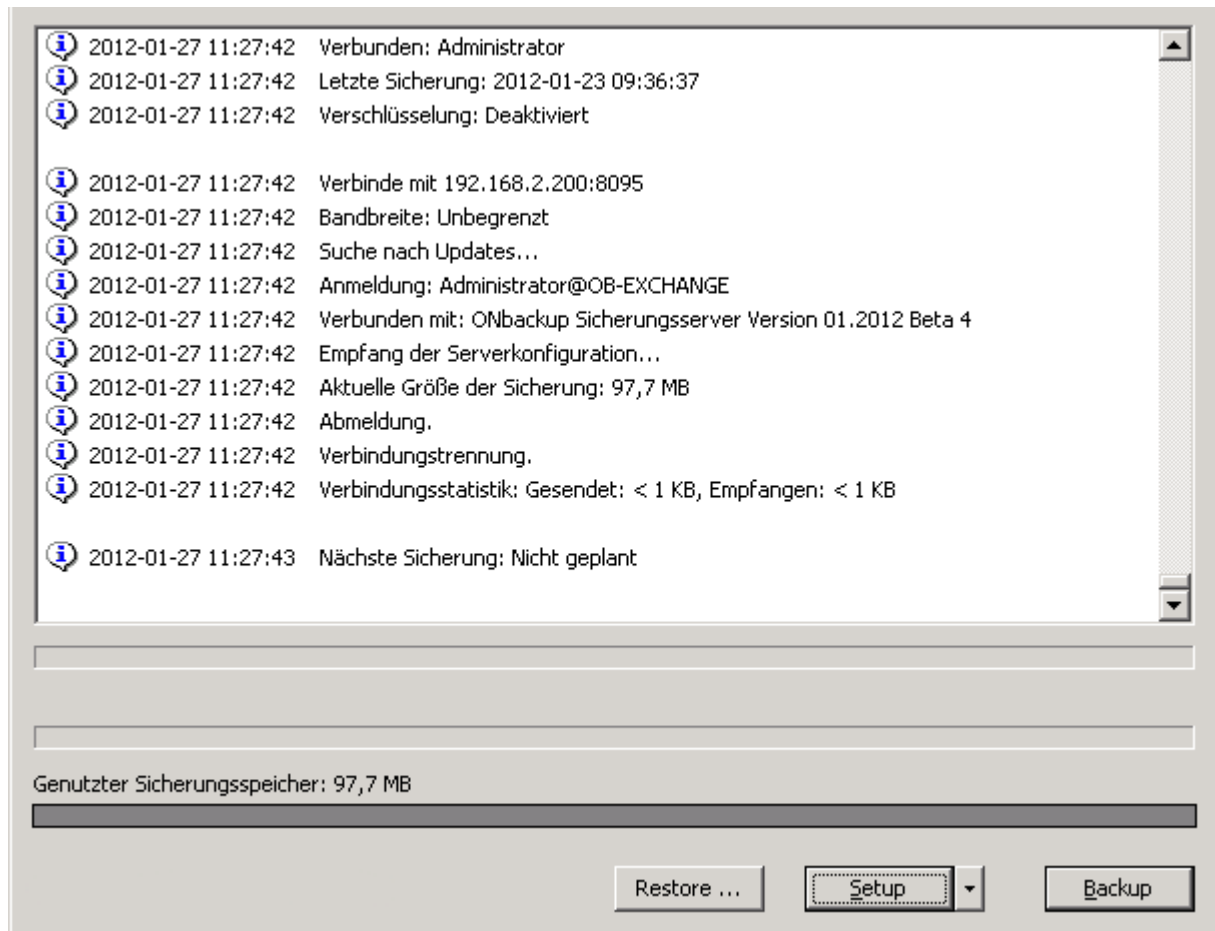


Bedienungsanleitung



Stand: 27.01.2012

Vorbemerkung

Diese Anleitung bezieht sich sowohl auf den Standard- als auch auf den ISP-Client. Einige Funktion, die in dieser Anleitung beschrieben werden, gibt es daher unter Umständen in dem von Ihnen verwendeten Programm nicht.

Inhalt

Vorbemerkung	II
1. Einführung	1
2. Die Installation	2
3. Konfiguration.....	3
3.1. Sicherung von geöffneten Dateien.....	3
3.2. Automatische Wiederholung der Sicherung.....	3
3.3. Standard- und Premium-Modus	3
3.3.1. Netzwerkpfade sichern	3
3.4. Verbindungseinstellungen.....	4
3.5. Benutzeranmeldung und Updates.....	4
3.5.1. Wann verwende ich den Benutzer- und wann den Maschinenmodus?.....	4
3.5.2. Sicherung nach Abmeldung	5
3.5.3. Updates	5
3.6. Start des Clients.....	5
3.7. Weitere Einstellungen	6
3.8. Sicherungsverzeichnisse	6
3.8.1. Netzlaufwerke und Freigaben.....	8
3.9. Netzwerk.....	9
3.10. Sicherungseinstellungen	9
3.10.1. Was bewirken die Aufbewahrungszeiten?	11
3.10.2. Lokaler Sicherungspfad.....	11
3.11. Zeitplanung	11
3.12. Wachdienste	12
3.13. Exchange Sicherung	14
4. Die Client-Oberfläche.....	15
4.1. Verfügbarer Speicher für Sicherungen.....	15
5. Erweiterte Funktionen	16
5.1. Serverkonfiguration laden	16
5.2. Kennwort ändern.....	16
5.3. Server Storage verwalten.....	17
5.4. Server Storage zurücksetzen.....	17
5.5. Update Client Software	18
5.6. Protokoll löschen.....	18
5.7. Vom Dienst trennen	18
6. Sonderfunktionen.....	19
6.1. Kommandozeilen Parameter (Automatisierung)	19
6.2. Anlegen einer Desktop-Verknüpfung	19
6.3. Initialsicherung	19
6.4. Dienste Scriptgesteuert beenden und starten	20
7. Wiederherstellen – Die Restore-Funktion	21
7.1. Lokale Wiederherstellung(für einen schnellen Restore).....	22
7.2. Exchange Wiederherstellung	23
8. OpenSSL Lizenzbedingungen	24

1. Einführung

Der Client ist darauf ausgelegt mit möglichst wenigen Eingriffen durch den Anwender einen höchstmöglichen Datensicherungserfolg zu erzielen. Zu diesem Zweck bietet der Client neben den Buttons „Backup“, „Setup“ und „Restore“, keine weiteren Funktionen an. Die folgenden Kapitel erläutern die Einstellungen und sollen Ihnen helfen, den Client auf den zu sichernden Computern einzurichten.

2. Die Installation

Die Installation ist denkbar einfach. Im ersten Schritt muss die Lizenz akzeptiert werden. Danach muss der Benutzername, für welchen der Client installiert werden soll, angegeben werden. Anschließend wird der Zielpfad verlangt. Standardmäßig ist dieser das Windows Programme-Verzeichnis. Der nächste Schritt führt auch schon die Installation durch. Der Client wird als Systemdienst installiert.

Nach der Installation startet der Client automatisch. Wie sie nun weiter vorgehen erfahren sie in Kapitel 3.

3. Konfiguration

Sofern sich der Client automatisch nach der Installation gestartet hat, befinden Sie sich nun in den Einstellungen der Software. Einige der Konfigurationseinstellungen können ggf. inaktiv und grau sein, wenn der angemeldete Benutzer keine Schreibrechte für diese Einstellungen besitzt. Speziell unter Windows Vista ist eine Anmeldung bzw. Ausführung der Anwendung als „Administrator“ notwendig, um diese Einstellungen ändern zu können. Das Schild-Symbol weist zusätzlich nochmal darauf hin.

3.1. Sicherung von geöffneten Dateien

Über die Funktion der so genannten „Schattenkopien“ oder auch „Shadowcopy“ ist der Client in der Lage geöffnete Dateien zu sichern. Sollten sie zum Beispiel gerade an einer Word Datei arbeiten, so wird das Dokument durch eine Sicherung des Clients ebenfalls mit dem zuletzt gespeicherten Status auf dem Server gesichert, obwohl die Datei geöffnet ist und Sie daran arbeiten.

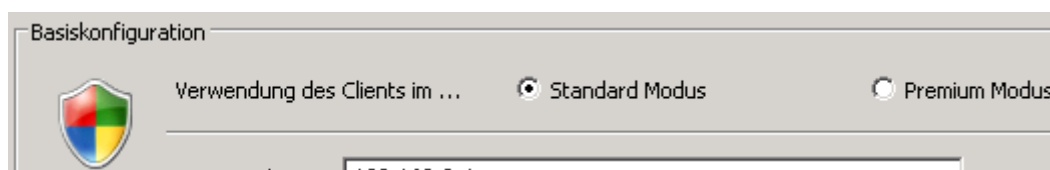
Die Schattenkopien sind ferner ein sehr nützliches Feature für Datenbanken und andere Systeme, auf die dauerhaft zugegriffen wird, da sie auf diese Weise trotzdem in die Sicherung einbezogen werden.

3.2. Automatische Wiederholung der Sicherung

Kommt es während einer Sicherung zu einer Verbindungstrennung, so versucht der Client 15 Minuten lang (alle 60 Sekunden) den Server erneut zu erreichen.

