

Administration von PCs im Active Directory der GWDG



Impressum

Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen

Telefon: 0551 201-1510
Telefax: 0551 201-2150
E-Mail: gwdg@gwdg.de
WWW: www.gwdg.de

© 2018

Titelbild: © Mihai Simonia - Fotolia.com

Vorwort

Schon seit einigen Jahren findet halbjährlich ein Einführungskurs für Institutsadministratoren in unser Active Directory (kurz AD) statt. Um das Gelernte zu ordnen und um Informationen darüber hinaus anzubieten, haben wir diese „Admin-Fibel“ verfasst. Sie richtet sich an Administratoren im Active Directory und soll sowohl als Anleitung als auch als Nachschlagewerk dienen.

In dem vorliegenden Heft haben wir alle Tätigkeiten eines Institutsadministrators beschrieben und sind auf bekannte Probleme und deren Lösungen eingegangen. Wir haben in vielen Abschnitten Hinweise zu weiteren Erläuterungen auf unseren Webseiten angegeben. Wenn Sie diese Links nicht abtippen möchten, können Sie dieses Heft auch als PDF-Dokument - mit funktionierenden Verknüpfungen auf die entsprechenden Webseiten der GWDG - herunterladen.

Zur besseren Lesbarkeit haben wir in diesem Admin-Heft auf Konstruktionen wie „Administratorinnen und Administratoren“ oder „Nutzerinnen und Nutzer“ verzichtet. Gleich in welcher Art wir die Beispiele formulieren, es sind natürlich immer beide Geschlechter angesprochen. Aus gleichem Grund sind URLs und Rechnernamen in Groß- bzw. Kleinschreibung gehalten, auch wenn diese nicht „case sensitive“ sind und es daher eigentlich egal ist, ob man sie groß oder klein schreibt.

Wir hoffen, dass diese Admin-Fibel auf lange Sicht die erste Anlaufstelle bei Problemen sein wird. Sollten Sie also Ideen, Anregungen und Ergänzungen zu unserem Heft haben, würden wir uns freuen, wenn Sie uns diese per E-Mail mitteilen würden, damit wir Ihre Vorschläge mit aufnehmen können.

Göttingen, August 2018

AD-Team der GWDG

Aufbau des Buches

Sie finden in diesem Buch thematisch gegliederte Kapitel zum Aufbau des Active Directory und der begleitenden Dienste wie Benutzerverwaltung, Speicherdienste, E-Mail-Service und Druckdienst. Die Einrichtung und Administration wird anhand praktischer Beispiele in allen Arbeitsschritten erklärt.

Typografische Konventionen

Im Text werden folgende Formatierungselemente verwendet:

Schattierte Hervorhebung	kennzeichnet die Hyperlinks und E-Mail-Adressen
Schwache Hervorhebung	wird für Kommandos und Verweise verwendet
Intensive Hervorhebung	Bezeichnung der Server o. Laufwerke u. Namensangaben
FETT- und GROßSCHREIBUNG	Angabe der Kürzel
Text mit Hintergrundschattierung	wird für Hinweise verwendet
<i>[Kursiv im eckigen Klammern]</i>	je nach Situation abweichende Namensvergabe
Betont	wird für Verweise verwendet

Wichtige Informationen vorab

Wir hoffen natürlich, dass Sie in diesem Heft alle nötigen Erstinformationen finden. Darüber hinaus gibt es aber auch andere Informationsquellen, die Sie nutzen können.

Mailingliste

Um immer auf dem neuesten Informationsstand zu bleiben, sollten Sie die Mailingliste **GWDG-AD** abonnieren. Über diese Liste werden aktuelle Änderungen, Aktualisierungen zentral verteilter Software sowie interessante Schulungsangebote rund um das AD mitgeteilt. Informationen zur Teilnahme an unseren Mailinglisten erhalten Sie auf unseren Webseiten unter <https://listserv.gwdg.de/mailman/admin>.

Die Mailingliste **GWDG-AD** können Sie auch direkt über folgende Webadresse abonnieren: <https://listserv.gwdg.de/mailman/admin/gwdg-ad>.

Abrechnung in Arbeitseinheiten

Die Abrechnung von Dienstleistungen der GWDG für die Institute niedersächsischer Hochschulen und der Max-Planck-Gesellschaft erfolgt über Arbeitseinheiten (AE). Jedes Institut verfügt über ein bestimmtes Kontingent an Arbeitseinheiten, mit dem Dienstleistungen in Anspruch genommen werden können. Die Kontingente werden quartalsweise zugeordnet. Sollte das Kontingent Ihres Institutes einmal aufgebraucht sein, wenden Sie sich bitte an Ihren

Netzwerkbeauftragten, der dann eine Aufstockung bei der GWDG beantragen kann. Weitere Informationen zu unserem Kontingentierungssystem finden Sie auf folgenden Webseiten: <https://www.gwdg.de/about-us/catalog/kontingentierung>

Support

Sollten Sie Probleme mit Ihrem Benutzerkonto haben, den Speicherplatz Ihres Kontos vergrößern wollen oder weitere Fragen haben, dann wenden Sie sich per E-Mail an unseren Support support@gwdg.de oder per Telefon unter **0551 201-1523**.

Das Beispielinstitut UXYZ

In diesem Heft werden die Beispiele anhand eines imaginären Instituts mit dem Kürzel **UXYZ** abgehandelt. Dieses Institut entspricht in seiner Struktur einer typischen Abteilung der Universität und besteht aus der Institutsleitung, wissenschaftlichen und nichtwissenschaftlichen Mitarbeitern, einigen Hilfswissenschaftlern, einer Administratorin (**Oadminid**) sowie diversen Gästen in wechselnder Anzahl. Das Institut verfügt über einen kleinen Raum mit öffentlich genutzten Computern und bringt auch ansonsten recht typische Gegebenheiten mit: Die Arbeitsplatzrechner und Benutzerkonten sollen in das AD integriert, die Institutsdrucker sollen gemeinsam genutzt und der CIP-Raum auch von Studierenden mit studIT-Account genutzt werden können.

Die Administratoren



Patrick Becker

patrick.becker@gwdg.de

Zentrale Verteilung von Betriebssystemen und Software, baramundi, Sophos Enterprise Console, zentrale Einrichtung von Institutsdruckern



Katrin Hast

katrin.hast@gwdg.de

Planen und Erstellen von Instituts-umgebungen innerhalb des Active Directory, Sophos Enterprise Console, zentrale Einrichtung von Institutsdruckern, Öffentlichkeitsarbeit für das Active Directory, Active Directory-Koordination



Eric Helmvoigt

eric.helmvoigt@gwdg.de

Exchange und MS Outlook, Schulungen zu MS Outlook, Benutzerverwaltung, Monitoring



Dr. Konrad Heuer

konrad.heuer@gwdg.de

Druckumgebung der GWDG, Samba-Server



Thomas Körmer

thomas.koermer@gwdg.de

Migration in das Active Directory, zentrale Verteilung von Betriebssystemen und Software, baramundi, Benutzerverwaltung



Stefan Quentin

stefan.quentin@gwdg.de

Verwaltung der Domänen des Active Directory, Windows-Fileservice, Tivoli für Windows, Serveradministration



Torsten Unruh

torsten.unruh@gwdg.de

Serverinstallation, Windows-Support, iDrac



Martina Willmann

martina.willmann@gwdg.de

Remote Desktop Server, Gruppenrichtlinien, virtuelle Desktops für Schulungen

Inhaltsverzeichnis

Vorwort	ii
Aufbau des Buches	iii
Typografische Konventionen.....	iii
Wichtige Informationen vorab	iii
Mailingliste.....	iii
Abrechnung in Arbeitseinheiten	iii
Support.....	iv
Das Beispielinstitut UXYZ.....	iv
Die Administratoren.....	v
Die Active Directory-Gesamtstruktur.....	1
Strukturübersicht.....	2
Voraussetzungen zur Teilnahme am Active Directory	6
Strukturen im Active Directory.....	6
Aufbau und Namensschema	6
<i>Domännennamen.....</i>	<i>6</i>
<i>Organisationseinheiten (OUs).....</i>	<i>6</i>
<i>Namensschema.....</i>	<i>7</i>
Rechteverteilung im Active Directory	7
<i>Zuordnung von Benutzerrechten.....</i>	<i>7</i>
<i>Sicherer Umgang mit dem Administratorkonto.....</i>	<i>8</i>
Benutzerkonten.....	8
Benutzerkataloge der GWDG.....	8
Das Benutzerkonto.....	9
<i>Ein Benutzerkonto beantragen.....</i>	<i>10</i>

<i>Passwort überprüfen und ändern</i>	10
<i>Gesperrtes Benutzerkonto</i>	11
<i>Passwortspeicher löschen</i>	11
Die Remotedesktopserver der GWDG	12
Eine Remotedesktop-Verbindung (RDP) zu einem Server herstellen	12
<i>GWD-WinTS1</i>	13
<i>GWD-WinTS3</i>	13
Active Directory -Benutzer und -Computer	13
Aufbau	14
Navigation im Active Directroy	14
Verwaltung von Benutzergruppen in der Instituts Umgebung	15
<i>Die Administratorengruppe</i>	16
<i>Gruppen erstellen</i>	16
<i>Mitarbeiter den Gruppen zuordnen</i>	17
<i>Gruppen und Ressourcen</i>	18
<i>Freigabeberechtigungen</i>	19
<i>NTFS-Rechte konfigurieren</i>	20
Der Container „Computers“	22
Die OU „Systeme“	23
<i>Gruppenrichtlinien</i>	23
<i>Softwareverteilung über Gruppenrichtlinien</i>	23
Die Migration eines Computers in das Active Directory	24
Ein neues Computerkonto anlegen.....	24
Netzwerkparameter	25
Einen Computer einer Domäne des Active Directory hinzufügen	26

<i>Computername ändern</i>	27
<i>Computer in die Domäne heben</i>	27
<i>Update der Gruppenrichtlinien auf dem Arbeitsplatzrechner</i>	28
Lokale Systemeinstellungen am PC im Active Directory	29
<i>Synchronisation von Offlinedateien deaktivieren</i>	30
Öffentliche Computer im Active Directory	31
Sophos Anti-Virus und die Sophos Enterprise Console	32
Vorbereitung der Arbeitsstation für die Verwendung der Enterprise Console.....	32
<i>Firewall-Einstellungen</i>	32
<i>Dienste</i>	32
<i>Einstellungen im Netzwerk- und Freigabecenter</i>	33
Verwaltung mit der Sophos Enterprise Console	33
<i>Rechner der Sophos-Gruppe hinzufügen</i>	34
<i>Sophos per Enterprise Console installieren</i>	35
<i>FAQ: Häufige Fehler während der Installation mit der Sophos Enterprise Console</i>	36
<i>Virenbekämpfung mit der Sophos Enterprise Console</i>	37
Sophos-Richtlinien.....	39
Migration der Benutzerumgebung	41
Übertragung der Daten auf das persönliche Laufwerk (P:).....	41
Das Benutzerprofil	42
Einstellungen für E-Mail und Internet sichern	42
Übertragung von Betriebssystem-Einstellungen.....	42
Servergespeicherte Benutzerprofile	43
Empfehlungen für die Verwendung des servergespeicherten Profils	43
<i>FAQ: Profilprobleme</i>	44

Drucker im Active Directory.....	46
Zentral verwaltete Institutsdrucker	46
Manuelle Druckerverbindungen unter Windows.....	47
Die E-Mail-Umgebung.....	47
E-Mail-Adresse	47
E-Mail-Zertifikate	48
<i>Verwendung des Zertifikats mit Outlook</i>	<i>48</i>
Exchange E-Mail-Server	49
Konfiguration von Outlook	50
<i>Konfigurationseinstellungen Outlook mit Exchange-Funktionalitäten</i>	<i>50</i>
<i>Konfigurationseinstellungen Outlook ohne Exchange-Funktionalitäten</i>	<i>52</i>
<i>FAQ: Automatische Konfiguration per Autodiscover schlägt für Outlook 2016 fehl</i>	<i>53</i>
Sicherung von Daten	54
Outlook Web App (OWA)	54
Mobiler E-Mail Zugang.....	54
Weitere Informationen & Hilfe.....	55
Speicherbereiche.....	55
Backupverfahren	55
Ein Netzlaufwerk manuell verbinden	56
Verwendung der Netzlaufwerke außerhalb des GÖNET (z. B. private PC)	57
<i>Zugang über VPN.....</i>	<i>57</i>
<i>Zugang über einen Remote Desktop Server.....</i>	<i>57</i>
Gemeinsames Laufwerk verwalten.....	58
Weitere Informationen	58
Support-Schnittstelle.....	58

TeamViewer	58
Kurse	59
<i>Teilnahmebedingungen</i>	59
Leihrechner	60
Unsere öffentlichen Rechner	60
GWDG-Benutzerraum.....	60
ANHANG	61
Checkliste.....	61
Glossar	62

Die Active Directory-Gesamtstruktur

Das Active Directory der GWDG besteht seit 2002 und hat sich seither stets weiterentwickelt. Die entstandene Struktur ist in verschiedene Domänen unterteilt. Eine Domäne ist ein Organisationskonstrukt, in dem diverse Objekte verwaltet und vernetzt werden. Eine solche Zusammenfassung ermöglicht eine zentrale administrative Verwaltung von Objekten wie z. B. Computer- und Benutzerkonten sowie die gemeinsame Verwendung von Ressourcen. Diese Ressourcen können z. B. Netzwerkdrucker oder Speicherbereiche sein. Alternativ dazu kann die Administration auch dezentral von den einzelnen Institutsadministratoren durchgeführt werden, also auf Teilstrukturen einer Domäne - sogenannte Organisatorische Einheiten (kurz **OU** für **Organizational Unit**) - begrenzt werden.

Das bedeutendste Merkmal der Active Directory-Struktur ist das „Single Sign-on“. Dies ermöglicht einem Benutzer nach einer einmaligen Authentifizierung den Zugriff auf alle Rechner und Dienste, für die er berechtigt ist, ohne sich an jeder Ressource neu anmelden zu müssen. Generell hat jeder Benutzer nur einen Account. Nimmt eine Person mehrere Rollen im System ein, so kann sie auch mehrere Benutzerkonten nutzen. Ein Administrator verfügt beispielsweise neben seinem normalen Benutzer-Account noch über einen Administrator-Account.

Ziel ist es, durch eine zentrale Verwaltung von Benutzerkennungen, Computern und Druckern den Zugriff auf Ressourcen im Netzwerk für die Anwender zu vereinfachen. Gleichzeitig soll auch eine Arbeitserleichterung und eine verbesserte Unterstützung seitens der GWDG für die IT-Verantwortlichen in den Instituten erreicht werden. Die Einführung neuer Techniken kann so zentral implementiert und universitätsweit einheitlich umgesetzt werden.

Strukturübersicht

Auf den nächsten beiden Seiten finden Sie eine Abbildung der AD-Gesamtstruktur. Das AD besteht aus drei Ebenen. Die Aufteilung in verschiedene Ebenen ist vor allem für die DNS-Namensgebung und das zentrale IT-Management relevant. Wir wollen als Beispiel den Baum [uni-goettingen](#) verwenden, um den Aufbau der Struktur zu erläutern.

In der obersten Domäne dieses Baumes, der [uni-goettingen.de](#)-Domäne, sind verschiedene administrative Funktionen (z. B. die Synchronisation mit anderen Domänen) etabliert.

In der zweiten Ebene befinden sich die Domänen, die den Fakultäten der Universität Göttingen entsprechen. Sie sind blau eingefärbt und werden von der GWDG zur Verfügung gestellt, um den Instituten einen Raum zur Migration der Arbeitsstationen in die Struktur zu bieten. In den Domänen der Fakultätsebene werden folglich verschiedene Institute und Abteilungen der Fakultät zusammengefasst. Der DNS-Name dieser Domänen setzt sich aus der Domäne der ersten Ebene ([uni-goettingen.de](#)) und einem Namenskürzel für die Fakultät zusammen (z. B. [bio.uni-goettingen.de](#)). Die Aufteilung in Organisationseinheiten innerhalb einer Domäne ermöglicht eine bedarfsorientierte administrative Anpassung der Institute und Abteilungen. Die weiteren Domänen der zweiten und der dritten Ebene sind Domänen von Instituten, deren IT-technische Bedürfnisse eine eigene Domäne erfordern und deren personelles und finanzielles Budget den Unterhalt einer eigenen Domäne erlauben.

Der Namensraum der dritten Ebene wird aus dem Namen der ersten und zweiten Domänenebene mit einem vorangestellten Namenskürzel des Institutes konstruiert (z. B. [avh.bio.uni-goettingen.de](#)).

Innerhalb dieser Struktur befinden sich vorwiegend die Systeme (Arbeitsstationen und Server), während die GWDG-Benutzerkonten sowie die zentralen Dienste in der Domäne [top.gwdg.de](#) angesiedelt sind.

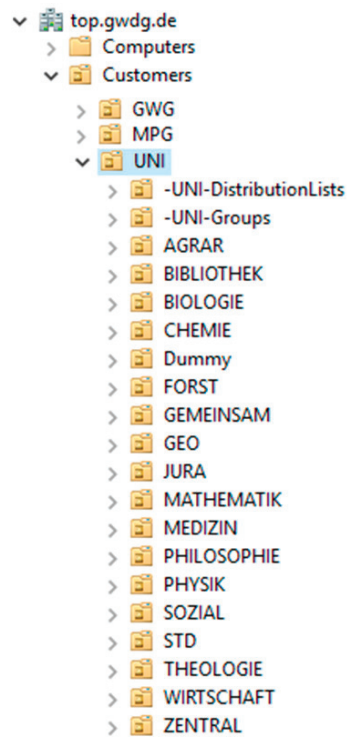
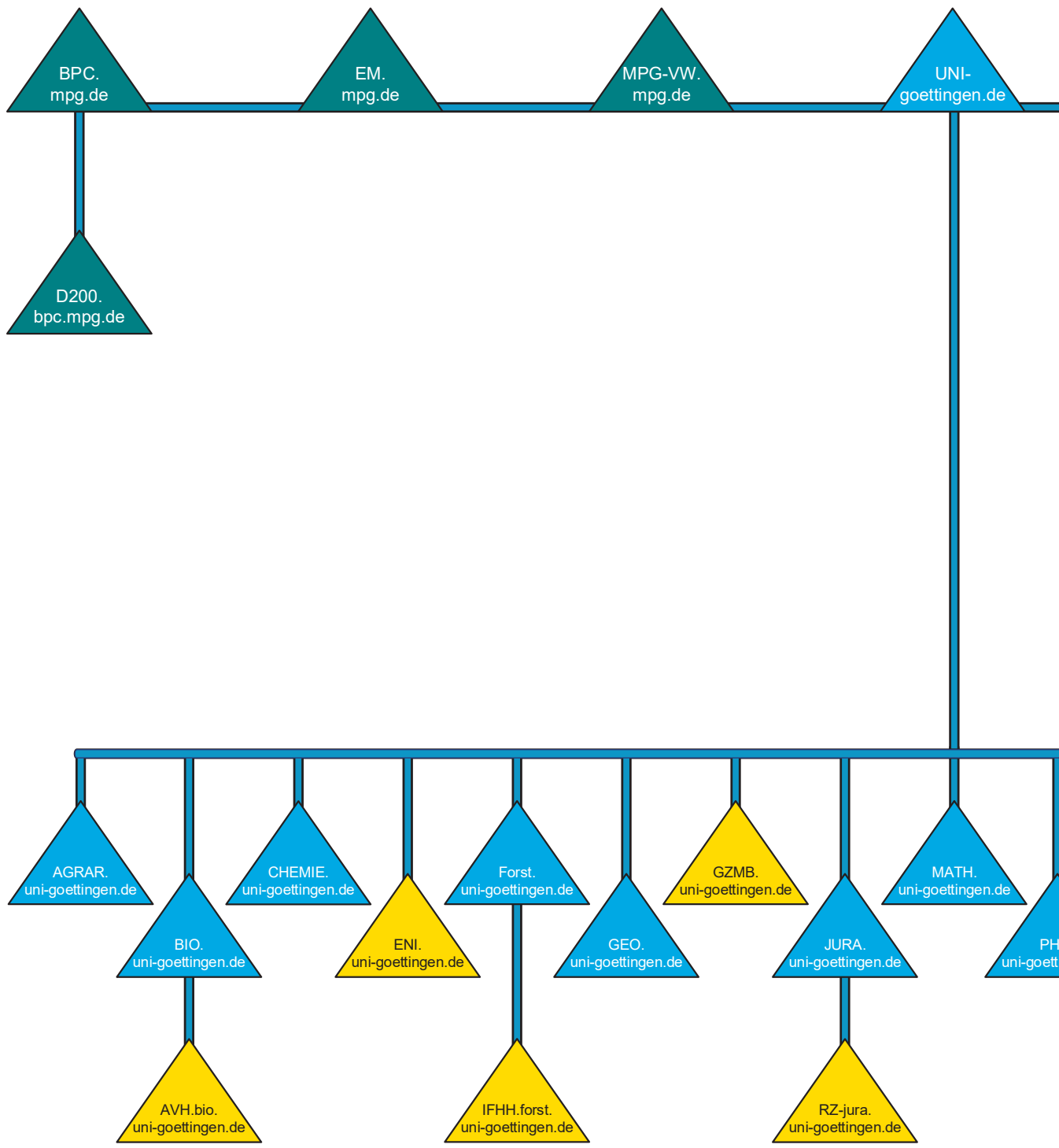


Abbildung 1: Einteilung der Benutzerkonten in Fachbereiche

Da die Kosten für Hardware und Lizenzen sowie der personelle Aufwand für die Verwaltung eigener Domänen ständig steigen, empfehlen wir, auf eigene Domänen zu verzichten bzw. die bereits vorhandenen in die Fakultätsdomänen zurück zu migrieren. Ein weiterer Grund für die Minimierung von Domänen liegt im technischen Fortschritt, also der deutlich erhöhten Kapazität von Domänen-Controllern, die mit neuen Betriebssystemen und häufig auch deutlich leistungsfähigerer Hardware ausgestattet sind. Dieses ermöglicht ein Hochstufen des Modus, in dem das Active Directory ausgeführt wird. Mit jedem Upgrade werden wieder neue technische Möglichkeiten eingeführt, aber auch die mögliche Anzahl der zu verwaltenden Objekte wird erweitert.

GÖ* Active Directory-Struktur



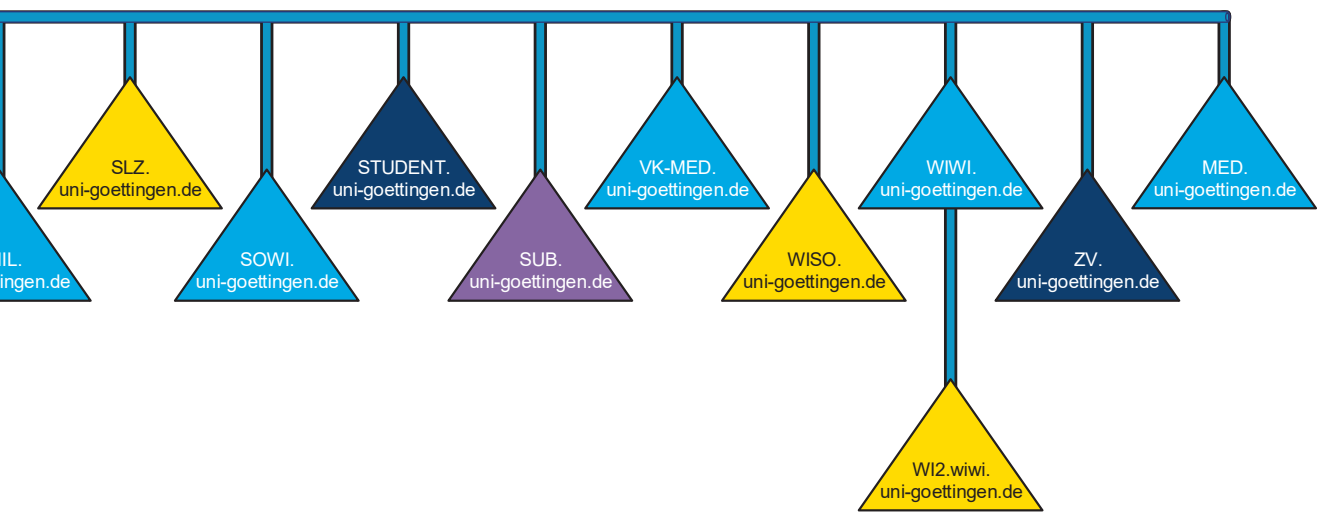
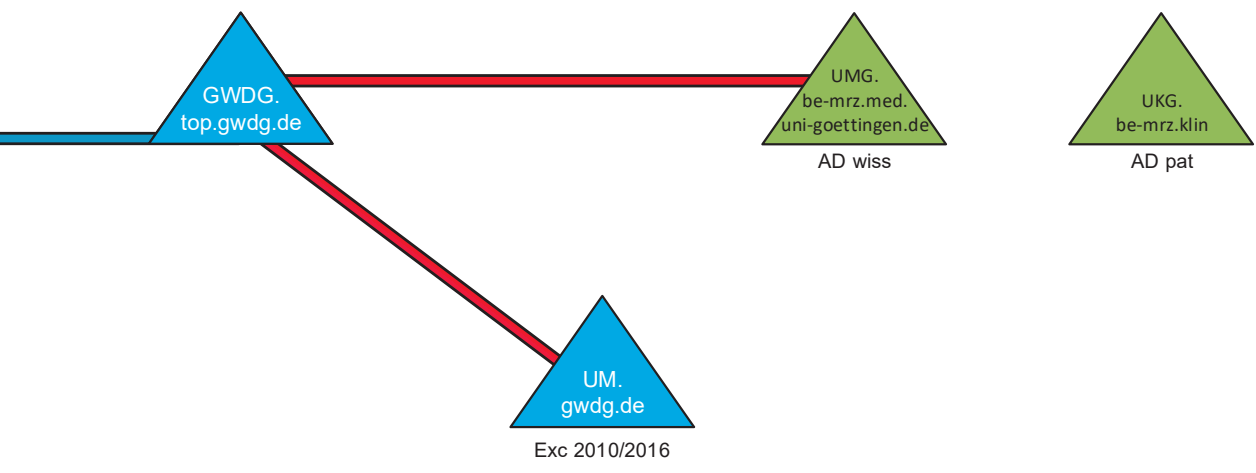
Legende:

AD-Bereiche verwaltet durch:



▬ Manuell erstellte Vertrauensstellung

Abbildung 2: Der Active Directory Forest



Domäne (Stand: Aug 2018)

Voraussetzungen zur Teilnahme am Active Directory

Wenn Sie mit Ihrem Institut an dem Active Directory der GWDG teilnehmen möchten, benötigen alle Mitarbeiter einen GWDG-Account oder alternativ ein studentisches Benutzerkonto der studIT. Dem Benutzerkonto werden innerhalb des AD die Zugriffsrechte für Ressourcen wie z. B. Laufwerksfreigaben oder Drucker zugeordnet. Außerdem wird es für die Anmeldung am Arbeitsplatzrechner verwendet.

