4LmM=
 Instance: C1
 PSK: in use
 Remote nets: 192.168.110.0/24

Peer Homeoffice Fr. Schmidt:
 Endpoint (configured): None
 State: offline
 Activation: passive / manual
 Keepalive: 60
 Public Key: VRs4mnam0dug6bYXzxUp4wRCmCQ0FySi5nMSboMMRDA=
 Instance: C10
 PSK: in use
 Remote nets: 192.168.40.1/32

66.3. Logs

All logs related to WireGuard VPN are logged in the system messages and can be accessed via the menu "Information > System > Logfiles". Messages with the service identifiers `i2n-wg` and `kernel: wireguard:` are relevant for WireGuard.

The public key of the remote site is included with every message. This can be used to match all messages of a connection. You can find an overview of all public keys under "Information > System > VPN".

If a connection has been successfully established, this is logged as in this example:

```
i2n-wg[2732]: Connection "Headquarter" (C1) is now online with peer
84.151.22.88:800; [wg800: +cO9V6mUY0PlAjB/6qgO2XpRFy3hUBIamIN2Mxk4LmM=]
```

If a connection changes to the offline status, the log looks like this:

```
i2n-wg[2732]: Connection "Headquarter" (C1) is now offline; [wg800:
+cO9V6mUY0PlAjB/6qgO2XpRFy3hUBIamIN2Mxk4LmM=]
```

Part 8. Appendix

Appendix A. Licenses

A.1. Intra2net Software License Agreement

Version 2.2 from 12. April 2022

Intra2net AG, Mömpelgarder Weg 8, 72072 Tübingen, Deutschland

This license agreement grants you as the licensee a non-exclusive, unlimited right of use of the software "Intra2net System Manager" developed by Intra2net AG under the following license terms and to the extent described below. By installing the software you agree to the following license conditions:

§1 Subject matter of the contract

1) The software products Intra2net Business Server, Intra2net Security Gateway and Intra2net Network Security (hereinafter referred to as "Intra2net Software") consist of the "Intra2net System Manager" and the "Linux Open-Source Distribution". Subject to the provisions in § 2 of this agreement, only "Intra2net System Manager" is the subject matter of this license agreement. The "Linux Open-Source Distribution" is subject to its own license terms, which are attached to the corresponding RPM packages.

2) The "Intra2net System Manager" consists of compressed files plus installation program (RPM package), which contain the executable code of the software programmed by Intra2net AG. The "Intra2net System Manager" is not distributed as open source software. All copyrights and other industrial property rights to the "Intra2net System Manager" are owned by Intra2net AG or have been granted to Intra2net AG for the contractual use of third parties. The components of the "Intra2net System Manager" are marked accordingly in the RPM packages.

2 Other Licenses

1) Together with the "Intra2net System Manager" you will also receive a program copy of a "Linux Open-Source Distribution". Intra2net AG leaves the program copy of the "Linux Open-Source Distribution" to you free of charge, so that the liability in this respect according to §§ 521 ff. BGB and is therefore limited to intent or gross negligence.

2) Intra2net AG does not grant the copyright rights to the distribution which are mandatory for the use of the "Linux Open-Source Distribution", but the respective authors of the respective program parts transfer the rights of use directly. The extent of your rights of use in relation to the "Linux Open-Source Distribution" is therefore determined exclusively by the license conditions attached to the "Linux Open-Source Distribution" and not by this contract.

3) When using the entire "Intra2net Software", in addition to the provisions of this license agreement, the user must observe the license conditions assigned to the open source program packages by the respective authors within the scope of a direct usage contract with the respective software manufacturer without intermediate connection of Intra2net AG. The corresponding license terms are attached in electronic form to the respective software.

4) As far as source code is subject to the free "Linux Open-Source Distribution" of the GNU General Public License (GPL) or the GNU Lesser General Public License (LGPL), the source code can be freely downloaded from the website www.intra2net.com.

5) Where libraries licensed under the LGPL are used within the licensed programs, these libraries will either be used as a shared program library, or you can - according to the regulations provided for this purpose in the LGPL - request the respective sources at the conditions stated in 4) above.

§ 3 Installation

1) The "Intra2net software" does not run in parallel with other operating systems on one system. In particular, the "Intra2net Software" formats the entire hard disk during installation and deletes all existing data. If data already exists on the system, the mandatory backup copies must be made prior to installation and then stored safely in such a way that they can be restored at any time.

2) The "Intra2net Software" works only with hardware components approved by Intra2net. These are listed in the documentation and on the website www.intra2net.com and are updated regularly. The licensee must observe these instructions. Intra2net AG has the right to withdraw the approval for hardware components for future versions, e.g. if they are no longer supported by future base systems with device drivers. All customers registered with Intra2net will be notified by email at least 3 months in advance (discontinuation).

§ 4 Rights of Duplication and Protection of Access

1) Duplication of the "Intra2net System Manager" is only permitted if the respective duplication is necessary for the use of the program. The necessary duplications include the installation of the program from the original storage medium or by way of downloading it to the hard drive of the hardware used and loading the program into the working memory.

2) If, for reasons of data safety or to ensure the rapid reactivation of the computer system after a total failure, regular backup of the entire data set including the computer programs in use is essential, the Licensee may make backup copies in the number absolutely necessary. The relevant storage media must be marked accordingly. The backup copies may only be used for archival purposes.