Gelingt dies nicht, so wird die Sicherung endgültig abgebrochen. Wird der Server wieder erreicht, so wird die zuvor begonnene Sicherung fortgesetzt. Standardmäßig sind zwei Wiederholungen für die Sicherung eingestellt, so dass maximal 3 (1 + 2) Sicherungen durchgeführt werden.

3.3. Standard- und Premium-Modus



Geben Sie an, ob der Client im Standard- oder im Premium-Modus ausgeführt werden soll. Im Premium-Modus stehen zusätzliche Funktionen zur Verfügung, die im Standard-Modus nicht enthalten sind. Zur Ausführung des Clients im Premium-Modus benötigen Sie eine entsprechende Serverlizenz auf dem Sicherungsserver. Ein späterer Wechsel zwischen vom Standard- zum Premium-Modus ist nur möglich, wenn zuvor am Sicherungsserver die Lizenz von „Standard“ auf „Premium“ gewechselt wurde. Der Vorteil des Premium-Modus im Einzelnen:

3.3.1. Netzwerkpfade sichern

Im Standard Modus haben Sie die Möglichkeit einen Netzwerkpfad zu sichern. Das bedeutet Sie können über das Netzwerk freigegebene Ressourcen zur Sicherung angeben - z.B. „\\Arbeitsrechner\Dokumente“.

Mit der Option „Premium-Modus“ haben Sie die Möglichkeit bis zu 5 Netzwerkpfade zu sichern. Wie Sie diese Pfade genau sichern, wird in Kapitel 3.5 beschrieben.

3.4. Verbindungseinstellungen



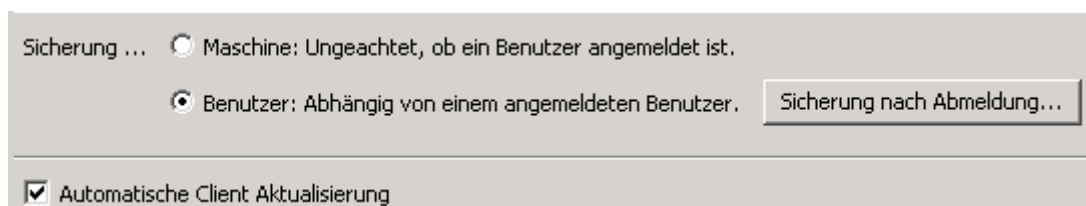
Zunächst muss die IP-Adresse oder der DNS-Name des Sicherungsservers angegeben bzw. geändert werden. Ferner ist hier auch der Server-Port anzugeben. Diese Einstellungen sind nötig, damit der Client mit dem Server kommunizieren kann.

Bei der Port-Eingabe kann auch entschieden werden über welche Verbindungsart auf den Server zugegriffen werden soll. Es besteht die Wahl zwischen SSL- und normalen TCP-Verbindungen (beim ISP-Client ist SSL obligatorisch). SSL ist ein Verschlüsselungssystem. Es verschlüsselt die gesamte Kommunikation zwischen Client und Server – Ihre Dateien werden auf dem Sicherungsserver dadurch aber nicht verschlüsselt. Die Verwendung von SSL-Verbindungen wird dringend empfohlen, wenn der Server über das Internet kontaktiert wird und kein VPN-Tunnel oder andere Sicherungsmechanismen verwendet werden.

SSL-Verbindungen bieten desweiteren den Vorteil, dass der Server über ein Zertifikat identifiziert werden kann. Der Client prüft dieses Zertifikat dann bei jedem Verbindungsaufbau und stellt auf diese Weise sicher, dass der Server auch wirklich der von Ihnen einstellte Server ist. Mit dieser Überprüfung stellen Sie sicher, dass Sie nicht ein Opfer von Datendiebstahl durch sogenannte „Man-In-The-Middle“-Attacken werden. Diese Option sollten Sie unbedingt aktivieren, wenn der Sicherungsserver über entsprechendes Zertifikat verfügt.

3.5. Benutzeranmeldung und Updates

Über die Optionen in der Mitte des Tabs „Verbindung“ können Sie die Art der Benutzeranmeldung, sowie das Update-Verhalten einstellen:



3.5.1. Wann verwende ich den Benutzer- und wann den Maschinenmodus?

Wenn Sie den Computer unabhängig von einem angemeldeten Benutzer sichern möchten (z.B. bei der Sicherung von Servern), wählen Sie bitte den Sicherungsmodus „**Maschine**“.

Der Vorteil des Maschinenmodus ist vor allem, dass hier eine völlig autarke Sicherung möglich ist. Selbst bei Ausfällen oder Fehlern in der Sicherung und daraus

folgenden Abbrüchen, versucht der Client immer wieder auf ein Neues zum Server zu verbinden und seine Sicherung durchzuführen.

Damit der Dienst im Maschinenmodus auch eventuelle Netzwerkfreigaben sichern kann, muss dafür gesorgt werden, dass der Dienst des Clients in einem Benutzerkontext läuft, der auch die Berechtigung hat auf die Freigaben zuzugreifen. Beim Standard-Client erfolgt die Anmeldung am Sicherungsserver in diesem Fall mit dem Anmeldenamen „[any]@Computername“.

Wenn Sie die Sicherung in Abhängigkeit von einem jeweils angemeldeten Benutzer durchführen möchten, so wählen Sie bitte die Option „**Benutzer**“.

Für jeden Benutzer dieses Computers wird dann ein eigenes Sicherungskonto auf dem Sicherungsserver verwaltet (Nur Standard-Client).

Auf diese Weise können die Sicherungen der Benutzer vollständig getrennt verwaltet und eingerichtet werden. Ferner bietet diese Option auch die Möglichkeit, durch Windows verschlüsselte Dateien der Benutzer zu sichern, was im Maschinenmodus nicht möglich ist.

Im Benutzermodus trennt sich der Dienst von dem GUI wenn der Server einmal nicht erreichbar war. Diese Funktionalität ist in den Benutzermodus eingebaut worden, damit der Client nicht permanent versucht den Server zu erreichen, wenn dieser gar nicht erreichbar sein kann (z.B. wenn man mit dem Notebook unterwegs ist). Mit Hilfe einer zeitgesteuerten Sicherung, kann man dieses Verhalten beeinflussen, wenn man allerdings in jedem Fall möchte, dass der Client seine Sicherung bei Problemen erneut aufnimmt, sollte man den Maschinenmodus einstellen.

Beim Standard-Client erfolgt die Anmeldung am Sicherungsserver dann mit dem Anmeldenamen „Benutzername@Computername“.

Bitte beachten: Die Einstellungen für den Benutzer- und den Maschinenmodus werden getrennt gespeichert. D.h. wenn Sie den Modus wechseln, müssen Sie auch Ihre gegebenenfalls zuvor bereits gemachten Einstellungen neu konfigurieren.

3.5.2. Sicherung nach Abmeldung

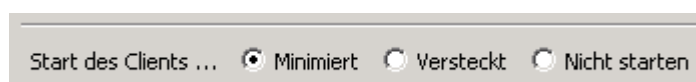
Über die Schaltfläche „Sicherung nach Abmeldung...“ können Sie einen Assistenten aufrufen. Diese hilft Ihnen dabei, ein Skript zu erstellen, welches dafür sorgt, dass bei jeder Abmeldung eines Benutzers automatisch eine Datensicherung durchgeführt wird.

3.5.3. Updates

Wenn Sie bei der automatischen Client-Aktualisierung einen Haken setzen, so prüft der Client mit jedem Verbindungsaufbau auf verfügbare Updates. Steht ein Update für den Client zur Verfügung, so wird dieses automatisch heruntergeladen und installiert. Den Verlauf des Updates können Sie anhand der Balloon-Tipps über der Uhr in der Taskleiste verfolgen.

3.6. Start des Clients

Im unteren Bereich des Tabs können Sie entscheiden wie sich der Client beim Systemstart verhalten soll.



Sie haben die Wahl zwischen:

- Minimiert: Die Client Oberfläche erscheint nicht, der Client startet und verschwindet im Bereich neben der Uhr
- Versteckt: Die Client GUI startet versteckt, weder die Oberfläche noch das Zeichen neben der Uhr erscheinen. Backups werden allerdings, soweit geplant, durchgeführt. Dies ist hilfreich wenn Sie eine Sicherung des PCs wünschen, der Benutzer dies aber nicht sehen soll.
- Nicht starten: Verhindert den Start des Clients allgemein. Der Systemdienst läuft im Hintergrund aber weiter. Sie können also nun zu einem beliebigen Zeitpunkt die Anwendung selbst starten. Eine automatisierte benutzerabhängige Sicherung (Benutzermodus) ist dann nicht möglich.

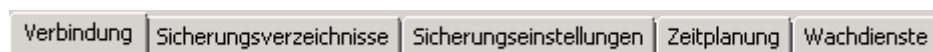
3.7. Weitere Einstellungen

Am unteren Rand des Tabs, können Sie noch einige Einstellungen zur vereinfachten Anmeldung, sowie ggf. Sicherheitseinstellungen treffen.