Besonders wichtig ist, dass Sie für Ihr Institut bzw. Ihre Abteilung einen lokalen Administrator benennen. Voraussetzung für diese Tätigkeit sind vor allem das Interesse an der IT und einige Grundkenntnisse in der Verwendung von Computern. Alles Weitere vermitteln wir in unseren eintägigen Kursen (siehe hierzu auch den Abschnitt **Kurse**) zur Administration von Arbeitsplätzen. Das komplette Kursangebot der GWDG finden Sie auf der Webseite <https://www.gwdg.de/kurse>.

Der lokale Administrator muss die Betreuung der Systeme vor Ort sicherstellen. Die Tätigkeit wird durch unsere umfangreichen zentralen Dienstleistungen deutlich benutzerfreundlicher und einfacher. Ein Support vor Ort kann von der GWDG aus personellen Gründen nur in Ausnahmefällen durchgeführt werden. Eine zeitnahe Reaktion muss durch den lokalen Administrator sichergestellt sein. Wir stehen darüber hinaus aber natürlich auch gerne bei Problemen zur Verfügung. Schreiben Sie bei Bedarf einfach eine E-Mail an support@gwdg.de.

Strukturen im Active Directory

Konventionen sorgen für Übersicht und Ordnung. Wenn die Organisation von Computerkonten sowie die Rechteverteilung einem festgelegten Schema folgen, erleichtert das den Support und die Fehlersuche. Bitte lesen Sie sich daher den folgenden Abschnitt gut durch und halten Sie sich an das darin aufgestellte Namensschema. Dadurch vermeiden Sie viele Probleme gleich im Voraus und verkürzen evtl. Supportzeiten.

Aufbau und Namensschema

Unser Active Directory besteht inzwischen aus rund 31 Domänen und über 13.000 Arbeitsplatzrechnern. Um das alles übersichtlich zu gestalten, folgt die Benennung einzelner Systeme einem einfachen Schema.

Domänennamen

Domänennamen werden, wie im Kapitel **Strukturübersicht** beschrieben, zusammengefügt. Eine Anpassung der Rechnernamen an die DNS-Struktur im IPAM (IP-Adress-Management) ist möglich.

Organisationseinheiten (OUs)

Eine Domäne wird in weitere Verwaltungseinheiten unterteilt. Diese Verwaltungseinheiten nennt man OUs. In der Regel stellen die OUs eine Abbildung von Instituten und Abteilungen da. Eine OU kann Objekte wie z. B. Benutzerkonten, Computer und Gruppen enthalten.

Namensschema

Das Namensschema folgt ein paar einfachen Regeln, die hier am Beispiel des Instituts UXYZ erläutert werden.

Der Name einer OU setzt sich aus dem Institutskürzel (UXYZ) und der Abteilungsnummer (100) zusammen. Hier gibt es verschiedene Ebenen:

1. Ebene: Das Institut (z. B. UXYZ)
2. Ebene: Die Abteilung (z. B. UXYZ100)
3. Ebene: Benutzer und Systeme (Hier befinden sich Computerkonten und Benutzergruppen).

Das für Sie relevante Institutskürzel und die Abteilungsnummer werden bei einer Migration in Abstimmung mit der GWDG festgelegt.

Für Benutzer und Computer gilt Folgendes:

Benutzergruppen	UXYZ100-Admins	(Administratorengruppe)
	UXYZ100	(Mitarbeiter und stud. und wiss. Hilfskräfte; bei Bedarf auch weitere)
	UXYZ100-Share	(steuert Freigaberechte auf gemeinsames Laufwerk und beinhaltet alle Gruppen einer Abteilung)
	UXYZ-all-Share	(steuert Freigaberechte auf gemeinsames Laufwerk und beinhaltet alle Share-Gruppen der Abteilungen)
Computerkonto der Arbeitsstationen	UG-UXYZ100-C001	(die letzten drei Zeichen können zur individuellen Nutzung verbleiben, viele verwenden die letzte Zahl der IP-Adresse)
Druckerkonto	UG-UXYZ100-P01	(alternativ letzte Ziffern der IP)
Computerkonto der Server	UG-UXYZ100-VS1	(virtueller Server)
	UG-UXYZ100-S1	(Hardware-Server)
Spezielle Benutzerkonten in Ausnahmefällen	UXYZ100-gast1/kurs1	(Gästekonten, Kurs- oder Besucher-Konten)

Rechteverteilung im Active Directory

Zuordnung von Benutzerrechten

Im Active Directory gibt es verschiedene Benutzergruppen, die unterschiedliche Rechte erhalten.

Benutzer	Mit einem normalen Benutzerkonto, also einem GWDG- oder studIT-Account, kann sich ein Benutzer an fast allen Rechnern im AD anmelden. Benutzer werden in Benutzergruppen organisiert, über die Zugriffsrechte auf Ressourcen gesteuert werden. Mit einem Benutzerkonto sind keine administrativen Tätigkeiten möglich.
----------	--

Administratoren	<p>Dieses Konto wird von den Instituten über den Antrag auf einen Funktionsaccount beantragt, der unter dem folgenden Link zu finden ist: https://lotus1.gwdg.de/gwdgdb/benutzer_input.nsf/Funktionsaccount?OpenForm</p> <p>Dieses Konto soll eine dem Namensschema entsprechende Form haben. Das GWDG-Benutzerkonto mit einer vorangestellten 0 (Null), z. B. 0adminid.</p> <p>Bitte melden Sie sich, sobald Ihnen das Konto zur Verfügung steht. Standardmäßig werden diese Administratoren mit folgenden Privilegien auf einer OU versorgt: Sie können in der zugeordneten OU neue Computer-Konten anlegen, Rechner in die OU integrieren sowie Gruppen erstellen und verwalten. Bei Bedarf können die Berechtigungen erweitert werden.</p>
Domänen-Administratoren (nur für Institute mit eigenen Domänen relevant)	<p>Ein Domänen-Administrator verwaltet eine gesamte Domäne und kann auf alle zugehörigen Objekte Einfluss nehmen. Bei den Objekten kann es sich z. B. um Computer, Benutzer, Gruppen oder Richtlinien handeln.</p>

Sicherer Umgang mit dem Administratorkonto

Um den Administrator und die Benutzer, für die er verantwortlich ist, zu schützen, sollte ein verantwortungsvoller Umgang mit dem Administratorkonto selbstverständlich sein. Hierzu gehört an erster Stelle ein sicheres Passwort (siehe hierzu auch den Abschnitt **Passwort überprüfen und ändern**). Des Weiteren sollte das Administratorkonto nur für Tätigkeiten genutzt werden, für die es auch notwendig ist. Für Standardaufgaben wie E-Mail-Bearbeitung und Textverarbeitung sind die nicht-administrativen Benutzerkonten vorgesehen.

Benutzerkonten

Benutzerkataloge der GWDG

Für die Benutzerkennungen gibt es bei der GWDG mehrere Benutzerkataloge. Jede Benutzerkennung existiert in der Regel in allen Systemen unter demselben Namen.

Ein Benutzerkatalog ist vom Typ **LDAP** (Lightweight Directory Access Protocol). Er überwacht die Anmeldungen im Workstation-Cluster (auch UNIX-Cluster genannt), auf den Parallelrechnern der GWDG, verschiedener Dienste sowie am **WLAN** (Wireless Local Area Network) des Göttingen Campus.

Ein zweiter Benutzerkatalog ist für den Zugang zu den Servern im Active Directory der GWDG zuständig. Der hier gelistete Benutzername mit Passwort regelt den Zugang zu den mit der Benutzerkennung verbundenen persönlichen und gemeinsamen Speicherbereichen, dem E-Mail-Konto sowie die Anmeldung im Active Directory der GWDG. Das Active Directory vereint alle angeschlossenen Arbeitsplatzrechner und Server zu einem Gesamtsystem mit den dazugehörigen Ressourcen.

Die Passwörter in beiden Katalogen werden über das Identity-Management-System (IDM) verwaltet und gleichgehalten bzw. abgeglichen.

Das Benutzerkonto

Um die Rechenanlagen, Datenübertragungsnetze und sonstigen Ressourcen der GWDG nutzen zu können, muss ein Mitarbeiter der Universität Göttingen oder der Max-Planck-Gesellschaft bei der GWDG eine Benutzerkennung besitzen. Die Beantragung einer Benutzerkennung können Mitarbeiter der Max-Planck-Gesellschaft über einen Online-Antrag auf den GWDG-Seiten durchführen:

<https://www.gwdg.de/de/ueber-uns/leistungskatalog/antragsformulare>

Für Mitarbeiter der Universität Göttingen wird seit dem 04.04.2016 der Account automatisch erzeugt, sobald dieser einen Arbeitsvertrag mit der Universität bzw. der Universitätsmedizin abgeschlossen hat. Analog erfolgt auch eine automatische Deaktivierung des Accounts, sobald er die Universität bzw. Universitätsmedizin wieder verlässt. Weitere Informationen zu dem Thema finden Sie hier:

https://info.gwdg.de/docs/doku.php?id=de:services:general_services:einhmitarb:start

Unabhängig davon müssen Funktionsaccounts (z. B. für die Administration im AD) weiterhin per Online-Formular beantragt werden:

<https://www.gwdg.de/de/ueber-uns/leistungskatalog/antragsformulare>

Die Benutzerkennung besteht aus drei Teilen: dem Benutzernamen (auch User-ID genannt), der Account-Nummer und dem Passwort (auch Kennwort).

Der Benutzername wird in der Regel aus dem ersten Buchstaben des Vornamens und den ersten sechs Buchstaben des Nachnamens des Benutzers gebildet. Ist der sich ergebende Name schon vorhanden, wird eine Ziffer angehängt. Lautet der Name einer Benutzerin beispielsweise **Monika Mustermann**, so ergibt sich als Benutzername **mmuster**.

Nach der Einführung des einheitlichen Mitarbeiteraccounts am 04.04.2016 wurde das Namensschema dem SAP angepasst. Das neue Format des Benutzernamens besteht aus dem Nachnamen und wird bei Dopplungen mit einer Zahl ergänzt (z. B. **mustermann12**).

Die Account-Nummer wird einem Konto zugeordnet. Über diese Nummer werden die in Anspruch genommenen Ressourcen der GWDG verbucht und später abgerechnet. Die Account-Nummer besteht aus acht Zeichen: einer vierstelligen Kennung für das Institut, in dem die Person arbeitet, gefolgt von vier Ziffern. Arbeitet **Monika Mustermann** beispielsweise im Institut **UXYZ**, dann setzt sich die zugehörige Account-Nummer aus der Institutskennung **UXYZ** und der Nummer **1234** zur Account-Nummer **UXYZ1234** zusammen.

Das Benutzerkonto wird mit einem Startpasswort generiert, welches innerhalb von 14 Tagen geändert werden muss. Aus sicherheitstechnischen Gründen gibt es gewisse Anforderungen an die Gestaltung eines Passwortes. Genaueres finden Sie unter dem Punkt **Passwort überprüfen und ändern** auf Seite 10.

Studierende der Universität Göttingen erhalten ebenfalls einen Account. Dieser Account wird allerdings von der studIT verwaltet. Der Benutzername hat üblicherweise die Form **vorname.nachname**. Wäre **Monika Mustermann** Studentin, würde ihr Benutzername also

monika.mustermann lauten. Mit einem Account der studIT sind auch viele weitere Services nutzbar, so z. B. das Lernmanagementsystem stud.IP und das Prüfungsmanagementsystem FlexNow. Für Fragen und weitere Informationen zum studentischen Nutzerkonto steht die studIT unter <https://studit.uni-goettingen.de> oder per E-Mail an die Adresse info@studit.uni-goettingen.de zur Verfügung.

Ein Benutzerkonto beantragen

Seit 2007 gibt es bei der GWDG ein webbasiertes System zur Beantragung einer GWDG-Benutzerkennung. Über die Webseite <https://www.gwdg.de/antragsformulare> erhalten Sie Zugang zu Antragsformularen auf Deutsch und Englisch. Das ausgefüllte Antragsformular muss von der Geschäftsführung Ihres Institutes bestätigt werden.

Auf der Webseite finden Sie zudem auch weitere Anträge, z. B. für Funktionsaccounts und Benutzerkennungen auf Zeit.

Passwort überprüfen und ändern

Die Funktionalität des eigenen Benutzerkontos und des dazugehörigen Passwortes kann man auf der Webseite <https://www.gwdg.de> prüfen. Über die Anmeldung wird man auf das Kundenportal weitergeleitet. Auf der Webseite kann ggf. auch das Passwort geändert werden. Das Kundenportal ist ein Teil des Identity-Management-Systems (IdM), welches dafür sorgt, dass Benutzerinformationen in alle angeschlossenen Systeme abgeglichen werden.

Hinweis: Das Passwort kann beim Bedarf auch von dem zuständigen Institutsadministrator neu gesetzt werden. Den Institutsadministratoren und den Mitarbeitern der GWDG steht für Passwortänderungen das zentrale IdM-Portal (<https://idm.gwdg.de>) zur Verfügung.

Alle Administrator(innen) sind mit dem IdM-Portal in der Lage:



- das Initialkennwort (nach der automatischen Erstellung des Account) dem Benutzer zugänglich zu machen (durch Ausdruck der Accountdaten)
- den Account eines Benutzers zurück zu setzen
- das Passwort wieder frei zu schalten
- eine Benutzersperre zu setzen/entfernen
- einen Account zu reaktivieren, wenn der Benutzer sein abgelaufenes Passwort nicht erneuert hat

Abbildung 2: Identity-Management-Portal

Um die Sicherheit Ihres Passwortes zu gewährleisten und Missbrauch zu vermeiden, sollte Ihr Passwort

- mindestens zehn Zeichen lang sein (Empfehlungen besagen inzwischen mindestens 16 Zeichen),
- mindestens ein **Sonderzeichen** enthalten (z. B. !? "\$%&^()=;@,.-_<>#*+~ oder Leerzeichen),
- sowohl **Groß-** als auch **Kleinbuchstaben** enthalten und
- neben Buchstaben auch **Zahlen** beinhalten.

Sie können Ihr Passwort nur ändern, wenn das neue Passwort diesen Anforderungen entspricht. Wenn Sie Schwierigkeiten haben, sich ein solches Passwort zu merken, lesen Sie bitte unsere Hinweise dazu unter „Passwortgestaltung“ auf der genannten Webseite durch.

Das Passwort muss vom Benutzer auf der Webseite <https://www.gwdg.de> jährlich aktualisiert werden.

Hinweis: Sollte der Benutzer das Passwort vergessen bzw. nicht rechtzeitig aktualisiert haben, so muss der Benutzer sich bei dem zuständigen Institutsadministrator oder an der Information der GWDG ein neues Passwort geben lassen. Hierzu ist ein Personalausweis erforderlich. Das nicht von Benutzer gesetzte Passwort muss innerhalb von 14 Tagen in ein eigenes Passwort geändert werden.

Gesperrtes Benutzerkonto

Für alle Benutzer die nicht zur Universität Göttingen gehören wird nach fünfzehnmaliger Falscheingabe des Passwortes wird Ihr Account für eine halbe Stunde gesperrt (Kurzzeitsperre) und danach automatisch wieder entsperrt. Mit diesen Maßnahmen beugt man den Angriffen durch Passwort-Crack-Programmen vor, die mittels einer automatisierten Routine verschiedene Passwörter ausprobieren.

Hinweis: Häufig kommt es nach Passwortänderungen zur Sperrung des Benutzerkontos durch die oben erwähnte Kurzzeitsperre. Meistens ist die Ursache eine bestehende Verbindung zu Netzlaufwerken, Druckern oder einem E-Mail-Konto. Zu diesem Zweck merkt sich ein Windows-System das Passwort des Benutzers. Deshalb empfehlen wir nach einer Änderung des Passwortes auch, den Windows-Passwortspeicher zu löschen. Bitte berücksichtigen Sie dabei, dass auch mobile Geräte Passwörter speichern.

Passwortspeicher löschen

Sie können die **Anmeldeinformationsverwaltung** über die **Systemsteuerung** erreichen.

Schneller erreichen Sie den Passwort-Tresor, wenn Sie unter **Start** → **Ausführen** (Windows-Taste **⊞**+R) den Befehl [control keymgr.dll](#) eingeben.

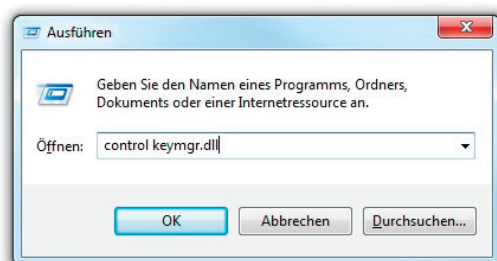


Abbildung 3: Aufruf des Passwort-Tresor

In dem dann folgenden Fenster können Sie Passwörter löschen, die falsch sind oder nicht mehr benötigt werden.

Systemsteuerung

Eigene Anmeldeinformationen verwalten

Sie können gespeicherte Anmeldeinformationen für Websites, verbundene Anwendungen und Netzwerke anzeigen und löschen.



Webanmeldeinformationen



Windows-Anmeldeinformationen

[Anmeldedaten sichern](#) [Anmeldedaten wiederherstellen](#)

Windows-Anmeldeinformationen

Windows-Anmeldeinformationen hinzufügen

email.gwdg.de	Geändert: 13.06.2014	▼
email.stud.uni-goettingen.de	Geändert: 25.06.2014	▼
gwd-winprint.top.gwdg.de	Geändert: 24.06.2014	▼
gwdg-print2	Geändert: 29.08.2014	▼
gwdg\gwdg (Windows-Identität)	Geändert: 13.06.2014	▲

Internet- oder Netzwerkadresse:
gwdg\gwdg (Windows-Identität)

Benutzername: gwdg\gwdg

Kennwort:

Dauerhaftigkeit: Unternehmen

Bearbeiten

Entfernen

Abbildung 4: Anmeldeinformationsverwaltung

Die Remotedesktop-Server der GWDG

Die GWDG betreibt zurzeit zwei Remotedesktop-Server (ehemals Windows-Terminalserver), die sich in ihrer Funktion unterscheiden. Um nun ein erstes Gefühl dafür zu bekommen, wie die Arbeitsumgebung im AD aussieht, hat man die Möglichkeit, sich an einem Remotedesktop-Server anzumelden. Zu diesem Zweck verwenden Sie bitte den [GWD-WinTS1](#). Auch hier erhalten Sie ein servergespeichertes Profil (siehe S. 43), welches aber nicht mit dem servergespeicherten Profil auf Ihren Arbeitsstationen im AD identisch ist. Bei der Anmeldung am Remotedesktop-Server werden Sie automatisch mit Ihrem **P:-Laufwerk** (Homeverzeichnis) und, falls vorhanden, mit Ihrem **W:-Laufwerk**, also dem gemeinsamen Speicherbereich (siehe S. 55) verbunden.

Eine Remotedesktop-Verbindung (RDP) zu einem Server herstellen

Um eine Verbindung mit einem Remotedesktop-Server herzustellen, starten Sie die **Remotedesktop-Verbindung**, die Sie über **Start** → **Zubehör** → **Remotedesktop-Verbindung** erreichen. Alternativ können Sie auch über **Start** → **Ausführen** den Befehl `mstsc` eingeben und so die RDP-Verbindung starten. Geben Sie im Feld **Computer** den jeweiligen Namen des Remotedesktop-Servers ein, mit dem Sie sich verbinden wollen. Der Server ist mit einem RDP-

Client (in jedem Windows-Betriebssystem ab Windows 2000 enthalten) zu erreichen. Linux-Benutzer verwenden **Remmina** oder **rdesktop** ab Version 1.6.0.

Unsere beiden Remotedesktop-Server im Detail:

GWD-WinTS1

Der Remotedesktop-Server [GWD-WinTS1.top.gwdg.de](https://gwdg.de/gwd-wintts1) bietet Software an, für die Campuslizenzen existieren.

An diesem Remotedesktop-Server können sich alle Benutzer mit einem GWDG-Konto anmelden.

Zusätzlich stellt der Server Software für Kursumgebungen bereit. Voraussetzung dafür ist, dass vom Kurshalter eine Vorlaufzeit von zwei Wochen zur Installation der Software auf dem Server eingehalten wird und die Lizenzanforderungen geklärt worden sind. Bei Bedarf melden Sie sich bitte unter support@gwdg.de.

GWD-WinTS3

Der zweite Remotedesktop-Server dient ausschließlich als Administrationsserver für Institutsadministratoren. Die Anmeldung am Server ist nur mit Ihrem Administratorkonto (z. B. **0adminid**) möglich. Über diesen Server können diverse Verwaltungskonsolen, z. B. **Active Directory Users and Computers** sowie **Sophos Enterprise Console**, benutzt werden, deren Funktionen in den folgenden Kapiteln ausführlich erklärt werden. Sobald Sie sich am Remotedesktop-Server [GWD-WinTS3](https://gwdg.de/gwd-wintts3) angemeldet haben, erscheinen auf dem Desktop Verknüpfungen zu verschiedenen administrativen Konsolen:

- Active Directory Users and Computers
- Group Policy Management
- baranuni Management Center
- Druckerverwaltung
- Sophos Enterprise Console.

Active Directory-Benutzer und -Computer

Mit dem Programm **Active Directory-Benutzer und -Computer** (Active Directory Users and Computers) können Sie als Institutsadministrator die Computer und Gruppen in Ihrem Verwaltungsbereich bzw. Ihrer Organisationseinheit (**OU**) verwalten.

Aufbau

Das Programm ähnelt dem bekannten Windows-Explorer:

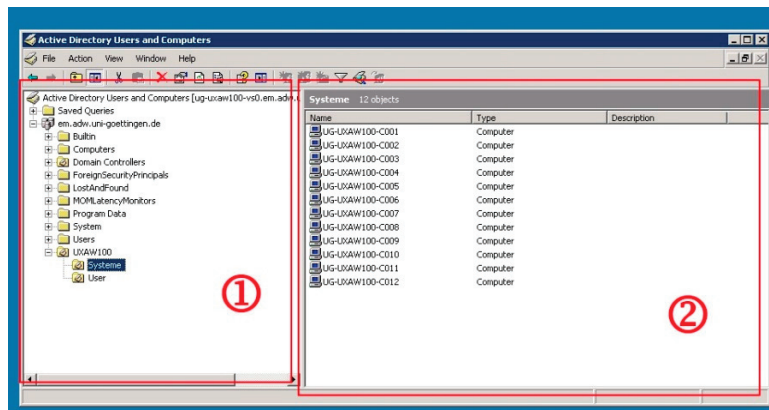


Abbildung 5: Active Directory Users and Computers

Im linken Feld (1) befindet sich der Domänenbaum mit der Domäne und den zugeordneten Containern. Klicken Sie links einen Container an, wird im rechten Feld (2) dessen Inhalt angezeigt.

In diesem Zusammenhang sei kurz der Unterschied zwischen **Containern** und **OUs** erklärt. Container sind Elemente, die andere Elemente beinhalten können. Eine OU ist z. B. ein Container; man erkennt sie an dem kleinen Buch innerhalb des OU-Icons.

Wichtig ist, dass man nur auf OUs Gruppenrichtlinien verknüpfen kann. Das bedeutet, dass Rechner, die in dem Container **Computers** liegen, keine Richtlinien bekommen. Aber dazu später mehr.

Navigation im Active Directroy

Um in Ihre Institutsumgebung zu gelangen, müssen Sie die Domäne auswählen und in die eigene OU hineinwechseln. Dazu klickt man mit der rechten Maustaste auf den aktuellen Domänennamen in **Active Directory Users and Computers** und wählt über **Change Domain...**(Domäne ändern...) → **Browse...** (Durchsuchen...) die gewünschte Domäne.

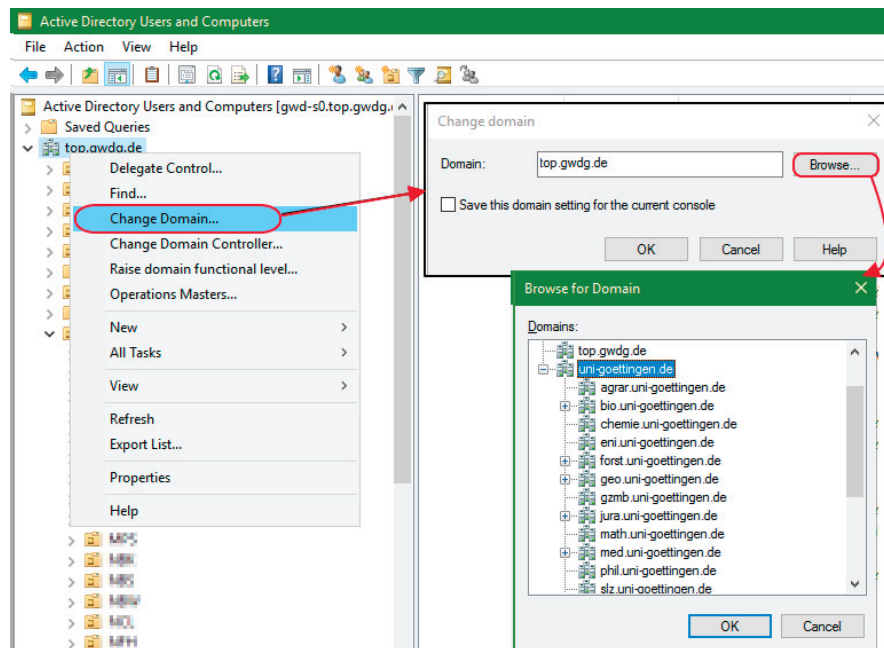


Abbildung 6: Navigation im Active Directory

Es wird der gesamte Domänenbaum angezeigt. Institute, die zur Universität Göttingen gehören, finden ihre Domäne unterhalb der Domäne [uni-goettingen.de](#). Erweitern Sie dazu die Ansicht mit Hilfe des Pluszeichens (+). Unterhalb der nun sichtbaren Fakultätsdomänen befinden sich manchmal weitere Domänen. So finden Sie z. B. die Domäne [avh.bio.uni-goettingen.de](#) unterhalb der Fakultätsdomäne [bio.uni-goettingen.de](#). Die markierte Domäne wird mit **OK** bestätigt. Wählt man im Fenster **Change Domain** (Domäne ändern) die Auswahl **Save this domain setting for the current console** (Diese Domäneneinstellung für die aktuelle Konsole speichern) mit einem Häkchen, so wird die gewählte Domäne in Zukunft immer beim Start der Konsole angezeigt. Diese Einstellung wird in Ihrem Profil gespeichert, so dass Sie diese nur einmal vornehmen müssen. Anschließend bestätigen Sie ein weiteres Mal mit **OK** und die Strukturanzeige des Fensters wechselt zur ausgewählten Domäne.