3) The licensee is obliged to take appropriate precautions to prevent unauthorized access by third parties to the installed programs and data. The licence codes supplied shall be stored in a place secured against unauthorised access by third parties.

4) The Licensee's employees must be expressly informed of their compliance with these Terms and Conditions of Contract and the provisions of copyright law.

5) The licensor is entitled to block license codes if there is evidence of a breach of the license agreement. The licensee will be notified, if valid contact data is available, and will be given a grace period of 14 days to re-license. In the event that a license code is blocked, the rightful owner of a license can obtain a new license code free of charge upon presentation of the proof of purchase. It is pointed out that contact data of licensees will be deleted within the required periods after termination of a support and maintenance contract for data protection reasons.

6) Access to the source code of the "Intra2net System Manager" is not owed.

§ 5 Restrictions of Use

1) The licensee may use the "Intra2net System Manager" on any available hardware. However, if the licensee changes the hardware, they must delete the "Intra2net System Manager" from the previously used hardware.

2) Simultaneous storage, holding or use is only permitted in one instance. If the licensee wants to use the software in several instances, they must purchase a corresponding number of additional licenses.

3) The licensee must prevent simultaneous reuse beyond the number of purchased licenses by means of access protection mechanisms.

4) If it is a license with a limited number of users, the system may only be used by the corresponding number of users.

5) The number of users is calculated from the sum of users created in the "User Manager" menu item, user accounts on remote servers that are used for emails forwarded by the system, and users that are not created in the User Manager but have the possibility to use the system's proxy server.

The licensee is not entitled to use the "Intra2net System Manager" or individual components thereof for hazardous applications which require faultless continuous operation with corresponding systems. Hazardous applications include, in particular, high-risk and high-availability activities such as the operation of nuclear power facilities, weapon systems, aeronautical navigation or communication systems, transport systems, hospital and healthcare equipment and other applications relevant to people's lives and health.

§ 6 Additional Services

1) If the license entitles you to limited-time services, such as software maintenance or support, the term of the license begins with entering the license code, registering the software or checking for updates.

2) If the right to these services is extended, the term of the extension shall commence retroactively with effect from the last expiry date.

§ 7 Evaluation license

1) If no license was purchased from an end customer, they receive a limited evaluation license, i.e. for 30 days the right to install the "Intra2net System Manager" on hardware and to use it for test purposes under these license conditions. If you enter a license key that you have not purchased yourself, the evaluation license expires immediately.

2) The evaluation license or any other, time-limited license may only be used for the corresponding period of time after installation. The remaining time is displayed on the user interface of the software.

3) At the end of this period, the software terminates functionality. The customer is responsible for securing all data in advance.

4) An evaluation license does not entitle to warranty claims unless Intra2net AG caused any defects intentionally or through gross negligence.

§ 8 Decompiling and Program Changes

1) The re-translation of the provided program code into other code forms (decompilation), as well as other types of redevelopment at the different stages of production in the software (reverse engineering), including program modification, are only permitted in the following cases.

2) The consent of the rights holder shall not be required if the reproduction of the code or the translation of the code form is essential in order to either a) meet the conditions of the LGPL or b) obtain the information necessary to establish the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

1. The actions are carried out by the licensee or by another person authorized to use a copy of the program or on their behalf by an authorized person;
2. the information necessary for establishing interoperability is not yet readily available to the persons referred to in point 1;
3. the actions are limited to those parts of the original software which are necessary to achieve interoperability.

In the case of information obtained from such acts referred to in (a) and (b), it shall not be permitted to

1. be used for purposes other than to achieve interoperability of the independently created programme,
2. provided to third parties unless this is necessary for the interoperability of the independently created programme,
3. used for the development, production or marketing of a program with substantially similar purposes or for any other acts infringing copyright.

3) Copyright notices, license codes, serial numbers and other features used to identify the program may not be removed or changed under any circumstances.

4) If software is installed on the system which has not been expressly approved by the licensor for this purpose, or if the installed software is modified, warranty or guarantee claims can only be asserted if the customer can prove that the defects are not related to the modifications.

§ 9 Resale and Rental

1) The Licensee may sell or give away the Software, including the User Manual and other accompanying material, to third parties on a permanent basis, provided that the acquiring third party agrees to the continuation of these Terms and Conditions of Contract. In the event of transfer, the Licensee must hand over to the new Licensee all copies of the program, including any backup copies that may be available, or destroy the copies that have not been handed over. As a result of the transfer, the right of the old licensee to use the program expires.

2) The Licensee may not rent the Software, including the accompanying material, to third parties.

3) The Licensee may not transfer the software to third parties if there is a reasonable reason to suspect that the third party will violate the contractual terms and conditions, in particular if it produces illegal copies. This also applies to employees of the licensee.

§ 10 Warranty

1) Defects in the software programmed by Intra2net AG, including the accompanying documents, will be remedied by the licensor within the warranty period of 24 months for consumers or 12 months for companies from the time of delivery after notification by the licensee. This shall be done at the discretion of the licensor by subsequent repair or delivery of a replacement.

2) In the event of two unsuccessful repair or replacement deliveries, the Licensee may withdraw from the contract or reduce the agreed remuneration and claim damages. Subject to § 11, the statutory regulations apply.