Über das Feld „Anmelde Einstellungen...“ (nur ISP-Client) können Sie Ihren Benutzernamen und das Kennwort abspeichern und müssen es so nicht jedes Mal eingeben. Außerdem können Sie die „Kryptographie Einstellungen...“ abspeichern und sparen sich damit das ständige Eingeben. Nur bei Sonderfunktionen (z.B. beim Restore) werden die Anmelde- und Sicherheitseinstellungen erneut abgefragt. Über das Feld „Einstellungen bearbeiten“ haben Sie die Möglichkeit, den Client mit einem anderen Benutzerkonto bzw. mit administrativen Rechten zu starten, damit Sie die Grundeinstellungen verändern können.

Sollte der Sicherungsserver Ihnen erlauben erweiterte eigene Einstellungen vorzunehmen, erhalten Sie zusätzliche „Reiter“ mit zusätzlichen Einstellungen am oberen Fensterrand (nur Standard-Client).



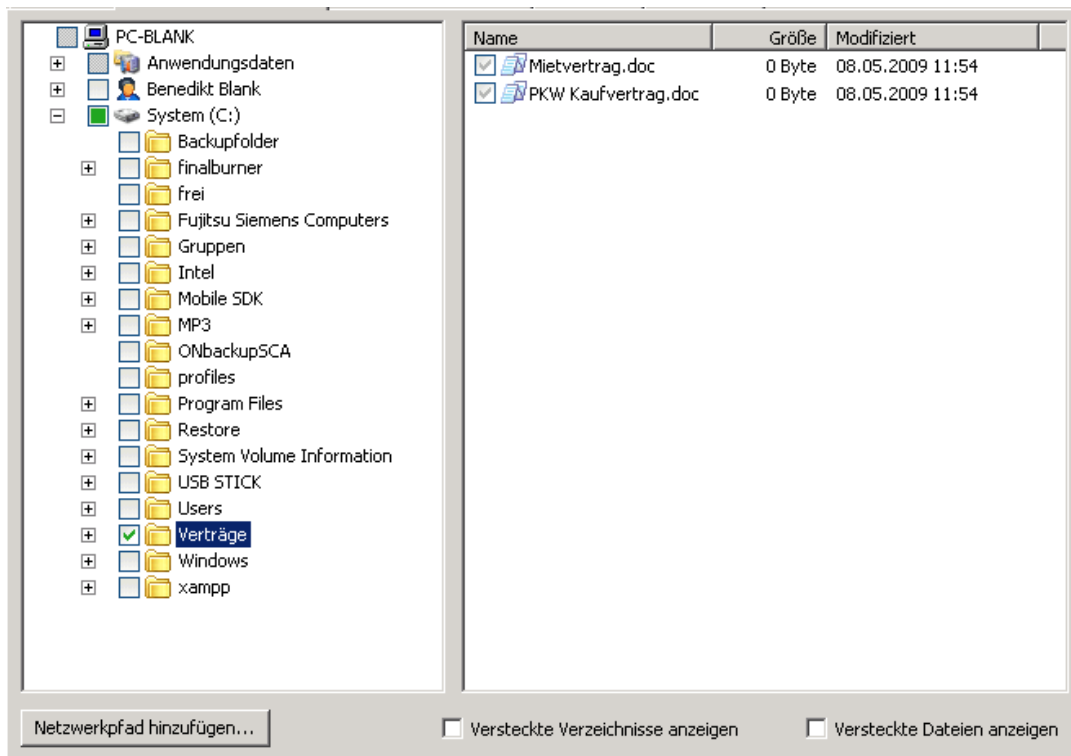
Die Funktionen der Reiter werden in den nächsten Kapiteln besprochen.

3.8. Sicherungsverzeichnisse

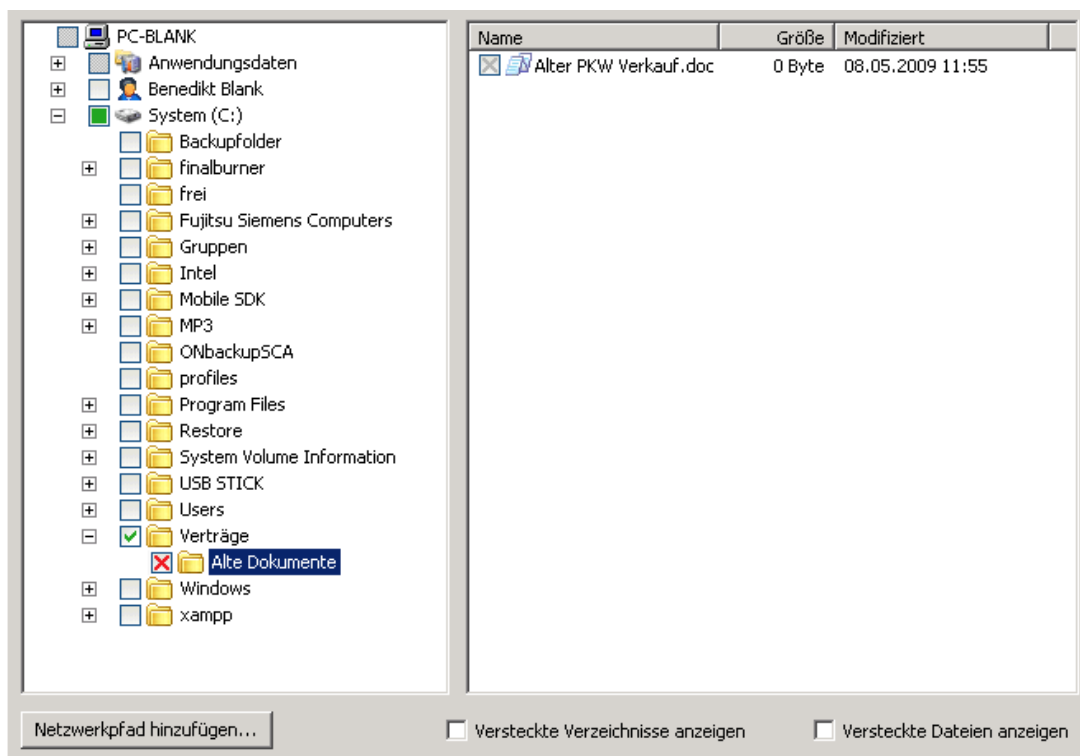
Bei dem Reiter „Sicherungsverzeichnisse“ handelt es sich um das eigentliche „Herzstück“ des Clients. Hier wird festgelegt, welche Ordner und Dateien gesichert und auf den Sicherungsserver übertragen werden sollen.

Zur Sicherung eines bestimmten Ordners – beispielsweise „C:\Verträge“ - gehen Sie wie folgt vor:

Öffnen Sie im linken Bereich das Laufwerk „C:“ indem Sie auf das kleine ‚+‘-Zeichen klicken. Nun sehen Sie alle Ordner, die sich auf der ersten Ebene von Laufwerk „C:“ befinden. Dort findet sich auch direkt der gesuchte Ordner „Verträge“. Mit einem Klick in die kleine Box neben dem Ordernamen, fügen Sie den Ordner Ihren zu sichernden Dateien hinzu. Ein grüner Haken zeigt die Auswahl des Ordners, mit allen seinen Unterverzeichnissen und Dateien an. Mit einem Klick auf „OK“ wird der Ordner endgültig in Ihren Sicherungssatz übernommen.



Sie haben auch die Möglichkeit, Unterverzeichnisse oder Dateien in einem ausgewählten Verzeichnis von der Sicherung auszuschließen. Gehen Sie dazu bitte wie folgt vor:



Navigieren Sie zum Ordner „Verträge“ und klicken auf das kleine ‚+‘Zeichen neben dem Ordernamen. Sie sehen nun alle in „Verträge“ enthaltenen Unterordner. Der Ordner „Alte Dokumente“ hat, im Gegensatz zu „Verträge“ einen grauen Haken neben dem Ordernamen. Dies zeigt an, dass der Ordner zu einer auf einer höheren Ebene gehörenden Auswahl gehört. Um den Ordner nun aus dem Sicherungssatz auszuschließen, klicken Sie auf diesen grauen Haken. Dieser wird nun zu einem roten Kreuz. Dies bedeutet, dass dieser Pfad zukünftig nicht mehr gesichert wird. Der Ordner „Verträge“ behält das grüne Kreuz und wird weiter gesichert – nun aber ohne den darin enthaltenen Ordner „Alte Dokumente“.

Um einen Ordner zu sichern, der sich nicht auf Ihrem Computer befindet, klicken Sie auf den Button „Netzwerkpfad hinzufügen...“. Geben Sie nun den Netzwerkpfad (Computer- und Freigabenamen) an, der in Ihrem Verzeichnisbaum aufgenommen werden soll und bestätigen Sie dies mit einem Klick auf „OK“.