Wenn dann die richtige Domäne angezeigt wird, kann man links durch Erweitern der Äste im Strukturbaum in seinen eigenen Verwaltungsbereich wechseln. Dieser Weg orientiert sich an Ihrem Institutskürzel. Dem Standard folgend finden Sie z. B. **UXYZ100** unter **UG-UX** → **UXYZ** → **UXYZ100**. Der eigene Verwaltungsbereich unterteilt sich dann in die **OUs Benutzer** und **Systeme**. In der **OU Benutzer** befinden sich Gruppen und in Einzelfällen Gast- oder Kursbenutzerkonten, in der **OU Systeme** die Computerkonten. Vereinzelt können auch vom Standard abweichende Strukturen auftreten. Diese sind dann aber in Absprache mit dem zuständigen Institutsadministrator eingerichtet worden.

Verwaltung von Benutzergruppen in der Institutsumgebung

Für jedes Institut bzw. jede Abteilung wird standardmäßig sowohl eine Mitarbeitergruppe (z. B. **UXYZ100**) als auch eine Administratorengruppe (z. B. **UXYZ100-Admins**) innerhalb des zu administrierenden Bereiches angelegt. Diese sind als „universelle“ Gruppe eingerichtet, so dass auch Benutzerkonten anderer Domänen integriert werden können, wie z. B. die studentischen Konten der Domäne [UG-Student](#).

Hinweis: Bei Kooperation mit MPG-Benutzern muss der administrative Account mit Leseberechtigungen für die MPG-Benutzerkonten berechtigt werden. Melden Sie sich in diesem Fall über unsere Support-Adresse support@gwdg.de.

Mit Hilfe dieser Benutzergruppen werden die Zugriffsberechtigungen für diverse Ressourcen, wie z. B. den Speicherbereich für gemeinsam genutzte Daten, die Institutsdrucker oder auch SharePoint-Bereiche zugeordnet. Da diese Gruppen im Verwaltungsbereich des lokalen Administrators liegen, kann der Zugriff auf die Ressourcen von den Mitarbeitern des Institutes selbst gesteuert werden. Bei Bedarf können auch weitere Gruppen erstellt werden, um die Zugriffsberechtigungen individueller zu gestalten.

Die Administratorengruppe

Benutzer, die Mitglied dieser Administratorgruppe (z. B. **UXYZ100-Admins**) sind, können standardmäßig folgende Aufgaben in ihrem Verwaltungsbereich durchführen:

- Computer-Konten erzeugen
- Computer migrieren
- Gruppen erstellen
- Gruppenmitgliedschaften verwalten

Bei der Migration eines Computers in das Active Directory muss diese Gruppe grundsätzlich der Gruppe der lokalen Administratoren auf dem migrierten System hinzugefügt werden (siehe **Lokale Systemeinstellungen am PC im Active Directory** auf Seite 29). Organisatorische Änderungen, z. B. bei Urlaubsvertretung oder Personalwechsel, sind durch diese Gruppe mit wenigen Mausklicks möglich – es ist ausreichend, die betreffenden Benutzerkonten aus der Gruppe zu entfernen oder hinzuzufügen, um einer Person administrative Rechte auf die Systeme und im Active Directory zu entziehen oder zu erteilen.

Gruppen erstellen

In der **OU Benutzer** können Sie mit einem Rechtsklick in das leere Feld auf der rechten Seite das Kontextmenü öffnen. Im Kontextmenü befindet sich der Punkt **Neu**, auf den Sie mit Ihrem Cursor zeigen, woraufhin sich eine Auswahl aufblättert. Diese Auswahl umfasst sämtliche Objekte, die vom Administrator in der OU angelegt werden können. Sie wählen das Objekt **Group**. Anschließend wird der Assistent **New Object - Group** gestartet und Sie haben die Möglichkeit, der Gruppe einen Namen zu geben. Des Weiteren befindet sich in diesem Fenster die Auswahl **Group scope** und **Group type**. In der Liste **Group scope** wählen Sie **Universal** und in der Liste **Group type** belassen Sie die Einstellung auf **Security**. Nach der Bestätigung mit **OK** wird die Gruppe erstellt.

Sollte die Zuordnung von Benutzerkonten aus anderen Domänen nicht funktionieren, liegt das häufig daran, dass vergessen wurde, die Gruppe als „universelle“ Gruppe anzulegen.

Nach dem Erstellen der Gruppe fügen Sie diese wiederum der Gruppe *[Institutskürzel/Abteilungsnummer]-Share* aus dem eigenen Bereich hinzu (z. B. **UXYZ100-Share**). Dies funktioniert genauso wie das Zuordnen von Mitarbeitern und wird im nächsten Absatz beschrieben. Die Zuordnung der neu erstellten Gruppe zu der **UXYZ100-Share**-Gruppe gewährleistet den Zugriff über die Freigabe auf das gemeinsame Laufwerk. Das heißt, mit dieser Gruppenmitgliedschaft werden die Freigabeberechtigungen bereitgestellt.

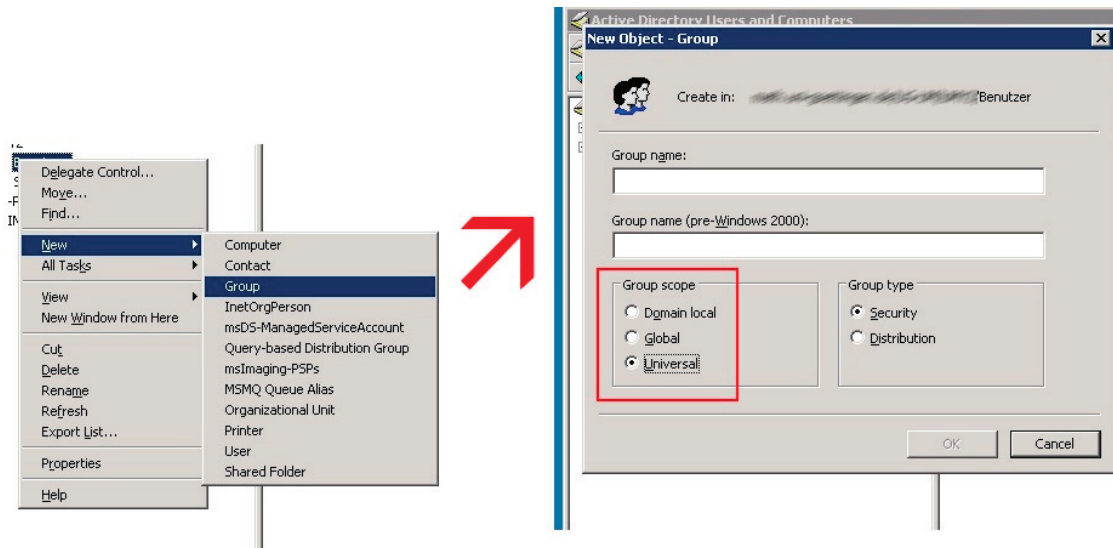


Abbildung 7: Gruppe erstellen

Mitarbeiter den Gruppen zuordnen

Wenn Sie nun für einen neuen Mitarbeiter den Zugriff auf die Institutsressourcen einrichten wollen, müssen Sie den betreffenden Benutzer-Account nur der Mitarbeitergruppe hinzufügen. Dazu klicken Sie mit Doppelklick auf die entsprechende Gruppe (z. B. **UXYZ100**) und es öffnet sich das Fenster **Properties** mit der Registerkarte **General**. Hier können Sie erkennen, dass es sich um eine universelle Gruppe handelt. Nur in einer universellen Gruppe ist es möglich, Benutzerkonten aus anderen Domänen hinzuzufügen. In der Registerkarte **Members** wird Ihnen angezeigt, welche Benutzerkonten bereits in dieser Gruppe eingetragen sind. Über die Schaltflächen **Add** und **Remove** können Sie nun Mitarbeiter der Gruppe hinzufügen bzw. entfernen.

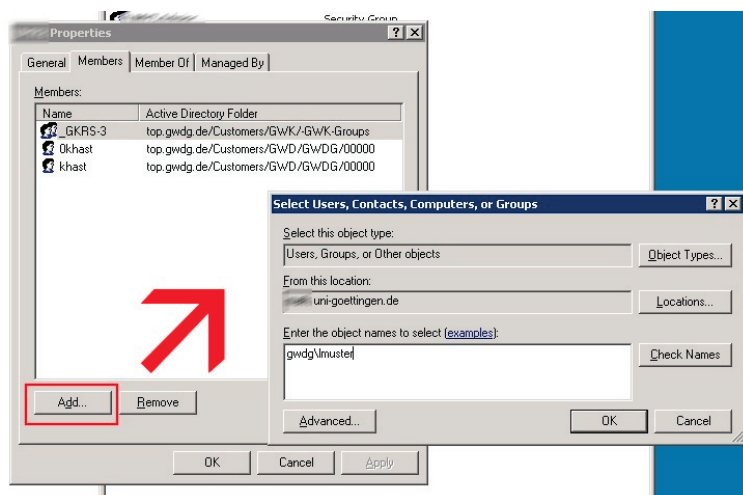


Abbildung 8: Hinzufügen von Benutzerkennungen

Hinweis: Beim Hinzufügen von GWDG-Benutzerkennungen müssen Sie das Benutzerkonto in der Form **GWDGuserid** angeben. Sollte es sich um ein Konto aus einer anderen Domäne

handeln, so muss `GWDG\` gegen den entsprechenden NetBios-Namen der Domäne ausgetauscht werden, im Fall eines studentischen Benutzerkontos z. B. `UG-Student\userid`. Alternativ können Sie unter **From this location:** die Domäne auswählen, in der sich das Benutzerkonto befindet und anschließend auf den vorangestellten NetBios-Namen der Domäne verzichten (statt `GWDG\userid` nur noch `userid`). Die jeweilige Aktion schließen Sie dann mit **OK** ab.

Zum Entfernen eines Benutzers markieren Sie das Benutzerkonto unter **Members** und klicken auf **Remove**.

Gruppen und Ressourcen

Die Verwendung von Gruppen erspart viel Arbeit bei der Zuordnung von Zugriffsrechten für Ressourcen. Ist z. B. ein Drucker für den Zugriff einer Gruppe konfiguriert, dann muss ein neuer Mitarbeiter nur diese Gruppe hinzugefügt werden, um ihn benutzen zu dürfen. Eine Gruppe kann selbstverständlich mehrfach verwendet werden. Das heißt, dieselbe Gruppe kann auch für die Steuerung des Zugriffs auf einen bestimmten Speicherbereich genutzt werden. Auf Grund dessen eignet sich bei der Strukturierung der Gruppen eine Zuordnung nach Arbeitsbereichen (z. B. Verwaltung, Projektgruppe A etc.)

Zugriffsrechte für Drucker

Bei einem Drucker kann im Kontextmenü unter **Eigenschaften** → **Sicherheit** die Gruppe eingetragen werden. Bei Bedarf kann man die Zugriffsrechte auch noch detaillierter zuordnen. Auf Wunsch werden die netzwerkfähigen Institutsdrucker über den zentralen Druckserver `\\GWD-Winprint` angeschlossen. Schon während der Installation der Drucker auf dem Server werden den Druckern die standardmäßig eingerichteten Gruppen aus dem Verwaltungsbereich des Institutes zugeordnet. Dabei erhalten die Gruppen die Berechtigung „Drucken“, während Mitglieder der Administratorgruppe Vollzugriff haben. Daraus folgt, dass eine entsprechende Konfiguration an den Druckern nur von Administratoren vorgenommen werden kann. In den seltensten Fällen ist eine tiefergehende Rechteverteilung für die Institutsdrucker notwendig. Weitere Informationen zum Thema **Drucker im Active Directory** finden Sie auf Seite 46.

Zugriffsrechte für Speicherbereiche

Für die Verteilung von Zugriffsberechtigungen auf Speicherbereiche des gemeinsamen Laufwerks sollten Sie zunächst einige Überlegungen hinsichtlich der unterschiedlichen Bedürfnisse anstellen. Grundsätzlich unterscheidet das Betriebssystem, ob ein Benutzer lokal oder über das Netz auf eine Ressource zugreift. Für den Zugriff aus dem Netz müssen Freigabeberechtigungen konfiguriert werden, der direkte Zugriff wird über NTFS-Rechte geregelt. Die NTFS-Rechte sind dabei wesentlich feiner abstufbar als die Freigabeberechtigungen. Beide Zugriffsrechte müssen für einen Benutzer/Gruppe gesetzt sein, bevor der Zugriff über eine Netzlaufwerksverbindung gewährt wird. Die Freigaberechte werden durch die Mitgliedschaft der Gruppen in der `[InstitutskürzelAbteilungsnummer]-Share-Gruppe` (z. B. `UXYZ100-Share`) gewährleistet. Deshalb sollten alle Gruppen einer Abteilung in dieser Gruppe enthalten sein.

Wir empfehlen, für die verschiedenen Abteilungen, Projekt- oder Arbeitsgruppen (z. B. Verwaltung oder Projekt XY) jeweils einen Ordner zu erstellen und namensgleich zu den Ordnern die entsprechenden Gruppen anzulegen. Im Einzelfall kann es notwendig werden, die Zugriffe

auch in „lesen“ oder „lesen, schreiben und ändern“ zu unterscheiden. In diesem Fall würden Sie zwei (oder mehr) Gruppen pro Ordner erzeugen. Anschließend können Sie die Mitarbeiter Ihres Institutes den verschiedenen Gruppen zuordnen.

Hinweis: Wenn Sie die Zugriffsrechte selbstständig verändern, dann achten Sie darauf, dass Sie nicht das System, die Enterprise-Administratoren oder die Fileservice-Gruppen löschen. Ein Löschen dieser administrativen Gruppen führt regelmäßig zu Problemen beim Backup oder anderen automatisch gesteuerten Routinen.

Freigabeberechtigungen

Hinweis: Die Freigabeberechtigungen für die gemeinsamen Speicherbereiche werden von den Mitarbeitern der GWDG auf den Servern verwaltet.

Um nun den Instituts- bzw. Abteilungsadministratoren die Zugriffssteuerung der Freigaberechte zu ermöglichen, haben wir die Gruppen *[InstitutskürzelAbteilungsnummer]-Share* (z. B. **UXYZ100-Share**) eingeführt. Alle Gruppen einer AD-Umgebung müssen in der *[InstitutskürzelAbteilungsnummer]-Share*-Gruppe enthalten sein. Diese wiederum ist in einer übergeordneten Institutsgruppe (z. B. **UXYZ-all-Share**) enthalten. Mit dieser Gruppenverschachtelung werden die Freigaberechte definiert.

NTFS-Zugriffsrechte und Freigabeberechtigungen

Die Vergabe von Benutzerrechten für Dateien und Verzeichnisse gehört zum täglichen Brot der Systemverwaltung. Wichtig ist, dass für die Erteilung von Zugriffsrechten grundsätzlich Gruppen verwendet werden.

Die Rechte sind teilweise kumulativ, ein höheres Recht kann also niedrigere enthalten. Wer z. B. das Recht „Ändern“ besitzt, darf auch lesen, schreiben und ausführen. Die folgende Tabelle zeigt das relativ komplizierte Rechtssystem:

Spezielle Berechtigungen	Vollzugriff	Ändern	Lesen, Ausführen	Ordnerinhalt auflisten	Lesen	Schreiben
<i>Ordner durchsuchen, Datei ausführen</i>	X	X	X	X		
<i>Ordner auflisten, Daten lesen</i>	X	X	X	X	X	
<i>Attribute lesen</i>	X	X	X	X	X	
<i>Erweiterte Attribute lesen</i>	X	X	X	X	X	
<i>Dateien erstellen, Daten schreiben</i>	X	X				X
<i>Ordner erstellen, Daten anhängen</i>	X	X				X
<i>Attribute schreiben</i>	X	X				X
<i>Erweiterte Attribute schreiben</i>	X	X				X
<i>Unterordner und Dateien löschen</i>	X	X				

Spezielle Berechtigungen	Vollzugriff	Ändern	Lesen, Ausführen	Ordnerinhalt auflisten	Lesen	Schreiben
Löschen	X	X				
Berechtigungen lesen	X	X	X	X	X	X
Berechtigungen ändern	X					
Besitz übernehmen	X					
Synchronisieren	X	X	X	X	X	X

NTFS-Rechte konfigurieren

Um die NTFS-Rechte eines Ordners zu setzen, verwendet man im Kontextmenü die Registerkarte **Eigenschaften** → **Sicherheit**.

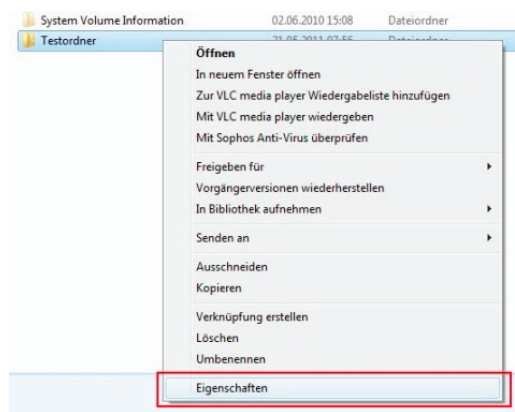


Abbildung 9: NTFS-Rechte konfigurieren I

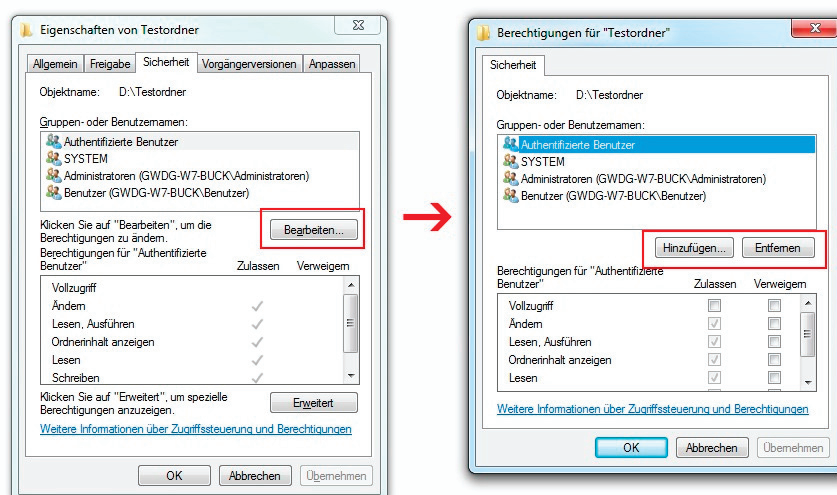


Abbildung 10: NTFS-Rechte konfigurieren II

Hier kann man über den Schalter **Bearbeiten** weitere Benutzer oder Gruppen hinzufügen oder entfernen.

Im oberen Fenster der Registerkarte **Berechtigungen für [Ordnername]** sind die mit Rechten versehenen Benutzer aufgelistet. Markiert man nun einen Benutzer oder eine Gruppe, kann man im unteren Fenster die zugeordneten Rechte anzeigen lassen bzw. ändern. Sollten die im unteren Fenster angezeigten Rechte wie im Beispielbild ausgegraut sein, sind die Rechte von einem übergeordneten Ordner vererbt. Neu angelegte Ordner und Dateien haben in diesem Fall die Zugriffsbeschränkungen des übergeordneten Verzeichnisses erhalten. Will man diese Rechte ändern, so muss zuerst die Vererbung aufgehoben werden.

Vererbung aufheben

Will man diese Voreinstellung deaktivieren, muss man die Option **Vererbte Berechtigungen des übergeordneten Objektes einschließen** abwählen. Dazu geht man wie folgt vor:

In der Registerkarte **Sicherheit** (Security) des Ordner-Kontextmenüs wird über den Schalter **Erweitert** (Advanced) das Fenster **Erweiterte Sicherheitseinstellungen für [Ordnername]** (Advanced Security Settings for [Foldername]) geöffnet. Anschließend verwendet man den Schalter **Berechtigungen ändern...** (Change Permissions...). Im dann folgenden gleichnamigen Fenster entfernt man den Haken für **Vererbte Berechtigungen des übergeordneten Objektes einschließen** (Include inheritable permissions from this object's parent).

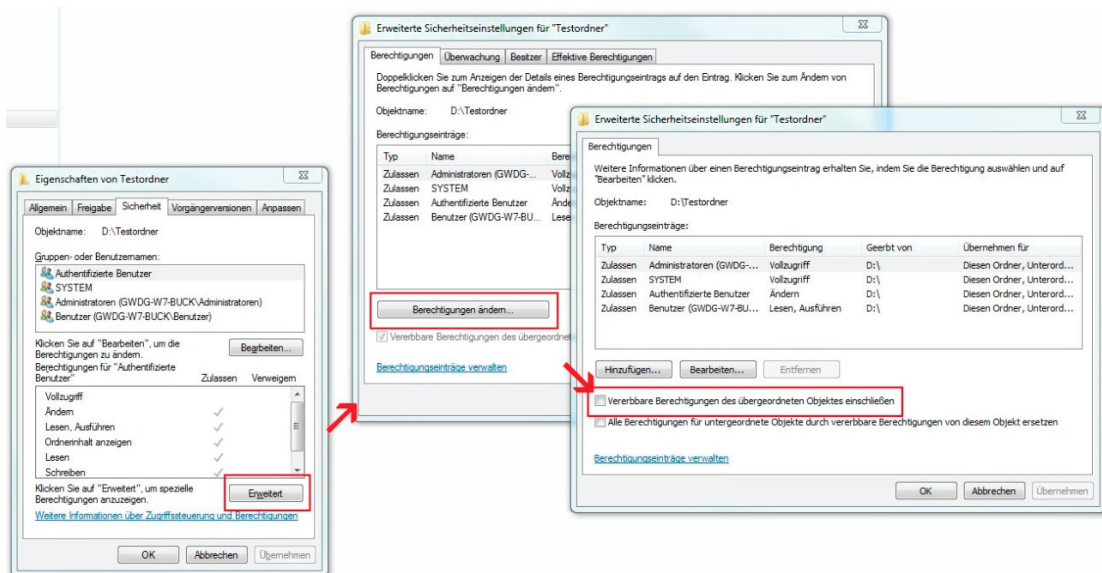


Abbildung 11: Vererbung aufheben I

Es erscheint ein Fenster mit der Überschrift **Windows-Sicherheit**. Wir empfehlen den Schalter **Hinzufügen** zu verwenden. In diesem Fall bleiben die Einträge für die Rechte erhalten, können aber verändert werden.

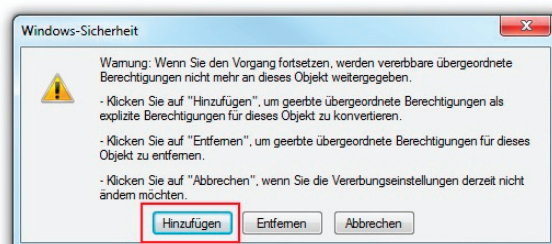


Abbildung 12: Vererbung aufheben II

Abschließend bestätigen Sie die Fenster mit **OK**, bis Sie wieder im Fenster **Eigenschaften von [Ordnername]** sind. Jetzt sind die Einträge im unteren Bereich nicht mehr ausgegraut und können bearbeitet werden. Hierbei ist zu berücksichtigen, dass die Rechte dieses Ordners wieder auf alle untergeordneten Ordner vererbt werden.

Die Zuweisung von Rechten an Benutzer erfolgt häufig mehrfach, wenn sie Mitglied in mehreren Gruppen sind. In diesem Fall gilt die großzügigste Regelung, egal, ob ein Recht dem Benutzer individuell oder über die Mitgliedschaft in einer Gruppe zuteil wurde. Die Option **Verweigern** dient vornehmlich dazu, einem Benutzer ein Recht explizit zu entziehen, das er über seine Zugehörigkeit zu einer Gruppe erhalten würde. Wir empfehlen, die Einstellung **Verweigern** nicht zu verwenden. Es kann bei späteren Konfigurationen zu Problemen kommen, wenn man sich nicht mehr an diese Einstellung erinnert.

Hinweis: Um die Zugriffsrechte übersichtlich und die Handhabung einfach zu gestalten, empfehlen wir, nur Gruppen für die Zuordnung von Rechten zu verwenden. Insbesondere wenn Mitarbeiter das Institut verlassen, wird es schwierig, das entsprechende Benutzerkonto aus den einzelnen Ordnerberechtigungen wieder zu entfernen.

Der Container „Computers“

In der Strukturansicht Ihrer Domäne (1) befinden sich verschiedene **Container**.

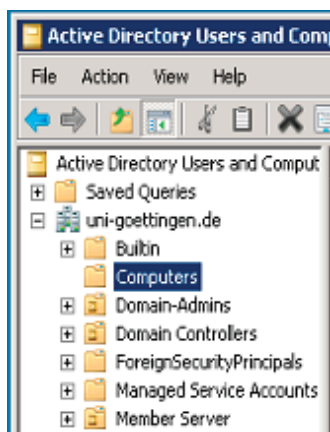


Abbildung 13: Der Container "Computers"

Einer davon ist der Container **Computers**. In ihm befinden sich Rechner, die nicht in eine Organisationseinheit (OU) eingefügt worden sind und damit auch keine Gruppenrichtlinien erhalten.

Hinweis: Nur Enterprise-Administratoren und die Domänen-Administratoren der jeweiligen Domäne können die Computerkonten aus dem Container **Computers** in die entsprechenden OUs verschieben.

Hinweis: Bei der Migration eines Computers müssen Sie **zuerst** das Konto in der richtigen OU erstellen und den Computer erst **danach** in die Domäne heben. Falls Sie den Computer in die Domäne heben, ohne zuvor das Konto angelegt zu haben, wird das Konto im Container **Computers** erstellt und Sie können ihn mit Ihrem Administratorkonto nicht in Ihre OU verschieben. Melden Sie sich in diesem Fall über unsere Support-Adresse support@gwdg.de. Wir verschieben dann das Computerkonto für Sie. Teilen Sie uns bitte mit, wie der Name des Computerkontos lautet und in welche **OU** (z. B. **UXYZ100**) es verschoben werden soll.

Die OU „Systeme“

OUs bieten die Möglichkeit, Gruppenrichtlinien zu verwenden. Diese finden in den OUs für die Systeme Anwendung.

Gruppenrichtlinien

Gruppenrichtlinien sind festgelegte Konfigurationen, die einer OU zugeordnet und auf ihr zugehörige Computer angewendet werden. Im Umkehrschluss bedeutet dies, dass nur Rechner, die einer OU zugeordnet sind, auch die entsprechenden Richtlinien erhalten. Nach Beitritt des Computers in eine Domäne werden die Richtlinien übernommen, sofern das Computerkonto der richtigen OU zugeordnet wurde. Gruppenrichtlinien werden innerhalb einer Domäne zentral gespeichert und können deshalb für mehrere OUs Gültigkeit haben. Um eine Richtlinie einer OU zuzuweisen, wird sie mit der OU verlinkt. Bei Bedarf kann auch eine Richtlinie aus einer anderen Domäne verwendet werden. Diese Tätigkeit wird normalerweise nur durch GWDG-Mitarbeiter vorgenommen. Unsere Standard-Gruppenrichtlinien sind in der Domäne **GWDG** angelegt und werden als verlinkte Gruppenrichtlinien für alle Arbeitsstationen des ADs zugewiesen. Diese reichen in den allermeisten Fällen aus, um alle Anforderungen zu erfüllen.