§ 11 Liability

1) The following provisions apply to all claims for damages made by the Licensee, irrespective of their legal basis, whether due to culpability at the time the contract was concluded, or due to other breaches of obligation, criminal, or other circumstances.

2) Intra2net AG is liable in full for damages resulting from injury to life, limb or health caused by an intentional or negligent breach of obligations by the legal representatives or persons employed by Intra2net AG.

3) Intra2net AG shall be liable in full for any other damages resulting from an intentional or grossly negligent breach of obligation by its legal representatives or persons employed in the performance of its obligations.

4) Intra2net AG is fully liable for the absence of a guaranteed quality of the promised service and for fraudulent concealment of a defect.

5) Intra2net AG shall be liable for the remaining damages arising from any culpable breach of fundamental obligations. Fundamental obligations are defined as contractual obligations, the fulfilment of which makes the correct performance of the contract possible and on whose adherence contractual partners may regularly rely. In such cases Intra2net AG shall be held liable to the extent limited to compensation for damages which were typical and foreseeable at the time of conclusion of the contract.

6) Liability under the Product Liability Act remains unaffected.

7) Otherwise, the liability of Intra2net AG is excluded.

8) Any contributory negligence on the part of the Licensee as a result of insufficient co-operation, delayed notification of damages, the use of hardware that has not been authorized or for other reasons shall be credited to the Licensee.

9) Intra2net AG shall not be liable for the loss of data and/or programs insofar as the damage is due to the Licensee's failure to carry out the necessary data backups or to regularly check the integrity of the data backups and thereby ensure that lost data can be restored with justifiable effort.

10) For damages caused by any additional installed software Intra2net AG is only liable in case of delivery and installation.

§ 12 Obligation to check and give notice of defects

1) The Licensee shall inspect the delivered software including the documentation within 8 working days after delivery, in particular with regard to the completeness of the storage mediums and manuals as well as the basic program functionality. Defects that are detected or ascertainable must be reported to the licensor within a further 8 working days. The notification of defects must include a detailed description of the defects, which must be as detailed as possible.

2) Defects that cannot be ascertained within the context of the described proper inspection must be reported within 8 working days of discovery, in compliance with the notification requirements set out.

3) In the event of a breach of the obligation to check and give notice of defects, the software shall be deemed to have been approved in view of the defect in question.

§ 13 Written Form

All agreements that include a change, amendment or specification of these contractual conditions as well as special assurances and agreements must be made in writing. If they are issued by the Licensor's representatives or assistants, they shall only be binding if the Licensor provides written consent.

§ 14 Governing Law

With regard to all legal relationships arising from and in connection with this contractual relationship, the parties agree to apply the law of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

§ 15 Place of Jurisdiction

Insofar as the Licensee is a trader within the definition of the German Commercial Code (Handelsgesetzbuch), a legal entity under public law or a special asset under public law or has no place of jurisdiction in Germany, Stuttgart shall be agreed as the place of jurisdiction for all disputes arising in connection with the establishment, performance and termination of this contractual relationship.

§ 16 Final provisions

Should individual terms and conditions be or become invalid, ineffective or contestable, they shall be interpreted or supplemented in such a way that the intended economic purpose is achieved in a legally permissible manner as closely as possible; the remaining terms and conditions shall remain unaffected. This shall also apply correspondingly to any omissions requiring further attention.

A.2. Licensed software

The components of the Linux Open-Source Distribution are subject to their own licenses. Some of these licenses are the GNU General Public License (GPL) and GNU Lesser General Public License (LGPL) in different versions. These can be viewed at the following URLs:

GPL v2	http://www.gnu.org/licenses/gpl-2.0.html
GPL v3	http://www.gnu.org/licenses/gpl-3.0.html
LGPL v2.1	http://www.gnu.org/licenses/lgpl-2.1.html

LGPL v3	http://www.gnu.org/licenses/lgpl-3.0.html
---------	---

Some parts of this product includes software from the following copyright owners:

Copyright 1990 Massachusetts Institute of Technology; Copyright (C) 1995,1996,1997 Lars Fenneberg; Copyright (c) 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006 Inferno Nettverk A/S, Norway; Copyright (C) 2002 Roaring Penguin Software Inc.; Copyright 1991 by the Massachusetts Institute of Technology; Copyright 1992 Livingston Enterprises, Inc.; Copyright 1992, 1993, 1994 Henry Spencer; Copyright 1996 Willem van Schaik, Singapore (willem@schaik.com); Copyright 1999-2000 Greg Roelofs (newt@pobox.com); Original Code Copyright (C) 1994, Jeff Hostetler, Spyglass, Inc.; Portions of Content-MD5 code Copyright (C) 1993, 1994 by Carnegie Mellon University; Portions of Content-MD5 code Copyright (C) 1991 Bell Communications; Research, Inc. (Bellcore); Portions extracted from mpack, John G. Myers – jgm+@cmu.edu; Content-MD5 Code contributed by Martin Hamilton (martin@net.lut.ac.uk) these portions extracted from mpack, John G. Myers – jgm+@cmu.edu; (C) Copyright 1993,1994 by Carnegie Mellon University; (c) Copyright 1989 Sun Microsystems, Inc. Sun design patents pending in the U.S. and foreign countries. OPEN LOOK is a trademark of AT&T. Used by written permission of the owners; (c) Copyright Bigelow & Holmes 1986, 1985.