3.8.1. Netzlaufwerke und Freigaben

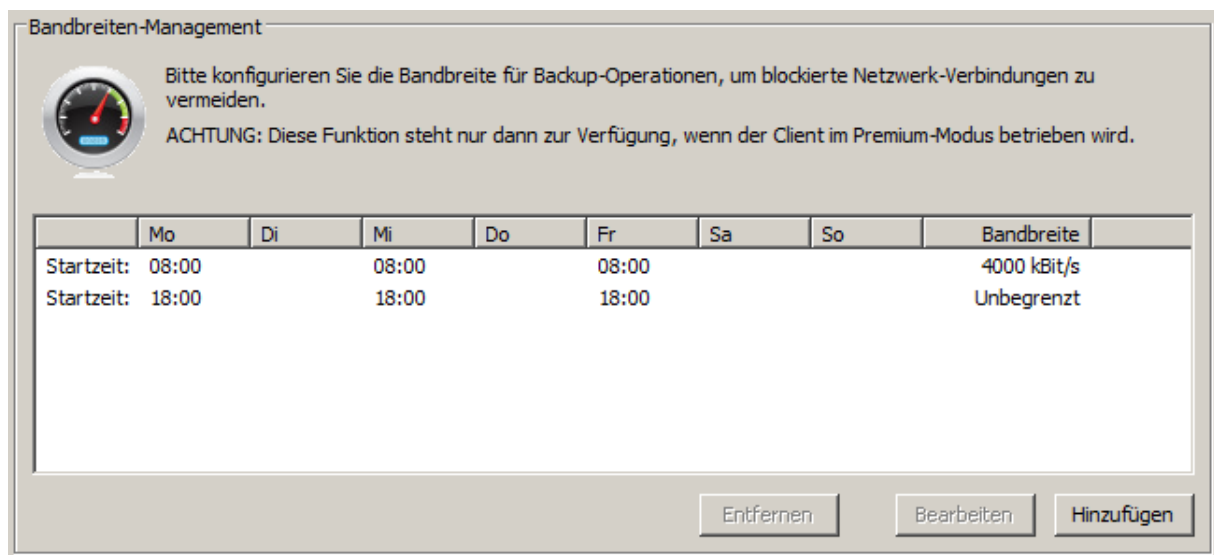
Sollten Sie eine Freigabe auf einem Netzlaufwerk sichern wollen, müssen Sie immer den gesamten UNC-Pfad angeben und nicht den Laufwerksbuchstaben des Netzlaufwerks.

Ein Beispiel: „X:\Freigabe“ muss gesichert werden als „\\PCNAME\Freigabe“

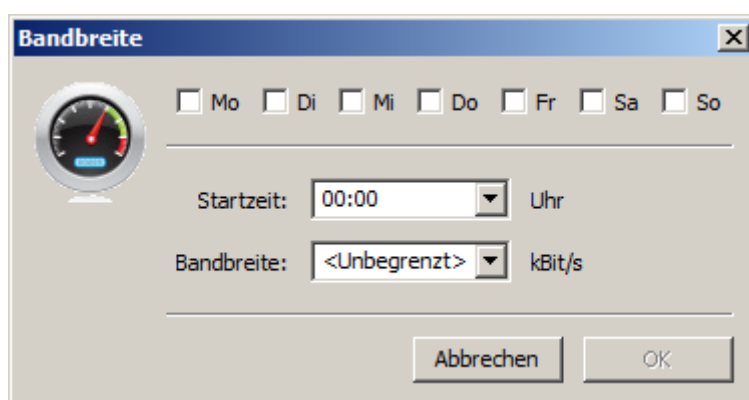
3.9. Netzwerk

Im Reiter „Netzwerk“ können Sie festlegen, dass der Client zu bestimmten Tageszeiten nicht die volle Bandbreite nutzen soll. Bitte beachten: Die Funktionalität steht **nur im Premium-Modus** zu Verfügung.

Diese Funktionalität ist z.B. dann nützlich, wenn Sie für eine große Sicherung durch eine relativ schmale Internetleitung eine sehr lange Zeit die Leitung beanspruchen. So können Sie z.B. tagsüber die Bandbreite die der Client beansprucht drosseln und können so trotzdem noch relativ problemlos das Internet benutzen, da dieses in dieser Zeit nicht komplett durch den Upload der Sicherung blockiert wird. Denkbar wäre also eine Drosselung zu den typischen Geschäftszeiten eines Betriebs.



Durch einen Klick auf „Hinzufügen“ gelangen Sie in ein neues Fenster, welches es ermöglicht die Bandbreite ab einer bestimmten Startzeit zu konfigurieren.

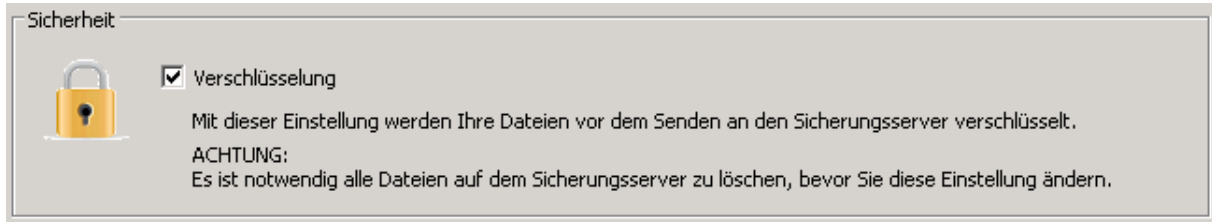


Haken Sie einfach die Tage an, an denen die Drosselung erfolgen soll. Bestimmen sie anschließend noch eine Startzeit und eine maximal Bandbreite und fügen Sie die Drosselung mit Klick auf „Ok“ dem Terminplan hinzu.

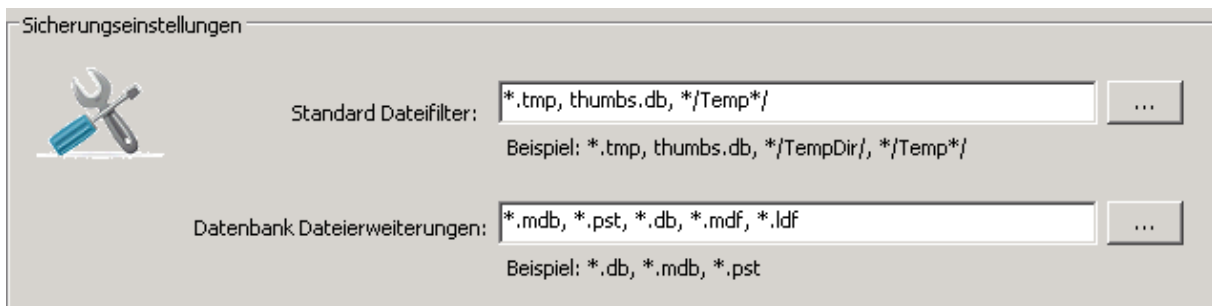
3.10. Sicherungseinstellungen

Im Reiter „Sicherungseinstellungen“ können Sie festlegen, ob Ihre Dateien vor der Übertragung auf den Sicherungsserver verschlüsselt werden sollen (nur Standard

Client). Damit haben Sie Gewissheit, dass unbefugte Personen keinen Zugriff auf Ihre Daten erlangen. Beim ISP-Client werden Ihre Dateien immer verschlüsselt – die Option ist daher immer ausgewählt und kann nicht deaktiviert werden.



Weiter unten können Sie im Feld „Standard-Filter“ Filter für Dateien angeben, die Sie niemals sichern möchten. Dabei können ganze Ordner, nur bestimmte Dateierweiterungen oder einzelne Dateien von der Sicherung ausgeschlossen werden.

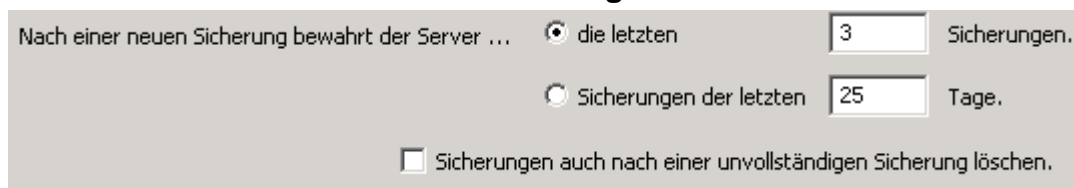


Geben Sie dazu die Namen der nicht zu sichernden Dateien, wie im Beispiel gezeigt, an.

- *.tmp : Alle Dateien mit der Endung „.tmp“ nicht sichern
- Thumbs.db : Alle Dateien mit dem Namen „Thumbs.db“ nicht sichern
- */Temp*/ : Alle Verzeichnisse, die mit Namen „Temp“ beginnen nicht sichern

Über die Filter „Datenbank-Dateierweiterungen“ haben Sie die Möglichkeit, einen schnelleren Datenabgleich für Datenbank-Dateien zu erzielen. Wenn Sie sicher sind, dass es sich bei den angegebenen Dateitypen um Datenbank-Dateien (z.B. von MS-Outlook, MS-Access, usw.) handelt, so können Sie die entsprechende Dateierweiterung hier angeben.

3.10.1. Was bewirken die Aufbewahrungszeiten?



Nach einer neuen Sicherung bewahrt der Server ... die letzten Sicherungen.
 Sicherungen der letzten Tage.
 Sicherungen auch nach einer unvollständigen Sicherung löschen.

Die letzte Einstellung die Sie hier vornehmen können, ist die Dauer für die Sie Ihre Sicherungen auf dem Server belassen wollen.

Ein Beispiel: Sie sichern regelmäßig Ihren Ordner „Eigene Dateien“. Die Dateien ändern sich laufend. Auf dem Sicherungsserver werden geänderte und / oder gelöschte Dateien aber weiterhin aufbewahrt. Das heißt, Sie können nicht nur die Dateien der letzten Sicherung wiederherstellen, sondern auch die Dateien von früheren Sicherungen. Nicht geänderte Dateien werden auf dem Sicherungsserver nur einmalig abgelegt, um Speicherplatz zu sparen.