Ausnahmen von dieser Regel gibt es nur in Domänen, die von den Instituten selbstständig verwaltet werden. Die Verwendung der Standardrichtlinien führt zu einer höheren Sicherheit, einer Fehlerbegrenzung und einer Erleichterung der Administration.

Unsere Standardrichtlinien:

- **GWD WSUS Client ServerALL:** „Windows Update Services“-Einstellungen
- **GWD SophoSAP Port Exceptions:** Firewall-Einstellungen und Konfiguration der Dienste für die Sophos Enterprise Console und SAP-Drucker-Ports

Spezielle Gruppenrichtlinien werden direkt für eine bestimmte OU angelegt. Das ermöglicht individuelle Einstellungen für eine bestimmte Arbeitsumgebung. Sie finden alle lokalen Gruppenrichtlinien einer Domäne im Container **Group Policy Objects**.

In der Regel werden die lokalen Gruppenrichtlinien von GWDG-Mitarbeitern in Absprache mit den Institutsadministratoren erstellt und zugewiesen.

Gruppenrichtlinien werden standardmäßig nach unten vererbt, so dass untergeordneten OUs ebenfalls alle Einstellungen der Gruppenrichtlinien aus den übergeordneten OUs zugewiesen bekommen.

Inhalt der speziellen Gruppenrichtlinien kann z. B. die automatische Verbindung mit dem gemeinsamen Laufwerk und den Druckern sein.

Softwareverteilung über Gruppenrichtlinien

Auf Wunsch kann die Verteilung von Software automatisiert und über Gruppenrichtlinien gesteuert werden. Für Open-Source- sowie für einige lizenzpflichtige Programme bieten wir Standardrichtlinien an. Diese werden von uns regelmäßig aktualisiert, so dass die Updates automatisch über die Richtlinie verteilt werden.

Aktuell werden folgende Programme angeboten:

- Firefox auf Deutsch und Englisch
- Flash Player Plug-In für Internet Explorer und Firefox
- Foxit PDF Reader
- PDF-XChange Pro
- Java JRE
- Microsoft Office in der aktuellen Version
- Citavi
- Open Office

Die Migration eines Computers in das Active Directory

Um einen Computer erfolgreich in das Active Directory zu migrieren, müssen ein paar Einstellungen vorgenommen sowie einige Konventionen beachtet werden. In diesem Kapitel lernen Sie, worauf Sie dabei achten müssen.

Ein neues Computerkonto anlegen

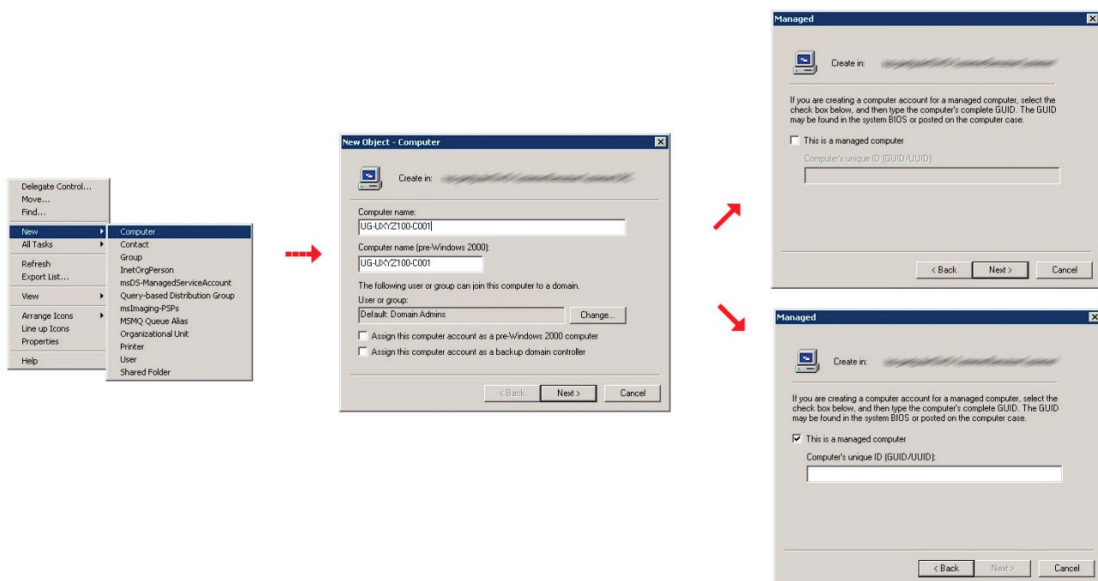



Abbildung 14: Computerkonto anlegen

Bevor Sie einen Rechner in die Domäne heben, müssen Sie ein neues Computerkonto in Ihrer OU **Systeme** anlegen. Dies tun Sie in der Konsole **Active Directory Benutzer und Computer**, die Sie, wie schon in den vorhergehenden Kapiteln beschrieben, über den Remotedesktop-Server **GWD-WinTS3** erreichen. Wechseln Sie in Ihren AD-Bereich in die OU **Systeme**, klicken Sie mit der rechten Maustaste auf die OU und wählen **New** → **Computer**. Geben Sie dem Computer einen dem Namensschema (siehe Abschnitt **Namensschema**) entsprechenden Namen. Die anschließende Abfrage im Fenster **Managed** ist nur für Rechner mit automatischer Betriebssysteminstallation über das Netzwerk gedacht. Diese Funktion wird aber von der GWDG nicht mehr genutzt. Bitte überspringen Sie dieses Fenster mit **Next**. Wenn Sie im nachfolgenden Fenster mit **Finish** bestätigen, wird das Computerkonto erstellt.

Netzwerkparameter

Damit der Rechner an das Netzwerk angeschlossen werden kann, muss er mit der zugeteilten Internetadresse (IP-Adresse), der Netzwerkmaske und der Adresse des Standard-Gateways versorgt werden. Fragen hierzu kann Ihnen Ihr Netzwerkbeauftragter beantworten. Erkundigen Sie sich ggf. in Ihrer Verwaltung danach, wer der zuständige Netzwerkbeauftragte für Ihr Institut ist.

Die Netzwerkparameter setzen Sie in den Eigenschaften des Internetprotokolls (TCP/IP), die Sie folgendermaßen erreichen:

- **Windows 7:** Start → Systemsteuerung → Netzwerk & Freigabecenter → Adaptereinstellungen ändern → (Kontextmenü der Netzwerkverbindung) Eigenschaften → Internetprotokoll Version 4 (TCP/IP) markieren → Eigenschaften
- **Windows 8 & Windows 10:** Bedienen Sie auf der Tastatur die Windows-Taste  und tippen Sie dann **Systemsteuerung** ein. Anschließend wählen Sie Netzwerk & Freigabecenter → Adaptereinstellungen ändern → (Kontextmenü der Netzwerkverbindung) Eigenschaften → Internetprotokoll Version 4 (TCP/IP) markieren → Eigenschaften

Wird die IP-Adresse im lokalen Netz automatisch vergeben, dann wählt man den Punkt **IP-Adresse automatisch beziehen**. Andernfalls füllt man die Felder **IP-Adresse**, **Subnetzmaske** und **Standardgateway** mit den zugeteilten Werten aus.

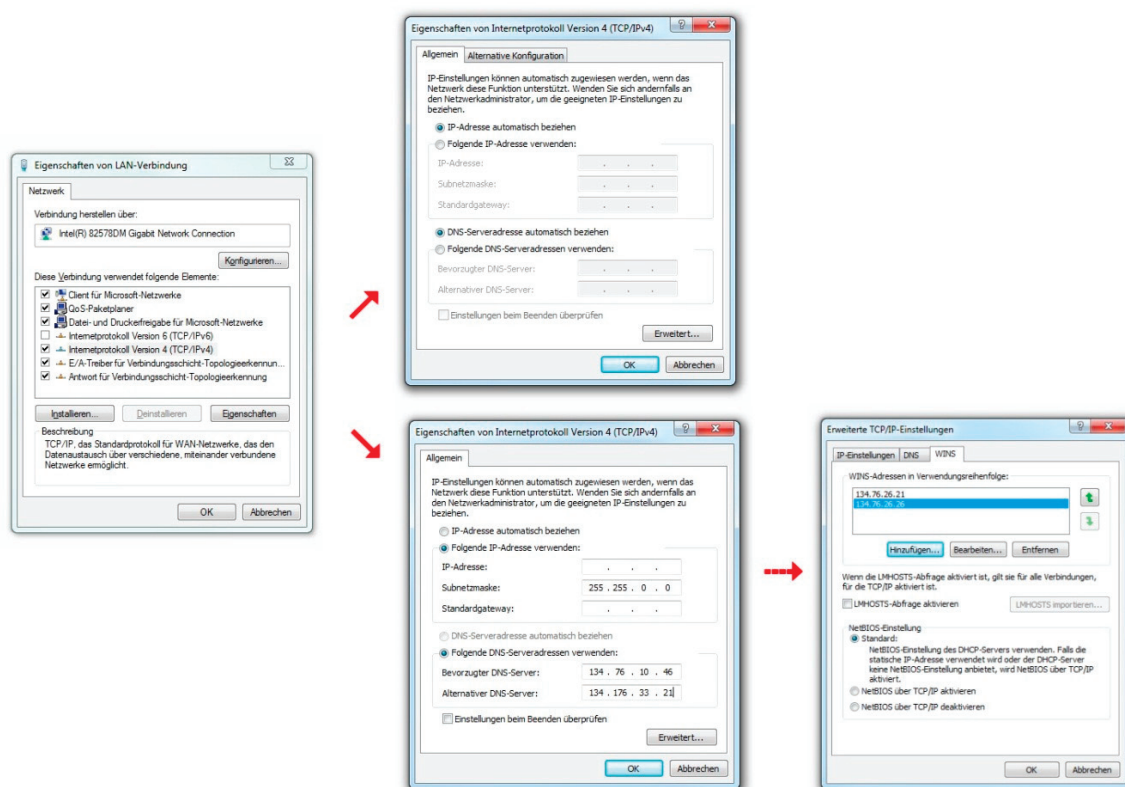


Abbildung 15: Netzwerkeinstellungen

Folgende Parameter werden eingetragen:

- **IP-Adresse:** Hier wird die zuvor im IPAM (siehe **Glossar** S. 64) eingetragene IP-Adresse verwendet.
- **Subnetzmaske:** In der Regel 255.255.255.0
- **Gateway:** Die Gateway-Adresse besteht in der Regel aus den ersten drei Ziffern der IP-Adresse und als letzte Ziffernfolge verwendet man die 254 (X.X.X.254).
- **DNS** (Nameserver): 134.76.10.46 und 134.76.33.21

Danach wählt man **Erweitert** → **WINS** und trägt Folgendes ein:

- **WINS-Server** (Windows-Nameserver): 134.76.26.21 und 134.76.26.26. Der WINS-Server 134.76.11.71 entfällt auf lange Sicht und sollte daher nicht mehr verwendet werden.

Hinweis: für Systeme ohne direkten Internetanschluss wie z. B. Drucker und Schulungsräume wird ein nicht-öffentliche IP-Bereich verwendet.


Nicht-öffentliche Systeme werden nach folgendem Schema eingerichtet:

- **IP-Adresse:** 10.76.0.0
- **Subnetzmaske:** 255.255.255.0
- **Gateway:** 10.76.0.254

Einen Computer einer Domäne des Active Directory hinzufügen

Hinweis: Legen Sie zuerst ein neues Computerkonto an, wie im Abschnitt **Ein neues Computerkonto anlegen** beschrieben wurde (S. 24).

Danach können Sie über die Computerverwaltung den Domänenbeitritt durchführen und ggf. den Computernamen anpassen. Die Computerverwaltung finden Sie hier:

- **Windows 7:** Start → Systemsteuerung → System → Erweiterte Systemeinstellungen → Computernamen → Ändern
- **Windows 8 & Windows 10:** Bedienen Sie auf der Tastatur die Windows-Taste  und tippen Sie dann **Systemsteuerung** ein. Anschließend wählen Sie System → Erweiterte Systemeinstellungen → Computernamen → Ändern.

Computername ändern

Wählen Sie einen Namen, der dem Namensschema entspricht, das auf Seite 7 beschrieben wurde. Nach der Namensänderung wird vom System ein Neustart angefordert. Sie können den Computer neu starten und dann in einem zweiten Arbeitsschritt den PC in die Domäne heben. Alternativ können Sie auch auf den Neustart verzichten und ohne Neustart nach der Namensänderung den Rechner in die Domäne heben. Die Erfahrung hat aber gezeigt, dass dieses Vorgehen nicht immer den gewünschten Erfolg bringt.

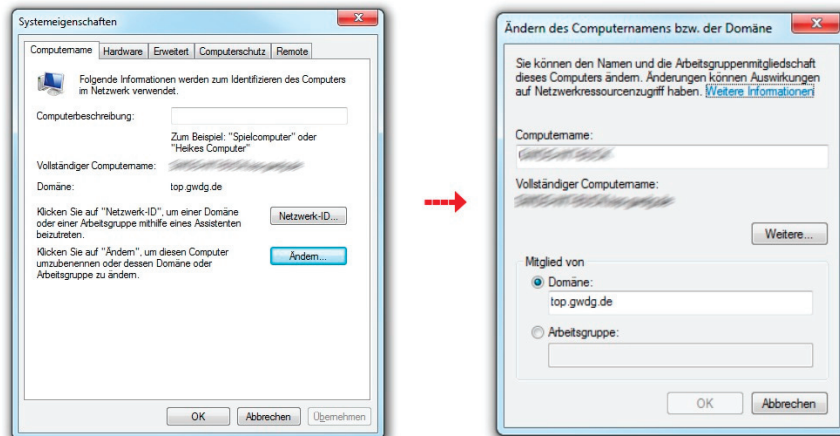


Abbildung 16: Computernamen ändern

Computer in die Domäne heben

Statt der Arbeitsgruppe (z. B. **WORKGROUP**) trägt man nun die Domäne ein, der der PC hinzugefügt werden soll. Hierfür können Sie sowohl den NetBios-Namen (z. B. **UG-UA**) als auch den DNS-Namen (z. B. **agrar.uni-goettingen.de**) verwenden.

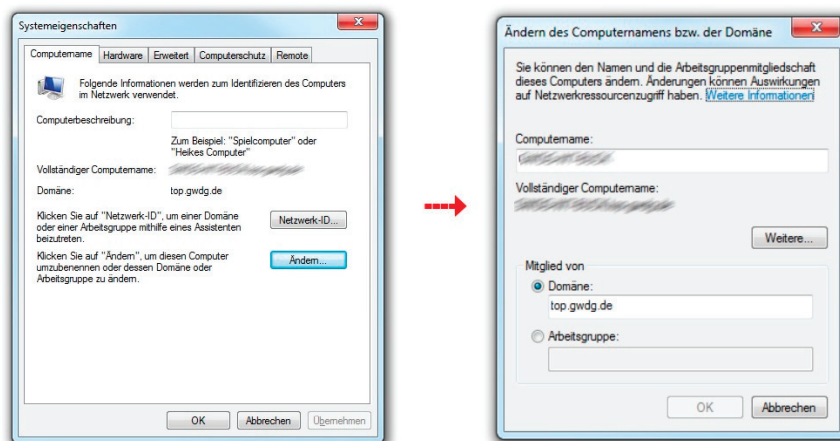


Abbildung 17: Computer in die Domäne heben

Nach der Bestätigung mit **OK** folgt das Fenster **Windows-Sicherheit** und verlangt die Eingabe eines Kontos. Dieses Konto muss über die Berechtigung verfügen, einem Computer den Beitritt zu der gewünschten Domäne zu erlauben, in der Regel also Ihr Administratorkonto. Benutzername und Kennwort sind einzugeben, wobei beim Benutzernamen ein vorangestelltes **GWDG** hinzuzufügen ist. War der Beitritt in die Domäne erfolgreich, wird man mit einem

„Willkommen in der Domäne!“ begrüßt. Danach muss der Computer neu gestartet werden, damit die Änderungen wirksam werden. Der PC ist jetzt in das Active Directory aufgenommen.

Update der Gruppenrichtlinien auf dem Arbeitsplatzrechner

Normalerweise sollte der Rechner bei einem Neustart „nachgucken“, ob es neue Richtlinien-einstellungen gibt. In Einzelfällen kann es vorkommen, dass die Richtlinien nicht vom System übernommen wurden. Sollten unsere Standardrichtlinien verwendet werden, kann man dies z. B. prüfen indem man sich die Firewall-Ausnahmen ansieht. Am schnellsten ist das durch die drei Ports, die zur Administration von **Sophos Anti-Virus** freigeschaltet sein müssen, erkennbar.

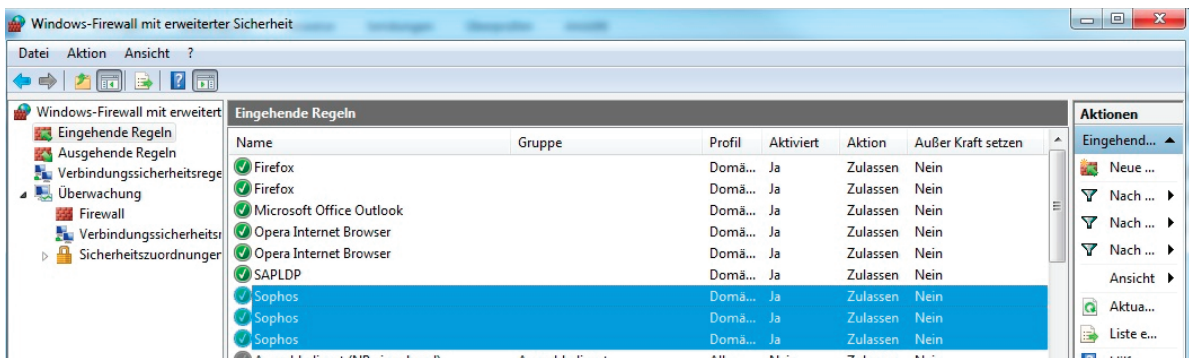


Abbildung 18: Gruppenrichtlinien prüfen

Sollte es notwendig werden, eine Übernahme der Gruppenrichtlinien zu erzwingen, geben Sie unter **Start** → **Ausführen** **cmd** ein, um die Eingabeaufforderung zu öffnen. In der Eingabeaufforderung verwenden Sie dann den Befehl **gpupdate /force**. Die Richtlinien werden aktualisiert. Ein Neustart wird im Allgemeinen nicht benötigt.



```
ex C:\WINDOWS\system32\cmd.exe - gpupdate /force
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>gpupdate /force
Die Richtlinie wird aktualisiert...

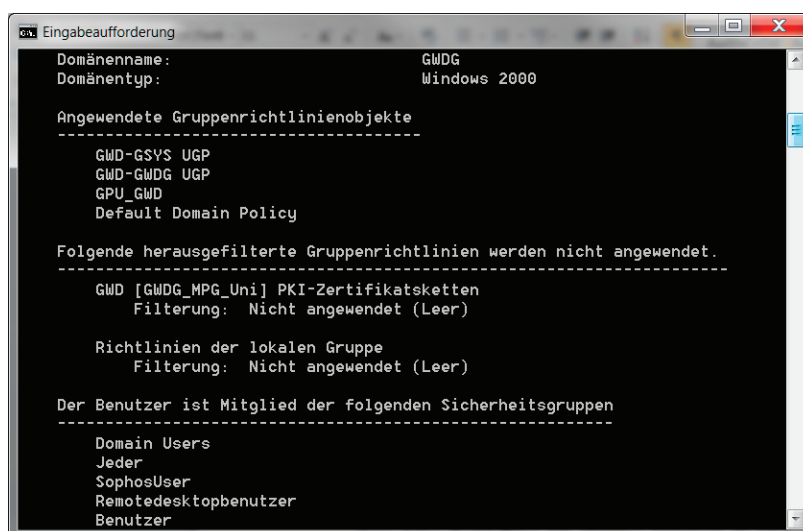
Die Aktualisierung der Userrichtlinie wurde abgeschlossen.
Die Aktualisierung der Computerrichtlinie wurde abgeschlossen.

Bestimmte Computerrichtlinien sind aktiviert, die nur beim Neustart ausgeführt
werden können.

Soll ein Neustart durchgeführt werden?. <J/N>j_
```

Abbildung 19: Richtlinienübernahme erzwingen

Um sich anzeigen zu lassen, welche Gruppenrichtlinien auf einem Rechner oder Benutzer wirksam werden, kann man den Befehl **gpresult /R** oder **gpresult /h GP.html** verwenden. Der zweite Befehl führt dazu, dass das Ergebnis in eine Datei im aktuellen Ordner geschrieben wird. Dies ist von Vorteil, wenn es bei der Abarbeitung der Gruppenrichtlinien zu Fehlern kommt und Sie andere Personen bei der Fehlersuche mit einbeziehen wollen.



```
Eingabeaufforderung
Domänenname: GWDG
Domänentyp: Windows 2000

Angewendete Gruppenrichtlinienobjekte
-----
GWD-GSYS UGP
GWD-GWDG UGP
GPU_GWD
Default Domain Policy

Folgende herausgefilterte Gruppenrichtlinien werden nicht angewendet.
-----
GWD [GWDG_MPG_Uni] PKI-Zertifikatsketten
Filterung: Nicht angewendet (Leer)

Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet (Leer)

Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen
-----
Domain Users
Jeder
SophosUser
Remotedesktopbenutzer
Benutzer
```


Abbildung 20: Fehlersuche in den Gruppenrichtlinien

Lokale Systemeinstellungen am PC im Active Directory

Diese Einstellungen können nur durchgeführt werden, wenn die Arbeitsstation bereits in das Active Directory eingetragen wurde. Wir empfehlen Ihnen, diese Einstellung vorzunehmen, bevor Sie sich das erste Mal in der Domäne anmelden. Für die Anmeldung am Rechner müssen Sie dann das lokale Administratorkonto nutzen. Um die Administration der Rechner zu vereinfachen, muss die in der Domäne angelegte Administratorgruppe (z. B. **UXYZ-Admins**, siehe Abschnitt **Aufbau und Namensschema** auf Seite 6) über die lokale Benutzerverwaltung des Computers in die Gruppe **Administratoren** eingetragen werden. Danach haben alle in der

AD-Administratorgruppe eingetragenen Benutzerkonten administrative Rechte auf dem System. Bei einem Personalwechsel kann man nun einfach die betreffenden Benutzer in diese zentral in der Domäne vorhandene Gruppe ein- oder austragen und kann so auf einfache Weise die Rechte zur Administration delegieren. Genauso können auch Dienstkonto in der Gruppe aufgenommen werden, die für automatisierte Prozesse benötigt werden, die nur mit Administratorrechten ausgeführt werden können. Dabei kann es sich z. B. um ein zeitgesteuertes Herunterfahren der Arbeitsstation oder eine automatisierte Sophos-Installation handeln.

Die lokale Benutzerverwaltung findet man in der Computerverwaltung unter

- **Windows 7:** Start → Computer (rechte Maustaste) → Verwalten
- **Windows 8 & Windows 10:** Bedienen Sie auf der Tastatur die Windows-Taste  und tippen Sie dann **Computerverwaltung** ein.

Die Gruppe trägt man dann unter System → Lokale Benutzer und Gruppen → Gruppen → Administratoren über den Punkt **Hinzufügen** ein.

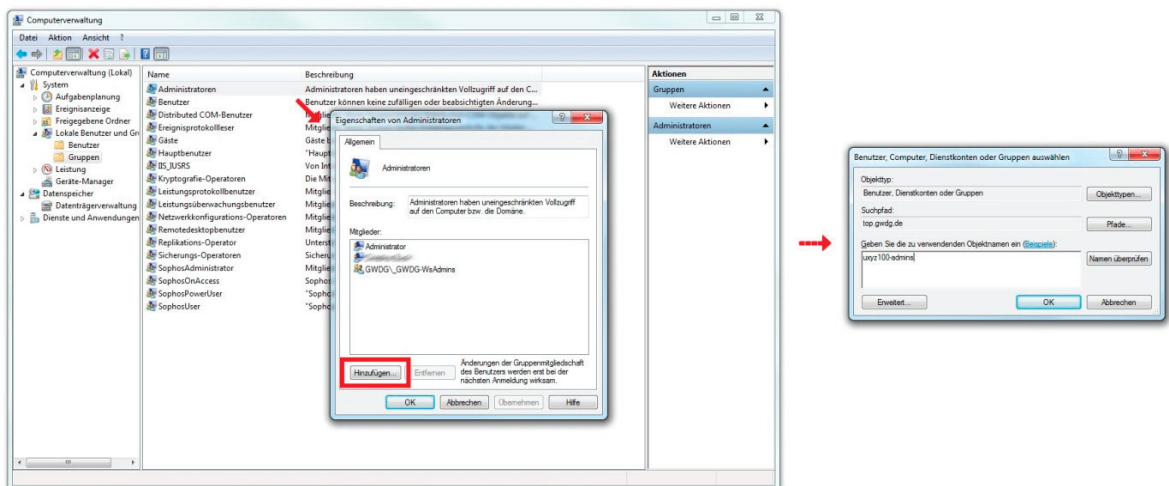


Abbildung 21: Administrator hinzufügen

Synchronisation von Offline-Dateien deaktivieren

Bei der Synchronisation von Offlinedateien werden sämtliche Dateien vom persönlichen oder gemeinsamen Laufwerk zusätzlich in den Offline-Bereich des Computers kopiert. Das kann praktisch sein, wenn man auch ohne eine Verbindung zum Netz arbeiten will, hat aber in der Vergangenheit oftmals zu Problemen geführt. Möchte man die Synchronisation von Offline-Dateien nutzen, sollte man statt der Standardeinstellungen gezielt die eigenen gewünschten Einstellungen vornehmen. Wenn die Offline-Synchronisation nicht benötigt wird, empfehlen wir sie zu deaktivieren.

Offline-Dateien deaktivieren unter Windows 7

Hier finden Sie die Einstellungen unter Windows-Explorer → Extras → Synchronisationscenter öffnen. Über den Punkt **Offlinedateien verwalten** können Sie dann die gewünschten Einstellungen vornehmen.

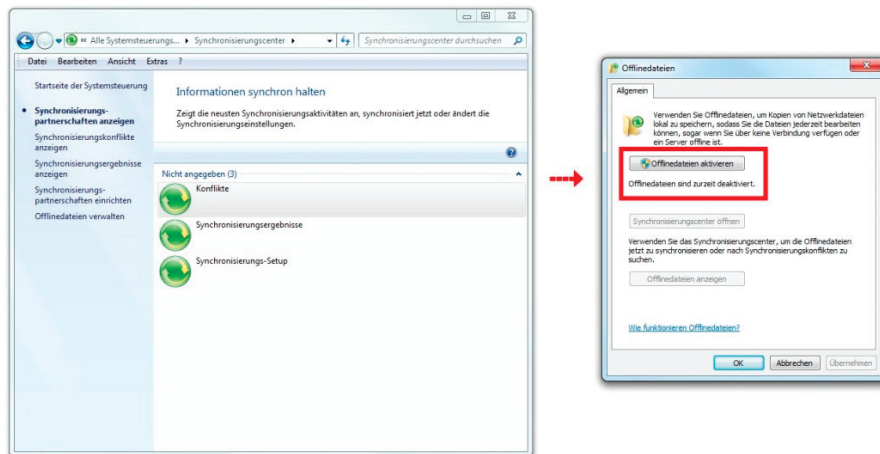


Abbildung 22: Offline-Dateien deaktivieren

Offline-Dateien deaktivieren unter Windows 8 & Windows 10

Bedienen Sie auf der Tastatur die Windows-Taste  und tippen Sie dann **Synchronisationscenter** ein.