This product includes software developed by:

Tim Hudson (tjh@cryptsoft.com); Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>); Paul Mackerras paulus@samba.org; Pedro Roque Marques pedro_m@yahoo.com; the Apache Software Foundation (<http://www.apache.org/>); the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>); by the University of California, Berkeley and its contributors; by Tommi Komulainen Tommi.Komulainen@iki.fi; Ian F. Darwin, 1987; the Regents of the University of Michigan and Merit Network, Inc.

This product includes:

"perl-Encode-Detect", which is licensed under the Mozilla Public License. The Source Code is available under the terms of this License at <http://search.cpan.org/~jgmyers/Encode-Detect/>; cryptographic software written by Eric Young (eay@cryptsoft.com); RSA Data Security, Inc. MD4 Message Digest Algorithm; RSA Data Security, Inc. MD5 Message Digest Algorithm and is based in part of the work of the FreeType Team and the Independent JPEG Group.

cryptographic software written by Eric Young (eay@cryptsoft.com); PHP software, freely available from <http://www.php.net/software/>; RSA Data Security, Inc. MD5 Message Digest Algorithm: software developed by: Inferno Nettverk A/S, Norway; Paul Mackerras paulus@samba.org; the Computer Systems Engineering Group at Lawrence Berkeley Laboratory and its contributors; the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>); the University of California, Berkeley and its contributors; Todd C. Miller.

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

A.3. Notes on return and disposal

The Electrical and Electronic Equipment Act (ElektroG) and the Battery Act (BattG) contain a large number of requirements for handling electrical and electronic equipment. The

most important information on the return and disposal of B2B waste electrical and electronic equipment and used batteries is summarized here.

A.3.1. Separate collection of old equipment

Electrical and electronic equipment that has become waste is referred to as old equipment. Owners of old equipment must dispose of it separately from unsorted municipal waste. In particular, old appliances do not belong in household waste, but in special collection and return systems.

A.3.2. Batteries and accumulators and lamps

As a rule, owners of waste equipment must separate spent batteries and accumulators that are not enclosed in the waste equipment, as well as lamps that can be removed from the waste equipment without causing damage, from the waste equipment before handing it over to a collection point. This does not apply if old equipment is prepared for reuse with the participation of a public waste management authority.

A.3.3. Options for the return of old equipment

In order to provide opportunities for the return of old equipment, we cooperate with several qualified recycling companies. If a device manufactured by us has become an end-of-life device and you would like to return it, please contact us and fill out the questionnaire: <https://www.intra2net.com/en/recycling/>

A.3.4. Data privacy notice

Old devices often contain sensitive personal data. This applies in particular to information and telecommunications technology devices such as computers and smartphones. In your own interest, please note that each end user is responsible for deleting the data on the old devices to be disposed of.

A.3.5. Meaning of the crossed out trash can symbol

The symbol of a crossed-out trash can regularly depicted on electrical and electronic equipment indicates that the respective device must be collected separately from unsorted municipal waste at the end of its service life.



A.3.6. Free collection of used batteries

Batteries must not be disposed of with household waste. You are legally obligated to return used batteries so that proper disposal can be ensured. You can return used batteries to a municipal collection point or to your local retailer.

A.3.7. Meaning of the battery symbols

Batteries are marked with the symbol of a crossed-out garbage can. This symbol indicates that batteries must not be disposed of in household waste. For batteries that contain more than 0.0005 mass percent mercury, more than 0.002 mass percent cadmium or more than 0.004 mass percent lead, the chemical designation of the respective pollutant is located below the trash can symbol - "Cd" stands for cadmium, "Pb" stands for lead, and "Hg" for mercury.

Appendix B. License

B.1. Intra2net Groupware Client License Agreement (EULA)

This license agreement grants a non-exclusive right to use the Groupware Client developed by Intra2net AG under the following license conditions. By installing the software you agree to the following license terms.

§ 1 Object of the Contract

1) The object of the contract is the "Intra2net Groupware Client", which comprises a MAPI Storage Provider application. This application can only be used in combination with Microsoft Outlook.

2) Intra2net AG grants the Licensee the non-exclusive right to use the above-mentioned and purchased "Intra2net Groupware Client" on a permanent basis and only in accordance with the following provisions. The software is protected by copyright (§§ 69a ff. UrhG).

§ 2 Authorized Use

1) A license for a specific number of users is issued to a natural or legal person. This license is part of the "Intra2net Business Server" license, is bound to it, and applies to the number of users listed there.

2) Simultaneous installation, storage or use is only permitted in the amount up to the number of licensed users.

§ 3 Restrictions of Use

1) The licensee must prevent repeated use beyond the maximum number of purchased users. If this number of users is exceeded, the functionality can be reduced for the surplus logged in users.

2) The licensee is not entitled to use the "Intra2net Groupware Client" or individual components thereof for hazardous applications which require faultless continuous operation with corresponding systems. Hazardous applications include, in particular, high-risk and high-availability activities such as the operation of nuclear power facilities, weapon systems, aeronautical navigation or communication systems, transport systems, hospital and healthcare equipment and other applications relevant to people's lives and health.