Hier können Sie nun einstellen, wie lange Sie die alten Sicherungen behalten wollen. Bedenken Sie dabei bitte, dass Ihr Sicherungskonto vielleicht nicht unendlich groß werden darf, da der Speicherplatz in der Regel begrenzt ist. Die Voreinstellung sieht vor, dass Dateien der letzten 3 Sicherungen aufbewahrt werden, also 3 Dateiversionen. Wenn Sie allerdings jeden Tag eine Sicherung durchführen und gerne die Dateiversionen einer ganzen Woche zur Verfügung haben möchten, müssten Sie „die letzten ... Sicherungen“ auf „7“ einstellen.

Sollten Sie stattdessen mehrmals an einem Tag Sicherungen durchführen und trotzdem am Ende der Woche auf Dateiversionen von allen Sicherungen Zugriff haben wollen, empfiehlt sich stattdessen die Option „Sicherungen der letzten ... Tage“ auf „7“ einzustellen und diese auszuwählen.

Die Option „Sicherungen auch nach einer unvollständigen Sicherung löschen“ empfiehlt sich vor allem dann, wenn bei einem System bekannt ist, dass die Sicherung z.B. aufgrund von nicht zu sichernden Dateien niemals erfolgreich verläuft aber nichts desto trotz komplett ist.

3.10.2. Lokaler Sicherungspfad




Lokaler Sicherungspfad:

Wenn hier ein Pfad konfiguriert wird, werden die Dateien nach jeder Online-Sicherung im angegebenen Verzeichnis aktualisiert. Es wird jeweils nur eine Dateiversion aufbewahrt.

3.11. Zeitplanung

Im Reiter „Zeitplanung“ können Sie eine Uhrzeit bestimmen zu der eine Sicherung durchgeführt werden soll. Außerdem können Sie festlegen, an welchen Tagen (um diese Uhrzeit) gesichert werden soll.

Zeitplanung



Client sollte Server alle Minuten kontaktieren.

Erzwinge Sicherung um Uhr ...

Mo Di Mi Do Fr Sa So

Erzwinge Sicherung Stunden nach der letzten Sicherung.

Im Beispiel wird an allen Wochentagen jeweils um 14:55 gesichert.


Zusätzlich zu den Sicherungszeiten können Sie auch bestimmen, in welchen Intervallen nach der letzten Sicherung unbedingt eine erneute Sicherung erfolgen soll. Dies geht mit einem Wert im Feld „Erzwinge Sicherung“.

3.12. Wachdienste

Im Reiter „Wachdienste“ können Sie einen SMTP-Server angeben, über den Sie dann zu bestimmten, wählbaren Ereignissen, E-Mails erhalten. Der Sicherungsserver sendet Ihnen in der Regel bereits mit jeder Operation (z.B. einer Sicherung) ein Protokoll. Wenn Sie zusätzliche Informationen wünschen, können Sie auch den Client veranlassen, Ihnen (z.B. im Fall von Sicherungsfehlern) ein Protokoll zuzusenden.

Die Felder erklären sich quasi von selber. Im obersten Feld geben Sie die Server Adresse, darunter dann den Port, sowie die optionalen Anmeldedaten ein. Zum Schluss wählen Sie noch eine E-Mail Adresse aus, von der der Client die E-Mails verschicken soll, sowie eine E-Mail Adresse an die die E-Mails verschickt werden sollen. In den meisten Fällen wäre dies Ihre persönliche E-Mail Adresse. Nähere Informationen zu Ihrem SMTP-Server erhalten Sie von Ihrem Administrator bzw. von Ihrem Internet-Service-Provider.

E-Mail Einstellungen



SMTP-Server:

SMTP-Port:

SMTP-Login:

SMTP-Kennwort:

Absender E-Mail Adresse:

Empfänger E-Mail Adressen:

Mit dem Button „Test“ können Sie ausprobieren, ob alle Einstellungen stimmen und ob Ihnen eine E-Mail zugestellt wird.

In der Mitte des Reiters bestimmen Sie nun noch in welchen Fällen ein Bericht gesendet werden soll.

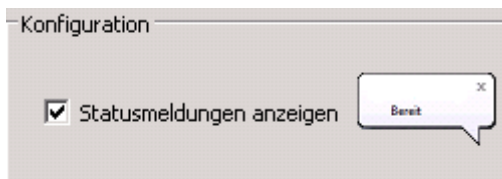


Bericht senden: Im Fall von Warnungen

Sie haben hier die Wahl zwischen:

- Niemals: Damit ist der Wachdienst deaktiviert
- Im Fall von Warnungen (z.B., dass die Prüfung des Zertifikats deaktiviert ist)
- Im Fall von Fehlern (z.B., dass der Server nicht erreichbar war)
- Immer: Damit erhalten Sie in sämtlichen denkbaren Fällen eine E-Mail.

Am unteren Rand des Reiters bestimmen Sie, ob die Status-Meldungen über der System-Uhr angezeigt werden sollen oder nicht.



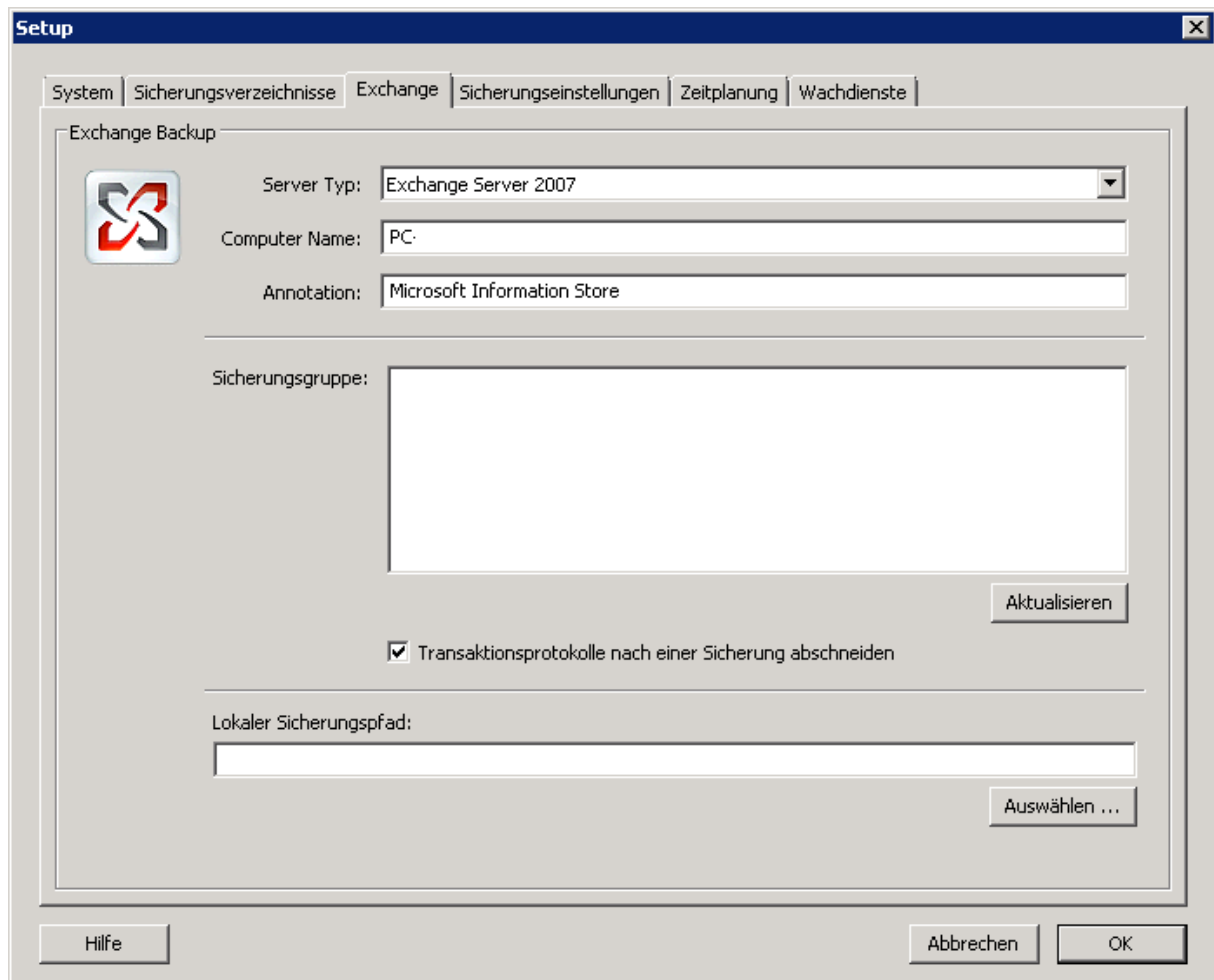
Konfiguration

Statusmeldungen anzeigen

Bericht

3.13. Exchange Sicherung

Wenn der Sicherungsserver es Ihnen erlaubt, haben Sie die Möglichkeit Exchange-Server zu sichern. Die Sicherung erfolgt anhand der Storage-Groups im Server.