Öffentliche Computer im Active Directory

Umgebungen, die vielen verschiedenen Nutzergruppen zugänglich sind, muss man in besonderer Weise vor Missbrauch schützen. Mehr Nutzer bedeuten auch mehr Potenzial für Viren oder Trojaner und eine höhere Ausfallquote durch unsachgemäße Benutzung. Der Wartungsaufwand ist ungleich höher als bei Mitarbeiterarbeitsplätzen im Institut. Deshalb bieten wir für CIP-Pools, Kursräume oder andere hochfrequentierte Computer ein „Rundum-sorglos“-Paket an, das Administratoren die Arbeit erleichtern soll. Dieses beinhaltet alle zentralen Dienste, die auch den Mitarbeitersystemen zur Verfügung stehen. Hinzu kommen deutlich restriktivere Gruppenrichtlinien, die der erhöhten Gefahr durch unsachgemäße Verwendung der Computer gerecht werden. Insbesondere bei Systemen in öffentlichen Bereichen empfehlen wir die Verwendung des Client-Management-Tools **baramundi**. Mit dieser Software können Sie neben der Software auch noch das Betriebssystem automatisch installieren lassen. Fragen hierzu beantworten wir gerne über support@gwdg.de.

Wenn Sie Ihre öffentlichen Arbeitsplätze in das Active Directory einbinden möchten und/oder noch Fragen zu dem Thema haben, melden Sie sich ebenfalls unter support@gwdg.de mit dem Betreff „Öffentliche Arbeitsplätze im Active Directory“.

Sophos Anti-Virus und die Sophos Enterprise Console

Das Antivirenprogramm **Sophos Endpoint Security and Control** wird für Angehörige der Max-Planck-Gesellschaft und der Georg-August-Universität Göttingen von der GWDG in zwei Varianten angeboten:

- Für Arbeitsplatzrechner im Active Directory mit zentraler Installation und Überwachung unter Verwendung der **Sophos Enterprise Console**.
- Für Rechner innerhalb und außerhalb Göttingens zur eigenhändigen Installation von der Webseite [Antivir.gwdg.de](http://antivir.gwdg.de).

In beiden Fällen wird das Antivirenprogramm automatisch aktualisiert. Die Lizenz berechtigt die betreffenden Nutzer außerdem dazu, die Software auf einem dienstlich genutzten PC zuhause zu installieren. In die Lizenz der Universität Göttingen sind auch die Studierenden eingeschlossen. Diese werden jedoch von der studIT betreut und nicht von der GWDG. Bei der studIT erhalten Studierende auch Informationen darüber, wie sie Zugang zu der Software erhalten.

In den folgenden Erläuterungen beziehen wir uns auf Arbeitsplatzrechner, die in das Active Directory der GWDG migriert sind und über die **Sophos Enterprise Console** verwaltet werden. Die Beschreibungen zu den Einzelplatzinstallationen finden Sie auf der Webseite <http://antivir.gwdg.de>.

Vorbereitung der Arbeitsstation für die Verwendung der Enterprise Console

Damit alle Funktionen der **Sophos Enterprise Console** fehlerfrei genutzt werden können, müssen auf den zu verwaltenden Rechnern ein paar Einstellungen durchgeführt werden. Folgende Einstellungen werden durch die Übernahme unserer Standardrichtlinien (siehe Seite 23 im Abschnitt **Gruppenrichtlinien**) sichergestellt. Sollten diese Richtlinien in Ihrer Institutsumgebung nicht verwendet werden, müssen diese Einstellungen manuell vorgenommen werden.

Firewall-Einstellungen

Für das Servernetz 134.76.26.0/23 der GWDG müssen folgende Einstellungen aktiviert werden:

- Freigabe der TCP-Ports 8192, 8193 und 8194
- die „Datei- und Druckerfreigabe“
- die Remoteverwaltung

Dienste

Folgende Dienste müssen gestartet bzw. als „automatisch“ konfiguriert sein:

- Computerbrowser
- Remoteregistrierung
- Server
- Taskplaner

- Arbeitsstation
- Windows Installer

Die „einfache Dateifreigabe“ in den Ordneroptionen des Windows Explorer unter der Registerkarte „Ansicht“ sollte deaktiviert sein. Also Haken raus!

Die folgenden Einstellungen werden nicht durch die Gruppenrichtlinien konfiguriert und müssen deshalb manuell vorgenommen werden.

Einstellungen im Netzwerk- und Freigabecenter

Die Netzwerkerkennung muss eingeschaltet sein.

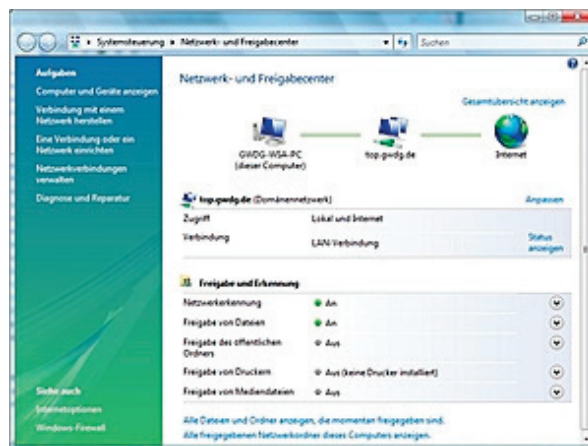


Abbildung 23: Netzwerk- und Freigabecenter

Verwaltung mit der Sophos Enterprise Console

Bevor die Rechner eines Instituts über die **Sophos Enterprise Console** verwaltet werden können, wird von einem GWDG-Mitarbeiter die Umgebung eingerichtet. Hierbei werden in Absprache mit dem Institutsadministrator eine Sophos-Gruppe vorbereitet sowie Richtlinien erstellt und zugewiesen. Der zuständige Institutsadministrator verwaltet dann die Sophos-Software auf den Arbeitsstationen über das Sophos-Verwaltungsprogramm **Sophos Enterprise Console** auf dem Terminal-Server **GWD-WinTS3** mit dem bei der GWDG beantragten Administratorkonto (z. B. **0adminid**).

Nach der Anmeldung am **GWD-WinTS3** (siehe S. 12) wird die Verwaltungskonsole über das Desktop-Icon **Enterprise Console** gestartet. Im oberen Bereich des Fensters befindet sich das Dashboard, das man aus Gründen der besseren Übersichtlichkeit am besten über die Schaltfläche **Dashboard** ausblenden lässt. Danach befinden sich in der Konsole drei Verwaltungsbereiche:

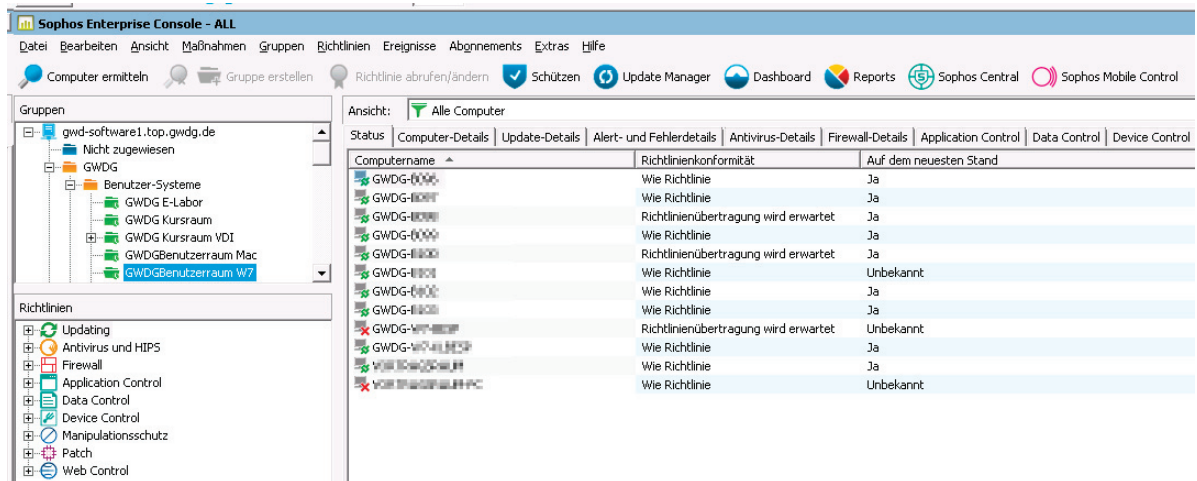


Abbildung 24: Sophos Enterprise Console

- **Gruppen:** Hier sind alle Sophos-Gruppen sichtbar, für die der lokale Administrator zuständig ist.
- **Computer-Konten:** Alle Konten der ausgewählten Sophos-Gruppe. Hier kann man z. B. erkennen, ob es Fehler und/oder Warnungen bei zugeordneten Rechnern gibt.
- **Richtlinien:** Alle der entsprechenden Sophos-Gruppe zugeordneten Richtlinien können hier eingesehen und verändert werden.

In der Regel wird die Umgebung so eingerichtet, dass sie sich mit dem Active Directory synchronisiert. Bei einer Synchronisation mit dem AD werden neue Computer-Konten, die im AD einer OU hinzugefügt worden sind, automatisch der entsprechenden Sophos-Gruppe zugeordnet. Klickt man also auf eine der Gruppen im linken oberen Feld, erscheinen im rechten Fensterbereich die zugehörigen Arbeitsstationen. Diese Synchronisation kann im Einzelfall bis zu 60 Minuten dauern.

Hinweis: Die Synchronisation kann manuell angestoßen werden, wenn man die Synchronisationszeit verändert.

Bitte berücksichtigen Sie, dass die Synchronisation nur dazu führt, dass die Computer der richtigen Sophos-Gruppe zugeordnet werden und nicht automatisch auch mit Sophos installiert werden. Bei Bedarf können wir diese Funktion für Sie einrichten. Melden Sie sich dazu einfach per E-Mail an support@gwdg.de.

Rechner der Sophos-Gruppe hinzufügen

Wird die Synchronisation mit dem Active Directory nicht verwendet, erscheint zusätzlich die Gruppe „Nicht zugewiesen“. Wenn die Arbeitsstationen in dieser Gruppe nicht angezeigt werden, müssen sie über die Schaltfläche **Computer ermitteln** eingebunden werden. Es erscheint das Fenster **Computer ermitteln**; Dort wählt man für den Punkt „Computer ermitteln“ das „Active Directory“ aus.

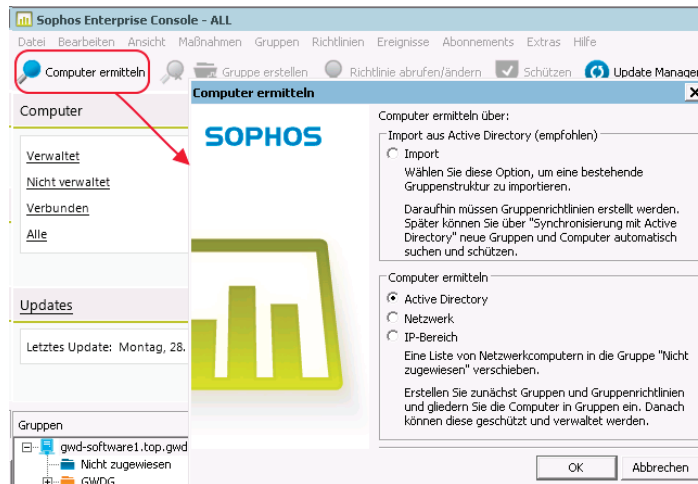


Abbildung 25: Enterprise Console - Computer ermitteln

Wenn Sie mit Ihrem Administratorkonto (z. B. **Oadminid**) angemeldet sind, müssen Sie Ihre Zugangsdaten nicht erneut eingeben. Anschließend wählt man die gewünschte Domäne aus und bestätigt mit **OK**. Nun wird eine Aktualisierung der Computerliste für die Klienten der entsprechenden Domäne vorgenommen und die Konten werden in der Gruppe **Nicht zugewiesen** angezeigt. Dort können sie einfach markiert und mit der Maus in die korrekte Gruppe verschoben werden. Anschließend öffnet sich selbständig der Assistent, der dazu auffordert, die Computer zu schützen.

Hinweis: Sollten Sie in der Konsole noch Rechner haben, die Sie neu installiert haben, so ist die Löschung dieses Rechners aus der Konsole nötig. Pflegen Sie den Rechner durch eine Neusynchronisierung wieder ein.

Sophos per Enterprise Console installieren

Hinweis: Für die Installation von Sophos ist es notwendig, zuvor das Administratorkonto in die lokale Administrator-Gruppe des Computers einzutragen.

Über die Schaltfläche **Schützen** wird ein Assistent gestartet, der Sophos Anti-Virus über die Konsole auf dem Arbeitsrechner installiert. Um diesen Assistenten zum Schützen von Computern zu starten, klickt man mit der rechten Maustaste auf den zu schützenden Rechner oder die zu schützende Rechnergruppe. Bei Bedarf können auch mehrere Computer gleichzeitig markiert und so mit Sophos versorgt werden. Hierzu verwendet man die Strg-Taste und klickt gleichzeitig die entsprechenden Computer an.

Es öffnet sich der **Assistent zum Schutz von Computern**. Im ersten Fenster heißt Sie der Assistent willkommen. Hier bestätigen Sie mit **Next**, danach folgt ein Fenster mit der Abfrage, welche Funktionen von der **Sophos Enterprise Console** installiert werden sollen. Als Standard sind hier die erste Einstellung „Application Control; Antivirus...“ und die zweite Einstellung „Third-Party Security Software Detection“ ausgewählt. Die beiden anderen Komponenten („Firewall“ und „Patch“) werden von der **Sophos Enterprise Console** nicht zur Verfügung gestellt, man behält also die Voreinstellung bei und geht mit **Next** zum nächsten Punkt über. Das nun folgende Fenster gibt einen Überblick über mögliche Installationsprobleme.

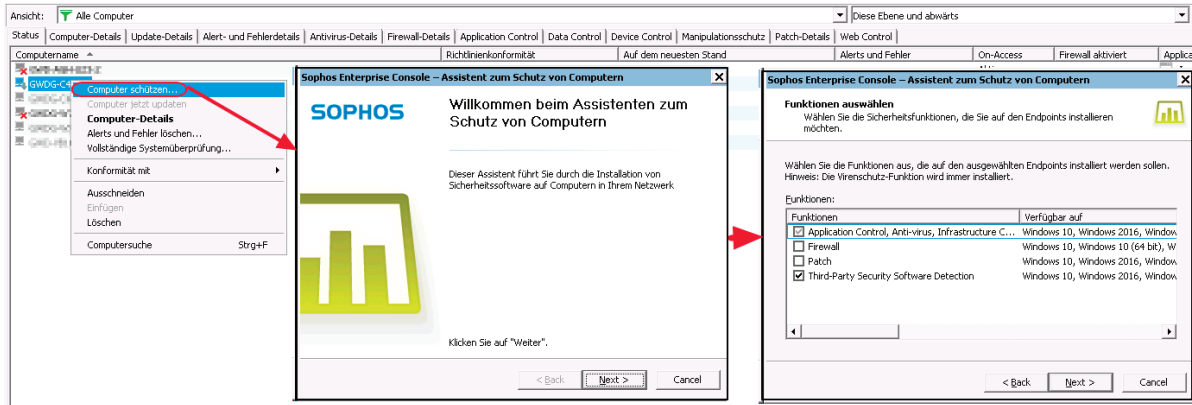


Abbildung 26: Computer schützen I

Ein grüner Pfeil signalisiert, dass alles in Ordnung ist. Sollte der Pfeil eine andere Farbe haben, versucht man dennoch eine Installation. Auch dieses Fenster wird wieder über **Next** abgeschlossen. Anschließend wird man aufgefordert, die Zugangsdaten einzugeben. Es wird ein Benutzerkonto mit administrativen Rechten verwendet. In den meisten Fällen ist das der bereits erwähnte Institutsadministrator und wird in folgender Weise angegeben: `GWDG\0adminid` und in der zweiten Zeile das zugehörige Passwort. Mit dieser Eingabe wird der Assistent abgeschlossen und der Installationsvorgang beginnt.

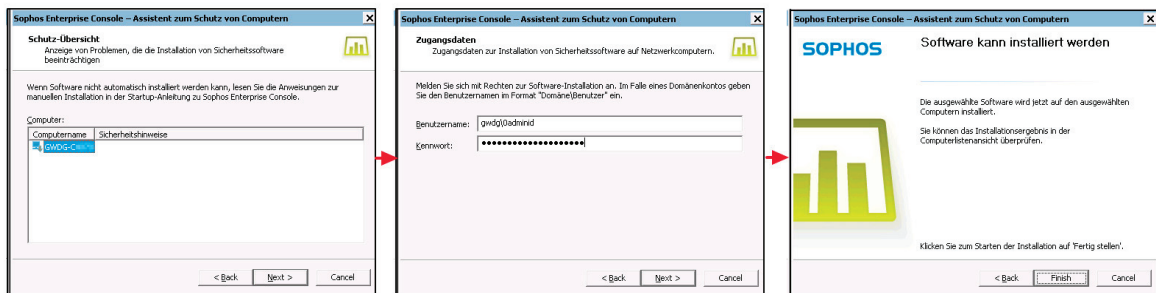


Abbildung 27: Computer schützen II

Sollte die Installation fehlschlagen, bekommt man nach Abschluss eine Fehlermeldung, die hilft, dem Problem auf den Grund zu gehen.

Hinweis: Sollte bei der Installation über die Sophos Enterprise Console ein Fehler zurückgemeldet werden, so kann das mehrere Ursachen haben.

FAQ: Häufige Fehler während der Installation mit der Sophos Enterprise Console

Mit einem Doppelklick auf einen Rechner erhalten Sie detaillierte Informationen über seinen Status. Hier können Sie dann auch ggf. genau nachlesen, welche Fehlermeldung Sophos zu einer fehlgeschlagenen Installation meldet.

Fehlermeldung:

Die Installation wurde nicht gestartet. Der Computer wurde evtl. heruntergefahren, umbenannt oder vom Netz getrennt oder ein erforderlicher Dienst läuft nicht.

Hier sollten Sie als erstes prüfen, ob der Rechner wirklich eingeschaltet ist. Danach sollten Sie kontrollieren, ob die erforderlichen Dienste wie im Kapitel **Gruppenrichtlinien** auf Seite 23 erwähnt laufen. Überprüfen Sie bitte, ob die Gruppenrichtlinien auch wirklich von dem Computer übernommen wurden.

Eine weitere Fehlerquelle kann die Sicherheitssoftware von Drittanbietern sein. Bekannt als Problemverursacher ist zum Beispiel das von Dell vorinstallierte Programm **Intel Management & Security Status**. Sollten Sie weitere Programme als Fehlerquelle identifizieren können, würden wir uns über eine Nachricht per E-Mail an support@gwdg.de freuen, damit wir diese Information an andere Nutzer weitergeben können.

Üblicherweise ist die administrative Freigabe **C\$** per Netzlaufwerkverbindung erreichbar. In Einzelfällen kann aber diese Freigabe deaktiviert sein. Dieses kann z. B. bei der Verwendung von Sicherheitssoftware vorkommen.

Virenbekämpfung mit der Sophos Enterprise Console

Die Beseitigung von Viren und Würmern ist umso schwieriger, je tiefer sie in das System eingedrungen sind. Über die **Sophos Enterprise Console** erhält man einen Überblick und kann unter Umständen auch einen Befehl direkt bereinigen.

Status der Systeme

Klickt man im linken oberen Feld auf eine Sophos-Gruppe, so werden im rechten Feld die zugehörigen Rechner angezeigt. In der Spalte **Alerts und Fehler** erkennt man, ob es Meldungen gibt. Befinden sich dort gelbe oder rote Dreiecke, dann sollte man per Doppelklick oder rechte Maustaste **Computer-Details** auf den Rechner klicken, um eine detaillierte Fehlerbeschreibung zu erhalten. Gelbe Dreiecke weisen auf Fehler im Ablauf hin, z. B. bei Update-Fehlern.

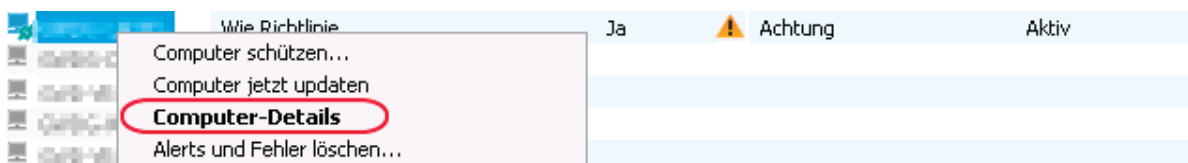


Abbildung 28: Computer-Details

Rote Dreiecke melden einen Virenverdacht, verdächtiges Verhalten oder das Erkennen von „potenziell unerwünschten Anwendungen (PUA)“.

Alerts und Fehler löschen und bereinigen

Über das Kontextmenü des Computerkontos (rechte Maustaste) > **Alerts und Fehler löschen** gelangt man zu einem Dialog, der die Meldungen verwaltet. Hier kann man die Meldungen löschen und, falls möglich über den Punkt **Bereinigen** den Befall aus dem System entfernen. Eine Bereinigung ist jedoch nicht immer möglich. Falls der Schadcode zu tief im System sitzt, kann es notwendig sein, sich direkt am betroffenen Rechner um das Problem zu kümmern.

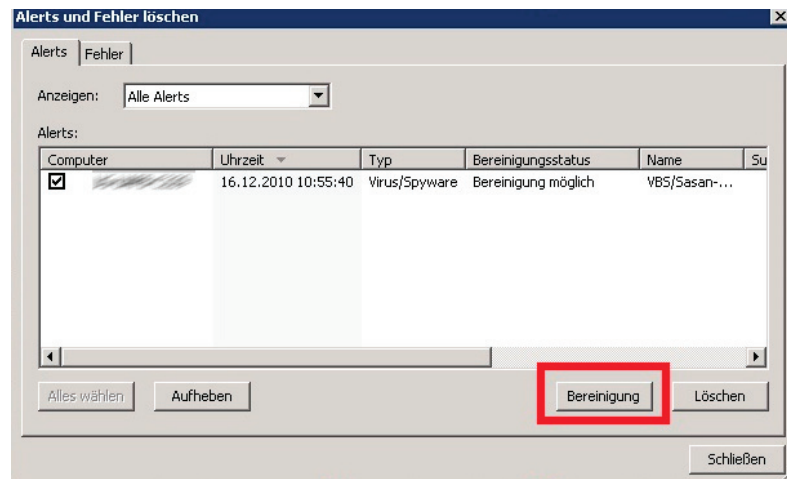


Abbildung 29: Alerts und Fehler löschen

Sofern Sie den Schadcode nicht löschen können oder dieser nach jedem Neustart wieder erzeugt wird, muss die Bereinigung des Systems stattfinden, wenn das Betriebssystem nicht läuft. Ausführlichere Beschreibungen finden Sie auf unseren Webseiten.

Außerdem gibt es die Möglichkeit, Viren mit **SAV32CLI**, der Befehlszeilen-Version von Sophos Anti-Virus, zu entfernen. Diese Version wird automatisch mitinstalliert. Für weitere Hinweise sollten Sie die ausführlich beschriebenen Erläuterungen auf der Sophos-Webseite lesen:

- SAV32CLI-Versionsinfo
<http://downloads.sophos.com/readmes/readcli.txt>
- Entfernen schädlicher Dateien mit SAV32CLI
<http://de.sophos.com/support/knowledgebase/article/13251.html>
- Scan-Optionen mit SAV32CLI
<http://de.sophos.com/support/knowledgebase/article/13252.html>
- Das Programm verfügt über eine integrierte Hilfedatei, geben Sie dazu Folgendes in die Befehlszeile ein: **SAV32CLI -H**

Vollständige Systemüberprüfung

Eine Systemüberprüfung sollte per Sophos-Richtlinie einmal am Tag durchgeführt werden. Unabhängig davon kann auch eine Systemüberprüfung von der Konsole aus über rechte Maustaste → **Vollständige Systemüberprüfung** an einzelnen Rechnern gestartet werden. Wollen Sie mehrere Rechner auf einen Schlag überprüfen, können Sie auch erst die Rechner markieren und dann den Befehl gleich für alle ausgewählten Rechner abgeben.

Sophos-Richtlinien

Sophos stellt innerhalb der **Sophos Enterprise Console** zehn verschiedene Kategorien von Richtlinien zur Verfügung. Diese Richtlinien haben nichts mit den Gruppenrichtlinien (GPO) innerhalb des Active Directory zu tun. Die Sophos-Richtlinien werden Sophos-Gruppen zugeordnet und damit auf allen enthaltenen Klienten wirksam. Im Kontextmenü Ihrer Sophos-Gruppe, unter dem Punkt **Gruppenrichtliniendetails...**, finden Sie die dort zugeordneten Richtlinien. Wenn keine spezielle Richtlinie für eine Sophos-Gruppe festgelegt wurde, wird nur die Standard-Richtlinie angezeigt, die im Allgemeinen keine speziellen Einstellungen enthält. Um eine Richtlinie zu verändern, klickt man im Richtlinien-Feld (unten links) der **Sophos Enterprise Console** mit der rechten Maustaste auf den Namen der Richtlinie, die man bearbeiten möchte, und wählt den Punkt **Richtlinie öffnen/ändern...** Neben den anderen selbsterklärenden Auswahlmöglichkeiten ist besonders der Punkt **Gruppen mit dieser Richtlinie anzeigen...** interessant. Damit werden alle Sophos-Gruppen aufgelistet, in der diese Richtlinie enthalten ist. In der Regel tragen die zu einem Institut zugehörigen Richtlinien als Name das *Institutskürzel + ggf. die Abteilungsnummer*.

Vom zuständigen Administrator können nur die Richtlinien bearbeitet werden, die seinen zugeteilten Sophos-Gruppen zugewiesen wurden. Standardmäßig werden von uns nur die „Antivirus- und HIPS“-Richtlinie und die „Updating“-Richtlinie zugewiesen. Wenn Sie weitere Richtlinien benötigen, wenden Sie sich bitte per E-Mail mit dem Betreff „Sophos Enterprise Console“ und der Info, um welche Gruppe es sich handelt und welche Richtlinie Sie benötigen, an support@gwdg.de.

„Updating“-Richtlinie

Die Update-Richtlinien definieren, von welchem Server, zu welchen Zeiten und in welchem Benutzerkontext ein Rechner aktualisiert werden soll. Die Update-Richtlinien werden ausschließlich durch Mitarbeiter der GWDG bearbeitet. Dabei werden die Sophos-Gruppen auf die verschiedenen Update-Verzeichnisse (Interchk) verteilt, wodurch ein manueller Lastenausgleich realisiert wird. Diese Verzeichnisse enthalten die aktuellen Virensignaturen, mit denen sich alle Sophos-Klienten, die von der Enterprise Console verwaltet werden, aktualisieren.