3) The Licensee shall observe the Licensor's instructions regarding the "Intra2net Groupware Client" operating environment, the approved versions of the operating system, Microsoft Outlook and Microsoft Outlook configurations that differ from the basic version. This applies in particular to the use of additional Outlook plugins and addins.

§ 4 Additional Services

If the license entitles the right to time-limited services (e.g. update service), their term is bound to the license of the "Intra2net Business Server".

§ 5 Evaluation license

1) If no license has been purchased from an end customer, they are entitled to an evaluation period of 30 days, which grants them the right to install and test the software in

non-production-critical environments under these license conditions. If a non-self-purchased license is entered, the evaluation license expires immediately.

2) The evaluation license or another, time-limited license may only be used for the corresponding period after installation and can only be extended with the written consent of Intra2net AG. The remaining time is displayed on the user interface of the software.

3) At the end of this period, the software terminates functionality. The customer is responsible for securing all data in advance.

4) An evaluation license does not entitle the licensee to warranty claims, except in cases where the licensor is responsible for intent or gross negligence.

§ 6 Decompiling and Program Changes

1) The re-translation of the provided program code into other code forms (decompilation), as well as other types of redevelopment at the different stages of production in the software (reverse engineering), including program modification, are only permitted in the following cases.

2) The consent of the rights holder shall not be required if the reproduction of the code or the translation of the code form is essential in order to either a) meet the conditions of the LGPL or b) obtain the information necessary to establish the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

1. The actions are carried out by the licensee or by another person authorized to use a copy of the program or on their behalf by an authorized person;
2. the information necessary for establishing interoperability is not yet readily available to the persons referred to in point 1;
3. the actions are limited to those parts of the original software which are necessary to achieve interoperability.

In the case of information obtained from such acts referred to in (a) and (b), it shall not be permitted to

1. be used for purposes other than to achieve interoperability of the independently created programme,
 2. provided to third parties unless this is necessary for the interoperability of the independently created programme,
 3. used for the development, production or marketing of a program with substantially similar purposes or for any other acts infringing copyright.
- 3) Copyright notices, license codes, serial numbers and other features used to identify the program may not be removed or changed under any circumstances.

4) If the "Intra2net Groupware Client" is modified, warranty or guarantee claims can only be asserted if the customer can prove that the defects are not related to the modifications.

§ 7 Resale and Rental

1) The Licensee may sell or give away the Software, including the User Manual and other accompanying material, to third parties on a permanent basis, provided that the acquiring third party agrees to the continuation of these Terms and Conditions of Contract. In the event of transfer, the Licensee must hand over to the new Licensee all copies of the program, including any backup copies that may be available, or destroy the copies that have not been handed over. As a result of the transfer, the right of the old licensee to use the program expires.

2) The Licensee may not rent the Software, including the accompanying material, to third parties.

3) The Licensee may not transfer the software to third parties if there is a reasonable reason to suspect that the third party will violate the contractual terms and conditions, in particular if it produces illegal copies. This also applies to employees of the licensee.

§ 8 Warranty

1) Defects in the software programmed by Intra2net AG, including the accompanying documents, will be remedied by the licensor within the warranty period of 24 months for consumers or 12 months for companies from the time of delivery after notification by the licensee. This shall be done at the discretion of the licensor by subsequent repair or delivery of a replacement.

2) In the event of two unsuccessful repair or replacement deliveries, the Licensee may withdraw from the contract or demand compensation for damages. Subject to § 9, the statutory regulations apply.

§ 9 Liability

1) The following provisions apply to all claims for damages made by the Licensee, irrespective of their legal basis, whether due to culpability at the time the contract was concluded, or due to other breaches of obligation, criminal, or other circumstances.

2) Intra2net AG is liable in full for damages resulting from injury to life, limb or health caused by an intentional or negligent breach of obligations by the legal representatives or persons employed by Intra2net AG.

3) Intra2net AG shall be liable in full for any other damages resulting from an intentional or grossly negligent breach of obligation by its legal representatives or persons employed in the performance of its obligations.

4) Intra2net AG is fully liable for the absence of a guaranteed quality of the promised service and for fraudulent concealment of a defect.

5) Intra2net AG shall be liable for the remaining damages arising from any culpable breach of fundamental obligations. Fundamental obligations are defined as contractual obligations, the fulfilment of which makes the correct performance of the contract possible and on whose adherence contractual partners may regularly rely. In such cases Intra2net AG shall be held liable to the extent limited to compensation for damages which were typical and foreseeable at the time of conclusion of the contract.

6) Liability under the Product Liability Act remains unaffected.

7) Otherwise, the liability of Intra2net AG is excluded.

8) Any negligence on the part of the Licensee as a result of insufficient participation, delayed notification of damages, the use of unreleased software or for other reasons shall be attributed to the Licensee.

9) Intra2net AG shall not be liable for the loss of data and/or programs insofar as the damage is due to the Licensee's failure to carry out the necessary data backups or to regularly check the integrity of the data backups and thereby ensure that lost data can be restored with justifiable effort.

10) For damages caused by any additional installed software Intra2net AG is only liable in case of delivery and installation.

11) No liability is accepted for the compatibility of the software with versions of the operating system, Microsoft Outlook and configurations of Microsoft Outlook that deviate from the basic version not explicitly approved by Intra2net AG. This applies in particular to the use of other Outlook plugins and addins.