Konfigurieren Sie im Reiter „Exchange“ nun die Sicherung Ihres Exchange-Servers, der auf diesem Computer ausgeführt wird. Weitere Informationen zur Konfiguration von Exchange entnehmen Sie bitte den Konfigurationsanleitungen Ihres Exchange-Servers.

Sobald die Sicherung dann später gestartet wird, erstellt der Client eine lokale Sicherung der ausgewählten Sicherungsgruppen, bevor diese dann an den Sicherungsserver übertragen werden. Diese lokalen Sicherungen bleiben auch nach der Übertragung an den Sicherungsserver erhalten und dienen somit als erste und schnelle Zugriffsmöglichkeit Ihren Exchange Server im Falle eines Totalausfalls wiederherzustellen. Desweiteren wird auf diese Weise die Sicherungszeit für Ihren Exchange-Server minimiert und das gesamte System somit entlastet.

Beachten Sie bitte, dass die lokale Sicherung Ihrer Exchange-Sicherungsgruppen erheblichen Speicherplatz benötigt, da eine 1:1 Kopie angelegt wird. Es wird empfohlen, die lokale Sicherung auf eine andere Maschine oder ein Storage-System im Netzwerk auszulagern.

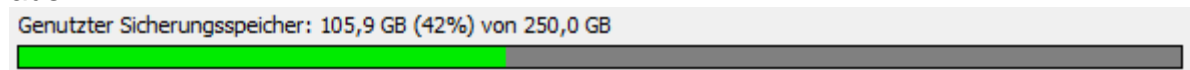
Sicherungen von „Exchange Server 2010“ erfolgen einfach über das Dateisystem. Sie wählen die Exchange 2010 Verzeichnisse über den Reiter „Sicherungsverzeichnisse“ aus. Diese werden dann auf dem herkömmlichen Weg gesichert. *Beim Exchange 2010 gibt es keine lokale Sicherung.* Während des anschließenden Backups werden die Logs die der Exchange 2010 nicht mehr braucht entfernt. Logs die noch benötigt werden, verbleiben im Logverzeichnis bis diese vom Exchange verarbeitet wurden.

4. Die Client-Oberfläche

Bei der Gestaltung des Sicherungsclients wurde darauf geachtet, dass die Bedienung leicht von der Hand geht. Der Startbildschirm des Clients gestaltet sich daher aufgeräumt und beinahe selbsterklärend. An dieser Stelle des Handbuchs gibt es Erklärungen zu den Punkten, die vielleicht nicht auf den ersten Blick ersichtlich sind.

4.1. Verfügbarer Speicher für Sicherungen

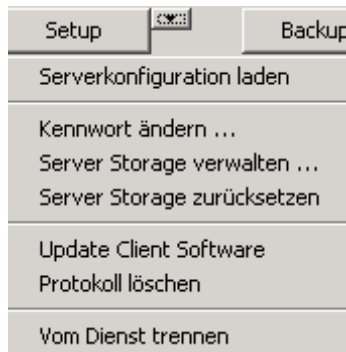
Am unteren Rand des Sicherungsclients sehen Sie eine Anzeige, die Auskunft gibt über die momentane Auslastung Ihres Sicherungskontos. Die Anzeige sieht z.B. so aus:



Die Anzeige zeigt als Prozentsatz und Prozentwert an, wie viel Speicherplatz auf dem Sicherungsserver durch den Client-Benutzer bereits belegt worden ist. In der Abbildung sind 42% von 250 GB belegt, was 105,9 GB entspricht.

5. Erweiterte Funktionen

Über den Pfeil rechts neben dem „Setup“-Button können Sie einige Sonderfunktionen auswählen, die im Folgenden beschrieben werden.

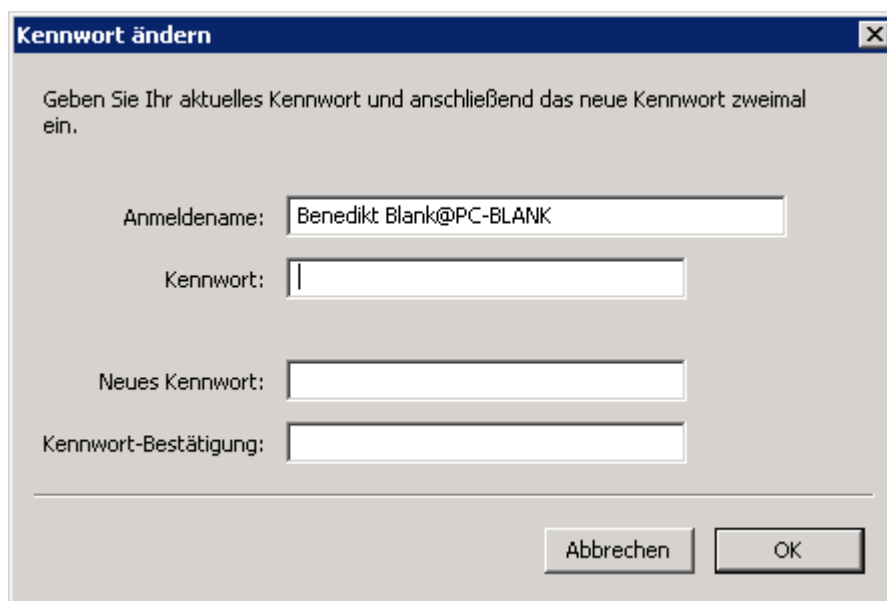


5.1. Serverkonfiguration laden

Es werden die aktuell für Ihr Benutzerkonto auf dem Server gemachten Einstellungen geladen. Unter anderem fällt darunter, wie viele Einstellungsmöglichkeiten Sie im Setup Menü (Kapitel 3) haben oder welche Pfade gesichert werden sollen, insofern Sie das nicht selber bestimmen dürfen (nur für Standard-Client).

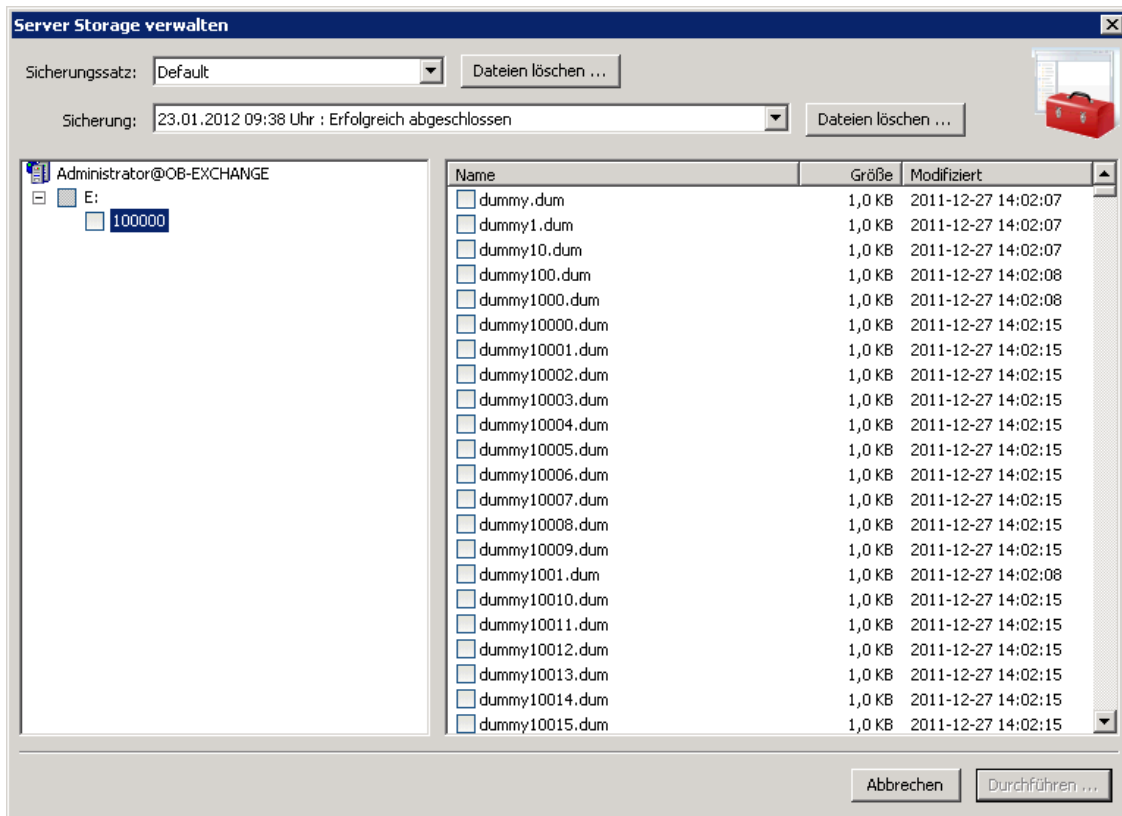
5.2. Kennwort ändern

Um sich am Sicherungsserver anzumelden ist ggf. ein Kennwort notwendig. Aus Sicherheitsgründen sollte ein Kennwort regelmäßig geändert werden. Dazu müssen der Benutzername sowie das zugehörige aktuelle Kennwort eingegeben werden. Wenn Sie noch kein Kennwort haben, lassen Sie das obere Feld (Kennwort) einfach leer. Das neue zukünftige Kennwort muss dann zur Sicherheit doppelt eingegeben werden. Nach erfolgreicher Änderung des Kennwortes wird dieses dann am Sicherungsserver sofort aktiv.

A screenshot of a dialog box titled 'Kennwort ändern'. The dialog contains the following text and fields: 'Geben Sie Ihr aktuelles Kennwort und anschließend das neue Kennwort zweimal ein.' followed by four input fields: 'Anmeldename:' with the value 'Benedikt Blank@PC-BLANK', 'Kennwort:' (empty), 'Neues Kennwort:' (empty), and 'Kennwort-Bestätigung:' (empty). At the bottom right, there are two buttons: 'Abbrechen' and 'OK'.

5.3. Server Storage verwalten

Über die Schaltfläche „Server Storage verwalten“ hat man die Möglichkeit, sich die gesicherten Daten aller Sicherungssätze anzusehen und nach Wunsch zu entfernen. So steht es dem Benutzer frei auch abseits der Aufbewahrungsregeln die im Client definiert sind nicht mehr benötigte Sicherungen zu entfernen.



Über die Schaltfläche „Dateien löschen ...“, neben der Auswahlbox der Sicherungen, werden alle Dateien und Ordner der ausgewählten Sicherung gelöscht. Über die gleichnamige Schaltfläche neben der Auswahlbox des Sicherungssatzes, wird der komplette Sicherungssatz gelöscht.

Einzelne Dateien können nicht zum löschen markiert werden. Der Benutzer kann sich im unteren Bereich des Fensters die in der Sicherung enthaltenen Dateien und Ordner ansehen, gelöscht wird aber immer die gesamte Sicherung bzw. der gesamte Sicherungssatz.

5.4. Server Storage zurücksetzen

Die Option „Server Storage zurücksetzen“ löst die bekannte Schaltfläche „Sicherung löschen“ ab. Mit „Server Storage zurücksetzen“ können alle gesicherten Dateien auf dem Sicherungsserver gelöscht werden. Für diesen Vorgang wird aus Sicherheitsgründen Ihr Kennwort verlangt. Das Löschen aller Dateien auf dem Sicherungsserver ist u.a. notwendig, wenn Sie Ihren Verschlüsselungstext ändern möchten oder die Verschlüsselung ein- bzw. ausschalten wollen.

ACHTUNG:

Sämtliche Sicherungssätze auf dem Server werden dabei gelöscht.

5.5. Update Client Software

Mit dieser Funktion können Sie auf das Vorhandensein einer neuen Client-Software-Version prüfen. Sollte Ihre Version nicht mehr aktuell sein, so erfolgt Installation automatisch und der Client startet neu.

5.6. Protokoll löschen

Diese Option löscht das Protokoll im Client.

5.7. Vom Dienst trennen

Mit der dieser Option, kann die Benutzeroberfläche vom Dienst getrennt werden. Damit meldet sich der Benutzer vom Dienst ab und es können nun solange keine Einstellungen mehr getroffen werden, bis sich der Benutzer wieder mit dem Dienst verbindet.

6. Sonderfunktionen

In diesem Kapitel geht es um einige spezielle Funktionen des Programms.

6.1. Kommandozeilen Parameter (Automatisierung)

Das Client GUI unterstützt folgende Startparameter:

- backup: Die Sicherung wird direkt gestartet und der Client danach direkt wieder beendet.
- delay: Verzögert den Start der Sicherung um zwanzig Sekunden und gibt dem Benutzer somit die Möglichkeit den Start der Sicherung zu verhindern.
- shutdown: Wenn der Client beendet wird, wird auch der Computer nach einer Verzögerung von zwanzig Sekunden heruntergefahren. Zu empfehlen ist diese Funktion in Kombination mit – backup also: „--backup --shutdown“. Somit wird das Backup durchgeführt, der Client beendet und der Computer heruntergefahren.
- hide: Der Client wird gestartet aber ist nicht sichtbar. Sicherungen erfolgen somit unbemerkt vom Benutzer.
- minimize: Der Client startet direkt minimiert. Die Oberfläche zeigt sich beim Start zunächst nicht, kann aber durch das Symbol neben der Uhr in der Taskleiste geöffnet werden.

Hinweis: Diese Parameter in eine Verknüpfung zu legen und zu starten ist nur dann sinnvoll, wenn Sie keinen automatischen Start der Anwendung im Bootvorgang eingestellt haben. (Kapitel 3.3)

6.2. Anlegen einer Desktop-Verknüpfung

Um eine Desktop-Verknüpfung mit einem oder mehreren dieser Parameter zu erstellen, gehen Sie wie folgt vor:

Legen Sie zunächst eine normale Verknüpfung zur Datei „ONbackupSvc.exe“ an. In den Eigenschaften der Verknüpfung können Sie dann die gewünschten Parameter ergänzen.

Beispiel:

```
C:\Programme\backupClientSvcV4\ONbackupSvc.exe --backup --delay --shutdown
```

6.3. Initialsicherung

Unter dem Stichwort „Initialsicherung“ versteht man die Erstsicherung, nachdem der Client auf Ihrem System installiert wurde. Die nun zu sichernde Datenmenge ist am größten, da erst einmal alle Dateien gesichert, d.h. übertragen werden müssen. Spätere Datensicherungen sind meist viel kleiner, da nur wenige neue oder geänderte Dateien hinzugekommen sind.

Falls die Sicherung also über eine sehr schmale Leitung erfolgen muss - wie beispielsweise über ein schwaches WLAN oder eine schmalbandige Internetanbindung – so bietet sich die Möglichkeit der Initialsicherung an. Dies bedeutet, dass die zu sichernden Dateien zunächst auf einen externen Datenträger an Ihrem Computer gespeichert werden und dann - „per Hand“ - in das Sicherungskonto auf dem Sicherungsserver kopiert werden. Sie können die auf diese Weise erstellte Initialsicherung aber auch auf einer DVD oder einem USB-Stick Ihrem Administrator bzw. Dienstleister zukommen lassen. Dadurch wird eine sehr lang andauernde Übertragung vermieden. Stimmen Sie die Vorgehensweise für eine Initialsicherung bitte mit Ihrem Anbieter jeweils ab.

Eine Initialsicherung wird wie folgt durchgeführt:
Halten Sie beim Klicken auf den „Backup“ Button die Shift-Taste gedrückt
Wählen Sie dann ein Verzeichnis, in dem die Dateien der Initialsicherung abgelegt werden sollen. Nach Klick auf „OK“ wird die Initialsicherung durchgeführt und im gewählten Ordner gespeichert.

Bitte beachten:

- Eine Offline-Initialsicherung sollte einer langsamen Erstsicherung über das Internet, die aufgrund von Zwangstrennungen und Bandbreitenschonung über mehrere Tage hingezogen wird, immer vorgezogen werden.
- Damit nach einer Erstsicherung der Restore verwendet werden kann, muss nach einer Offline-Initialsicherung zunächst eine Online-Sicherung gemacht werden, da erst nach der ersten Online-Sicherung der Restore funktionstüchtig ist.

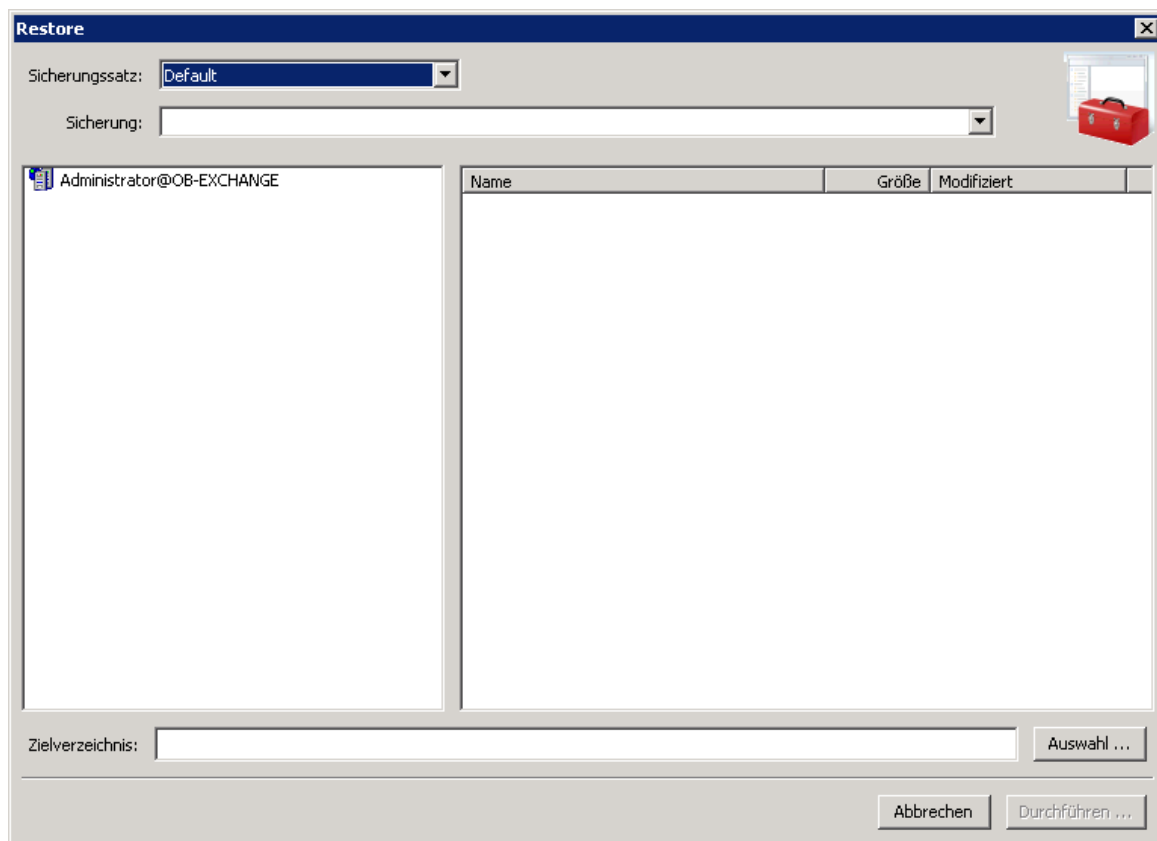
6.4. Dienste Scriptgesteuert beenden und starten