Die Zuweisung der Update-Richtlinie kann auch durch den lokalen Administrator erfolgen. Diese Einstellung finden Sie im Kontextmenü der Sophos-Gruppe. Verwenden können Sie eine der folgenden Richtlinien:

- EC-Sophos_http
- GWD-Software1_http

„Antivirus und Hips“-Richtlinie

In den Antivirus-Richtlinien ist festgelegt, wie sich das Programm bei der Suche und bei einem Virenbefall verhalten soll. Das Erkennen eines Schadcodes kann durch die **On-Access-Überprüfung** oder in Folge eines geplanten Scans stattfinden. Für beide Prozesse muss das Vorgehen konfiguriert werden. Des Weiteren kann eingerichtet werden, ob und wie bei einem Virenvorfall jemand benachrichtigt wird und ob, wann und wie eine automatische zeitgesteuerte Virensuche auf dem Zielcomputer stattfindet. Über diese Richtlinie kann man außerdem bestimmte Laufwerke, Ordner und Dateien von der Virensuche ausschließen. Sollte Sophos Programme als problematisch erkennen, die in Wahrheit keine Gefahr darstellen, kann man diese über den Menüpunkt **Autorisierungen...** von weiteren Überprüfungen ausnehmen.

Wichtig: Sorgen Sie bitte unbedingt dafür, dass die eingetragene E-Mail-Adresse zur Benachrichtigung bei Virenfunden aktuell ist. Sie können die Adresse über **Benachrichtigungen** → **E-Mail-Benachrichtigungen** → **Umbenennen** ändern oder weitere hinzufügen.

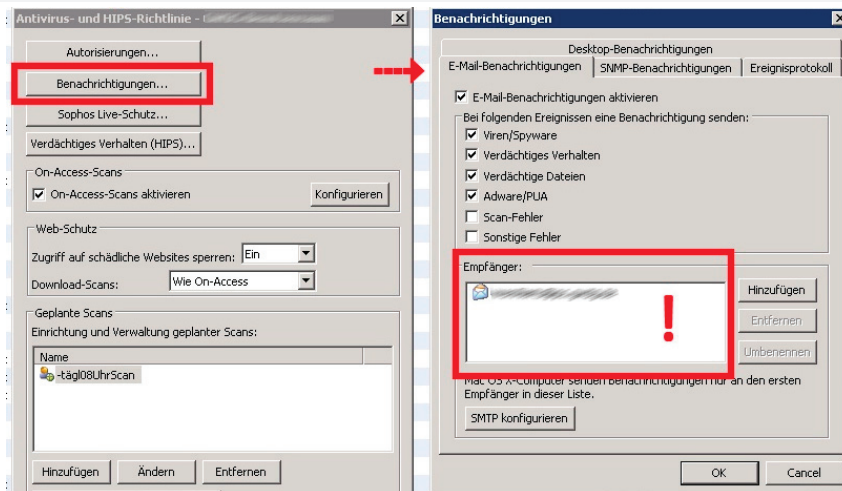


Abbildung 30 Sophos Enterprise Console - Benachrichtigungen

Exploit-Abwehr

Exploit-Abwehr stellt einen aktuellen Schutz vor Angriffen bereit. Die Anwendungen werden überwacht, um verdächtige Aktivitäten festzustellen, die das System angreifbar machen. Die Exploit-Abwehr ist nicht Bestandteil des Lizenzumfangs.

„Firewall“-Richtlinie

Die Firewall-Richtlinie kommt nicht zum Einsatz, weil die zugehörige Firewall-Software nicht in dem für die Universität geltenden Lizenzvertrag mit Sophos enthalten ist. Da ja inzwischen in allen aktuellen Betriebssystemen eine Firewall einhalten ist, kann man auf diese Funktion verzichten.

„Application Control“-Richtlinie

Kann verwendet werden, um das Ausführen unerwünschter Anwendungen auf den Arbeitsstationen zu verhindern.

„Data Control“-Richtlinie

Diese Funktion soll ungewollte Datenübertragungen durch Mitarbeiter reduzieren, z. B. um Kontodaten zu schützen. Die „Data Control“-Richtlinie kann so konfiguriert werden, dass Dateitypen, -namen oder -inhalte bei der Übertragung von Dateien auf Speichermedien (Wechselspeicher, optische Speicher und Festplatten) sowie beim Hochladen von Dateien in Anwendungen (Webbrowser, E-Mail-Clients usw.) überwacht werden.

„Device Control“-Richtlinie

Mit der „Device Control“-Richtlinie können Administratoren die Verwendung von Speichermedien und Netzwerkschnittstellen verwalten.

Die „Device Control“-Richtlinie führt teilweise zu Fehlermeldungen, die auf eine fehlerhafte Übernahme der Richtlinien hinweisen. Als Lösung dafür haben wir eine Kopie mit dem Namen **Nichts** erstellt und haben diese den meisten Sophos-Gruppen zugewiesen. Die Kopie entspricht der Standardrichtlinie, produziert aber keine Fehlermeldungen mehr.

„Manipulationsschutz“-Richtlinie

Mit der Manipulationsschutz-Richtlinie kann eingeschränkt werden, wer die Sophos-Software konfigurieren, deinstallieren oder deaktivieren darf. In der Richtlinie ist der Manipulationsschutz standardmäßig nicht aktiviert. Bei Aktivierung muss ein Passwort angegeben werden, welches dann zur Änderung der Sophos-Konfiguration am Arbeitsplatzrechner verwendet werden muss.

„Patch“-Richtlinie

Analysiert die Systeme auf fehlende Patches.

„Web Control“-Richtlinie

Mit dieser Richtlinie kann man die Zugriffe auf Webseiten einschränken. Neben den Standardmaßnahmen kann man einzelne Webseiten erlauben bzw. den Zugriff blockieren.

Migration der Benutzerumgebung

Bei der Migration der Benutzerumgebung werden die persönlichen Daten und Einstellungen sowie ggf. die E-Mail-Umgebung aus dem lokalen Profil in das servergespeicherte Profil übertragen. Auf diese Weise fällt den Mitarbeitern der Umstieg auf die Arbeitsumgebung des GWDG-Benutzerkontos leichter. Andererseits ist das Übertragen der Benutzereinstellungen in ein neues servergespeichertes Profil mitunter aufwändiger als eine Neueinrichtung des Profils. Hier ist also zuvor die Notwendigkeit abzuwägen.

Zu einer Migration der Benutzerumgebung gehören die folgenden drei Schritte:

1. Daten auf das persönliche Laufwerk übertragen
2. Einstellung des E-Mail-Programms sichern
3. Ggf. Einstellungen für das Betriebssystem und weitere Programme übertragen

Übertragung der Daten auf das persönliche Laufwerk (P:)

Bei einer Anmeldung mit dem GWDG-Benutzerkonto auf einem Rechner im AD wird automatisch das persönliche Laufwerk unter dem Laufwerksbuchstaben **P:** verbunden. Daher ist es sinnvoll, die bisher auf der lokalen Festplatte gespeicherten Dateien auf dieses Laufwerk zu verschieben. So sind sie von jedem Rechner innerhalb des Active Directory verfügbar und werden automatisch gesichert. Standardmäßig haben Sie eine Speicherplatzbeschränkung von 100 GB. Bei Bedarf können Sie aber eine Erhöhung der Quotierung anfordern. Wenden Sie sich dazu an support@gwdg.de.

Wenn Sie die Dateien übertragen wollen, so müssen Sie sich zunächst mit Ihrem bestehenden lokalen Konto auf Ihrem Rechner anmelden. Dann stellen Sie eine Netzlaufwerkverbindung zu Ihrem **P:-Laufwerk** her (siehe Abschnitt **Ein Netzlaufwerk manuell verbinden** auf Seite 56). Anschließend können Sie über den Datei-Explorer bequem die Dateien verschieben.

Erwähnenswert in diesem Zusammenhang ist, dass der Windows-Ordner **Eigene Dateien** auf Ihr **P:-Laufwerk** verweist, so dass Sie auch über die Windows-Ordnerstruktur leicht Ihre Daten erreichen können.

Das Benutzerprofil

Im Benutzerprofil werden alle persönlichen Einstellungen für das Betriebssystem und die Programme wie Office, E-Mail-Programm oder Browser abgelegt. Ist das Profil lokal, liegt es auf der Systempartition des Rechners. Ein Plattencrash sorgt dann auch für einen Verlust des Profils. Bei einem servergespeicherten Profil liegt das Profil, mit Ausnahme der lokalen Einstellungen (normalerweise unter **C:\Users\userid\AppData\Local**), nicht mehr nur auf dem eigenen Rechner, sondern auch auf einem Server der GWDG. Das Profil auf dem Rechner wird dann bei der Anmeldung an der Domäne GWDG mit dem Profil auf dem Server abgeglichen oder muss bei einer Erstanmeldung an einem Rechner vollständig kopiert werden. Ein servergespeichertes Profil hat den Vorteil, dass man es an jedem Rechner im Active Directory verwenden und damit überall auf seine persönlichen Einstellungen zugreifen kann.

Hinweis: Die Profile wurden zwischen Windows XP (Profile2) und Windows 10 (Profile2.V5 oder Profile2.V6) zweimal geändert, so dass ein Wechsel zwischen diesen Systemen auch das Arbeiten mit unterschiedlichen Profilen zur Folge hat.

Einstellungen für E-Mail und Internet sichern

Je nachdem, mit welchem E-Mail-Programm bisher gearbeitet wurde, muss überprüft werden, ob hier Einstellungen und/oder E-Mails gesichert und übertragen werden müssen.

Falls im Browser Favoritenlisten/Lesezeichen gespeichert sind, müssen diese gesichert und übertragen werden.

Beide Fälle lassen sich in modernen Programmen zumeist über eine **Export/Import**-Funktion bequem lösen.

Übertragung von Betriebssystem-Einstellungen

Die verschiedenen Windows-Betriebssysteme bieten unterschiedliche Programme an, um Systemeinstellungen und persönliche Einstellungen für die verschiedenen (Microsoft-) Anwendungsprogramme zu sichern. Diese können dann nach einem Systemwechsel wieder in das neu eingerichtete System übernommen werden. Diese Programme können auch genutzt werden, um diese Einstellungen in das servergespeicherte Profil zu übertragen. Meist lohnt sich das allerdings nur, wenn wirklich viele Einstellungen gemacht worden sind, weil dieser Weg doch recht zeitaufwändig ist und es daher oftmals schneller geht, ein paar Einstellungen neu vorzunehmen. Außerdem arbeiten diese Programme erfahrungsgemäß nicht 100 % zuverlässig bzw. sichern standardmäßig nicht alle Einstellungen, die man gern gesichert hätte.

Hinweis: Die lokalen Einstellungen (normalerweise unter `C:\Users\userid\AppData\Local`) werden nicht im servergespeicherten Profil abgelegt und können folglich auch nicht mit gesichert werden.

Servergespeicherte Benutzerprofile

Servergespeicherte Benutzerprofile werden mit Hilfe eines Eintrags in das Benutzerobjekt erstellt. Erzeugt wird das erste servergespeicherte Benutzerprofil während der ersten Anmeldung an einem Windows-System innerhalb des AD. Die Grundlage des ersten Profils bildet das Standardprofil des verwendeten Rechners. In diesem Profil werden die persönlichen Einstellungen für das Betriebssystem und der verwendeten Software, z. B. Office- und E-Mail-Programme oder Browserkonfigurationen, gespeichert. Dieses Benutzerprofil wird anschließend bei der Abmeldung als Kopie auf dem Server gespeichert und bei jeder An- und Abmeldung mit dem lokalen Profil synchronisiert.

Vorteilhaft sind servergespeicherte Benutzerprofile vor allen für Nutzer, die häufig ihren Standort wechseln, da der Nutzer seine gewohnte Umgebung quasi „mitnehmen“ kann, was die Verwendung der Arbeitsplätze deutlich angenehmer macht.

Hinweis: Die Größe des Profils hat großen Einfluss auf die Dauer des Anmeldevorgangs. Als Richtwert für die Profilgröße schlagen wir maximal 500 MB vor.

Hinweis: Das Profil liegt auf dem persönlichen Laufwerk des Benutzers und geht damit in die Quotierung von 100 GB mit ein (z. B: `P:_GWDGsys\Profile2.V6`)!

Hinweis: Einige Ordner des Profils werden unter Verwendung von Gruppenrichtlinien in einen Ordner direkt unter `P:\` umgeleitet. Man nennt diesen Vorgang **Ordnerumleitung**. Dies betrifft die folgenden Ordner:

- Downloads
- Musik
- Bilder
- Videos

Diese Maßnahme wurde ergriffen, um das servergespeicherte Profil klein zu halten. Außerdem wurden für die Standardordner von Filesharing-Programmen wie GWDG Cloud Share (PowerFolder), GWDG ownCloud und Dropbox so eingerichtet, dass sie nicht zu dem servergespeicherten Teil des Profils gehören, sondern nur lokal vorhanden sind.

Empfehlungen für die Verwendung des servergespeicherten Profils

Um Anmeldezeiten möglichst kurz zu halten, sollte das servergespeicherte Profil möglichst klein sein (maximal 500 MB). Dazu ein paar Hinweise:

- Es sollten keine große Dateien auf dem Desktop abgelegt werden. Dadurch wird das Profil unnötig vergrößert. Empfehlen Sie den Nutzern, die Dateien lieber auf ihrem P-Laufwerk abzulegen, das bequem über Eigene Dateien erreichbar ist. Alternativ können Sie für besonders häufig genutzte Ordner oder Dateien eine Verknüpfung als Desktop-Icon erzeugen (Rechte Maustaste auf den Ordner Senden an... → Desktop).

- Kontrollieren Sie den versteckten Ordner „Anwendungsdaten“ bzw. „AppData“ im Profil. Im Ordner Roaming legen viele Anwendungen Daten ab, die dann synchronisiert werden. Passen Sie ggf. die Einstellungen an, verringern Sie beispielsweise die Größe des Cache bei Firefox und richten Sie bei den Benutzern, die gerne Thunderbird nutzen möchten das Programm so ein, dass das Thunderbird-Profil nicht im Benutzerprofil liegt.

FAQ: Profilprobleme

Es kann immer mal wieder zu Problemen mit einem servergespeicherten Profil kommen. In den meisten Fällen liegt es dann an der Größe des Profils. Wie schon erwähnt, sind 500 MB ein guter Richtwert für ein servergespeichertes Profil. Sollte das Profil aber nicht mehr zu reparieren sein, sollten Sie das servergespeicherte Profil zurücksetzen und das lokal abgelegte Profil löschen.

Servergespeichertes Profil zurücksetzen

Melden Sie sich dazu an dem Arbeitsplatzrechner der betroffenen Person als Benutzer mit administrativen Rechten an.

Hinweis: Für die Zurücksetzung des Profils können Sie bei der Anmeldung nicht das betroffene Benutzerkonto verwenden.

Anschließend erstellen Sie eine Netzlaufwerkverbindung zum persönlichen Laufwerk (**P:**) des Benutzers, stellen Sie dabei die Verbindung über **Anmelden unter anderem Benutzernamen** her und verwenden Sie dafür das Benutzerkonto des betreffenden Mitarbeiters. In dem Ordner **_GWDGsys** befinden sich die Profile, die sich je nach Betriebssystem unterscheiden. Das aktuell verwendete Profil erkennen Sie am Änderungsdatum. Wählen Sie nun den entsprechenden Ordner und benennen ihn um, z. B. in **_GWDGsys\Profile2_old**. Bei der nächsten Anmeldung wird dann ein neues Profil erzeugt, das alte Profil bleibt dann als Backup im Ordner **_GWDGsys\Profile2_old** vorhanden.

Pfad des servergespeicherten Profils:

- P:_GWDGsys\Profile2.V2 Windows 7
- P:_GWDGsys\Profile2.V3 Windows 8
- P:_GWDGsys\Profile2.V4 Windows 8.1
- P:_GWDGsys\Profile2.V5 Windows 10
- P:_GWDGsys\Profile2.V6 Windows 10 ab Version 1607

Nun müssen Sie noch das lokale Profil löschen; Hier gibt es betriebssystemabhängige Unterschiede:

Ab Windows 7 liegen die Benutzerprofile im Pfad **C:\Users** oder **C:\Benutzer** und auch hier ist es ggf. ratsam, ein Backup zu erzeugen. Dazu wird der Ordner mit dem Namen des betroffenen Benutzers kopiert und in einem anderen Speicherbereich eingefügt.


Wichtig: Sie dürfen das Profil nicht verschieben, umbenennen oder löschen!

Hinweis: Das Löschen von Profilen darf ausschließlich über die Systemsteuerung erfolgen.

Windows 7: Lokale Kopie des servergespeicherten Profils löschen

Über **Start** → **Systemsteuerung** → **System** → **Erweiterte Systemeinstellungen** öffnet sich das Fenster **Systemeigenschaften**. Unter Umständen wird die Eingabe des Administratorkontos angefordert. Über den Reiter **Erweitert** → **Benutzerprofile** → **Einstellungen** können Sie das Profil auswählen und löschen. Bitte kontrollieren Sie anschließend, ob die Profildateien auf dem Computer entfernt wurden. Falls nicht, können Sie jetzt den Profilordner von der Systempartition (meistens **C:**) entfernen.

Windows 8 & Windows 10: Lokale Kopie des servergespeicherten Profils löschen

Bedienen Sie auf der Tastatur die Windows-Taste  und tippen Sie dann **Systemsteuerung** ein. Weiter geht es mit **System** → **Erweiterte Systemeinstellungen**. Es öffnet sich das Fenster **Systemeigenschaften**. Unter Umständen wird die Eingabe des Administratorkontos angefordert. Über den Reiter **Erweitert** → **Benutzerprofile** → **Einstellungen** können Sie das Profil auswählen und löschen. Bitte kontrollieren Sie anschließend, ob die Profildateien auf dem Computer entfernt wurden. Falls nicht, können Sie jetzt den Profilordner von der Systempartition (meistens **C:**) entfernen.

Wenn das Profil nicht über die Systemsteuerung gelöscht wurde, oder der Benutzer immer wieder mit einem temporären Profil angemeldet wird, prüfen Sie bitte in der Registrierung des Rechners den folgenden Eintrag:

Pfad:

Computer\HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Dazu geben Sie unter **Start** → **Ausführen** den Befehl **regedit** ein und bestätigen mit Eingabetaste. Es öffnet sich das Fenster „Registrierungs-Editor“. Hier folgt man dem oben angegebenen Pfad, bis die Profilliste angezeigt wird. Die einzelnen Einträge der Profile werden als lange Zahlenfolgen angezeigt. Sollte eine der Zahlenfolgen mit einem **.bak** enden, wird sie unter Verwendung des Kontextmenüs gelöscht. Anschließend sollte bei der nächsten Anmeldung wieder ein servergespeichertes Profil geladen werden. Dies gilt für alle aktuellen Betriebssysteme.

Fehler bei der Anmeldung „Zu wenig Speicherplatz“

Während der Anmeldung am Rechner wird das Benutzerprofil geladen und auf der System-Partition abgelegt. Ist auf der Partition nicht genügend Speicherplatz vorhanden, wird der Nutzer mit einem temporären Profil angemeldet und die persönlichen Einstellungen stehen nicht zur Verfügung. Dieses wird während der Anmeldung als Fehlermeldung angezeigt.

Überprüfen Sie also über **Arbeitsplatz** bzw. **Computer**, ob auf **C:** ausreichend Platz für das Profil vorhanden ist. Um festzustellen wieviel Speicherplatz das Profil benötigt, können Sie im persönlichen Verzeichnis (**P:**) des Nutzers in dem Pfad **_GWDGsys\Profile2.xy** nachsehen. Verwenden Sie die **rechte Maustaste** → **Eigenschaften**, um die Größe des Profils zu bestimmen. Sollten Sie zu dem Ergebnis kommen, dass das Profil deutlich größer ist als die empfohlenen 500 MB, so sollten Sie kontrollieren, welche Dateien viel Platz im Profil beanspruchen und ggf. diese Dateien löschen oder in einen Bereich außerhalb des Profils

verschieben. Wenn die Profilgröße dem empfohlenen Wert in etwa entspricht, löschen Sie auf der Systempartition unwichtige Daten, z. B. in den Ordnern **Temp** oder **Temporäre Internetfiles**. Häufig befinden sich auch im Ordner **Benutzer** überflüssig gewordene Profile. Diese können mit dem im Abschnitt **FAQ: Profilprobleme** auf Seite 44 beschriebenen Verfahren gelöscht werden.

Fehler bei der Abmeldung „Zu wenig Speicherplatz“

Wenn die Nutzer die Grenze der Quotierung für das **P:**-Laufwerk erreicht haben, überprüfen Sie, ob überflüssige Daten auf dem Laufwerk liegen und löschen Sie diese. Falls Sie keinen Speicherplatz frei räumen können, haben Sie die Möglichkeit, per E-Mail an support@gwdg.de die Speicherkapazität erhöhen zu lassen. Bitte prüfen Sie zunächst, ob das Profil die empfohlene Größe von 500 MB nicht deutlich überschreitet.

„Eigene Dateien“ liegen im Profil

Durch einen Fehler im System oder durch manuelle Konfiguration kann es passieren, dass der Ordner **Eigene Dateien** innerhalb des Profils liegt. In diesem Fall ist es ratsam, den Ordner aus dem lokal gespeicherten Profil zu löschen und zuvor die evtl. enthaltenen Dateien direkt im Homeverzeichnis unter **P:** zu speichern.

Fehler durch E-Mail-Programme

Es kann passieren, dass der E-Mail-Client den Speicherbereich in das Profil legt. Standardmäßig ist das bei der Software Mozilla Thunderbird der Fall.

Drucker im Active Directory

In den meisten Instituten haben die Mitarbeiter heute keine eigenen Drucker mehr an ihrem Arbeitsplatz. Stattdessen verfügen die Institute über Netzwerkdrucker, die von allen Mitarbeitern gemeinsam genutzt werden. Deshalb bietet die GWDG seit einigen Jahren den Anschluss und die Verwaltung der institutseigenen Drucker über die Server der GWDG an.

Zentral verwaltete Institutsdrucker

Eine Einbindung der Institutsdrucker an zentraler Stelle ermöglicht auch eine zentrale Verwaltung der Druckerressourcen, woraus sich viele weitere Vorteile ergeben:

- **Zugriffsberechtigungen** können unter Verwendung der GWDG-Konten über die Einstellungen der Drucker-Warteschlangen gesteuert werden.
- **Vorkonfigurierte Druckereinstellungen** können für alle Nutzer vorgegeben werden.
- Die **Verfügbarkeit von Druckern** ist nicht von den Arbeitsstationen abhängig, auf denen die Drucker ggf. bereitgestellt werden.
- **Weniger Sicherheitslücken**, da auf den Arbeitsstationen keine Ressourcen (z. B. Drucker) freigegeben werden müssen.
- **Druckertreiber für Windows-Computer** werden vom Druckservice bereitgestellt und auf den Windows-Arbeitsstationen der Benutzer automatisch beim ersten Zugriff auf den Drucker installiert.
- **Gruppenrichtlinien** ermöglichen eine automatische Verbindung mit dem Drucker, sofern man sich innerhalb des Active Directory angemeldet hat.

Manuelle Druckerverbindungen unter Windows

Werden die Drucker nicht automatisch durch ein Logon-Skript verbunden, kann der Institutsdrucker manuell verbunden werden. Je nach Betriebssystem benutzt man den Link im Startmenü **Geräte und Drucker** → **Drucker hinzufügen** → **Einen Netzwerkdrucker hinzufügen**. Falls der gesuchte Drucker in der Liste nicht aufgeführt wird, folgt man dem Link: **Der gewünschte Drucker ist nicht in der Liste enthalten**.

Hinweis: Der Link ist schlecht als solcher erkennbar. Hier wählt man nun den Punkt **Freigegebene Drucker über den Namen auswählen** und fügt Folgendes ein:

[\\gwd-winprint.top.gwdg.de\\[Institutsdrucker\]](#)

Alternativ kann man auch über **Start** → **Ausführen** → [\\gwd-winprint](#) direkt per Doppelklick auf die gewünschte Druckerwarteschlange einen Drucker verbinden. Sofern man nicht im AD angemeldet ist, folgt ein Anmeldefenster, in dem man sein GWDG-Benutzerkonto mit [GWDG\userid](#) und das dazugehörige Passwort verwendet. Der Name des Institutsdruckers hat in der Regel gemäß dem Namensschema die Form **UG-UXYZ-P01** (siehe das Abschnitt **Namensschema**).

Die Zugriffsberechtigungen werden über Gruppenmitgliedschaften gesteuert (siehe S. 7). Bei Bedarf kann der zuständige Administrator für die Nutzer des Druckers Voreinstellungen vorgeben. Dieses erleichtert oftmals die Verwendung des Druckers.

Da die Anzahl der Multifunktionsgeräte immer weiter steigt, bieten wir innerhalb der zentralen Druckerverwaltung auch die Möglichkeit, Dateien von gescannten Objekten in einen zentralen Speicherort zu verschieben. Die in vielen Instituten verwendeten gemeinsamen Laufwerke bieten hierfür einen geeigneten Platz (siehe S. 55).

Die E-Mail-Umgebung

Der Microsoft Exchange-Server bietet neben der Bereitstellung von eigenen Kontakten und Kalendern auch Funktionalitäten zur Zusammenarbeit (Workgroup, Collaboration). Normalerweise erhalten neue Benutzer bei der Einrichtung eines Accounts automatisch ein Postfach auf dem Exchange-System.

E-Mail-Adresse

Als **E-Mail-Adressen** für das Postfach können drei Varianten in Abhängigkeit der Institutszugehörigkeit zur Verfügung stehen:

- userid@gwdg.de
- userid@uni-goettingen.de
- Vorname.Nachname@fakultaet.uni-goettingen.de

Dieses gilt derzeit nur für Accounts, die vor dem 04.04.2016 eingerichtet wurden. Jede E-Mail, die an eine dieser drei E-Mail-Adressen gesendet wird, wird in ein und demselben Postfach gespeichert. Die E-Mail-Adresse userid@uni-goettingen.de steht nur Universitätsangehörigen zur Verfügung, nicht den der GWDG angeschlossenen anderen Einrichtungen. Die E-Mail-Adresse Vorname.Nachname@fakultaet.uni-goettingen.de enthält zusätzlich die Fakultät, in der das Institut angesiedelt ist.

Seit der Einführung des **einheitlichen Mitarbeiteraccounts** am 04.04.2016 seitens der Universität Göttingen hat sich die Vergabe der E-Mail-Adressen geändert. Automatisch werden nur noch Adressen der Form **Vorname.Nachname@uni-goettingen.de** gebildet. Auch die Benutzernamen werden in neuen Format gebildet (siehe den Abschnitt **Das Benutzerkonto**).