§ 10 Obligation to check and give notice of defects

1) The Licensee shall inspect the delivered software including the documentation within eight working days after delivery, in particular with regard to the integrity of the data storage and manuals as well as the functionality of basic software functionality. Defects that are discovered or identifiable must be reported to the licensor within a further eight working days. The notification of defects must include a thorough description of the defects.

2) Defects that cannot be detected within the scope of the described examination must be reported within eight working days of discovery, in compliance with the notification requirements set out.

3) In the event of a breach of the obligation to check and give notice of defects, the software shall be deemed to have been approved in view of the defect in question.

§ § 11 Written Form

All agreements that include a change, amendment or specification of these contractual conditions as well as special assurances and agreements must be made in writing. If they are issued by the Licensor's representatives or assistants, they shall only be binding if the Licensor provides written consent.

§ 12 Governing Law

The parties agree to accept the application of the law of the Federal Republic of Germany with regard to all legal relationships arising from this contractual relationship, excluding the UN Convention on Contracts for the International Sale of Goods.

§ 13 Place of Jurisdiction

Insofar as the Licensee is a trader within the definition of the German Commercial Code (Handelsgesetzbuch), a legal entity under public law or a special asset under public law or has no place of jurisdiction in Germany, Stuttgart shall be agreed as the place of jurisdiction for all disputes arising in connection with the establishment, performance and termination of this contractual relationship.

§ 14 Severance Clause

Should individual terms and conditions be or become invalid, ineffective or contestable, they shall be interpreted or supplemented in such a way that the intended economic purpose is achieved in a legally permissible manner as closely as possible; the remaining terms and conditions shall remain unaffected. This shall also apply correspondingly to any omissions requiring further attention.

EULA Version 2.2 from 30. November 2022

B.2. Licensed Software

Parts of the Intra2net Groupware Client are subject to other licenses. If these licenses are required to be mentioned in the documentation, you will find them in the following section.

B.2.1. Info-ZIP

Copyright © 1990-1999 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution.
3. Altered versions -- including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions -- must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases -- including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP email addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "WiZ", "Pocket UnZip", "Pocket Zip" and "MacZip" for its own source and binary releases.

The Intra2net Groupware Client contains customized ("*altered*") parts of the program code of Info-ZIP.

B.2.2. JsonCpp

The JsonCpp library's source code, including accompanying documentation, tests and demonstration applications, are licensed under the following conditions:

Baptiste Lepilleur and The JsonCpp Authors explicitly disclaim copyright in all jurisdictions which recognize such a disclaimer. In such jurisdictions, this software is released into the Public Domain.

In jurisdictions which do not recognize Public Domain property (e.g. Germany as of 2010), this software is Copyright © 2007-2010 by Baptiste Lepilleur and The JsonCpp Authors, and is released under the terms of the MIT License (see below).

In jurisdictions which recognize Public Domain property, the user of this software may choose to accept it either as 1) Public Domain, 2) under the conditions of the MIT License (see below), or 3) under the terms of dual Public Domain/MIT License conditions described here, as they choose.

The full text of the MIT License follows:

Copyright © 2007-2010 Baptiste Lepilleur and The JsonCpp Authors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Index

A

- ACME protocol, 49-50
- Active Directory
 - Distributing Certificates, 48-49
 - Recipient Address Check, 85-87
 - Software Distribution, 130-131
- ADSL, 53
- Android
 - VPN Client, 290-297
- Antivirus
 - Email, 93-94
 - Proxy, 66-67
- ARP
 - Proxy, 57-58
- Assign colors, 169-172

B

- Backup
 - Backup, 178
 - Creation, 116-117
 - from Another Version, 118
 - Remote Storage, 117-118
 - Restore, 118
- BADMAC, 249
- Bandwidth Management, 59-61
- BIOS
 - Scheduled Startup, 123
 - Settings, 3-5

C

- Cable Connection, 54
- Cable Modem, 54
- Catch-All account, 81-83
- Categories, 169-172
- Certificate
 - for SSL/TLS, 44-45
 - installing onto a Client, 45-49
 - with Active Directory distribution, 48-49
- Certificate Authority (CA), 49-51, 260-261
- Certificates
 - for IPSec, 260-261
- Clients
 - Import and Export, 42-43
 - Registering, 41-42
- Cold standby system, 120
- Compatibility List, 3
- Configuration
 - Check, 34
 - Conflict, 33-34

- Restore, 30
- Upon Delivery, 2
- Configuring Outlook, 132-134
- Connection Establishment
 - to the Internet, 58
 - via Alternative Provider, 59
- Connection Monitoring, 59
- console
 - serial, 6
- Console, 29
 - serial, 29

D

- Data Privacy
 - Statistics, 72-73
- Data, Import Existing Data, 137-143
- De-Militarized Zone (DMZ), 55-58
- Default Settings, 2
- Demo Mode, 32
- DHCP, 41-42
 - Pool, 42
- DiffServ, 61
- DKIM, 96-102
 - Configuration, 98-100
 - Header, 96
 - Ways to get a signature, 97-98
- DMARC, 97
- DNS, 37-41
 - Firewall, 244
 - Forwarding, 38-41
 - Rebind, 39-41
- Domain, 37-41
- DSL-Modem, 53
- DynDNS, 62-63

E

- Email
 - Addresses, 87-88
 - Alias, 87-88
 - Antivirus, 93-94
 - Archiving
 - Interface, 102-103
 - MailStore Server, 103-110
 - Attachment Filter, 94-96
 - Automatic Transfer, 110
 - Deletion, 89
 - DKIM, 96-102
 - DMARC, 97
 - External server name (EHLO), 78
 - Forwarding
 - Domain, 84-87
 - Emails of a User, 88

- POP Accounts, 87
- Header, 177
- IMAP
 - on the Intra2net System, 79
- Mailinglist, 110
- Mailinglists, 110
- POP3
 - on the Intra2net System, 79
 - Polling and Forwarding, 87
 - Retrieving from Provider, 80-81
- Postmaster
 - Address, 110-111
- Queue, 111
- Read Status, 158
- Recipient Address Check, 84-87
 - Active Directory / LDAP, 85-87
 - SMTP, 84-85
- Relay
 - Client, 77
 - Direct, 78
 - Relay Permission, 74-75
 - Relay Server, 77
 - SMTP-Submission, 77
- Size, 111
- SMTP
 - Authentication, 74-75
 - Forwarding, 84-87
 - Receiving, 80-82
- Sorting, 89
- Source Text, 177
- Spamfilter
 - Detection, 90
 - Global, 90-91
 - Potential Spam, 90
 - Quarantine, 91
 - Scores, 90
 - SMTP, 89
 - Trusted Servers, 92-93
 - User-Dependent, 91-92
- SPF, 97
- Vacation Mode, 88-89
- Email folder (IMAP)
 - Shared, 157-158
- Email Folder (IMAP)
 - Synchronization Frequency, 167-168
- Email:
 - Flags, 116-117
 - IMAP
 - Flags, 116-117
- Emails
 - Tracking, 183
- Evasion
 - on Other Providers, 59

- Exchange
 - Migration from, 193-197
- Export
 - Clients, 43
 - User, 76

F

- Factory Settings, 2
 - Restore to, 30
- Fallback, 59
- Firewall
 - Automatic response rule, 244-245
 - before the Intra2net System, 122-123
 - Blocking after Login Errors, 249
 - Checking MACs, 249
 - DNS, 244
 - Emergency Mode, 30, 249
 - Entering Ports, 243
 - in VMware vSphere Hypervisor, 15-18
 - Netgroups, 243
 - on a Virtual Machine, 8-9
 - Registering IPs, 243
 - Routing, 43
 - Rulesets
 - Full, 243-248
 - Internet, 239
 - LAN, 239
 - Selecting, 239-240
 - Simple Profiles, 241-242
 - Services, 243
 - Terms, 245
- Folder
 - Excluding Folders from Synchronization, 153-154
 - Linking Own Folders, 152-153
 - Linking Shared Folders, 155-156
 - public, 189-190
 - Shared, 157-158
 - Synchronization Frequency, 167-168
- Forced Separation, 58
- Free/Busy, 172-175

G

- Groupware data
 - Import Existing, 137-143

H

- Hard Drive Damage, 118-119
- Hardware
 - compatible, 3
 - Replacement or Defect, 118-119
- Hot standby system, 121

I

- ibx_sub, 167
- IKE, 257-258
- IMAP
 - on the Intra2net System, 79
- IMAP Folder
 - Shared, 157-158
 - Synchronization Frequency, 167-168
- Import
 - Clients, 42-43
 - Existing Groupware Data, 137-143
 - User, 76
- Installation
 - from DVD, 6
 - from USB flash drive, 5-6
 - of Microsoft Hyper-V, 20-28
 - on VMware vSphere Hypervisor, 10-19
- Internet
 - Connection Establishment, 58
 - Connection Monitoring, 59
- Internet Speedometer, 33
- iOS
 - VPN Client, 288-289
- IP
 - Configuration, 29-30, 36
 - Official, 55-58
 - Private Network Areas, 30
 - Range, 42
- IPSec, 257
 - Aggressive Mode, 257-258
 - Certificates, 260-261
 - Client
 - Android, 290-301
 - iOS, 288-289
 - macOS, 285-287
 - MacOS X, 278-284
 - Windows, 271-277
 - Comparison with WireGuard, 338-340
 - Connecting a Client, 262-270
 - Connection Phases, 257-258
 - dynamic IP, 302
 - Encryption Algorithms, 258
 - Logs, 332-334
 - Main Mode, 257-258
 - Mode Config, 269
 - NAT, 327-331
 - Network-to-Network, 302-304
 - Perfect Forward Secrecy (PFS), 258
 - Pre-Shared Key, 257
 - Quick Mode, 258
 - Virtual IP, 269
 - XAUTH, 268

- IPSecuritas
 - VPN Client, 278-284
- ISAKMP, 257-258

L

- Lancom
 - VPN Connections, 314-323
- LDAP
 - Recipient Address Check, 85-87
- Let's Encrypt, 49-50
- Liability, 1
- License
 - Code Input, 114
 - Demo Mode, 114
 - Expiration, 114
 - Groupware Client, 369-373
 - Intra2net, 361-366
 - Open Source, 366-367
- License Code, 32
- Linus
 - Shell, 31
- Linux
 - VPN, 324-326
- Log files
 - Proxy, 68
- Logfiles
 - System, 123
- Login Error
 - Blocking IPs, 249

M

- MAC
 - Allocation, 41
 - Firewall, 249
- MailStore Server, 103-110
- Main Page, 32-34
- Mainpage
 - to Access via Internet, 63
- Microsoft Exchange
 - Migration from, 193-197
- Migration
 - from Microsoft Exchange, 193-197
- Monitoring
 - SNMP, 113
- Multidrop, 81-83

N

- NAT
 - for VPNs, 327-331
 - Masquerading (N:1), 61-62
 - statisch (1:1), 56-57
 - VPN Remote Side, 269

NCP
 Secure Android Client Premium, 298-301
 Secure Entry macOS Client, 285-287
 Secure Entry Windows client, 271-274
Network Card, 29-30, 36
 Type, 30, 36
NTP, 113

O

Openswan, 324-326
Outlook Profile, 132-134

P

Password
 Administrator, 2
 Root, 31
Perfect Forward Secrecy (PFS)
 IPSec, 258
 SSL/TLS, 51-52
POP3
 Collective Accounts (Multidrop, Catch-All), 81-83
 on the Intra2net System, 79
 Polling and Forwarding, 87
 Retrieving from Provider, 80-81
Postmaster
 Address, 110-111
Poweroff, 34
PPPoE, 53
 Passthrough, 53
PPTP, 53
Pre-Shared Key, 257, 336
Private Marking, 175-176
Proxy
 Access Lists, 65-66
 Antivirus, 66-67
 Destination Ports, 65
 Logging, 68
 Port, 64
 Profile, 65
 Statistics, 68-69
 Time Management, 66
 Transparent, 64-65
 URL Filter, 65-66
 Web Content Filter, 66
Proxy-ARP, 57-58

Q

Quality-of-Service (QoS), 59-61

R

RAID

 Hardware, 5
 Software, 5
Range, 42
Registry, 204-213
Reminders, 176
Remote Access
 on the Intra2net System, 63
Remote Support, 63
Rescue System, 115-116
Rights
 Network Object, 37
 User, 74-75
Root Password, 31
Router, 53-55
Routing
 DMZ, 55-58
 Internet, 53-55
 LAN, 43

S

Search Indexer, 136-137
Serial console, 6
Shared
 from Email Folders, 157-158
Shared Folders
 Reminders, 176
Shrew Soft
 VPN Client for Windows, 275-277
Shutdown, 34
 Scheduled, 123
SMTP
 Authentication, 74-75
 Forwarding, 84-87
 Receiving, 80-82
 Recipient Address Check, 84-85
 Relay
 Direct, 78
 Relay Server, 77
SNMP, 113
Spamfilter
 Detection, 90
 Global, 90-91
 Potential Spam, 90
 Quarantine, 91
 Scores, 90
 SMTP, 89
 Trusted Servers, 92-93
 User-Dependent, 91-92
SPF, 97
SSL
 Certificate, 44-45
 Encryption Methods, 51-52

- Perfect Forward Secrecy (PFS), 51-52
- Principles, 44
- Standby system, 120-122
 - Cold standby, 120
 - Hot standby, 121
- Statistics
 - Data Privacy, 72-73
 - Internet, 69-70
 - Proxy, 68-69
 - Space usage, 72
 - Speedometer, 70-72
- strongSwan, 324-326
- Synchronization Frequency
 - Groupware Folder, 167-168

T

- Time Synchronization, 113
- TLS
 - Certificate, 44-45
 - Principles, 44
- Tracking Function, 183

U

- Update
 - Antivirus, 115
 - Reboot, 115
 - Remote Operation via Partner Web, 115
 - Rescue System, 115-116
 - Spamfilter, 115
 - System, 114-115
- Update folder list
 - Update folder list, 154-155
- URL Filter, 65-66
- User
 - Group, 74
 - Import and Export, 75-76
 - Rights, 74-75
- user account
 - shared, 189-190

V

- VDSL, 53
- Version, 1
- Virtual Machine, 8-28
- Virus Scanner
 - Email, 93-94
 - Proxy, 66-67
- VLAN
 - Dial-up with DSL (PPPoE), 53
 - VLAN Tagging, 36-37
- VMDirectPath, 15-18
- Voice-over-IP (VoIP)

- Prioritize, 61
- VPN, 257
 - Address Conflict, 327-331
 - Comparison of IPSec with WireGuard, 338-340
 - Connect client
 - WireGuard, 343-344
 - Connecting a Client
 - IPSec, 262-270
 - dynamic IP, 302
 - FRITZ!Box, 353-357
 - NAT, 327-331
 - Network-to-Network, 302-304
 - Site-to-site, 349-352
 - WireGuard, 336-338

W

- Wake-On-LAN, 41
- Web Content Filter, 66
- Web Interface
 - to Access via Internet, 63
- WireGuard
 - Basics, 336-338
 - Client installation, 345
 - Comparison with IPSec, 338-340
 - Connect client, 343-344
 - FRITZ!Box, 353-357
 - Interface, 341
 - Private key, 341
 - Site-to-site, 349-352
 - UDP port number, 341

X

- X.509
 - for IPSec, 260-261
 - for SSL/TLS, 44-45
- XAUTH, 268

Z

- ZyWALL VPN-Router, 305-309