Falls Sie vor einem Backup einen Dienst beenden müssen, damit das Backup auch ordnungsgemäß durchläuft(z.B. Datenbankdienste), können Sie vom Backup-Client vor und nach dem Backup die fraglichen Dienste beenden und wieder starten lassen. Fügen Sie dazu die nötigen Befehle in die Dateien *BackupStarting.cmd* und *BackupFinished.cmd* im Client-Verzeichnis ein. Falls die Dateien noch nicht existieren, müssen diese zunächst angelegt werden.

7. Wiederherstellen – Die Restore-Funktion

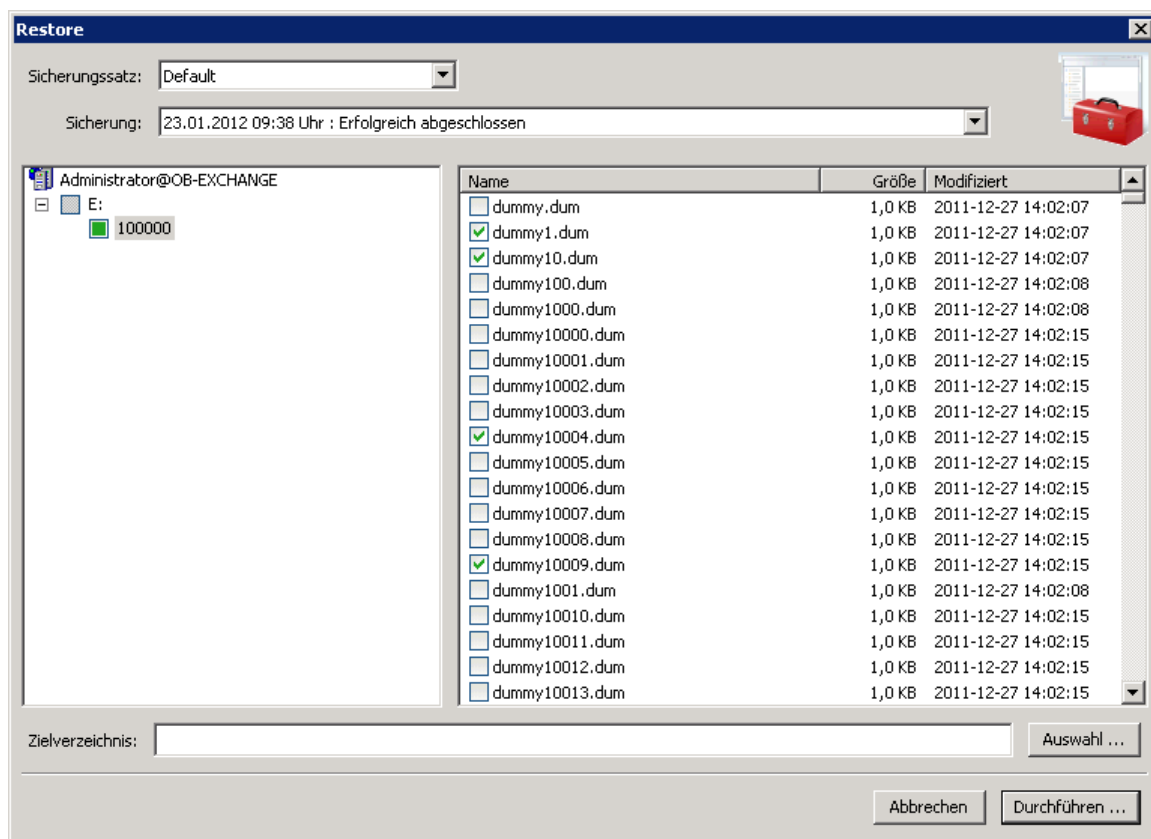
Um Dateien nach einem Datenverlust oder nach einer unerwünschten Änderung wiederherzustellen, verwendet Sie die Schaltfläche „Restore ...“.

Nach Eingabe eines Benutzernamens und des zugehörigen Kennwortes lädt der Client die Sicherungssätze vom Server und öffnet danach das folgende Fenster:



Im oberen Bereich steht die Wahl zwischen einem bestimmten Sicherungssatz (momentan „Default“) und anschließend die Wahl zwischen einer bestimmten Sicherung aus diesem Satz.

Nach Auswahl einer Sicherung, werden auf der linken Seite die darin enthaltenen Pfade in einer, dem Windows-Explorer ähnlichen Darstellung, angezeigt. Wählen Sie nun im linken Bereich einen oder mehrere Ordner und / oder im rechten Bereich einzelne oder mehrere Dateien aus. Mit einem Klick auf das Kästchen wird der Ordner bzw. die Datei zur späteren Wiederherstellung markiert.



Über die Schaltfläche „Auswahl“ hinter dem Eingabefeld „Zielverzeichnis“ kann das Verzeichnis für die Wiederherstellung angegeben werden. Alle wiederhergestellten Dateien werden im angegebenen Ordner abgelegt. Bleibt das Zielverzeichnis leer, so werden die Dateien am ursprünglichen Ort wiederhergestellt.

Mit einem Klick auf den Button „Durchführen ...“ beginnt die Wiederherstellung.

7.1. Lokale Wiederherstellung(für einen schnellen Restore)

Im Falle eines 100 prozentigen Datenverlusts, kann es vorkommen, dass sie sehr viele Daten wiederherstellen müssen. Eine Übertragung, auch über eine recht schnelle Anbindung, würde da eine nicht zu unterschätzende Zeit lang laufen. Aus diesem Grund bietet der Sicherungs-Client zusätzlich die Funktion der lokalen Wiederherstellung.

Sie fordern dazu von ihrem Sicherungs-Konto Anbieter einen Datenträger mit einer Kopie ihres Benutzerkontos an inkl. Ihren verschlüsselten Datensicherungen.

Als nächstes halten Sie beim Klick auf die Schaltfläche „Restore“ die Shift-Taste gedrückt. Ein Fenster öffnet sich, in dem Sie nun den Ordner auswählen müssen, den Sie von Ihrem Anbieter bekommen haben.


Geben Sie anschließend Ihr Passwort sowie Ihre Kryptografie-Phrase an.

Nach kurzer Zeit stellt der Sicherungs-Client nun Ihre verschlüsselte Datensicherung aus dem lokalen Ordner dar, so als würden Sie auf den Sicherungs-Server zugreifen. In gewohnter Manier können Sie nun die Daten, die Sie benötigen, wiederherstellen.

7.2. Exchange Wiederherstellung

Wenn es der Sicherungsserver erlaubt können Sie neben der Konfiguration des Exchange-Backups auch den Exchange-Restore durchführen. Dazu müssen Sie den „ONbackup Exchange Restore Assistent“ aufrufen, der sich in einem Dropdown-Menü neben dem Restore-Button verbirgt.

Im Restore-Assistent können Sie in wenigen Schritten Ihren Exchange-Restore konfigurieren und die Daten in den Exchange-Server einspielen.



The screenshot shows a window titled "ONbackup Exchange Restore Assistent" with a close button in the top right corner. The main area has a logo on the left and the text "Schritt 1: Vorbereitungen" in large bold font. Below this, there are four input fields with labels and buttons:

- Computer Name (ohne Domäne):
- Pfad zur Exchange-Sicherung:
- Pfad für temporäre Dateien:
- Annotation:

At the bottom of the window, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Beachten Sie vor allem auch die Hinweise im ersten Schritt: Bevor man mit dem Restore beginnt, sollte man bei den Datenbanken die man wiederherstellen möchte die Bereitstellung aufheben und in den Spezifikationen der Datenbank die Option „Diese Datenbank kann bei einer Wiederherstellung überschrieben werden“ aktivieren. Anschließend kann man mit den Restore-Vorbereitungen beginnen und den Restore durchführen.

8. OpenSSL Lizenzbedingungen

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

```
/* =====
 * Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 * software must display the following acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For written permission, please contact
 * openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 * nor may "OpenSSL" appear in their names without prior written
 * permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 * acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * =====
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com). This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 */
```

Original SSLeay License

```
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * "This product includes cryptographic software written by
 * Eric Young (eay@cryptsoft.com)"
 * The word 'cryptographic' can be left out if the rouines from the library
 * being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 * the apps directory (application code) you must include an acknowledgement:
 * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed. i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```