Einen Sonderfall bilden die Mitarbeiter der Universitätsmedizin, deren E-Mail-Accounts in einem eigenen UMG-Mailsystem liegen. Die E-Mail-Adressen werden analog zu denen der GWDG in der Form **Vorname.Nachname@med.uni-goettingen.de** gebildet. Diese Accounts werden von der UMG direkt betreut.

E-Mail-Zertifikate

Sie haben über die Zertifizierungsstelle der MPG, Uni Göttingen und GWDG die Möglichkeit, ein persönliches E-Mail-Zertifikat für Ihren Account zu beantragen. Dazu müssen Sie eine zuständige Registration Authority, kurz RA, auswählen:

- MPG-Mitarbeiter → [Liste der RAs](#)
https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:mpgras
- Uni Göttingen-Mitarbeiter → [Liste der RAs](#)
https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:uniras
- GWDG-Mitarbeiter → [Liste der Ras](#)
https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:gwdgras

Nach der Auswahl der hauseigenen RA wählen Sie aus dem oberen Menü **Nutzerzertifikat** aus und geben die E-Mail-Adresse(n) ein, für welche das Zertifikat beantragt wird. Nachdem Sie das Formular ausgefüllt und die Angaben bestätigt haben, können Sie Ihren Antrag im PDF-Format herunterladen. Diesen Antrag sollten Sie ausgedruckt und unterschrieben zur hauseigenen RA mitbringen. Bringen Sie dazu Ihren gültigen Personalausweis oder Reisepass mit, damit eine persönliche Identifizierung durchgeführt werden kann. Erst danach kann der Antrag weiterbearbeitet und das Zertifikat ausgestellt werden. Weitere Informationen bekommen Sie per E-Mail.

Wichtig: Beachten Sie, dass Sie später Ihr Zertifikat ausschließlich auf demselben Rechner, unter demselben Account und mit dem gleichen Browser (momentan nur unter Mozilla Firefox möglich) abholen können, mit dem Sie das Zertifikat beantragt haben.

Hinweis: Verwenden Sie somit für die Beantragung einen Rechner, auf den Sie immer Zugriff haben. Nach der Abholung kann das Zertifikat aber auf beliebig viele weitere Rechner transferiert werden.

Zur Sicherheit exportieren Sie das Zertifikat z. B. auf Ihr persönliches Laufwerk (siehe den Abschnitt **P-Laufwerk**).

Weitere Informationen finden Sie auf der folgenden Webseite:

https://info.gwdg.de/docs/doku.php?id=de:services:it_security:pki:start

Verwendung des Zertifikats mit Outlook

Im Outlook für Windows navigieren Sie im Menüpunkt **Datei** zu **Optionen** und klicken dort auf das **Trust Center**. Weitere Einstellungen für das **Trust Center** rufen Sie mit einem Klick auf die Schaltfläche **Einstellungen für das Trust Center...** (unten rechts) auf. Mit einem Klick auf die

Schaltfläche **Importieren/Exportieren...** fügen Sie Ihr Zertifikat hinzu. Bestätigen Sie den Import des Zertifikats im Outlook mit Eingabe des Zertifikat-Kennwortes.


Im Outlook für Mac gehen Sie über **Einstellungen** → **Konten** → **Erweitert** → auf das Register **Sicherheit**, wo Sie das Zertifikat zum Signieren und Entschlüsseln auswählen können.

In beiden Programmen können Sie auswählen, ob Sie standardmäßig alle E-Mails signieren und/oder verschlüsseln wollen.



Abbildung 31 signieren und verschlüsseln in Outlook

Nach dem Neustart von Outlook sollte im Nachrichtenfenster (E-Mail-Eingabe) eine Zertifikatsoption erscheinen.

Nun können Sie beim Erstellen einer neuen E-Mail diese mit dem ausgewählten Zertifikat signieren, indem Sie über den Reiter **Optionen** digitales **Signieren** oder **Verschlüsseln** auswählen. Bei dem Empfänger wird je nach verwendetem E-Mail-Programm der Hinweis dazu angezeigt. Häufig weist ein Icon, z. B. , auf eine Signatur hin oder es steht das Wort „Signiert“ neben der E-Mail.

Exchange E-Mail-Server

Der Exchange-Server bietet zahlreiche Zugangsmöglichkeiten:

- MAPI-Anbindung (Outlook)
- RPC über HTTPS (Outlook)
- die Standard-Protokolle IMAP4 und POP3 (beide nur über SSL / TLS)
- HTTPS (Webmail-Zugang: email.gwdg.de)
- EAS (Exchange ActiveSync für die mobilen Geräte)
- EWS (Exchange Web Services z. B. für Mac OS X)

Hinweis: Es bestehen einige generelle Beschränkungen, darunter die Standardpostfachgröße von maximal 10 GB und die maximale Anzahl zu versendender E-Mails (500 E-Mails innerhalb von 24 Stunden). Sollte in Ausnahmefällen mehr benötigt werden, muss dies über support@gwdg.de beantragt werden.

Die Exchange-Server stellen darüber hinaus das MAPI-Protokoll zur Verfügung. Die wesentlichen Vorteile gegenüber dem IMAP-Protokoll sind:

- Synchronisation von Kalendern, Aufgaben, Kontakten und Notizen
- Mobiler Mailabruf via Microsoft-Direct-Push-Technologie

- Globales Adressbuch
- Serverseitige Filterdefinition

Deshalb empfiehlt es sich Outlook mit Exchange-Funktionalitäten einzurichten.

Konfiguration von Outlook

Falls Outlook vor der Konfiguration schon einmal geöffnet worden ist, wurde bereits ein Profil erstellt, mit dem es zu unschönen Überraschungen kommen kann. Daher sollte vorab überprüft werden, ob unter **Start** → **Systemsteuerung** der Punkt **E-Mail** oder **Mail** auftaucht. Wenn ja, dann wurde bereits ein Profil erstellt, das Sie über **E-Mail** → **Profile anzeigen** sehen.

Fügen Sie in diesem Fall über **Hinzufügen** ein neues Profil hinzu und tragen Sie es unter dem Punkt **Immer dieses Profil verwenden** ein. Sie können das Profil mit einem beliebigen Namen versehen. Nun muss in dem sich neu öffnenden Fenster das Profil konfiguriert werden.

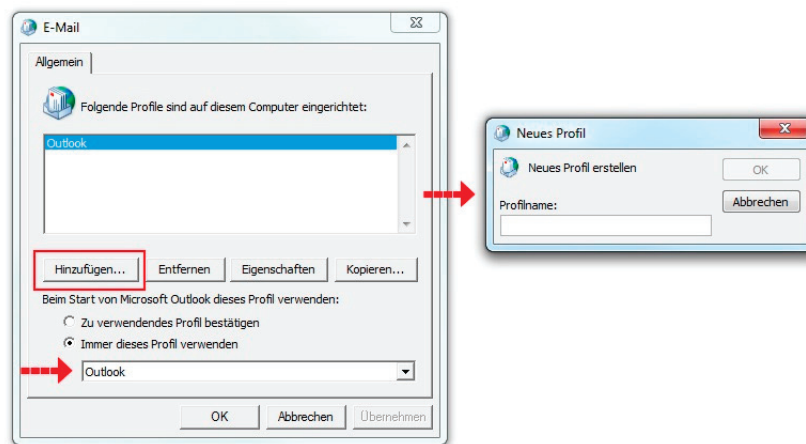


Abbildung 32 Neues Outlookprofil erstellen

Es wird der Dialog **Neues E-Mail-Konto hinzufügen** gestartet. Wenn der Rechner ins Active Directory eingebunden ist, so werden der Name und die E-Mail-Adresse automatisch eingetragen, andernfalls muss man das an dieser Stelle nachholen. Als E-Mail-Adresse wird die primäre E-Mail-Adresse eingetragen. Diese kann über das Kundenportal (siehe **Passwort überprüfen und ändern**) kontrolliert werden.

Konfigurationseinstellungen Outlook mit Exchange-Funktionalitäten

Die Einstellungen in den verschiedenen Outlook-Versionen unterscheiden sich. Sie sind ausführlich auf den entsprechenden Webseiten der GWDG beschrieben. Generell gilt bei der Einrichtung Folgendes:

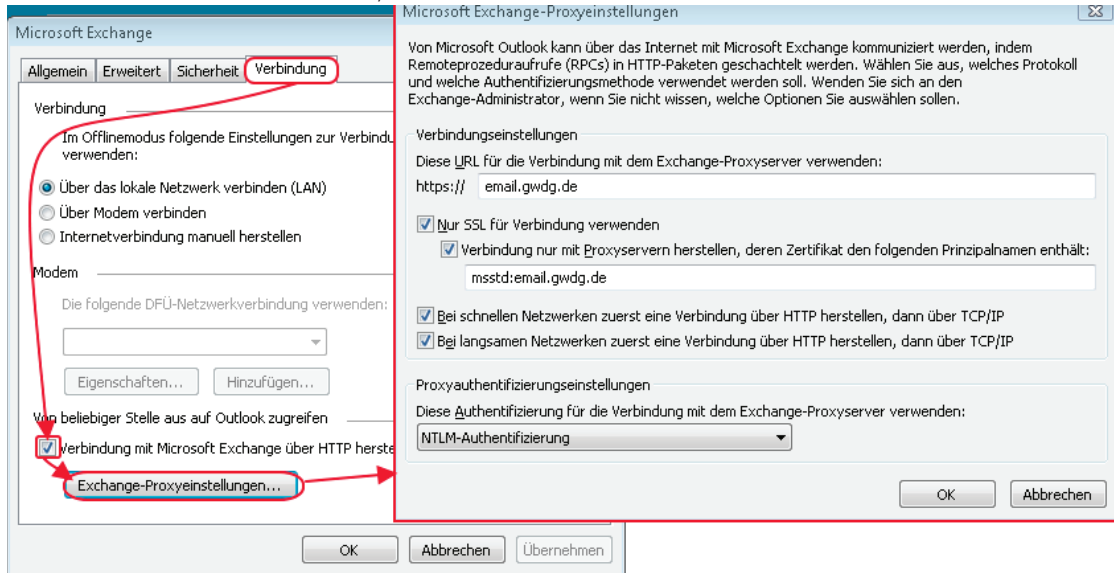
- **E-Mail-Dienst:** Microsoft Exchange
- **Microsoft Exchange-Server:** email.gwdg.de

Im Active Directory wird der Benutzername automatisch aufgelöst. Ist das nicht der Fall, so gilt Folgendes:

- **Ihr Name:** Vorname Nachname

- **Benutzername:** GWDG\userid
- **E-Mail-Adresse:** userid@gwdg.de (primäre E-Mail-Adresse)
- **Kennwort:** GWDG-Passwort

Für den Fall, dass man nicht im AD angemeldet ist, sind in den Kontoeinstellungen unter der Schallfläche **Weitere Einstellungen** die Proxyeinstellungen wie folgt vorzunehmen (nur Outlook 2010 und Outlook 2013):



Exchange-Cache-Mode

Bei der Einrichtung des Exchange-Postfachs kann unter anderem eine Option für den Exchange-Cache-Modus definiert werden.

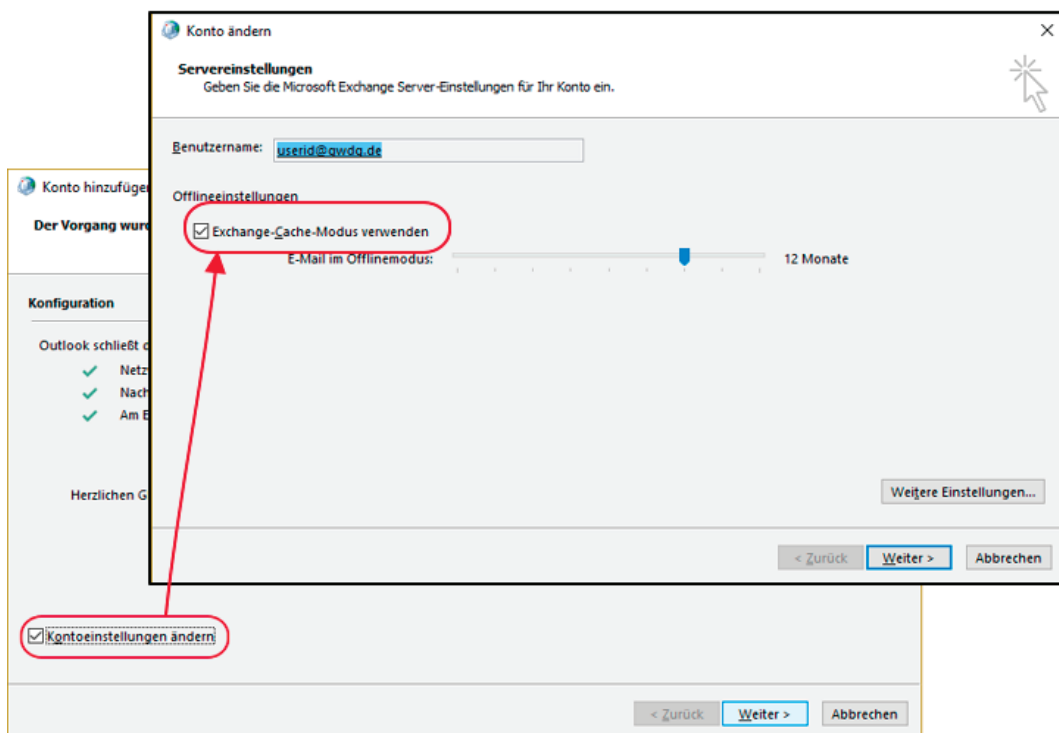


Abbildung 33 Exchange-Cache-Modus I

Wenn Sie Outlook mit Exchange verwenden und der Exchange-Cache-Modus eingeschaltet ist, so werden die Daten standardmäßig nicht nur auf dem Server, sondern auch in einer Offline-Cache-Datei im lokalen Benutzerprofil in einer Datei mit der Erweiterung **.ost** gespeichert (OST-Datei). Diese Datei sorgt dafür, dass auch ohne eine Verbindung zum Exchange-Server gearbeitet werden kann. Steht eine Verbindung zum Exchange-Server zur Verfügung, so findet eine Synchronisation zwischen Outlook und Exchange statt.

Das Aktivieren des Exchange-Cache-Modus ist dann sinnvoll, wenn z. B. die Verbindung zwischen Ihrem Computer und dem Exchange Server für längere Zeit nicht vorhanden ist, z.B. bei der Verwendung eines Notebooks im Zug. Auch bei einer langsameren Internetverbindung werden Sie vom Exchange-Cache-Modus profitieren. Ist der Cache-Modus in einer Umgebung eingeschaltet, in der z. B. mit freigegebenen Kalendern gearbeitet wird, kann es zu einem verzögerten Abgleich und zu Synchronisationskonflikte kommen.

Den Exchange-Cache-Modus können Sie bei oder nach der Einrichtung des Outlook-Profiles unter Kontoeinstellungen anpassen.

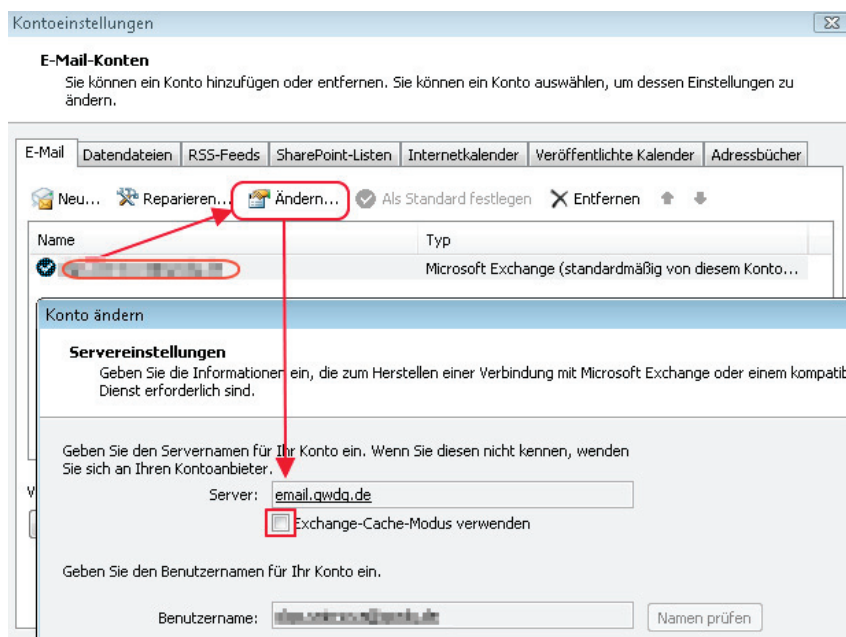


Abbildung 34 Exchange-Cache-Modus II

Hinweis: Die Option kann auch per GPO deaktiviert werden. In diesem Fall ist die Einstellung im Outlook ausgegraut dargestellt und kann nicht geändert werden.

Konfigurationseinstellungen Outlook ohne Exchange-Funktionalitäten

Soll Outlook nicht mit Exchange-Funktionalitäten eingerichtet werden, so gelten folgende Einstellungen:

- **Posteingangsserver (POP3, IMAP4):** email.gwdg.de
Postausgangsserver (SMTP): email.gwdg.de

Generell muss dabei immer die sichere Verbindung über **SSL / TLS / STARTTLS** (je nach E-Mail-Programm) gewählt werden:

- POP3S: Port 995
- IMAPS: Port 993
- SMTP: Port 587

FAQ: Automatische Konfiguration per Autodiscover schlägt für Outlook 2016 fehl

Bei der automatischen Konfiguration kann es vorkommen, dass die Anmeldeinformationen vom Exchange-Server nicht verifiziert werden können. Dieser Fehler kann bei Windows-Rechnern auftreten, die sich z. B. nicht im Active Directory befinden, oder wenn es in der Institution generell eingeschränkte Netzwerkeinstellungen gibt. In diesem Fall geben Sie bitte die Windows-Anmeldeinformationen für den Exchange-Server wie in dem folgenden Beispiel ein. Rufen Sie dazu in der Systemsteuerung die Option **Anmeldeinformationsverwaltung** auf und legen Sie bei Windows-Anmeldeinformationen einen neuen Eintrag an.

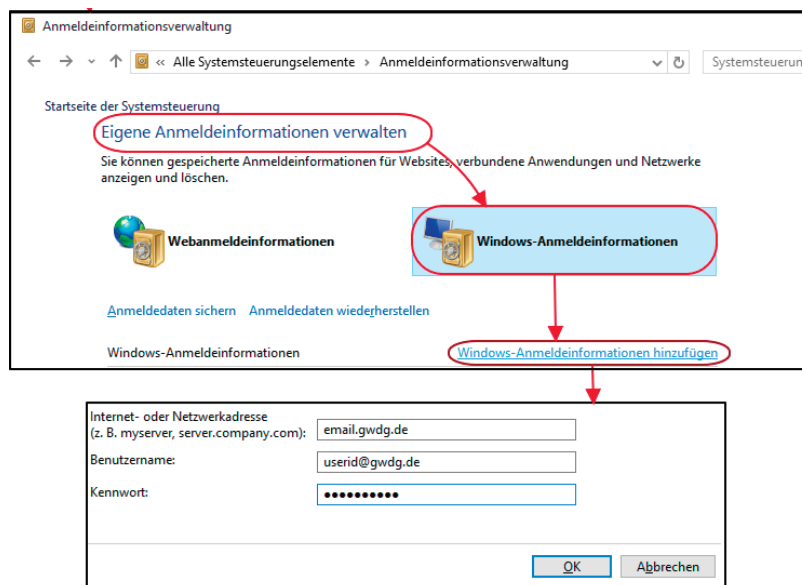


Abbildung 35 Anmeldeinformationsverwaltung

Hinweis: Nach einer Passwortänderung muss diese Information aktualisiert werden.

E-Mail-Server als vertrauenswürdige Sites eintragen

Fügen Sie den Link <https://email.gwdg.de> zu den sicheren Seiten hinzu (**Systemsteuerung** -> **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites** oder **Lokales Intranet**), um die Verbindung zum E-Mail-Server zu optimieren.

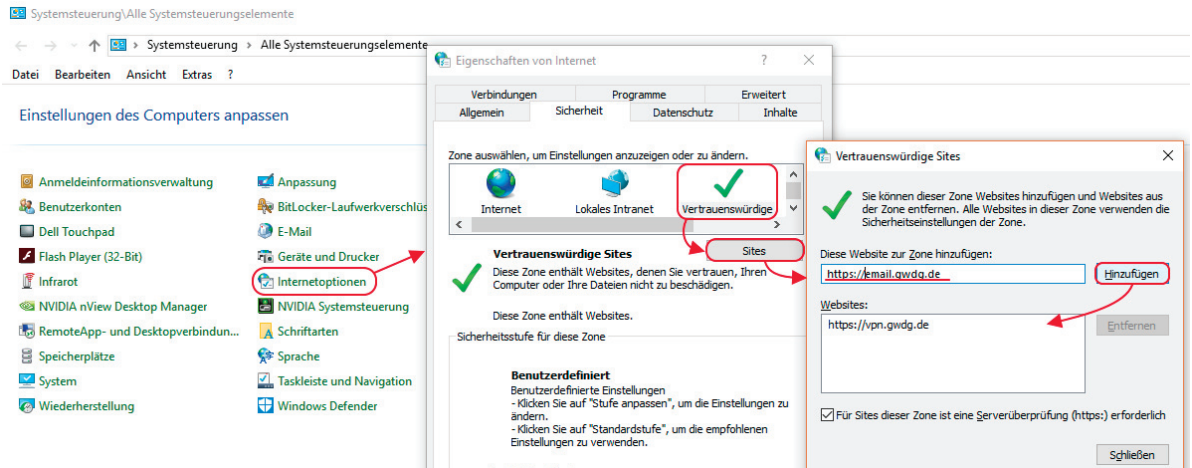


Abbildung 36 Vertrauenswürdige Sites

Outlook als Standardprogramm in Windows festlegen

Unter **Start** → **Systemsteuerung** → **Standardprogramme** vergewissern Sie sich, dass Outlook als Standardprogramm für E-Mails festgelegt ist. Wenn Sie nach Outlook ein anderes E-Mail-Programm installieren, kann dieses die Einstellung für das Standard-E-Mail Programm überschreiben.

Sicherung von Daten

Zur Sicherung des Postfachs kann eine Exportierung in eine Datei mit der Erweiterung **.pst** stattfinden (PST-Datei), die z. B. lokal auf dem Rechner gespeichert wird. Eine PST-Datei kann direkt von Outlook geöffnet oder in das Postfach importiert werden.

Outlook Web App (OWA)

Neben einem lokal installierten E-Mail-Programm kann auf das Exchange-Konto auch über die Webseite email.gwdg.de zugegriffen werden. Sollen alle Funktionalitäten zur Verfügung stehen, so muss im Anmeldefenster angegeben werden, dass es sich um einen privaten Computer handelt. Nicht alle Webbrowser bieten jedoch alle Funktionalitäten an.

Mobiler E-Mail Zugang

Sie können von einem mobilen Endgerät aus per Browser die OWA (Outlook Web App) erreichen und so online Ihre E-Mail Korrespondenz bearbeiten.

Alternativ können Sie eine E-Mail-App verwenden, um die Verbindung mit Exchange aufzubauen und um Ihre E-Mails, Kalenderdaten, Kontakte, Notizen usw. auf Ihr mobiles Endgerät zu synchronisieren. Dabei ist es wichtig, dass die E-Mail-App und Ihr Endgerät aktuellen Sicherheitsstandards entsprechen. Dazu zählen folgende Punkte:

- Exchange ActiveSync wird von Ihrem Smartphone unterstützt.
- Eine Displaysperre ist auf dem Smartphone eingerichtet.
- E-Mail App hat Geräteadministrator Rechte bekommen.

Hinweis: Bei der Auswahl der E-Mail-Apps achten Sie darauf, dass diese keine Daten und Passwörter unverschlüsselt überträgt oder Ihre Daten und Passwörter auf fremden Servern speichert.

Anleitungen für die Einrichtung eines Exchange-Postfachs für verschiedene mobile Betriebssysteme finden Sie über den folgenden Link:

- https://info.gwdg.de/docs/doku.php?id=de:services:email_collaboration:email_service:3mobile_access

Weitere Informationen & Hilfe

Ausführliche Informationen zum Exchange-Server finden Sie ebenfalls auf unseren Webseiten, als Einstiegsseite wählen Sie hier:

- https://info.gwdg.de/docs/doku.php?id=de:services:email_collaboration:email_service

Ausführliche bebilderte Anleitungen zur Konfiguration von Outlook finden Sie unter dem folgenden Link:

- https://info.gwdg.de/docs/doku.php?id=de:services:email_collaboration:email_service:1windows

Halbjährlich findet bei der GWDG ein Anwenderkurs zu Outlook statt, in dem der gesamte Umfang der Funktionalitäten im Outlook im Zusammenhang mit dem Exchange-Server vorgestellt wird (workgroup collaboration). Außerdem wird der Umgang mit dem Programm und den besagten Funktionalitäten in der Gruppe geübt. Weitere Informationen zum Kurs finden Sie im Kapitel **Kurse** auf Seite 59.

Speicherbereiche

Die GWDG stellt Ihnen zwei verschiedene Speicherbereiche zur Verfügung. Den persönlichen Speicherbereich, der im Active Directory standardmäßig unter dem Laufwerksbuchstaben **P:** verbunden wird und standardmäßig 100 GB Platz für eigene Daten bietet. Bei Bedarf wird die Speicherkapazität erweitert. Wenden Sie sich dazu bitte an unseren Support unter support@gwdg.de mit dem Betreff „Speicherplatz erweitern“.

Des Weiteren können Sie für Ihre Arbeitsgruppe einen gemeinsamen Speicherbereich anfordern, der dann bei einer Anmeldung im AD unter dem Laufwerksbuchstaben **W:** eingebunden wird und für den die Zugriffsrechte von den Institutsadministratoren selbst verwaltet werden (siehe S. 58).

Backupverfahren

Die Dateien werden auf redundanten Systemen bereitgestellt und von dort aus täglich mit **IBM Spectrum Protect – ISP** (früher IBM Tivoli Storage Manager) gesichert. So können ggf. Daten bis zu 90 Tage nach dem Löschen wiederhergestellt werden. Bei entsprechendem Bedarf lassen Sie uns Datei- oder Ordnernamen und das gewünschte Wiederherstellungsdatum per E-Mail an support@gwdg.de zukommen.

Daten selbst durch „Schattenkopien“ wiederherstellen

Um eine verlorene Datei im **P:-** oder **W:-Laufwerk**, eine frühere Dateiversion oder einen Ordner wiederherzustellen, verwenden Sie im Kontextmenü der Datei oder dem Ordner den Punkt **Eigenschaften** und anschließend die Registerkarte **Vorgängerversionen**. Auf dieser Registerkarte befinden sich die verschiedenen Versionen der vergangenen Tage.

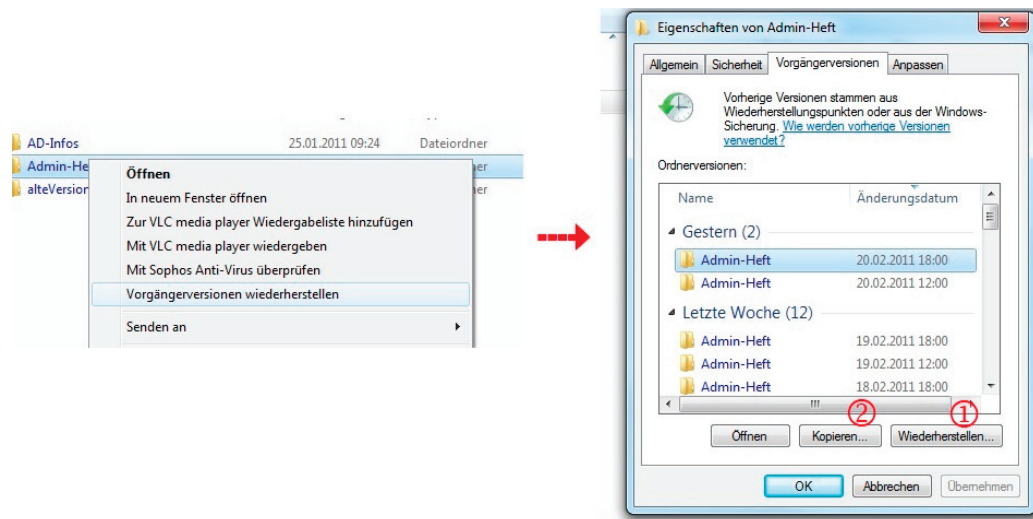


Abbildung 37 Schattenkopien

Sie haben nun zwei Möglichkeiten, eine der angebotenen Dateiversionen wieder verfügbar zu machen:

1. Wählen Sie eine Version aus und verwenden Sie dann den Schalter „**Wiederherstellen...**“. Bei Bedarf können Sie auch mit einem Doppelklick auf die angezeigten Ordner tiefer in die Struktur hineingehen.
2. Alternativ haben Sie die Möglichkeit, die Datei aus der Auswahl zu kopieren und an anderer Stelle wieder einzufügen.

Ein Netzlaufwerk manuell verbinden

Falls der Rechner, an dem Sie arbeiten, nicht in das AD integriert ist oder Sie nicht in der Domäne **GWDG** angemeldet sind, müssen Sie Ihre Netzlaufwerke manuell verbinden. Der Pfad zu einem Netzlaufwerk besteht üblicherweise aus dem Servernamen (z. B. [\\winfs-uni.top.gwdg.de](http://winfs-uni.top.gwdg.de)) und einem Freigabennamen (z. B. **userid\$**). Servername und Freigabename werden mit einem „\“ getrennt. Das Dollarzeichen hinter dem Freigabennamen zeigt an, dass es sich um eine versteckte Freigabe handelt. Sie ist also beim Anzeigen der Netzwerkumgebung nicht sichtbar.

Um ein Netzlaufwerk zu verbinden, gehen Sie im **Windows Explorer** mit der rechten Maustaste auf **dieser PC** und wählen **Netzlaufwerk verbinden...**

Für das **persönliche Laufwerk** wählen Sie den Buchstaben **P:** und für das **gemeinsame Laufwerk** den Buchstaben **W:**. Im Feld **Ordner** muss der Pfad zum Netzlaufwerk angegeben werden, der abhängig von der Institutszugehörigkeit ist.

Persönlicher Speicherbereich (P:)

- MPG
[\\winfo-mpg.top.gwdg.de\userid\\$](\\winfo-mpg.top.gwdg.de\userid$)
- Universität Göttingen
[\\winfo-uni.top.gwdg.de\userid\\$](\\winfo-uni.top.gwdg.de\userid$)
- GWDG
[\\winfo-gwd.top.gwdg.de\userid\\$](\\winfo-gwd.top.gwdg.de\userid$)
- Sonstige
[\\winfo-son.top.gwdg.de\userid\\$](\\winfo-son.top.gwdg.de\userid$)

Gemeinsamer Speicherbereich (W:\)

- Institutslaufwerke
[\\wfs-\[Fakultät\].top.gwdg.de\XYZ-all\\$\XYZ100](\\wfs-[Fakultät].top.gwdg.de\XYZ-all$\XYZ100)
für [Fakultät] setzen Sie Ihren Fachbereich ein (z. B. „Biologie“ oder „Forst“).

Sie müssen außerdem den Haken bei **Die Verbindung unter anderem Benutzernamen/anderen Anmeldeinformationen** setzen. Im darauffolgenden Fenster geben Sie Ihren GWDG-Benutzernamen mit vorangestelltem **GWDG** und dem dazugehörigen Passwort ein.

Verwendung der Netzlaufwerke außerhalb des GÖNET (z. B. private PC)

Falls Sie von außerhalb des GÖNET Ihre Daten erreichen wollen, z. B. von Ihrem PC zu Hause, haben Sie zwei Möglichkeiten: (1) den Zugang über VPN oder (2) den Zugang über einen Terminalserver.

Zugang über VPN

Sie können über einen VPN-Zugang mit Ihren Daten verbunden werden. Der kurze Weg erfolgt über <https://webvpn.gwdg.de>. Hier müssen Sie sich lediglich mit Ihrer GWDG-Benutzerkennung anmelden. Alternativ können Sie einen lokalen VPN-Klienten installieren.

Weitere Informationen finden Sie auf der folgenden Webseite:

- https://info.gwdg.de/docs/doku.php?id=de:services:network_services:vpn:start

Nachdem die Verbindung mit dem VPN-Client hergestellt ist, verbinden Sie das Laufwerk manuell, wie auf Seite 56 beschrieben.

Zugang über einen Remotedesktop-Server

Als zweite Möglichkeit können Sie auch unseren Remotedesktop-Server GWD-WinTS1.top.gwdg.de verwenden. Wenn Sie sich auf dem Server mit Ihrer GWDG-Benutzerkennung anmelden, wird automatisch Ihr persönliches Laufwerk verbunden. Bei Bedarf können Sie weitere Laufwerke zusätzlich einbinden.

Wie Sie sich auf einem Remotedesktop-Server anmelden, wird im Kapitel „Eine Remotedesktop-Verbindung (RDP) zu einem Server herstellen“ auf Seite 12 beschrieben.

Gemeinsames Laufwerk verwalten

Der gemeinsame Speicherbereich kann mit einer formlosen E-Mail an support@gwdg.de angefordert werden. Für die Regelung der Zugriffsrechte werden AD-Gruppen erstellt, die von den zuständigen Administratoren verwaltet werden. Eine detaillierte Beschreibung finden Sie im Abschnitt **Verwaltung von Benutzergruppen in der Instituts Umgebung** auf Seite 15.

Für die Beantragung des gemeinsamen Speicherbereiches sollten Sie zunächst einmal abschätzen, wie viel Speicherplatz benötigt wird und wer darauf zugreifen soll. Üblicherweise wird der Speicherplatz für gemeinsame Speicherbereiche nicht eingeschränkt bzw. quotiert. Benutzern, die sich in der Domäne **GWDG** anmelden, kann eine automatische Verbindung mit dem Laufwerk per Gruppenrichtlinie eingerichtet werden.

Weitere Informationen

Support-Schnittstelle

Allgemeine Fragen können Sie unter dem folgenden Link unter der Kategorie „Allgemeine Anfrage“ an uns richten: <https://www.gwdg.de/de/support>

SUPPORT

Wählen Sie ein Themengebiet, um mit dem Erstellen einer Anfrage fortzufahren.







 Speicherdienste Backup, Date- und Stagedienste wie GWDG ownCloud, GWDG Cloud Share, GWDG CrashPlan PRDe sowie Archivierungsdienste	 E-Mail & Kollaboration E-Mail-, Management- und Team-Dienste wie Exchange und SharePoint	 Allgemeine Dienste Drucken, Software- und Lizenzverwaltung, Identity Management und Kurse
 Anwendungsdienste High Performance Computing, Persistent Identifier, Umfragen und allgemeine Anfragen zu Software	 Serverdienste Hosting & Housing, virtuelle Server, Webhosting und GWDG Cloud Server	 Netzwerkdienste IP-Adressmanagement, eduroam, Active Directory und LDAP
Allgemeine Anfrage Wählen Sie dies aus, wenn Sie bei der Auswahl eines Themengebietes unsicher sind.		

Abbildung 38 Supportschnittstelle

TeamViewer

Diese Software ermöglicht ein erweitertes Support-Angebot, um einem Benutzer bei einem Problem mit seiner Arbeitsstation zu helfen. GWDG-Mitarbeiter können sich über diese Software in die bestehende Sitzung am Rechner einwählen und so den Hilfesuchenden unterstützen.

Die Verwendung von TeamViewer ist sehr einfach, am effektivsten ist die Nutzung bei einem gleichzeitigen Telefonat mit dem entsprechenden Mitarbeiter:

1. Über die Webseite <http://www.gwdg.de/qs> wählen Sie Ihr Betriebssystem aus und klicken auf das entsprechende Logo.

- Die angebotene Datei laden Sie herunter oder führen sie ggf. gleich aus.



Abbildung 39 Fernsteuerung über Teamviewer I

- Per Telefon teilen Sie dem GWDG-Mitarbeiter die Zahlen unter „Ihre ID“ mit.



Abbildung 40 Fernsteuerung über Teamviewer II

- Der GWDG-Mitarbeiter wählt sich mit dieser ID in Ihre Sitzung ein. Er sieht dann Ihren kompletten Desktop und kann per Maus und Tastatur Befehle an Ihren Rechner abgeben. Sie können dabei immer sehen, was der Support-Mitarbeiter gerade macht.

Falls keine Möglichkeit besteht zu telefonieren, kann die ID auch per E-Mail übermittelt werden. Die TeamViewer-Software verfügt über ein Chat-System, so dass Sie sich auch per Chat mit dem Support-Mitarbeiter verständigen können. Sie können die Verbindung jederzeit beenden.

Kurse

Die GWDG bietet diverse Kurse aus dem IT-Bereich der EDV an. Die benötigten Informationen finden Sie hier:

- <https://www.gwdg.de/de/web/guest/allgemeine-dienste/kurse>

Teilnahmebedingungen

Unsere Kurse richten sich an Mitarbeiter der Universität Göttingen und der Max-Planck-Gesellschaft sowie weiterer wissenschaftlicher Einrichtungen aus dem erweiterten Benutzerkreis der GWDG. Informationen über Teilnahmebedingungen, Anmeldung und Kursprogramm erhalten Sie auf unseren Webseiten unter:

- https://info.gwdg.de/dokuwiki/doku.php?id=de:services:general_services:courses:terms

Leihrechner

Die GWDG verwaltet einen Pool von Rechnern, die von den Instituten ausgeliehen werden können, falls, beispielsweise nach einem Hardwaredefekt, ein Ersatzrechner benötigt wird.

Ein Leihrechner ist so konfiguriert, dass er sofort im Active Directory eingesetzt werden kann:

- Der Rechner ist Mitglied im Active Directory.
- Der Rechner ist mit Software im Umfang eines Standard-Windows-Arbeitsplatzrechners ausgestattet.

Im Institut muss nur noch die vorhandene Peripherie (Bildschirm, Tastatur, Maus und Drucker) angeschlossen und die Internetadresse (IP-Adresse) eingestellt werden. Wenn der Benutzer des Leihrechners bereits Teilnehmer des Active Directory ist, kann er sofort weiterarbeiten. Auch seine E-Mails kann er gleich wieder bearbeiten, sofern er seine E-Mails mit MS Outlook über den Exchange-Server der GWDG abgewickelt oder als E-Mail-Umgebung einen Webbrowser verwendet hat.

Unsere öffentlichen Rechner

GWDG-Benutzerraum

Die GWDG bietet am Faßberg allen Nutzern öffentliche Arbeitsplätze, die zu den GWDG-Öffnungszeiten, werktags von 7:00 bis 21:00 Uhr und an den Wochenenden von 10:00 bis 18:00 Uhr, genutzt werden können. Dort finden Sie kompetente Beratung sowie ein umfangreiches Angebot an Betriebssystemen, Software und Peripheriegeräten.

ANHANG

Checkliste

Neuen Rechner im Active Directory einrichten

1. Migration in das AD (siehe Seite 24)
2. AD-spezifische Konfigurationen am PC (siehe Seite 29)
3. Installation und Verwaltung von Sophos Anti-Virus (siehe Seite 35)
4. Bei Bedarf: Migration der Benutzerumgebung (siehe Seite 41)

Gemeinsamen Speicherbereich nutzen

1. Gemeinsamen Speicherbereich über support@gwdg.de anfordern
2. Gruppen erstellen
3. Mitarbeiter den Gruppen zuordnen

Glossar

Account, Konto, Benutzerkonto, Benutzer-Account

Um Ressourcen wie Rechner oder Drucker im Active Directory nutzen zu können, benötigt man eine Zugangsberechtigung. Diese besteht aus **Userid, Passwort** und **Account-Nummer**. Je nach Aufgaben im System hat dieser Account bestimmte Rechte; unterschieden werden zum Beispiel Benutzer-Accounts und Administrator-Accounts.

Active Directory (AD)

Die Computer, Server, Drucker und Benutzerkonten der Universität Göttingen und der Max-Planck-Institute werden in einem großen Netzwerk zusammengefasst. Das Active Directory von Microsoft ist ein Verzeichnisdienst, mit dem diese Struktur abgebildet und verwaltet werden kann. Das AD wird zentral von der GWDG und dezentral von den Institutsadministratoren verwaltet.

Administrator, Administrator-Account, Administratorkennung, Administratorkonto

Ein Administrator verwaltet Computersysteme und sorgt für einen reibungslosen Funktionsablauf. Das Administratorkonto nimmt eine privilegierte Rolle im System ein, es ist mit umfangreicheren Benutzerrechten ausgestattet. Mit einem Administrator-Account kann man in der Regel auf alle Daten und Funktionen eines Systems zugreifen. In größeren Systemen wie dem AD sind Administrator-Accounts zusätzlich gestaffelt. (Siehe **Institutsadministrator, Domänenadministrator**)

Administratorgruppe

Die Administratorgruppe ist eine im AD angelegte Benutzergruppe. Einem Computer, der Mitglied im AD ist, sollte diese Gruppe der lokalen Gruppe der Administratoren hinzugefügt werden. Dies ermöglicht ein schnelles Einrichten von administrativen Rechten für das System.

Anti-Viren-Programm, Virenschanner, Virenschutz

Ein Anti-Viren-Programm ist eine Software, die auf einem Computer bekannte Computerviren, -würmer oder Trojaner aufspürt, blockiert oder beseitigt. Die Universität Göttingen und die Max-Planck-Institute haben eine Lizenz für das Programm „Sophos Endpoint Security and Control“, die sowohl Mitarbeiter als auch Studierende einschließt. Sophos kann über die Sophos Enterprise Console verteilt und gesteuert werden.

Benutzer, Benutzer-Account, Benutzerkennung, Benutzerkonto

Siehe **Account**.

Benutzerprofil

Siehe **Profil**.

Benutzerrechte

Siehe **Rechte**.

Container

Ein Objekt innerhalb des AD, welches andere Objekte enthalten kann.

Datei-Server

Siehe **File-Server**.

Delegation

Unter Delegation ist die Zuweisung von administrativen Rechten an spezielle Nutzer für bestimmte Aufgaben, wie z. B. die Teilverwaltung einer Domäne, zu verstehen.

DHCP-Server

Ein DHCP-Server (Dynamic Host Configuration Protocol) verwaltet einen festgelegten Bereich von IP-Adressen eines Netzwerkes. Wenn in diesem Bereich ein Rechner einen „DHCP-Request“ startet, also eine IP-Adresse anfordert, teilt der DHCP-Server ihm eine freie Adresse zu.

Domain-Name-Server, DNS, Name-Server

Ein Domain-Name-Server beantwortet Anfragen zur Namensauflösung. Das heißt, er gibt auf Anfrage zu einem Hostname die dazugehörige IP-Adresse aus und umgekehrt.

Domäne

Eine Domäne ist ein in sich abgeschlossener Verwaltungsbereich im AD. In diesem Konstrukt werden z. B. Computer und Benutzerkonten gemeinsam und zentral verwaltet und können so gemeinsame Ressourcen verwenden.

Domänenadministrator

Ein Domänenadministrator hat administrative Rechte in einer gesamten AD-Domäne.

Druck-Server, Print-Server

Ein Druck-Server verwaltet netzwerkfähige Drucker, wie z. B. die Institutsdrucker, und verteilt bei Bedarf die notwendigen Treiber an die Klienten.

Eigene Dateien

Siehe **persönliches Laufwerk**.

E-Mail-Adresse, E-Mail-Postfach

Ein Benutzer erhält mit seinem GWDG-Account ein E-Mail-Postfach für eine E-Mail-Adresse der Form [userid@gwdg.de](mailto:user@gwdg.de).

E-Mail-Programm

Wir empfehlen die Nutzung von Microsoft Outlook in Verbindung mit dem GWDG-Account, denn nur mit Outlook entfaltet sich der volle Funktionsumfang. Alternativ kann auch über einen Browser der Web-Zugang email.gwdg.de genutzt werden.

E-Mail-Server

Ein E-Mail-Server versendet und empfängt E-Mails, die er seinen Nutzern in Postfächern zur Verfügung stellt.

Exchange, Exchange-Server

Der Exchange-Server stellt neben den E-Mail-Funktionalitäten auch weitere Groupware-Funktionalitäten bereit, die am besten in Verbindung mit Outlook funktionieren.

File-Server, Datei-Server

Ein File-Server verwaltet Speicherplatz zentral und ermöglicht dadurch eine einheitliche Handhabung von Backup und Restore.

Gemeinsames Laufwerk, gemeinsamer Speicherbereich, W-Laufwerk

Für Institute, Abteilungen und Arbeitsbereiche können gemeinsame Speicherbereiche eingerichtet werden. Dies ermöglicht ein kollaboratives Arbeiten. Die Zugriffsrechte werden von den Institutsadministratoren gesteuert.

GÖNET

Das GÖNET ist ursprünglich das Universitätsnetz der Universität Göttingen gewesen und ist durch den Anschluss der Max-Planck-Gesellschaft, der SUB, der HAWK (Hochschule für angewandte Wissenschaft und Kunst), des deutschen Primatenzentrums und weiterer Forschungseinrichtungen zum Wissenschaftsnetz angewachsen. Die GWDG betreibt das GÖNET und sorgt für eine Anbindung an das deutsche Wissenschaftsnetz X-WiN und an das Internet.

Gruppenrichtlinie, GPO, Group Policy Object, Richtlinie

Ein Gruppenrichtlinienobjekt ist eine Sammlung von Konfigurationen, die mit einer OU verknüpft wird und damit auf die in der OU enthaltenen Systeme wirkt. In einer GPO können Einstellungen für die Firewall, Sicherheitseinstellungen, Remote-Einstellungen oder auch die Installation von Software-Paketen vorgenommen werden. Gruppenrichtlinien werden in der Regel nur von GWDG-Mitarbeitern bearbeitet.

IdM (Identity Management)

Das IdM gleicht Nutzerdaten wie Userid und Passwort in den verschiedenen Benutzerkatalogen (LDAP und Active Directory) der GWDG ab.

Institutsadministrator, Lokaler Administrator

Ein Institutsadministrator ist zuständig für die IT-Infrastruktur in seinem Institut. Er überwacht und verwaltet innerhalb des AD eine oder mehrere OUs mit Hilfe der Administrationskonsolen.

Internet-Parameter

Für eine reibungslos laufende Internet-Verbindung müssen bestimmte Internet-Parameter in den TCP/IP-Einstellungen an den Systemen vorgenommen werden: Es müssen die IP-Adresse, die Subnetz-Maske, das Standard-Gateway, die DNS-Server und die WINS-Server angegeben werden.

IP-Adresse, Internet-Adresse

Eine IP-Adresse ist eine Adresse in Computernetzen, die, wie z. B. das Internet, auf dem Internet-Protokoll (IP) basieren. Sie wird Geräten zugewiesen, welche an das Netz angebunden werden und macht die Geräte so adressierbar und damit erreichbar. Die IP-Adresse kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Umgekehrt können einem Computer auch mehrere IP-Adressen zugeordnet werden.

IPAM

Im **IP-Adress-Management-System** der GWDG verwalten Netzwerkbeauftragte IP-Adressen für ihre Institute.

Kennwort

Siehe **Passwort**.

Konto

Siehe **Account**, Konto, Benutzerkonto, Benutzer-Account.

LDAP

Ein Benutzerkatalog, der die Anmeldungen im UNIX-Cluster, den Parallelrechnern sowie dem WLAN überwacht.

Lokaler Administrator

Siehe **IdM (Identity Management)**

Das IdM gleicht Nutzerdaten wie Userid und Passwort in den verschiedenen Benutzerkatalogen (LDAP und Active Directory) der GWDG ab.

Institutsadministrator, Lokaler Administrator.

Lokales Profil

Siehe **Profil, Benutzerprofil**.

Migration eines Computers

Als „Migration eines Computers“ verstehen wir die Integration eines Computers in das Active Directory der GWDG.

Name-Server

Siehe **Domain-Name-Server**.

Netzwerkbeauftragter

Jedes Institut hat einen ernannten Netzwerkbeauftragten. Dieser verwaltet die **IP-Adressen** des Institutes im IPAM.

Netzwerkmaske

Siehe **Subnetz-Maske**.

Objekt

Das Active Directory ist ein objektbasiertes Verzeichnissystem. Objekte können Attribute haben; beispielsweise ist ein Benutzerkonto ein Objekt, das einen Namen als Attribut besitzt.

Organisationseinheit, Organizational Unit (OU)

Gehört zu den Containerobjekten. Das besondere Merkmal einer OU ist die Möglichkeit, Richtlinien (GPO) an sie zu binden.

Passwort

Ein ideales Passwort ist sicher und dabei noch leicht zu merken. Insbesondere für administrative Konten ist es ratsam, das Passwort öfter zu wechseln. Ein Passwort in unserem AD muss mindestens zehn Zeichen lang sein und den Komplexitätsregeln von Seite 10 entsprechen. Ein Beispiel für ein gutes, leicht zu behaltendes Kennwort könnte z. B. aus folgendem Satz hergeleitet sein: „Ich habe zwei Katzen, Susi und Peter.“ Es würde dann lauten: „Ih2K,Su&Pe“.

Persönliches Laufwerk, persönlicher Speicherbereich, P-Laufwerk, P:, Eigene Dateien

Mit einem GWDG-Account sind nicht nur die Zugangsberechtigung zur Anmeldung an AD-Rechnern und ein E-Mail-Konto verbunden, sondern auch ein persönlicher Speicherbereich für eigene Dateien. Dieser Bereich wird an einem AD-Rechner in der Regel unter dem Laufwerksbuchstaben **P:** verbunden und ist standardmäßig 100 GB groß. Unter Windows-Betriebssystemen wird das Netzlaufwerk auch mit dem Systemordner **Eigene Dateien** verknüpft.

Print-Server

Siehe **Druck-Server**.

P-Laufwerk

Siehe **Persönliches Laufwerk**, persönlicher Speicherbereich, P-Laufwerk, P:, Eigene Dateien.

Profil, Benutzerprofil

Viele persönliche Einstellungen, die ein Nutzer auf einem Windows-Betriebssystem vornimmt, werden in einem Benutzerprofil gespeichert. Dazu gehören z. B. Programmeinstellungen wie z. B. E-Mail oder auch die Einrichtung des Desktops. Das Profil liegt lokal auf dem Arbeitsrechner. Bei Anmeldung am Active Directory erhält ein Nutzer mit GWDG-Account ein servergespeichertes Profil.

Rechte, Benutzerrechte, Zugriffsrechte

Einem Benutzer-Account werden bestimmte Rechte erteilt. Diese steuern auf welche Ressourcen der Nutzer Zugriff hat.

Remotedesktop-Server (früher: Windows-Terminalserver)

Ein Remote Desktop Server stellt Anwendungen zur Verfügung, die sonst auf den einzelnen Arbeitsstationen installiert und aktualisiert werden müssten.

Richtlinie

Siehe **Gruppenrichtlinie**, GPO, Group Policy Object, Richtlinie.

SAN, Storage Area Network

Das SAN ist ein Massenspeicher, welcher nicht mehr über Bussysteme direkt an einzelne Rechner (Server) angeschlossen ist, sondern mit vernetzten seriellen Leitungen hoher Bandbreite (Glasfasertechnik) mit dem Netz verbunden ist.

Server

Ein Server ist ein Computer in einem Netzwerk, der anderen Benutzern und Computern auf Anfrage Dienste zur Verfügung stellt. Meist sind die Aufgaben sehr speziell, so dass es für verschiedene Aufgaben verschiedene Server gibt, z. B. E-Mail-Server, DNS-Server, WINS-Server usw.

Servergespeichertes Profil

Ein servergespeichertes Profil liegt zentral auf einem Server und wird bei Anmeldung mit einem GWDG-Account an einem Rechner geladen. Bei der Abmeldung werden Änderungen zurückgespeichert. Somit können Einstellungen von einem Rechner zum anderen „mitgenommen“ werden.

Single Sign-on

Im Active Directory reicht eine einzige Benutzerkennung und eine einmalige Anmeldung aus, um alle Ressourcen nutzen zu können, auf die man Zugriff hat.

Sophos

Sowohl die Max-Planck-Gesellschaft als auch die Universität Göttingen haben das Anti-Viren-Programm der Firma Sophos lizenziert, das alle Mitarbeiter und Studierende nutzen dürfen.

Storage Area Network

Siehe **SAN**, Storage Area Network.

Standard-Gateway

Das Standard-Gateway ist das Verbindungselement eines Rechners „nach draußen“, also ins Internet. Die IP-Adresse des Standard-Gateways muss in den Internetparameter-Einstellungen

angegeben werden. Üblicherweise stimmen die ersten drei Zahlen der IP-Adresse überein und als letzte Zahl wird die 254 verwendet (z. B. 134.76.6.254).

Subnetzmaske, Netzwerkmaske

Die Subnetz-Maske ist eine Bitmaske, die im Netzwerkprotokoll den Geräteteil vom Netzwerkteil der IP-Adresse trennt. Die Netzmasken aller an einem IP-Netz beteiligten Rechner sollten somit gleich konfiguriert sein.

Windows-Nameserver, WINS

Der WINS sorgt in Windows-Netzwerken für die Namensauflösung und muss daher in den Internetparameter-Einstellungen angegeben werden. Im Unterschied zum DNS werden vom WINS die NetBios-Namen der Rechner in IP-Adressen übersetzt und umgekehrt.

WINS

Siehe **Windows-Nameserver**.

W-Laufwerk

Siehe

Gemeinsames Laufwerk, gemeinsamer Speicherbereich, W-Laufwerk.

Virenschanner, Virenschutz

Siehe **Anti-Viren-Programm**, Virenschanner, Virenschutz.

WSUS, Windows Server Update Services

Ein Windows-Server, der regelmäßig wichtige Sicherheits-Patches vom Microsoft-Update-Server holt und für Windows-Systeme zum automatischen Update bereitstellt.



Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen