Faronics™
Simplifying Computer Management



Deep Freeze

ADVANCED System Integrity

Benutzerhandbuch

Letzte Anderung: Oktober 2019

© 1999 – 2019 Faronics Corporation. Alle Rechte vorbehalten. Faronics, Deep Freeze, Deep Freeze Cloud, Faronics Core Console, Faronics Anti-Executable, Faronics Anti-Virus, Faronics Device Filter, Faronics Data Igloo, Faronics Power Save, Faronics Insight, Faronics System Profiler und WINSelect sind Warenzeichen und/oder eingetragene Warenzeichen der Faronics Corporation. Alle anderen Firmen- und Produktnamen sind Marken ihrer jeweiligen Besitzer.
Durch folgende Patente geschützt: US 7,539,828 | US 7,917,717 | US 9,152,824 | US 9,785,370

Inhalt

Vorwort 9

Wichtige Informationen 10
Informationen zu Faronics 10
Produktdokumentation 10
Technischer Support 11
Kontaktinformationen 11

Einführung 13

Deep Freeze – Übersicht 14
Systemanforderungen 15
Deep Freeze Enterprise-Dateien 16

Deep Freeze installieren 17

Installationsübersicht 18
Deep Freeze Enterprise-Konfigurationsadministrator und Enterprise Console installieren 18
Anpassungscode 21
Erneute Initialisierung mit dem Anpassungscode 21
Update-Modus 21
Einmalige Passwörter 23

Den Deep Freeze Enterprise-Konfigurationsadministrator verwenden 25

Auf den Konfigurationsadministrator zugreifen 26
Symbolleiste und Menüs 26
Registerkarte „Passwörter“ 28
Registerkarte "Laufwerke“ 29
Eingefrorene Laufwerke 29
Auftauplatz 30
Vorhandener Auftauplatz 32
Externe Festplatten immer auftauen 33
Registerkarte "Arbeitsplatzaufgaben" 34
Windows Update 35
Neustart 39
Herunterfahren 40
Inaktivität 41
Stapeldatei 42
Zeitraum im Zustand "aufgetaut" 44
Registerkarte "Windows Update" 48
Registerkarte "Stapeldatei" 51
Registerkarte „Erweiterte Optionen“ 53
Netzwerk 53
Erweiterte Optionen 54
Tarnmodus 57

Lizenz 57
Arbeitsplatzinstallationsprogramm und Arbeitsplatz-Seed erstellen 58

Deep Freeze Enterprise-Konsole verwenden 61

Deep Freeze-Konfiguration 62
Deep Freeze-Konfiguration anwenden 62
Deep Freeze-Konfiguration bearbeiten 63
Deep Freeze-Konfiguration löschen 63
Deep Freeze-Konfiguration exportieren 63
Konfigurationsgenerator 64
Den Konfigurationsgenerator über die Befehlszeile verwenden 65
Parameter der Konfigurationsdatei 65
Deep Freeze Enterprise-Konsole 70
Die Enterprise-Konsole starten 70
Die Enterprise-Konsole aktivieren 70
Statussymbole 71
Spalten anzeigen 73
Statusbasierte Auswahl 74
Die Kommunikation zwischen der Konsole und den Arbeitsplätzen verwalten 75
Den lokalen Dienst konfigurieren 75
Eine Verbindung zu einem lokalen Dienst bearbeiten oder entfernen 77
Die Proxy-Server-Verbindung konfigurieren 77
Remote-Konsolen 79
Für Remote-Steuerung aktivierte Verbindungen einrichten 79
Verbindung zu einer Remote-Konsole herstellen 80
Deep Freeze mit der Konsole verwalten 81
Eine vorgegebene Anzahl von Malen im Zustand „Thawed"/„Thawed und gesperrt" neu starten 82
Nachrichten an Computer senden 82
Eine Deep Freeze-Konfigurationsdatei aktualisieren 83
Windows Update ausführen 83
Remote-Ausführung 84
Pushen und ausführen 85
Auftauplatz formatieren 86
Auftauplatz löschen 86
Die Konsolenprotokolldatei anzeigen 87
Zielinstallation von Deep Freeze 88
Deep Freeze-Software aktualisieren 88
Auftau-Warnmeldungen 89
Lizenzen 90
Manuelle Aktivierung 91
Lizenzsymbol 92
Deep Freeze-Aufgaben terminieren 93
Geplante Aufgaben bearbeiten 97
Computer terminierten Tasks zuordnen 98
Eine Aufgabe hinzufügen 98
Eine Aufgabe bearbeiten 98
Eine Aufgabe anhalten 98
Eine Aufgabe fortsetzen 98

Aufgaben löschen . . . 99
Eine Task sofort ausführen . . . 99
Eigenschaften von terminierten Tasks . . . 99
Netzwerk und Gruppen verwalten . . . 100
Eine Gruppe hinzufügen . . . 100
Eine benutzerdefinierte Gruppenstruktur erstellen . . . 103
Gruppen aus Active Directory importieren . . . 103
Verlauf . . . 104
Computer zu einer Gruppe hinzufügen . . . 105
Benutzerdefinierte Aktionen konfigurieren . . . 106
Kontrolle über RDC . . . 106
Remote-Ausführung . . . 107
MSI-Datei verteilen und installieren . . . 108
Pushen und ausführen . . . 108
Remote-Ausführung . . . 109
Benutzerdefinierte Aktionen löschen, importieren und exportieren . . . 110
Konsolen-Customizer . . . 112
Deep Freeze Enterprise-Konsole herunterfahren . . . 113
Deep Freeze auf dem Arbeitsplatz installieren . . . 114
Überwachte Installation oder Deinstallation . . . 114
Deep Freeze über die Konsole auf dem Arbeitsplatz installieren . . . 116
Stille Installation oder Deinstallation . . . 117
Beispiel Befehlszeile . . . 117
Stille Installation oder Deinstallation über eine Verknüpfung . . . 118
Netzwerkinstallation für mehrere Computer . . . 118
Installation über vorhandene Deep Freeze-Versionen . . . 119
Installation über Imaging . . . 119
Zielinstallation . . . 120
Nach Updates suchen . . . 121

Deep Freeze-Computer verwalten . . . 123

Anmeldebildschirm . . . 124
Deep Freeze auf Touchscreen-Geräten starten . . . 124
Registerkarte Status . . . 125
Status beim nächsten Hochfahren . . . 125
Klonen . . . 125
Lizenz . . . 125
Registerkarte "Passwort" . . . 128
Registerkarte „Netzwerk“ . . . 129
Registerkarte „Auftauplatz“ . . . 130
Dauerhafte Softwareinstallationen, Änderungen oder Entfernungen . . . 131

Anti-Virus verwalten . . . 133

Anti-Virus – Übersicht . . . 134
Migration zum neuen Anti-Virus . . . 135
Anti-Virus auf der Enterprise Console aktivieren . . . 136
Den Anti-Virus Client auf dem Arbeitsplatz installieren . . . 137

Anti-Virus-Konfiguration 138
Anti-Virus-Konfiguration erstellen 138
Anti-Virus-Konfiguration anwenden 156
Anti-Virus-Konfiguration bearbeiten 156
Anti-Virus-Konfiguration löschen 156
Faronics Anti-Virus über die Enterprise Console verwenden 157
Anti-Virus-Befehle 157
Anti-Virus-Aufgaben terminieren 161
Anti-Virus auf dem Arbeitsplatz verwenden 162
Anti-Virus auf dem Arbeitsplatz starten 162
Den Arbeitsplatz durchsuchen 163
Eine Datei bzw. einen Ordner per Rechtsklick durchsuchen 164
Suchverlauf anzeigen 164
In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen 165
Antivirus-Definitionen auf dem Arbeitsplatz aktualisieren 166
Anti-Virus über die Taskleiste auf dem Arbeitsplatz verwalten 167
Nach Anti-Virus-Updates suchen 169
Faronics Anti-Virus aktualisieren 170
Anti-Virus-Definitionen aktualisieren 171
Den Anti-Virus-Client über die Enterprise Console deinstallieren 172
Faronics Anti-Virus über die Enterprise Console deaktivieren 173

Deep Freeze Befehlszeilensteuerung 175

Deep Freeze Befehlszeilensteuerung (DFC.EXE) 176
DFC-Rückgabewerte 176
Deep Freeze Befehlszeilensyntax 177
Befehlszeilensyntax für Faronics Anti-Virus 181

Anhang A Ports und Protokolle 183

Anhang B Netzwerkbeispiele 185

Beispiel 1 – Einzelnes Subnet 186
Beispiel 2 – Mehrere Subnets, ein lokaler Dienst 187
Beispiel 3 – Mehrere Ports, Fernzugriff auf Konsole 188
Beispiel 4 – Mehrere Subnets, mehrere lokale Services 189

Anhang C Fehlerbehebung für eine Verbindung zur Remote-Konsole 191

Keine Clients in der Konsole 191
Fehler 'Port wird verwendet' bei Start der Konsole 192

Anhang D Eine angepasste Deep Freeze Enterprise-Konsole erstellen 193

Anhang E Deep Freeze-Aktionsdateien – RDC-Beispiel 195

Deep Freeze-Aktionsdateien 195
Beispiel für eine Aktionsdatei 195
Struktur von Deep Freeze-Aktionsdateien 196

Konsolenparameter 198



Vorwort

Dieses Benutzerhandbuch beschreibt die Installation, Konfiguration und Verwendung von Deep Freeze Enterprise.

Themen

Wichtige Informationen
Technischer Support

Wichtige Informationen

Dieser Abschnitt enthält wichtige Informationen über Ihr Faronics-Produkt.

Informationen zu Faronics

Faronics liefert marktführende Lösungen, die dabei helfen, komplexe IT-Umgebungen zu verwalten, zu vereinfachen und abzusichern. Unsere Produkte stellen eine hundertprozentige Verfügbarkeit von Maschinen sicher und haben bereits einen dramatischen Einfluss auf das tägliche Leben Tausender von Fachleuten im Informationstechnologiebereich gehabt. Bildungsinstitutionen, Einrichtungen des Gesundheitswesens, Bibliotheken, Regierungsorganisationen und Firmen profitieren von den marktzentrisch fokussierten Technologieinnovationen von Faronics.

Produktdokumentation

Die folgenden Dokumente bilden das Deep Freeze Enterprise Dokumentationspaket für:

- Deep Freeze Enterprise Benutzerhandbuch – Dies ist das Dokument, das Sie gerade lesen. Dieses Dokument hilft Ihnen bei der Verwendung des Produkts.
- Deep Freeze Enterprise Versionshinweise – Dieses Dokument führt die neuen Funktionen sowie bekannte und gelöste Probleme auf.

Technischer Support

Alle Anstrengungen wurden unternommen, um diese Software benutzerfreundlich und problemfrei zu gestalten. Sollten dennoch Probleme auftreten, setzen Sie sich bitte mit unserem technischen Kundendienst in Verbindung.

E-Mail: support@faronics.com

Telefon: +1-800-943-6422 oder +1-604-637-3333

Geschäftsstunden: 07:00 Uhr bis 17:00 Uhr (Pazifische Zeit)

Kontaktinformationen

Web: www.faronics.com

- E-Mail: sales@faronics.com
- Telefon: +1-800-943-6422 oder +1-604-637-3333
- Fax: +1-800-943-6488 oder +1-604-637-8188
- Geschäftsstunden: 07:00 Uhr bis 17:00 Uhr (Pazifische Zeit)
- Adresse:

  Faronics Technologies USA Inc.
  5506 Sunol Blvd, Suite 202
  Pleasanton, CA, 94566 USA

  Faronics Corporation (Headquarters)
  609 Granville Street, Suite 1400
  Vancouver, BC V7Y 1G5
  Canada

  Faronics EMEA
  8, The Courtyard, Eastern Road
  Bracknell, Berkshire
  RG12 2XB, United Kingdom

  Faronics Pte Ltd
  6 Marina Boulevard
  #36-22 The Sail At Marina Bay
  Singapore, 018985



Einführung



Deep Freeze schützt die Computer, die so eingerichtet sind, dass sie von der Festplatte aus hochgefahren werden. Konfigurieren Sie das CMOS so, dass es nur über die Festplatte hochfährt. Das CMOS muss mit einem Passwort geschützt werden, um unbefügte Änderungen zu verhindern. Deep Freeze schützt den Master Boot Record (MBR), wenn sich der Computer im Zustand "eingefroren" befindet.

Themen

Deep Freeze – Übersicht
Systemanforderungen
Deep Freeze Enterprise-Dateien

Deep Freeze – Übersicht

Faronics Deep Freeze hilft dabei, Computerbeschädigungen und Ausfallzeiten zu eliminieren, indem es Computerkonfigurationen unzerstörbar macht. Nachdem Deep Freeze auf einem Computer installiert wurde, sind Änderungen am Computer – ganz gleich, ob sie zufällig oder böswillig vorgenommen werden – niemals dauerhaft. Deep Freeze bietet sofortige Immunität gegen viele Probleme, denen Computer heute ausgesetzt sind: unvermeidliche Konfigurationsänderungen, versehentliche Fehlkonfigurationen des Systems, schädliche Software-Aktivität und beiläufige Systemschwächung.

Faronics Anti-Virus kann jetzt über Deep Freeze Enterprise verwaltet werden (eine separate Lizenz ist für Faronics Anti-Virus erforderlich). Faronics Anti-Virus bietet Schutz vor Sicherheitsbedrohungen, ohne Computer aufgrund langsamer Suchzeiten und erheblichem Platzbedarf zu verlangsamen. Faronics Anti-Virus, das mit Technologie der nächsten Generation erstellt wurde, bietet Ihnen eine leistungsstarke integrierte Antiviren-, Anti-Rootkit- und Anti-Spyware-Software. Diese schützt Sie vor aktuellen komplexen Malware-Bedrohungen und lässt sie sich reibungslos mit Deep Freeze integrieren.

Eine Integration von Deep Freeze mit Faronics Anti-Virus stellt sicher, dass Ihr Schutz so einfach wie möglich auf dem aktuellsten Stand gehalten wird, indem Implementierungs- und Verwaltungsfunktionen über die Deep Freeze Enterprise Console bereitgestellt werden. Die Produkte wurden für eine nahtlose Integration entwickelt, und Faronics Anti-Virus wird auch dann aktualisiert, wenn sich die Arbeitsplätze im Zustand „eingefroren“ befinden, so dass Sie ein umfassendes Schutzsystem erhalten.

Systemanforderungen

- Deep Freeze und Faronics Anti-Virus werden unterstützt auf:
  - Windows 7 (32 und 64-bit)
  - Windows 8.1 (32 und 64-bit)
  - Windows 10 Version 1903 (32 und 64-bit)
  - Windows Server 2008 R2 (32 und 64-bit)
  - Windows Server 2012 (64-bit)
  - Windows Server 2016 (64-bit)
  - Windows Server 2019 (64-bit)
  - Windows Embedded 7 und 8
- Für Deep Freeze müssen 10 % des Festplattenspeichers frei sein
- Der Deep Freeze Enterprise-Konfigurationsadministrator und die Enterprise Console werden unterstützt auf:
  - Windows 7 (32 und 64-bit)
  - Windows 8.1 (32 und 64-bit)
  - Windows 10 Version 1903 (32 und 64-bit)
  - Windows Server 2008 R2 (32 und 64-bit)
  - Windows Server 2012 (64-bit)
  - Windows Server 2016 (64-bit)
  - Windows Server 2019 (64-bit)

Deep Freeze Enterprise-Dateien

Deep Freeze verwendet unterschiedliche farbige Symbole, um seine Komponenten darzustellen. Die durch ein rotes Symbol gekennzeichneten Dateien sollten in der Regel nur auf einem Administratorcomputer installiert werden.

Symbol	Definition
	Deep Freeze Enterprise-Konfigurationsadministrator und Installationsdatei für die Enterprise Console
	Die Anwendung ‚Konfigurationsadministrator' wird verwendet, um benutzerdefinierte, vorkonfigurierte Computerinstallationsprogrammdateien und Arbeitsplatz-Seeds zu erstellen.
	Die Anwendung ‚Enterprise-Konsole' wird verwendet, um Deep Freeze-Installationen zentral zu implementieren, zu überwachen, zu verwalten und zu pflegen.
	Eine maßgeschneiderte Deep Freeze-Installationsdatei für Arbeitsplätze wird im Konfigurationsadministrator erstellt und auf den Arbeitsplätzen im Unternehmen implementiert. Diese Datei enthält den Arbeitsplatz-Seed. Wenn die Deep Freeze-Arbeitsplatzinstallationdatei installiert ist, brauch der Arbeitsplatz-Seed nicht separat installiert zu werden.
	Ein Arbeitsplatz-Seed ermöglicht eine nahtlose Kommunikation zwischen der Enterprise Console und Computer innerhalb eines Netzwerks. Wenn der Arbeitsplatz-Seed auf einem Computer installiert wird, wird der Computer in der Enterprise Console sichtbar. Sobald ein Computer in der Enterprise Console sichtbar ist, können aus der Ferne diverse Aktionen für die Rechner durchgeführt werden: er kann neu gestartet, heruntergefahren oder über Wake-on-LAN aus dem Ruhezustand hochgefahren werden. Deep Freeze kann außerdem aus der Ferne auf sichtbaren Computern installiert werden, so dass Deep Freeze in der Lage ist, verbundene Aktionen auf Remote-Computern durchzuführen.

Deep Freeze installieren

In diesem Kapitel wird der Installationsprozess für Deep Freeze beschrieben.

Themen

Installationsübersicht
Anpassungscode
Einmalige Passwörter

Installationsübersicht

Deep Freeze Enterprise-Konfigurationsadministrator und Enterprise Console installieren

Der Konfigurationsadministrator ist nur für eine Installation auf dem Computer gedacht, der für die Verwaltung von Deep Freeze vorgesehen ist. Der Konfigurationsadministrator wird verwendet, um benutzerdefinierte Deep Freeze-Installationsdateien und Arbeitsplatz-Seeds zu erstellen. Die Deep Freeze Enterprise Console wird automatisch gemeinsam mit dem Deep Freeze Enterprise-Konfigurationsadministrator installiert.



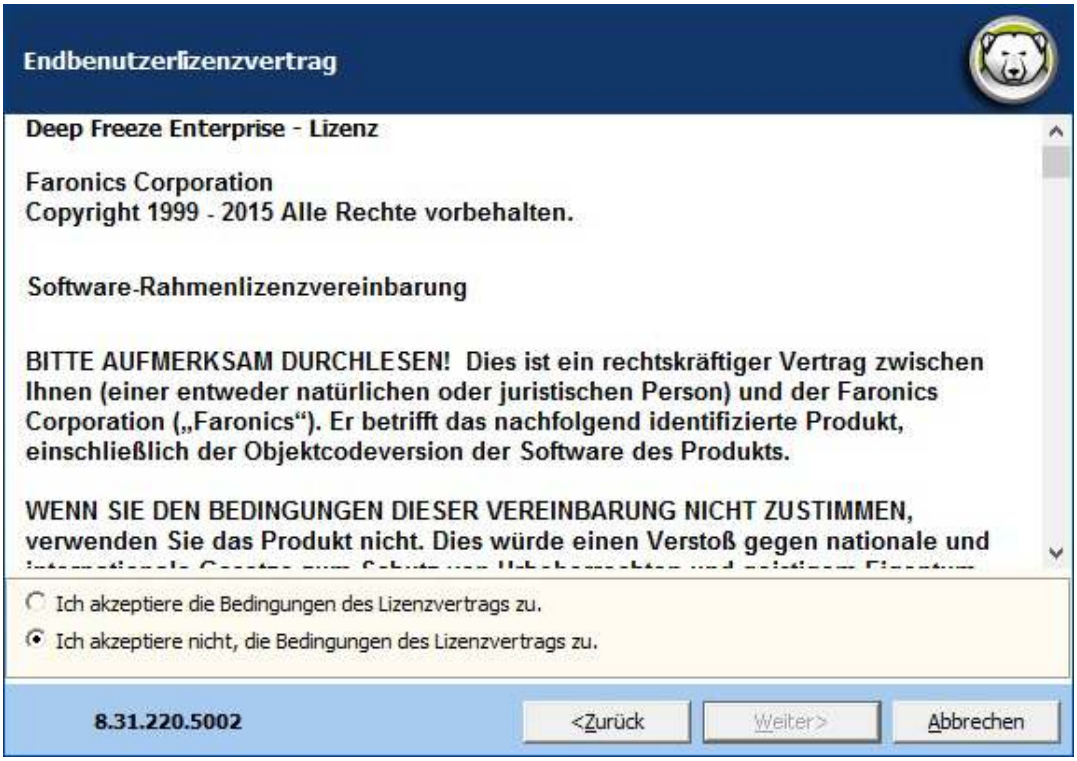
Wenn Sie Deep Freeze 6.5 (oder höher) verwenden, haben Sie die Option, bei der Installation von Deep Freeze 8.1 (oder höher) die Enterprise Console, den Konfigurationsadministrator und die Installations- bzw. Konfigurationsdateien für Deep Freeze (im Ordner "Programme installieren) automatisch zu aktualisieren.

Führen Sie die folgenden Schritte aus, um den Konfigurationsadministrator zu installieren:

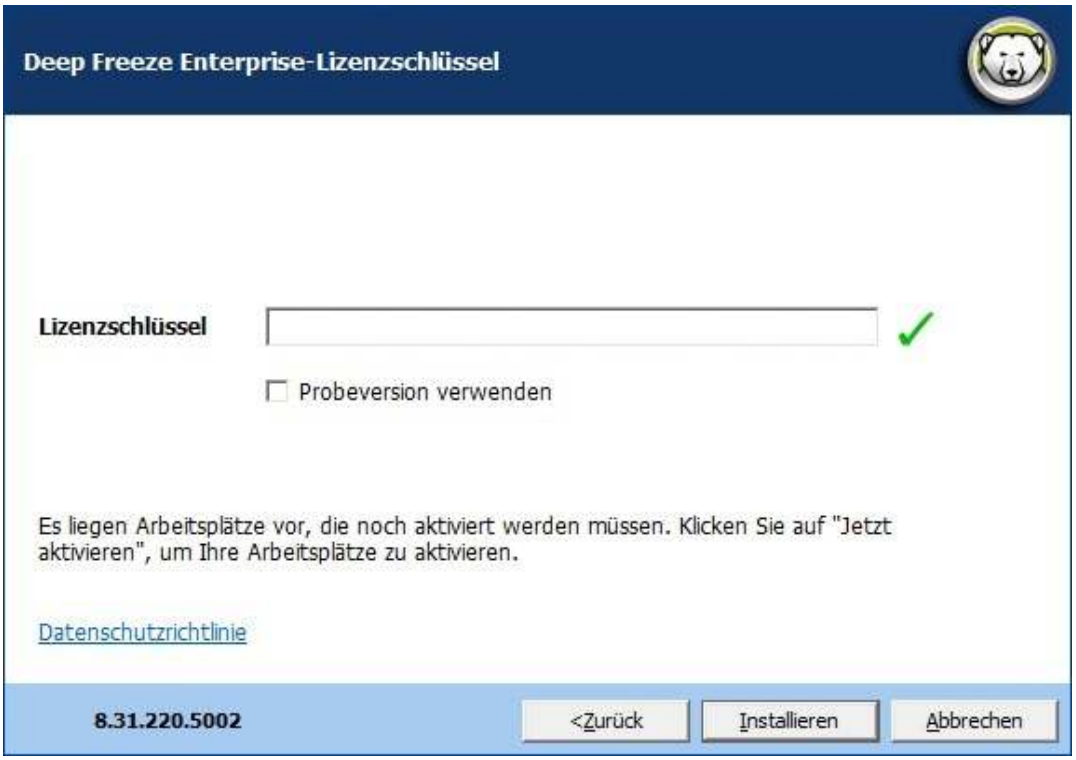
1. Klicken Sie doppelt auf die Datei *DFEnt.exe*, um den Installationsprozess zu beginnen. Der folgende Bildschirm wird angezeigt:



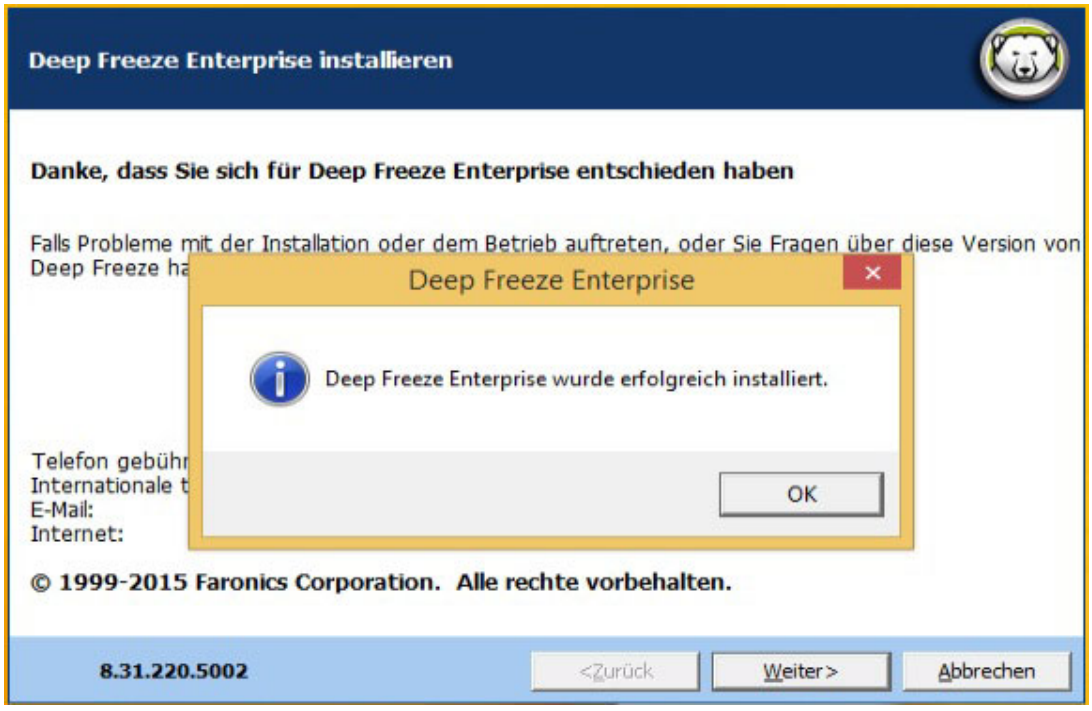
2. Klicken Sie auf *Weiter*. Lesen und akzeptieren Sie die Lizenzvereinbarung. Klicken Sie auf *Weiter*.



3. Geben Sie den Lizenzschlüssel in das Feld *Lizenzschlüssel* ein, oder markieren Sie das Kontrollkästchen *Probeversion verwenden*, um die Installation im Probemodus durchzuführen. Klicken Sie auf *Weiter*. (Deep Freeze aktiviert die Arbeitsplatzlizenzen automatisch. Deep Freeze muss innerhalb von 30 Tagen aktiviert werden, um zu vermeiden, dass das Produkt abläuft.)



4. Geben Sie den Lizenzschlüssel in das Feld *Lizenzschlüssel* ein, oder markieren Sie das Kontrollkästchen *Probeversion verwenden*, um die Installation im Probemodus durchzuführen. Klicken Sie auf *Installieren*.



5. Der Bildschirm Anpassungscodewird angezeigt.



6. Geben Sie den *Customization Code* an, und klicken Sie auf *Weiter*. Der *Customization Code* muss mindestens acht Zeichen umfassen.

Anpassungscode

Der Anpassungscode ist eine eindeutige Kennung, die den Konfigurationsadministrator, die Enterprise Console, die Installationsdateien für Computer, das System für die Generierung von Einmalpasswörtern und die Deep Freeze Befehlszeilensteuerung verschlüsselt. Bei diesem Code handelt es sich nicht um ein Passwort, das für den Zugriff auf Deep Freeze verwendet werden kann.

Der Anpassungscode stellt sicher, dass unbefugte Administratoren nicht auf einen Computer zugreifen bzw. diesen kontrollieren können. Wenn mehrere Deep Freeze-Administratoren dieselbe Gruppe von Computern steuern, müssen sie einen übereinstimmenden Anpassungscode verwenden.



Der Anpassungscode muss aufgezeichnet und sorgfältig aufbewahrt werden. Faronics ist nicht in der Lage, einen verlorenen oder vergessenen Anpassungscod wiederzuerlangen.

Erneute Initialisierung mit dem Anpassungscode

Wenn ein anderer Administrator Installationsdateien mit demselben Konfigurationsadministrator und unter Verwendung eines anderen Anpassungscodes erstellen möchte, führen Sie die folgenden Schritte aus:

1. Führen Sie *DFInit.exe* aus.
2. Hierdurch wird der vorhandene Anpassungscode für den Konfigurationsadministrator und die Enterprise Console zurückgesetzt.
3. Geben Sie einen neuen Anpassungscode ein.
4. Klicken Sie auf *OK*, um den neuen Anpassungscode zu aktivieren.

Update-Modus

Der Update-Modus kann verwendet werden, um automatisch aktualisierte Versionen existierender Dateien von Deep Freeze Enterprise zu erstellen, indem ein spezieller Befehl *Update* ausgeführt wird. Dieser Befehl führt zwei Aufgaben aus:

- Aktualisierung vorheriger Versionen der Deep Freeze Enterprise-Konsole und des Deep Freeze Server Enterprise-Konfigurationsadministrators. (Zu finden unter *Faronics > Deep Freeze Enterprise*.)
- Aktualisierung aller von Benutzern erstellen Dateien, die im Ordner *Faronics > Deep Freeze Enterprise > Installationsprogramme* gespeichert sind.

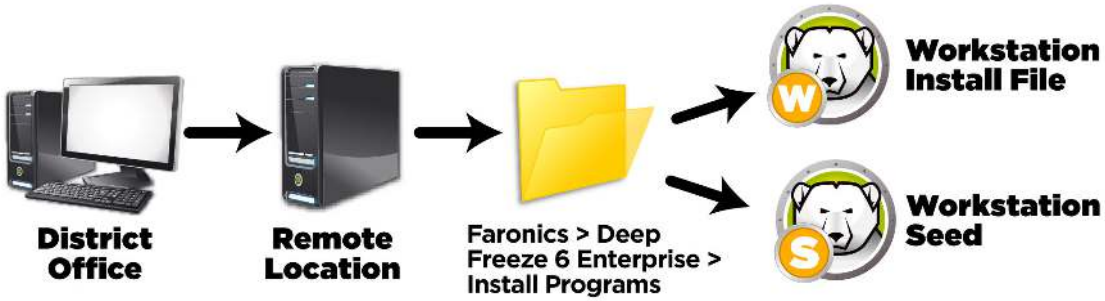
Der Vorteil dieser Updates besteht darin, dass mehrere Dateien auf die aktuellste Version aktualisiert werden können, ohne dass ihre (mit einer älteren Version von Deep Freeze Enterprise erstellten) Konfigurationsdaten verloren gehen.

Der Befehl aktualisiert automatisch Dateien, die von einem Administrator erstellt wurden administrator (*.exe*, *.rdx*), und die sich im Ordner *Faronics > Deep Freeze Enterprise > Installationsprogramme* befinden. Hierzu zählen die folgenden Unterverzeichnisse:

- Arbeitsplatzinstallationsdateien

- Arbeitsplatz-Seed-Dateien

Im nachfolgenden Beispiel hat die Zweigstelle eine neue Version des Deep Freeze Enterprise-Konfigurationsadministrators erhalten und kann vorhandene Deep Freeze-Arbeitsplatzinstallationsdateien und Arbeitsplatz-Seeds an einem fernen Standort automatisch aktualisieren.



Für den Update-Befehl ist kein Passwort erforderlich, es muss jedoch ein Anpassungscode verwendet werden. Verwenden Sie die folgende Befehlssyntax:

```
\PfadZuDatei\DFEnt.exe /update=”Anpassungscode” c:\dfupdate.log
```

- *PfadZuDatei* muss durch den tatsächlichen Pfad zur Installationsdatei (*DFEnt.exe*) ersetzt werden
- *DFEnt.exe* muss der tatsächliche Name der Installationsdatei sein (dieser kann unterschiedlich sein, wenn die Datei heruntergeladen wurde)
- Anpassungscode muss in Anführungszeichen stehen, wenn er Leerzeichen enthält
- Anpassungscode muss mit dem Anpassungscode der alten Installationsdateien übereinstimmen

Die Protokolldatei bietet die vollständigen Details darüber, welche Dateien aktualisiert wurden.

Der Update-Prozess kann einige Minuten dauern.

Der Update-Modus aktualisiert nicht die vorhandene Version von Deep Freeze auf den Computern. Computer müssen über die Enterprise-Konsole aktualisiert werden.

Einmalige Passwörter

Das System zur Generierung einmaliger Passwörter wird verwendet, um vorläufige Passwörter für Deep Freeze zu generieren, die um Mitternacht des Tags, an dem sie generiert werden, ablaufen.

Zugriff auf den Dialog „Einmalige Passwörter" ehralten Sie über

- *Tools* > *Einmalige Passwörter* in der Enterprise-Konsole. Weitere Informationen finden Sie unter Deep Freeze Enterprise-Konsole verwenden.
- *Datei* > *Einmalige Passwörter* im Konfigurationsadministrator. Weitere Informationen finden Sie unter Den Deep Freeze Enterprise-Konfigurationsadministrator verwenden.

Ein einmaliges Passwort (One Time Password, OTP) kann beispielsweise hilfreich sein, wenn ein Deep Freeze-Passwort vergessen wurde, oder eine Konfigurationsdatei ohne Definition von Passwörtern erstellt wurde. Ein Einmalpasswort kann außerdem verwendet werden, um einer Person, die Wartungsaufgaben ausführt, Zugang zu einem Computer zu bieten, ohne dass diese Person das dauerhafte Deep Freeze-Passwort kennen muss.

Führen Sie die folgenden Schritte aus, um ein Einmalpasswort zu erstellen:

1. Wählen Sie entweder *Passwort nur für einmalige Verwendung gültig* oder *Passwort für mehrere Verwendungen gültig* aus. Alle Einmalpasswörter laufen unabhängig vom Typ um Mitternacht des Tags ab, an dem sie erstellt wurden.
2. Geben Sie im Feld *Token* den Einmalpasswort-Token des Computers ein, der ein Einmalpasswort benötigt. Der OTP-Token für den Computer befindet sich im Anmeldedialog, wie nachfolgend dargestellt.



3. Klicken Sie auf *Generieren*.



Die Deep Freeze-Befehlszeilenschnittstelle unterstützt nicht die Verwendung einmaliger Passwörter.



Den Deep Freeze Enterprise-Konfigurationsadministrator verwenden

Themen

Auf den Konfigurationsadministrator zugreifen
Registerkarte „Passwörter“
Registerkarte "Laufwerke“
Registerkarte "Arbeitsplatzaufgaben"
Registerkarte "Windows Update"
Registerkarte "Stapeldatei"
Registerkarte „Erweiterte Optionen“
Arbeitsplatzinstallationsprogramm und Arbeitsplatz-Seed erstellen

Auf den Konfigurationsadministrator zugreifen

Öffnen Sie den Konfigurationsadministrator, indem Sie den folgenden Pfad im Startmenü auswählen:

Start > Programme > Faronics > Deep Freeze Enterprise > Deep Freeze Administrator

Der Konfigurationsadministrator bietet mehrere Registerkarten, über die Passwörter, eingefrorene Laufwerke, Arbeitsplatzaufgaben, Windows-Updates, Stapeldateien und erweiterte Optionen konfiguriert werden können. Nach Konfiguration der Einstellungen kann eine Installationsdatei für Arbeitsplätze erstellt werden. Die Installationsdatei für Arbeitsplätze kann auf den Computern installiert werden, die über Deep Freeze geschützt werden sollen. Auf Deep Freeze Enterprise-Konfigurationsadministrator kann auch von der Deep Freeze Enterprise Console aus zugegriffen werden.

Symbolleiste und Menüs

Symbolleiste

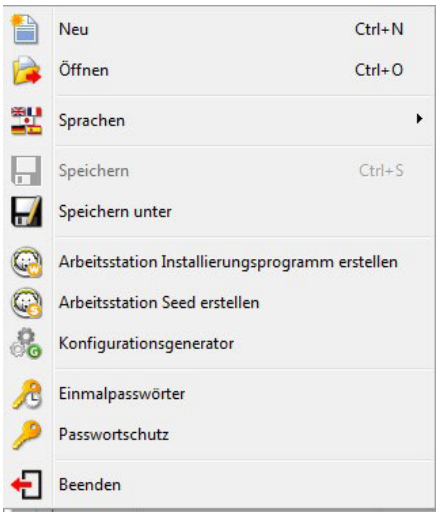
Die Symbolleiste ist am oberen Ende aller Registerkarten im Konfigurationsadministrator verfügbar.



Symbol	Funktion
Neu	Löscht alle bestehenden Konfigurationseinstellungen. Öffnet das Programm mit der Standardkonfiguration.
Offen	Öffnet eine gespeicherte .rdx-Datei, Arbeitsplatzinstallationsdatei oder Arbeitsplatz-Seed-Datei.
Speichern	Speichert eine .rdx-Datei, Arbeitsplatzinstallationsdatei oder Arbeitsplatz-Seed-Datei. Der Dateiname und -pfad ist im unteren Bereich des Konfigurationsadministrators unter "Status" angegeben.
Speichern unter	Dient zum Speichern der Konfiguration als .rdx-Datei.
Hilfe	Öffnet die Deep Freeze-Hilfsdatei.
Erstellen	*Arbeitsplatzinstallationsdatei erstellen* erstellt ein benutzerdefiniertes Installationsprogramm für die Installation an Arbeitsplätzen. Diese Arbeitsplätze können daraufhin von der Deep Freeze Enterprise-Konsole aus verwaltet werden. *Arbeitsplatz-Seed-Datei erstellen* erstellt ein Seed, das es der Deep Freeze-Konsole erlaubt, mit verschiedenen Arbeitsplätzen im Netzwerk zu kommunizieren. Sobald das Seed auf den Arbeitsplätzen installiert ist, kann die Deep Freeze-Arbeitsplatzinstallationsdatei remote bereitgestellt werden.

Menü ‚Datei'

Das Menü *Datei* enthält dieselben Optionen, wie diejenigen, die in der Symbolleiste verfügbar sind. Darüber hinaus stehen Optionen zur Verfügung, um eine Auswahl unter den verfügbaren Sprachen zu treffen, sowie für die Einrichtung eines *Passwortschutzes*.



Passwortschutz

Der Passwortschutz bietet dem Administrator eine zusätzliche Sicherheitsebene.

Führen Sie die folgenden Schritte aus, um den Zugriff zum Konfigurationsadministrator durch ein Passwort zu schützen:

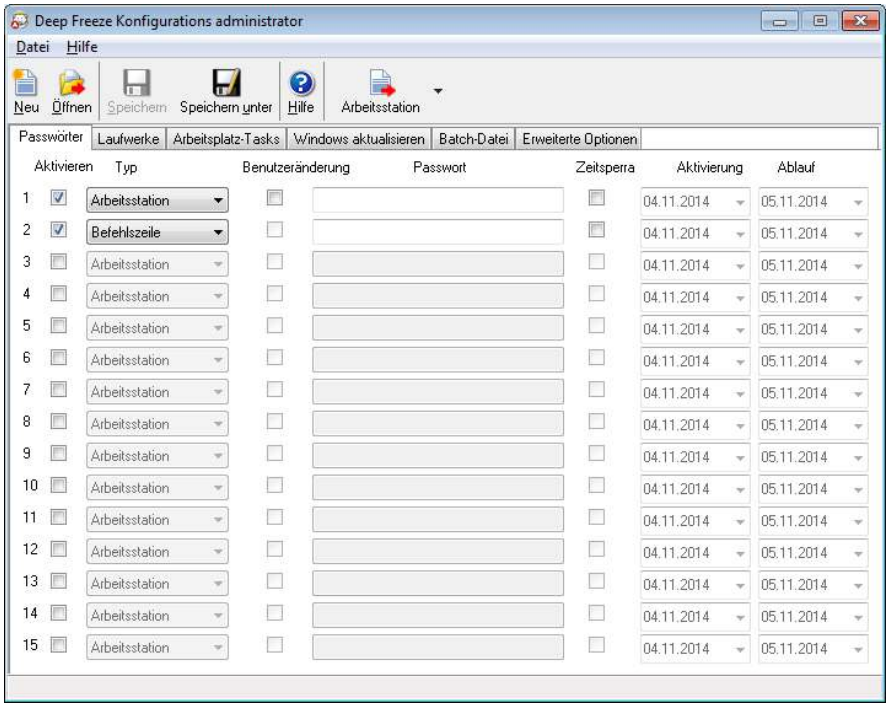
1. Öffnen Sie das Menü *Datei*, und wählen Sie *Passwortschutz* aus.
2. Aktivieren Sie das Kontrollkästchen *Mit Passwort schützen*.
3. Geben Sie das Passwort ein, und bestätigen Sie es.
4. Klicken Sie auf *OK*, um das Passwort einzustellen, oder auf *Abbruch* , um den Dialog zu verlassen, ohne ein Passwort einzustellen.



Notieren Sie das Passwort an einem sicheren Ort. Wenn es verloren geht, kann es nicht wiederhergestellt werden. In einem solchen Fall muss Deep Freeze erneut installiert werden.

Registerkarte „Passwörter“

Deep Freeze Enterprise bietet dem Administrator die Möglichkeit, bis zu 15 feste Passwörter zu bestimmen.



Führen Sie die folgenden Schritte aus, um ein Passwort zu erstellen:

1. Wählen Sie in der entsprechenden Zeile *Aktivieren* aus.
2. Wählen Sie in der Drop-Down-Liste *Typ* die bevorzugte Passwortart aus. Die folgenden Optionen sind verfügbar:
   - Arbeitsplatz – für die Verwendung am Arbeitsplatz vorgesehen, wenn der Anmeldebildschirm gestartet wird.
   - Befehlszeile – für die Verwendung mit Befehlszeilensteuerungen vorgesehen. Das Befehlszeilensteuerungstool (*DFC.exe*) funktioniert nur, wenn mindestens ein Befehlszeilenpasswort definiert wurde.
3. Optional – Wählen Sie für Passwörter die Checkbox *Benutzeränderung* aus, um es Benutzern zu ermöglichen, das Passwort am Computer zu ändern.
4. Geben Sie das Passwort ein.



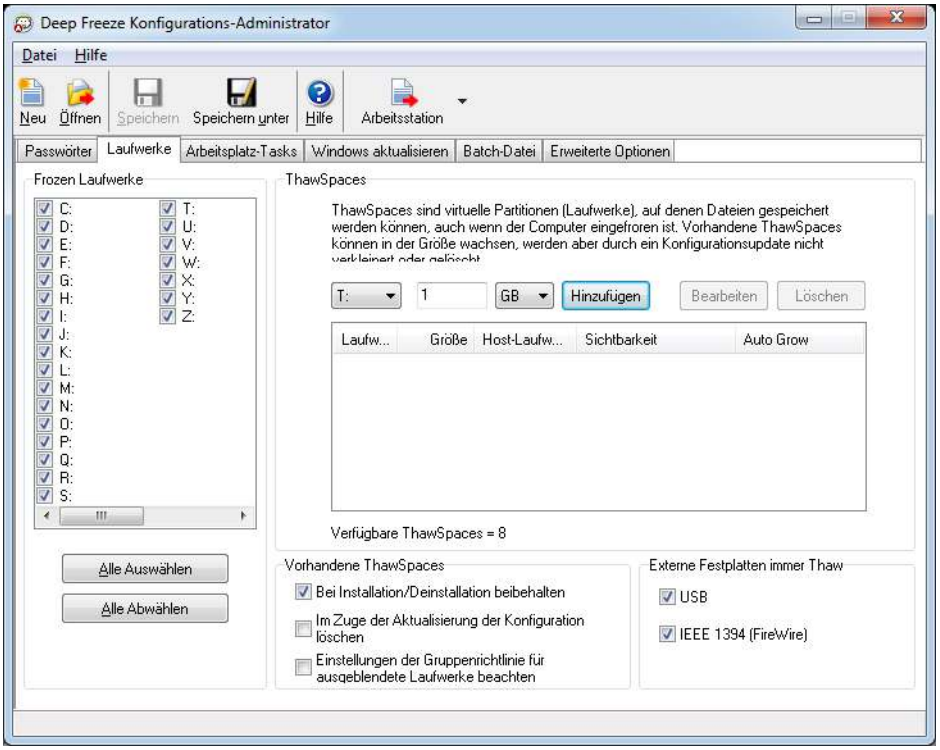
Das im Feld *Passwort* eingegebene Passwort wird nicht ausgeblendet.

Verwenden Sie nicht dasselbe Passwort für die Befehlszeile und die GUI.

5. Sie können die Aktivierung und den Ablauf eines Passworts zu bestimmten Terminen einstellen, indem Sie die Checkbox *Zeitlimit* auswählen und die Drop-Down-Kalender verwenden, um ein *Aktivierungsdatum* und ein *Ablaufdatum* anzugeben.

Registerkarte "Laufwerke“

Die Registerkarte "Laufwerke" dient zur Auswahl von gefrorenen Laufwerken (im Zustand "eingefroren" und von Deep Freeze gesichert) oder aufgetauten Laufwerken (im Zustand "aufgetaut" und somit ungesichert). Sie können auch einen Auftauplatz erstellen. Dabei handelt es sich um eine virtuelle Partition, die auf einem lokalen, gefrorenen oder aufgetautem Laufwerk gehostet wird, auf der Dateien permanent gespeichert werden können, ohne dass sie von Deep Freeze bei einem Neustart gelöscht werden.



Eingefrorene Laufwerke

Standardmäßig befinden sich alle Laufwerke im Zustand "eingefroren". Sie können ein Laufwerk in den Zustand "aufgetaut" versetzen, indem Sie die Markierung für das gewünschte Laufwerk entfernen.

Obwohl nur lokale Laufwerke (Partitionen oder physische Laufwerke) eingefroren werden werden können, werden alle Laufwerkbuchstaben angezeigt, da die vorkonfigurierte Installationsdatei auf zahlreichen Computern mit unterschiedlichen Hardware- und Software-Einstellungen installiert werden kann.

Beispiel

Im voranstehenden Bildschirm ist das Laufwerk D: in der Liste der eingefrorenen Laufwerke nicht ausgewählt. Daher werden alle Laufwerke bis auf D: in den Zustand „eingefroren“ versetzt.

Auftauplatz

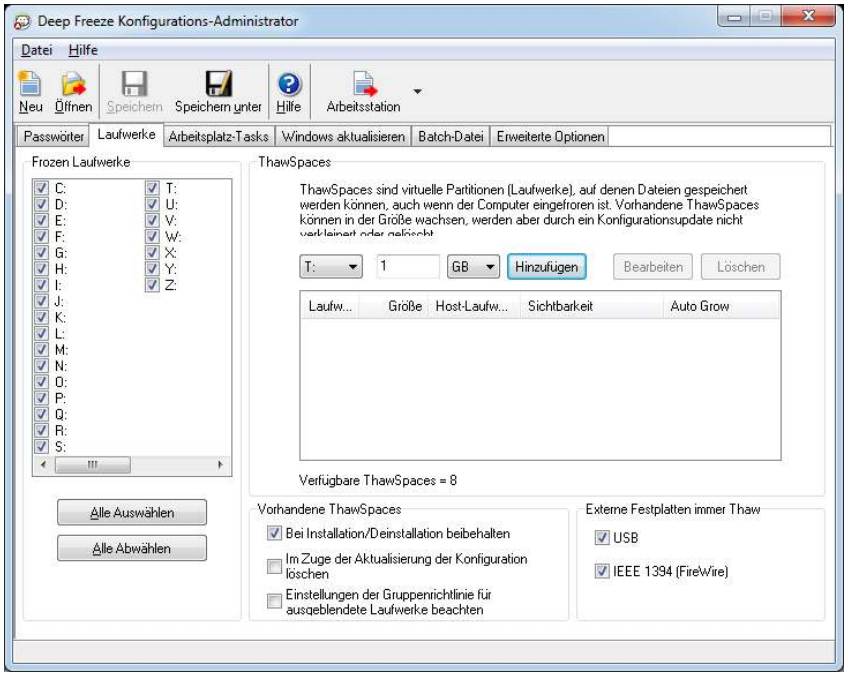
Ein Auftauplatz ist eine virtuelle Partition, die verwendet werden kann, um Programme zu speichern, Dateien zu sichern oder dauerhafte Änderungen vorzunehmen. Alle am Auftauplatz gespeicherten Dateien bleiben nach einem Neustart erhalten, selbst wenn sich der Computer im Zustand "gefroren" befindet. Ein Auftauplatz kann in einem Laufwerk erstellt werden, das als "gefroren" oder "aufgetaut" konfiguriert ist.

Über die Option Automatisch vergrößern kann ein ThawSpace so eingerichtet werden, dass er sich automatisch vergrößert. Hierdurch lässt sich verhindern, dass der Speicherplatz knapp wird. Der ThawSpace wird automatisch um 25 % seiner aktuellen Größe erweitert, wenn der freie Speicherplatz auf 25 % oder weniger sinkt. Er wird bis zu der in der ThawSpace-Konfiguration definierten Maximalgröße erweitert.



Der ThawSpace wird nur im Zustand „Thawed" erweitert.

Nachdem der ThawSpace erweitert wurde, wird er nicht wieder verkleinert, selbst wenn der freie Speicherplatz mehr als 25 % beträgt oder die Arbeitsplatzkonfiguration so aktualisiert wird, dass sie eine geringere Größe für den jeweiligen Laufwerksbuchstaben des ThawSpace vorgibt.

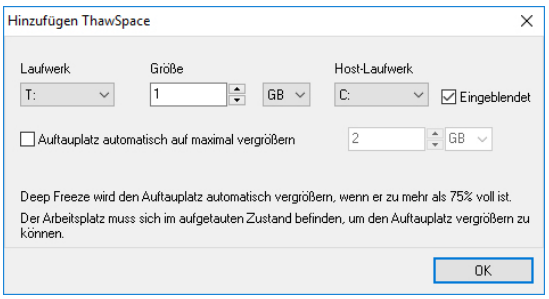


Führen Sie die folgenden Schritte aus, um über den Konfigurationsadministrator einen oder mehrere Auftauplätze zu erstellen:

1. Wählen Sie den *Laufwerksbuchstaben* aus. Der Standardbuchstabe ist *T:*. Es kann jedoch ein beliebiger Buchstabe gewählt werden. Wenn der ausgewählte Laufwerkbuchstabe bereits auf einem Computer vorhanden ist, wenn Deep Freeze installiert wird, wird automatisch der nächste verfügbare Buchstabe verwendet.
   - Wenn ein *Laufwerkbuchstabe* in der Drop-Down-Liste ausgewählt und für die Erstellung eines Auftauplatzes verwendet wird, wird er aus der Drop-Down-Liste entfernt.

- Wenn ein Auftauplatz entfernt wird, wird der entsprechende *Laufwerkbuchstabe* wieder zur Drop-Down-Liste hinzugefügt.
- Der *Laufwerkbuchstabe* darf nicht dem *Host-Laufwerk* entsprechen.

2. Klicken Sie auf Hinzufügen. Der Dialog „Auftauplatz hinzufügen" wird angezeigt:



3. Geben Sie die *Größe* ein. Dies ist die Größe des Auftauplatzes. Die maximale Größe beträgt 1024 GB, minimal sind 16 MB erforderlich.
   - Wenn der Computer nicht über genügend freien Speicherplatz verfügt, um die ausgewählte Größe für den Auftauplatz zu ermöglichen, wird die Größe des Auftauplatzes nach unten hin angepasst, um einen ordentlichen Betrieb des Computers zu gewährleisten.
   - Wenn Sie eine Größe von weniger als 16 MB auswählen, wird ein Auftauplatz von 16 MB eingerichtet.
   - Wenn Sie eine Größe von mehr als 1024 GB (1TB) auswählen, wird ein Auftauplatz von 1024GB (1TB) eingerichtet.
4. Wählen Sie als Einheit für den Speicher des Auftauplatzes *MB* oder *GB* aus.
5. Wählen Sie das *Host-Laufwerk* aus.
   - Das *Host-Laufwerk* ist das Laufwerk, auf dem der Auftauplatz erstellt wird.
   - Der für den Auftauplatz erforderliche Speicherplatz belegt einen Teil des auf dem *Host-Laufwerk* verfügbaren Gesamtspeicherplatzes.
6. Wählen Sie im Markierungsfeld *Sichtbarkeit* die Option *sichtbar* oder *ausgeblendet* aus.
   - Wenn Sie *Sichtbar* auswählen, ist das Laufwerk im Windows Explorer sichtbar.
   - Wenn Sie *Ausgeblendet* auswählen, ist das Laufwerk im Windows Explorer nicht sichtbar.
   - Sie können jedoch auf das ausgeblendete Laufwerk zugreifen, indem Sie unter *Start* > *Ausführen* den Laufwerksbuchstaben eingeben.
7. Aktivieren Sie das Kontrollkästchen *Auftaplatz automatisch auf maximal vergrößern*, und konfigurieren Sie die Maximalgröße des ThawSpace.
8. Klicken Sie auf *Hinzufügen*, um den Auftauplatz hinzuzufügen.

Einen Auftauplatz entfernen

Sie können einen Auftauplatz entfernen, indem Sie ihn auswählen und auf *Entfernen* klicken. Der Auftauplatz wird entfernt, und der Laufwerksbuchstabe wird wieder zur Drop-Down-Liste *Laufwerksbuchstabe* hinzugefügt. Klicken Sie auf *Alle entfernen*, um alle Auftauplätze zu entfernen.



Wenn ein Auftauplatz im Konfigurationsadministrator entfernt wird, tritt die Änderung erst in Kraft, wenn die Konfiguration auf den Arbeitsplatz angewandt wird.



Entfernen Sie vor der Entfernung eines Auftauplatzes sämtliche symbolischen Verknüpfungen bzw. Umleitungen des Benutzerprofils.

Wenn ein Auftauplatz entfernt wird, werden sämtliche dort gespeicherten Daten ebenfalls gelöscht.

Ein Auftauplatz wird nicht von Deep Freeze geschützt. Nehmen Sie deswegen normale Datensicherungsmaßnahmen vor, z.B. Sicherheitskopien oder Antivirenprogramme.

Beispiel

Im oben dargestellten Bildschirm wird ein *Auftauplatz* mit einer Größe von 16 MB auf dem *Host-Laufwerk* C: erstellt, und der Auftauplatz erhält den Laufwerksbuchstaben T:. Der Auftauplatz T: ist auf *Sichtbar* eingestellt, so dass über den Windows Explorer darauf zugegriffen werden kann.



Es wird empfohlen, Laufwerksbuchstaben am Ende des Alphabets (X, Y, Z) zuzuordnen, um eine automatische Neuzuordnung bei Anschluss von Wechseldatenträgern zu vermeiden.

Vorhandener Auftauplatz

Das Markierungsfeld *Bei Installation/Deinstallation beibehalten* ist standardmäßig ausgewählt, um zu verhindern, dass Auftauplätze, die bei früheren Installationen erstellt wurden, gelöscht werden. Bei einer überwachten Installation wird immer ein Dialog angezeigt, der fragt, ob der Auftauplatz beibehalten oder gelöscht werden soll, unabhängig davon, ob *Bei Installation/Deinstallation beibehalten* ausgewählt ist oder nicht. Diese Option wird nicht angezeigt, wenn die Deinstallation über die Enterprise-Konsole vorgenommen wird.

Wählen Sie *Bei Konfigurations-Update löschen* aus, um alle bestehenden Auftauplätze auf dem Arbeitsplatz zu löschen und bei Anwendung der Konfiguration neu zu erstellen. Die bestehenden Auftauplätze und die Daten in den Auftauplätzen werden gelöscht, und die neuen Auftauplätze werden gemäß den Einstellungen erstellt, wenn die Konfiguration angewandt wird.

Die Einstellung *Einstellungen für Gruppenrichtlinie für ausgeblendete Laufwerke beachten* stellt sicher, dass die Gruppenrichtlinieneinstellungen für ausgeblendete Laufwerke keinen Konflikt mit den Deep Freeze-Einstellungen für ausgeblendete Laufwerke auslösen.

Die Einstellungen für ausgeblendete Laufwerke für Gruppenrichtlinien sind benutzerspezifisch. Die Einstellungen für ausgeblendete Laufwerke für Deep Freeze sind global, wenn die Option *Einstellungen für Gruppenrichtlinie für ausgeblendete Laufwerke beachten* deaktiviert ist.

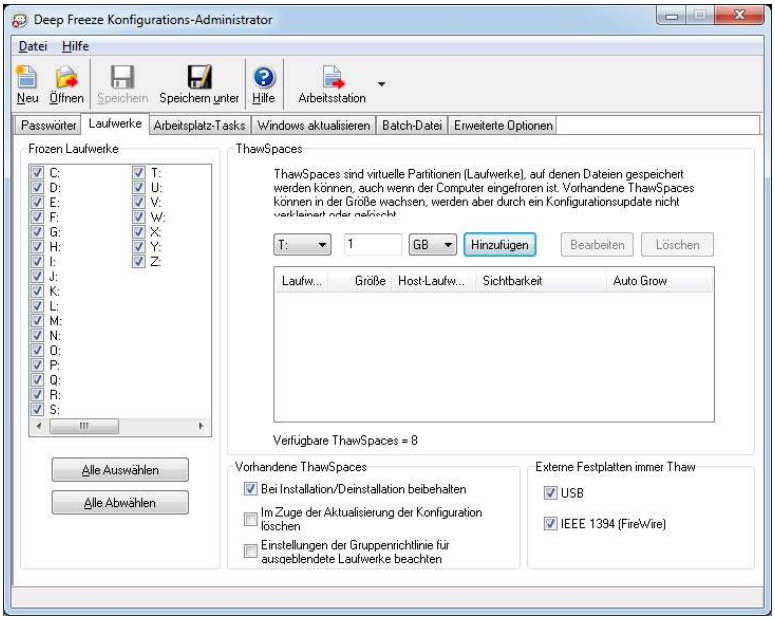
Wenn keine Gruppenrichtlinien für ausgeblendete Laufwerke vorliegen, wird empfohlen, diese Option zu deaktivieren.

Externe Festplatten immer auftauen

Das Teilfenster *Externe Festplatten immer auftauen* enthält die beiden Checkboxes *USB* und *IEEE 1394 (FireWire)*, und beide Checkboxes sind standardmäßig ausgewählt. Hierdurch wird sichergestellt, dass USB- oder IEEE 1394- (FireWire-) Laufwerke immer aufgetaut sind.

Wenn die Checkboxes für die externen Festplatten USB und/oder IEEE 1394 (FireWire) nicht ausgewählt sind, wird das entsprechende Laufwerk *eingefroren* oder *aufgetaut*, je nachdem, was für den entsprechenden verwendeten Laufwerksbuchstaben im Abschnitt Eingefrorene Laufwerke angegeben ist.

Netzwerklaufwerke und entfernbare Medienlaufwerke (Diskette, USB-Laufwerk, CD-RW, etc.) sind von Deep Freeze nicht betroffen und können daher nicht eingefroren werden.



Beispiel

Im oben dargestellten Bildschirm sind die Laufwerke E: und F: im Teilfenster *Eingefrorene Laufwerke* ausgewählt.

Angenommen, E: entspricht einer USB-Festplatte, und F: entspricht einer IEEE 1394- (FireWire-) Festplatte

Die Checkboxes *USB* und *IEEE 1394 (FireWire)* sind im Teilfenster *Externe Festplatten immer auftauen* ausgewählt, die externen Festplatten würden also den Status *aufgetaut* haben.

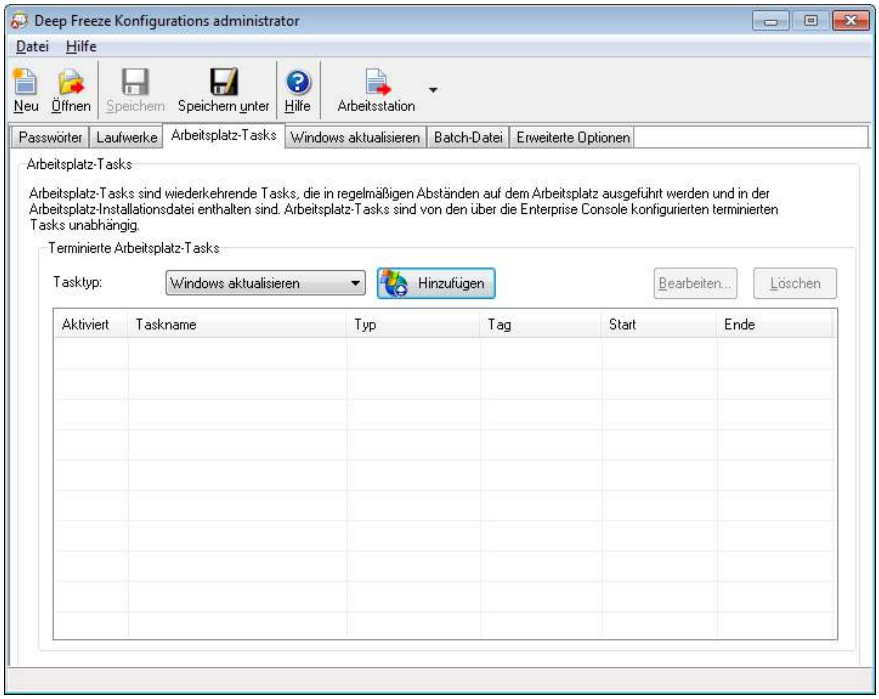
Die Checkbox für USB ist ausgewählt. Die Checkbox für *IEEE 1394 (FireWire)* ist nicht ausgewählt. In diesem Beispiel wäre das *USB*-Laufwerk (*D:*) aufgetaut, während das *IEEE 1394 (FireWire)*-Laufwerk (*F:*) eingefroren wäre.

Registerkarte "Arbeitsplatzaufgaben"

Die Registerkarte "Arbeitsplatzaufgaben" dient zur Planung verschiedener Aufgaben, die auf einem Arbeitsplatz ausgeführt werden. Arbeitsplatzaufgaben werden lokal auf dem jeweiligen Arbeitsplatz gespeichert und auch dann ausgeführt, wenn kurzfristig die Verbindung mit dem Netzwerk verloren geht und der betroffene Arbeitsplatz nicht mit der Deep Freeze-Konsole kommunizieren kann. Arbeitsplatzaufgaben sind Teil der Arbeitsplatzinstallationsdatei oder der Deep Freeze-Konfigurationsdatei (.rdx). Die folgenden Arbeitsplatzaufgaben stehen zur Verfügung:

- Windows Update – Aktualisierungen durch Windows Update planen. Sie können zusätzliche Einstellungen über die Registerkarte "Windows Update" konfigurieren.
- Neustart – Arbeitsplätze periodisch neu starten, um diese auf die ursprüngliche Konfiguration zurückzusetzen oder unerwünschte Daten zu löschen.
- Herunterfahren – Arbeitsplätze zu bestimmten Zeitpunkten jeden Tag herunterfahren, um Strom zu sparen.
- Inaktivität – Arbeitsplätze herunterfahren oder neu starten, wenn Sie über einen bestimmten Zeitraum hinweg inaktiv sind.
- Stapeldatei – Eine Stapeldatei auf einem bestimmten Arbeitsplatz ausführen. Sie können zusätzliche Einstellungen über die Registerkarte "Stapeldatei" konfigurieren.
- Zeitraum im Zustand "aufgetaut" – Den Computer neu starten und über einen bestimmten Zeitraum hinweg im Zustand "aufgetaut" belassen, um Software manuell zu installieren, durch Software von Drittanbietern automatische Software-Updates durchzuführen oder andere dauerhafte Änderungen an der Konfiguration vorzunehmen.

Die einzelnen Aufgaben werden in den folgenden Abschnitten ausführlich erläutert.



Arbeitsplatzaufgaben oder geplante geplante Aufgaben: Wenn die Kommunikation zwischen der Enterprise-Konsole und dem Zielcomputer scheitert, werden Arbeitsplatzaufgaben dennoch ausgeführt, da diese direkt auf dem Zielcomputer gespeichert werden.



Die über den Assistenten für geplante Aufgaben in der Enterprise-Konsole erstellten Aufgaben sind auf der Konsole, nicht jedoch auf den Zielcomputern vorhanden. Daher ist eine dauerhafte Verbindung zwischen der Konsole und dem Zielcomputer erforderlich, damit die geplanten Aufgaben ausgeführt werden können. Weitere Informationen hierzu finden Sie im Abschnitt Deep Freeze-Aufgaben terminieren.



Auf der Registerkarte "Arbeitsplatzaufgaben" können keine sich überlappenden Aufgaben erstellt werden. Wenn sich eine neu erstellte Aufgabe mit einer vorhandenen Aufgabe überschneidet, wird eine Nachricht angezeigt.



Eine Nachricht kann dem Benutzer maximal 5 Minuten lang angezeigt werden. Zwischen zwei Aufgaben müssen mindestens 5 Minuten verstreichen.



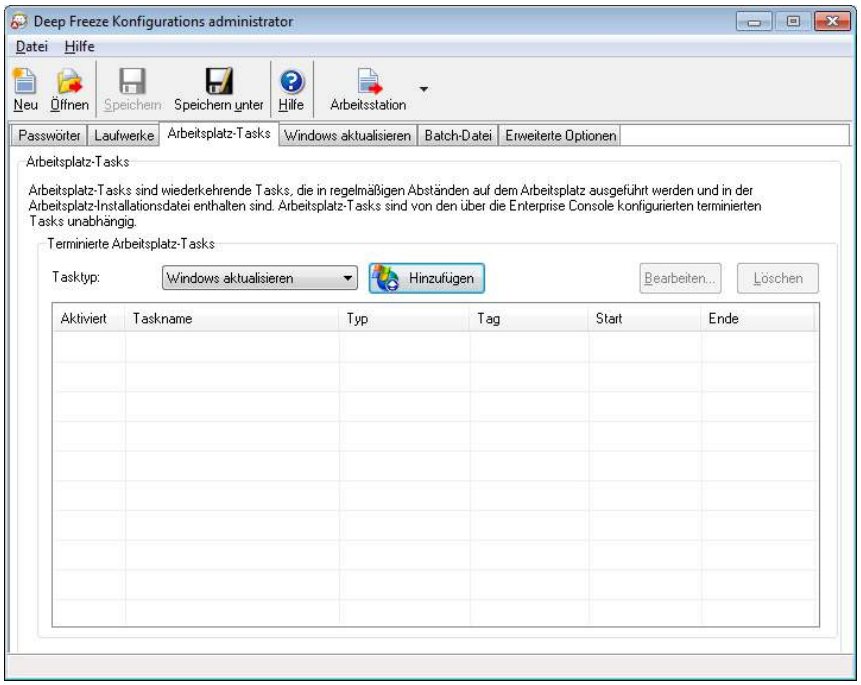
Eine Arbeitsplatzaufgabe wird nur dann ausgeführt, wenn sich Deep Freeze im Zustand "gefroren" befindet.

Windows Update

Windows Update-Aufgaben werden eingeplant, um Windows-Aktualisierungen auf den einzelnen Arbeitsplätzen herunterzuladen. Auch wenn sich der Arbeitsplatz im Zustand "gefroren" befindet, können Windows Updates heruntergeladen werden. Eine Windows Update-Aufgabe hat eine Start- und eine Endzeit. Nachdem die Windows-Aktualisierungen heruntergeladen wurden, startet der Arbeitsplatz im Zustand "aufgetaut" erneut, um diese zu installieren.

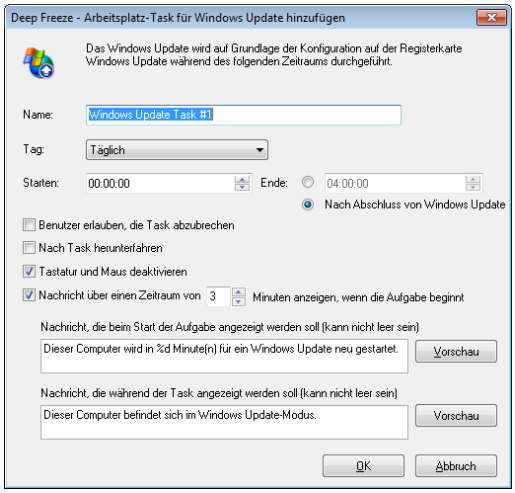


Windows-Updates können außerdem manuell am Arbeitsplatz angewandt werden, indem Sie den Arbeitsplatz auswählen und über das Kontextmenü der Deep Freeze Console den Befehl *Windows-Update ausführen* ausführen. Weitere Informationen hierzu finden Sie unter Deep Freeze mit der Konsole verwalten.



Die Aufgabe "Windows Update" kann über die folgenden Schritte geplant werden:

1. Wählen Sie *Windows Update* in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Tag – Wählen Sie den Tag aus, oder geben Sie an, ob die Aufgabe an Wochentagen oder an Wochenenden ausgeführt werden soll.
- Start – Wählen Sie die Startzeit aus.
- Ende – Wählen Sie die Endzeit aus. Das kleinstmögliche Zeitintervall beträgt 15 Minuten. Alternativ hierzu können Sie auch *Nach vollständiger Ausführung des Windows Update* auswählen. Wenn die Aufgabe "Windows Update" nach 6 Stunden nicht abgeschlossen wurde, wird sie von Deep Freeze beendet.

- Benutzer erlauben, die Aufgabe abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen, bevor sie gestartet wird.
- Versuchen, lokal hochzufahren – Wählen Sie dieses Markierungsfeld aus, um den Arbeitsplatz lokal hochzufahren, ohne dass Kommunikation mit der Enterprise-Konsole erforderlich ist.



Ob der Arbeitsplatz lokal hochgefahren werden kann, hängt von den Hardware-Spezifikationen Ihres Arbeitsplatzes ab. Diese Option funktioniert nur, wenn sie von Ihrer Hardware unterstützt wird.

- Nach Aufgabe herunterfahren – Wählen Sie diese Checkbox aus, um den Computer nach Durchführung einer Aufgabe herunterzufahren.
- Tastatur und Maus deaktivieren – Wählen Sie diese Checkbox aus, um Tastatur und Maus während der Durchführung der Aufgabe zu deaktivieren.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um *vor* und *während* der Durchführung einer Aufgabe eine Nachricht auf dem Computer anzuzeigen. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein, die vor Beginn der Aufgabe angezeigt werden soll.

3. Klicken Sie auf OK. Sie werden jetzt zur Registerkarte "Windows Update" geführt, um zusätzliche Einstellungen zu konfigurieren, soweit Sie dies nicht bereits getan haben.



Die Nachricht *Dieser Computer wird in %d für Windows Update neu gestartet* wird im Feld *Nachricht, die vor der Aufgabe angezeigt werden soll* angezeigt. Diese Nachricht kann bearbeitet werden. Fügen Sie das Wort *Minuten* nach *%d* in die Nachricht ein, um das Wort "Minuten" in die Nachricht aufzunehmen.



Bei der Konfiguration der Aufgabe "Windows Update" können Sie entweder die Option *Nach vollständiger Ausführung des Windows Update* wählen oder sicherstellen, dass Sie einen ausreichenden Zeitraum konfigurieren, damit alle erforderlichen Updates installiert werden können. Unter den Microsoft Security Bulletins auf der Technet-Internetseite (http://technet.microsoft.com/de-de/security/bulletin) können Sie Details zu kritischen Updates und Sicherheitsupdates nachschlagen, um den erforderlichen Zeitraum abschätzen zu können.

Wenn Sie WSUS nicht verwenden, wird der Deep Freeze Windows Update-Prozess nur kritische Updates und Sicherheitsupdates sowie Funktionsupdates für Windows 10 installieren, bei denen kein Benutzereingriff erforderlich ist. Wenn Sie WSUS verwenden, werden alle von WSUS genehmigten Updates installiert.

Wenn Sie WSUS nicht verwenden, wird die Windows Update-Aufgabe immer versuchen, Funktionsupdates zu installieren, sobald sie für die aktuelle Version des Windows 10-Systems verfügbar sind. Sie können die Installation von Funktionsupdates zurückstellen, indem Sie unter „Erweiterte Optionen" der Windows Update-Systemeinstellungen die Option „Auswählen, wann Updates installiert werden" auswählen oder die lokale Computerrichtlinie „Auswählen, wann Preview-Builds und Funktionsupdates erhalten werden" aktivieren. Diese finden Sie unter *Computerkonfiguration* > *Administrative Vorlagen* > *Windows-Komponenten* > *Windows Update* > *Windows Update for Business*.

Eine andere Möglichkeit, andere verfügbare Updates zu installieren, ist, die Microsoft Update Catalog-Internetseite zu besuchen (http://catalog.update.microsoft.com), auf der die einzelnen Updates als individuelle KB-Downloads zur Verfügung stehen. Diese können dann durch eine Deep Freeze Stapeldatei-Arbeitsplatzaufgabe angewandt werden. Stapeldateiaufgaben können auch verwendet werden, um Softwareupdates von Drittanbietern zu durchzuführen.

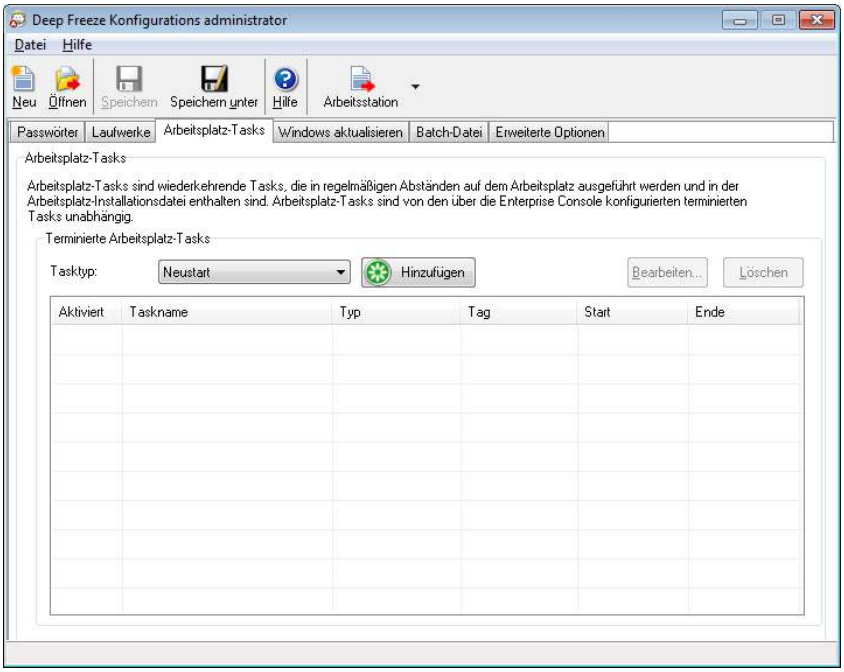
Die Einstellungen, die auf der Deep Freeze-Registerkarte "Windows Update" vorgenommen werden, haben Vorrang vor den Windows Update-Einstellungen der einzelnen Arbeitsplätze.

Beispiel

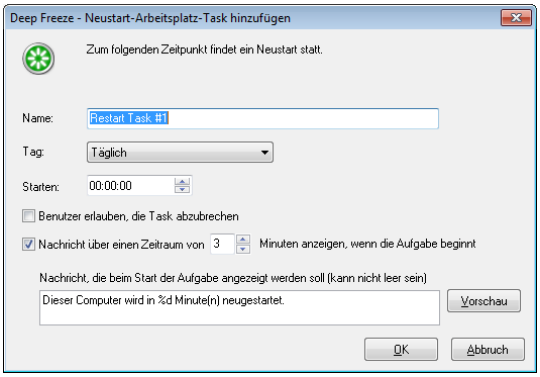
Im oben dargestellten Bildschirm wurde ein Windows Update-Aufgabe erstellt, der jeden Tag um 00:00 Uhr die Windows-Installationen aktualisiert und nach Abschluss von *Windows Update* beendet wird. Diese Aufgabe ist so konfiguriert, dass dem Benutzer vor dem Start von Windows Update eine Nachricht angezeigt wird. Tastatur und Maus sind deaktiviert.

Neustart

Die Aufgabe "Neu starten" kann über die folgenden Schritte geplant werden:



1. Wählen Sie *Neustart* in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Tag – Wählen Sie den Tag aus, oder geben Sie an, ob die Aufgabe an Wochentagen oder an Wochenenden ausgeführt werden soll.
- Start – Wählen Sie die Startzeit aus.
- Benutzer erlauben, die Aufgabe abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen, bevor sie gestartet wird.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um eine Nachricht auf dem Computer anzuzeigen, bevor die Aufgabe startet. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein, die vor Beginn der Aufgabe angezeigt werden soll.

3. Klicken Sie auf OK.

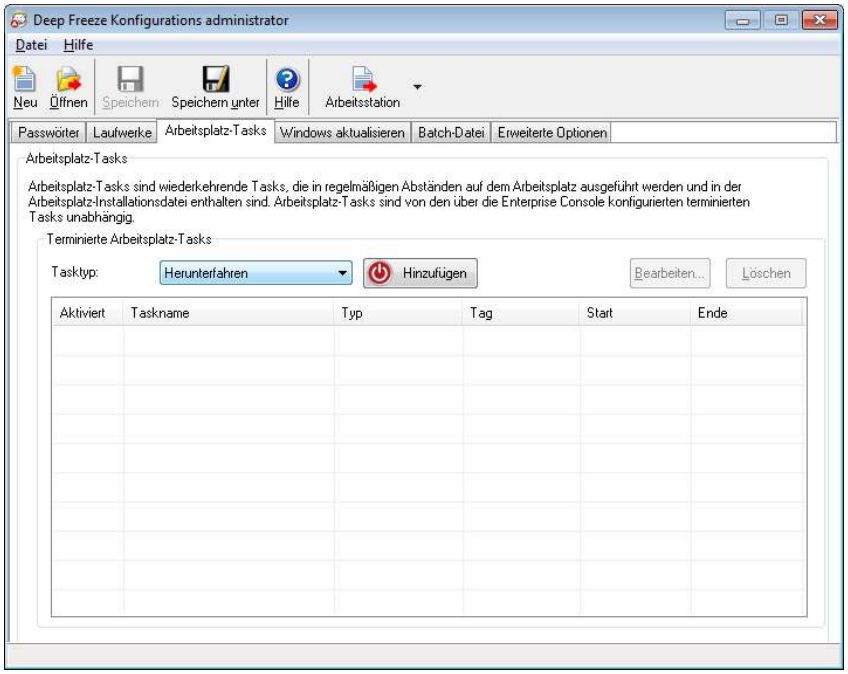
Die Nachricht *Dieser Computer wird in %d Sekunden neu gestartet* wird im Feld *Nachricht, die vor der Aufgabe angezeigt werden soll* angezeigt. Diese Nachricht kann bearbeitet werden. Fügen Sie das Wort *Minuten* nach *%d* in die Nachricht ein, um das Wort "Minuten" in die Nachricht aufzunehmen.

Beispiel

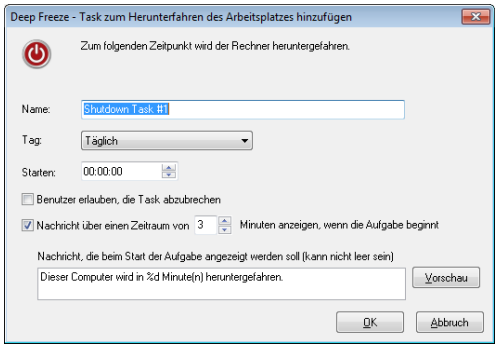
Im oben dargestellten Bildschirm wurde eine Arbeitsplatzaufgabe erstellt, der den Computer jeden Tag um Mitternacht neu startet. Diese Aufgabe ist so konfiguriert, dass dem Benutzer 1 Minute vor dem Neustart eine Nachricht angezeigt wird.

Herunterfahren

Die Aufgabe "Herunterfahren" kann über die folgenden Schritte geplant werden:



1. Wählen Sie *Herunterfahren* in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Tag – Wählen Sie den Tag aus, oder geben Sie an, ob die Aufgabe an Wochentagen oder an Wochenenden ausgeführt werden soll.
- Start – Wählen Sie die Startzeit aus.
- Benutzer erlauben, die Task abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen, bevor sie gestartet wird.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um eine Nachricht auf dem Computer anzuzeigen, bevor die Aufgabe startet. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein, die vor dem Start der Aufgabe angezeigt werden soll.

3. Klicken Sie auf OK.



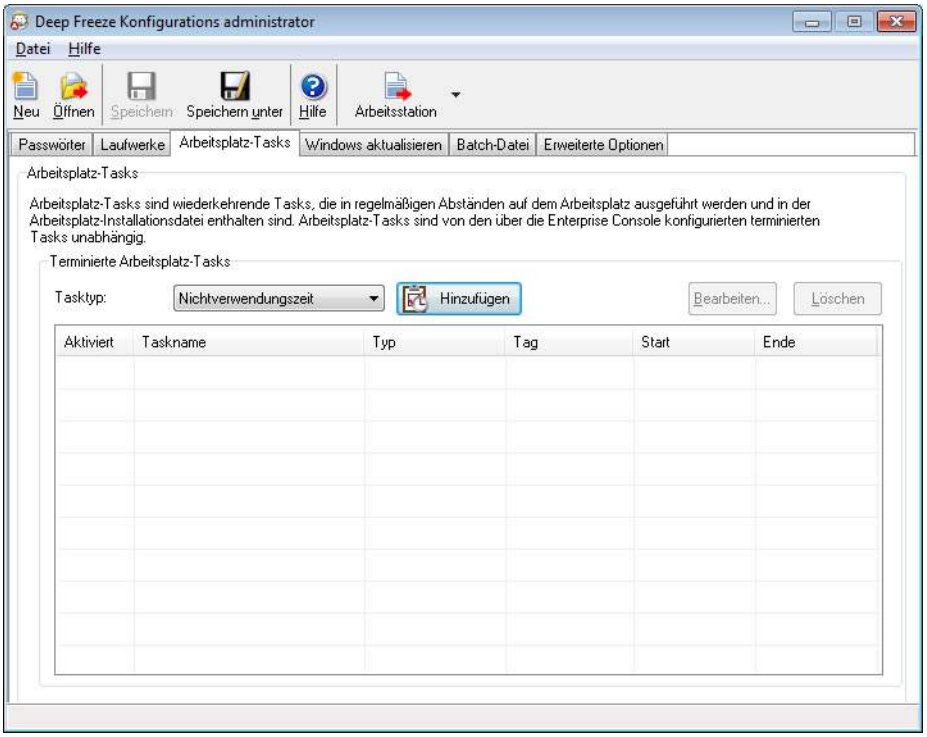
Die Nachricht *Dieser Computer wird in %d Sekunden heruntergefahren* wird im Feld *Nachricht, die vor der Aufgabe angezeigt werden soll* angezeigt. Diese Nachricht kann bearbeitet werden. Fügen Sie das Wort *Minuten* nach *%d* in die Nachricht ein, um das Wort "Minuten" in die Nachricht aufzunehmen.

Beispiel

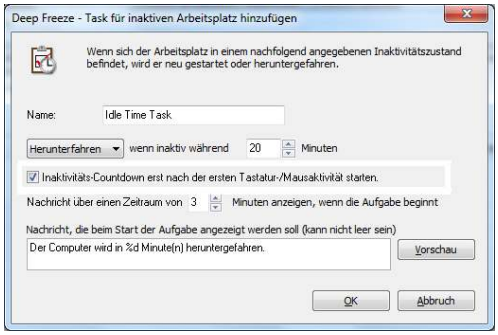
Im oben dargestellten Bildschirm wurde die Aufgabe "Herunterfahren" erstellt, der den Computer jeden Tag um Mitternacht herunterfährt. Diese Aufgabe ist so konfiguriert, dass dem Benutzer 1 Minute vor dem Herunterfahren eine Nachricht angezeigt wird.

Inaktivität

Die Aufgabe "Inaktivität" kann über die folgenden Schritte geplant werden:



1. Wählen Sie *Inaktivität* in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Neustart oder Herunterfahren – Wählen Sie *Neustart* oder *Herunterfahren* aus, und geben Sie die Inaktivität (in Minuten) an, nach der die Aufgabe ausgeführt wird.
- Inaktivitäts-Countdown erst nach der ersten Tastatur-/Mausaktivität starten – Diese Option ist nur für die Aufgabe „Herunterfahren" vorgesehen. Wählen Sie diese Checkbox aus, damit der Countdown des Timers erst nach der ersten Tastatur- oder Mausaktivität gestartet wird. Wenn die Inaktivitätszeit beispielsweise als 20 Minuten angegeben ist und diese Option ausgewählt wird, fährt die Arbeitsplatzaufgabe den Computer 20 Minuten nach der ersten Tastatur- oder Mausaktivität herunter.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um eine Nachricht anzuzeigen. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein.



Nachdem der Computer gestartet wurde, wird die Inaktivitätsmessung erst nach der ersten Tastatur- oder Mausaktivität eingeleitet. Während einer Remote Desktop-Sitzung wird die Messung der Inaktivitätszeit verwendet, um die Aufgabe zu aktivieren.

3. Klicken Sie auf OK.

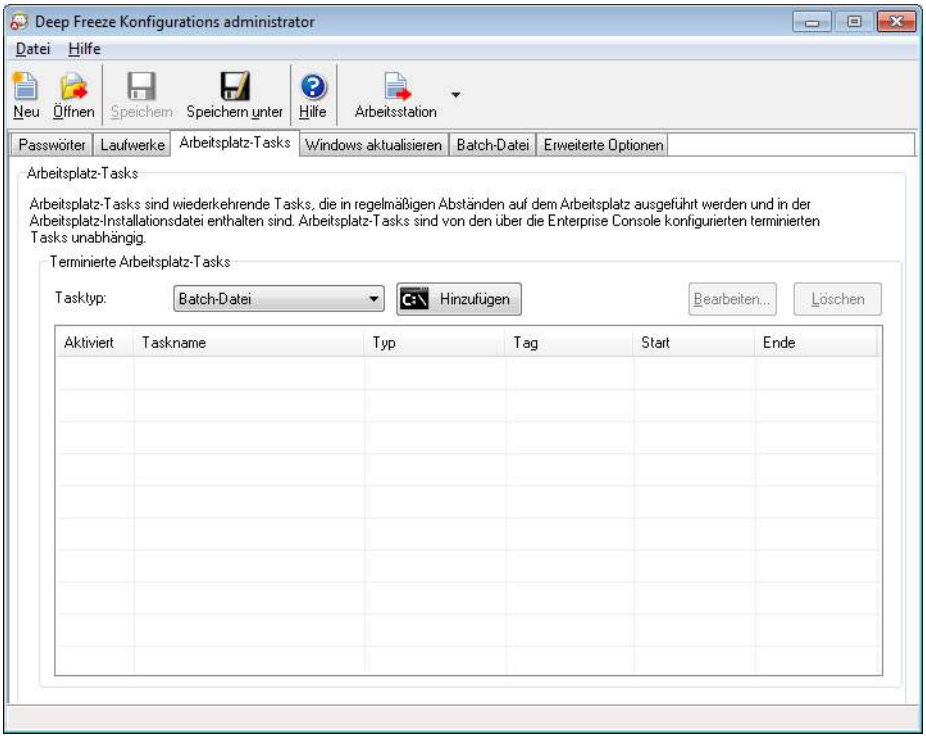
Beispiel

Im oben dargestellten Bildschirm wurde die Aufgabe "Inaktivität" auf *Neu starten* eingestellt, wenn der Computer 1 Minute lang inaktiv bleibt. Nach Ablauf der Inaktivitätszeit wird dem Benutzer 1 Minute lang eine Nachricht angezeigt. Wenn der Benutzer die Aufgabe nicht über den angezeigten Nachrichtendialog abbricht, wird der Computer neu gestartet.

Stapeldatei

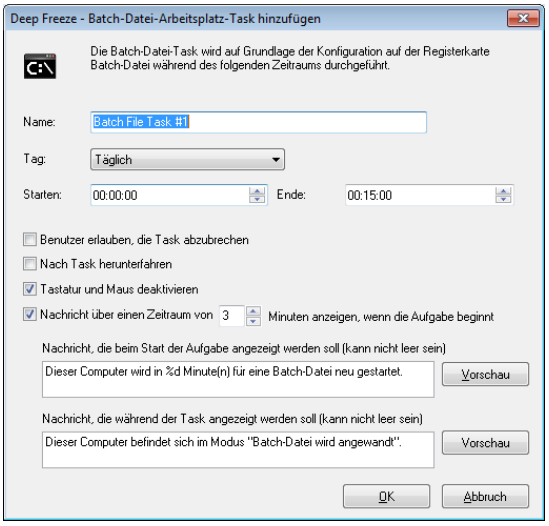
Stapeldateiaufgaben werden verwendet, um die Ausführung von Stapeldateien auf den einzelnen Arbeitsplätzen zu planen. Eine Stapeldateiaufgabe hat eine Start- und eine Endzeit. Während dieses Zeitraums wird die Stapeldatei auf dem Arbeitsplatz ausgeführt. Die müssen auf der Registerkarte "Stapeldatei" zusätzliche Einstellungen konfigurieren,

damit die Aufgabe "Stapeldatei" erfolgreich durchgeführt werden kann. Sie können den Arbeitsplatz so konfigurieren, dass er automatisch nach Beendigung der Stapeldateiaufgabe heruntergefahren wird. Nach Ausführung der Stapeldatei werden die Arbeitsplätze im Zustand *gefroren* neu gestartet.



Die Aufgabe "Stapeldatei" kann über die folgenden Schritte geplant werden:

1. Wählen Sie *Stapeldatei* in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Tag – Wählen Sie den Tag aus, oder geben Sie an, ob die Aufgabe an Wochentagen oder an Wochenenden ausgeführt werden soll.
- Start – Wählen Sie die Startzeit aus.

- Ende – Wählen Sie die Endzeit aus. Das kleinstmögliche Zeitintervall beträgt 15 Minuten.
- Benutzer erlauben, die Aufgabe abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen, bevor sie gestartet wird.
- Nach Aufgabe herunterfahren – Wählen Sie diese Checkbox aus, um den Computer nach Durchführung einer Aufgabe herunterzufahren.
- Tastatur und Maus deaktivieren – Wählen Sie diese Checkbox aus, um Tastatur und Maus während der Durchführung der Aufgabe zu deaktivieren.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um *vor* und *während* der Durchführung einer Aufgabe eine Nachricht auf dem Computer anzuzeigen. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein, die vor Beginn der Aufgabe angezeigt werden soll.

3. Klicken Sie auf OK.
4. Wechseln Sie zur Registerkarte "Stapeldatei", um zusätzliche Einstellungen zu konfigurieren.



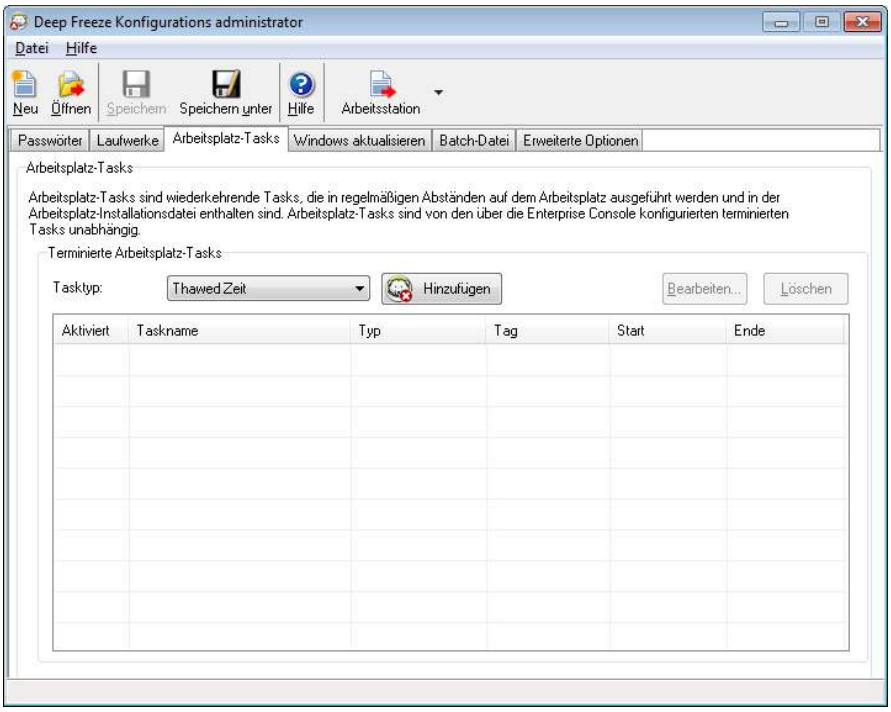
Die Nachricht *Dieser Computer wird in %d für eine Stapeldatei neu gestartet* wird im Feld *Nachricht, die vor der Aufgabe angezeigt werden soll* angezeigt. Diese Nachricht kann bearbeitet werden. Fügen Sie das Wort *Minuten* nach *%d* in die Nachricht ein, um das Wort "Minuten" in die Nachricht aufzunehmen.

Beispiel

Im oben dargestellten Bildschirm wurde ein Stapeldateiaufgabe erstellt, der jeden Tag zwischen 00:00 Uhr und 00:15 Uhr eine Stapeldateiaufgabe auf dem Computer durchführt. Diese Aufgabe ist so konfiguriert, dass dem Benutzer vor Ausführung der Stapeldatei eine Nachricht angezeigt wird. Tastatur und Maus sind deaktiviert.

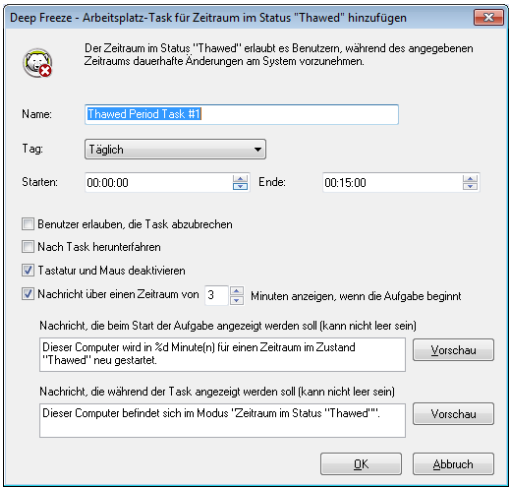
Zeitraum im Zustand "aufgetaut"

Diese Aufgabe wird verwendet, um einen Arbeitsplatz im Zustand "aufgetaut" neu zu starten. Ein Zeitraum im Zustand "aufgetaut" ist besonders nützlich für Anwendungen, die automatisch in regelmäßigen Abständen aktualisiert werden. Ein Zeitraum im Zustand "aufgetaut" ist außerdem für Administratoren nützlich, um Wartungsarbeiten zu planen und dauerhafte Änderungen an Computern vorzunehmen. Dabei kann zum Beispiel neue Software installiert bzw. bestehende Software aktualisiert werden, es können Änderungen an der Konfiguration vorgenommen oder andere Wartungsfunktionen ausgeführt werden. Ein Zeitraum im Zustand "aufgetaut" hat eine Start- und eine Endzeit.



Der Zeitraum im Zustand "aufgetaut" kann über die folgenden Schritte geplant werden:

1. Wählen Sie *Zeitraum im Zustand* "*aufgetaut*" in der Drop-Down-Liste *Aufgabenart* aus, und klicken Sie anschließend auf *Hinzufügen*.
2. Die folgenden Optionen werden angezeigt:



- Name – Geben Sie einen Namen für die Aufgabe an.
- Tag – Wählen Sie den Tag aus, oder geben Sie an, ob die Aufgabe an Wochentagen oder an Wochenenden ausgeführt werden soll.
- Start – Wählen Sie die Startzeit aus.
- Ende – Wählen Sie die Endzeit aus. Das kleinstmögliche Zeitintervall beträgt 15 Minuten.
- Benutzer erlauben, die Aufgabe abzubrechen – Wählen Sie diese Checkbox aus, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen, bevor sie gestartet wird.
- Versuchen, lokal hochzufahren – Wählen Sie dieses Markierungsfeld aus, um den

Arbeitsplatz lokal hochzufahren, ohne dass Kommunikation mit der Enterprise-Konsole erforderlich ist.



Ob der Arbeitsplatz lokal hochgefahren werden kann, hängt von den Hardware-Spezifikationen Ihres Arbeitsplatzes ab. Diese Option funktioniert nur, wenn sie von Ihrer Hardware unterstützt wird.

- Nach Aufgabe herunterfahren – Wählen Sie diese Checkbox aus, um den Computer nach Durchführung einer Aufgabe herunterzufahren.
- Tastatur und Maus deaktivieren – Wählen Sie diese Checkbox aus, um Tastatur und Maus während der Durchführung der Aufgabe zu deaktivieren.
- Nachricht anzeigen – Wählen Sie diese Checkbox aus, um *vor* und *während* der Durchführung einer Aufgabe eine Nachricht auf dem Computer anzuzeigen. Geben Sie das Zeitintervall in Minuten an, und geben Sie eine kurze Nachricht ein, die vor Beginn der Aufgabe angezeigt werden soll.

3. Klicken Sie auf OK.



Die Nachricht *Dieser Computer wird in %d für Wartungszwecke neu gestartet* wird im Feld *Nachricht, die vor der Durchführung der Aufgabe angezeigt werden soll* angezeigt. Diese Nachricht kann bearbeitet werden. Fügen Sie das Wort *Minuten* nach *%d* in die Nachricht ein, um das Wort "Minuten" in die Nachricht aufzunehmen.

Beispiel

Antivirus-Programme benötigen regelmäßige Updates der Virusdefinitionen, um das System schützen zu können. Virusdefinitionen können im Zustand "aufgetaut" aktualisiert werden.

In oben stehender Abbildung wird zum Beispiel täglich von 12:00 bis 12:15 der Computer in den Zustand "aufgetaut" versetzt. Der Benutzer kann die Aufgabe nicht abbrechen, bevor sie gestartet wird. Der Computer wird nach dem Wartungszeitraum heruntergefahren. Tastatur und Maus werden während des Wartungszeitraums deaktiviert. Diese Aufgabe ist so konfiguriert, dass dem Benutzer 5 Minute vor Start einer Aufgabe eine Nachricht angezeigt wird. Die folgende Nachricht wird um 11:55 Uhr auf dem Computer angezeigt: *Der Computer wird in 5 Minuten im Zustand "aufgetaut" neu gestartet*.

Um sicherzustellen, dass die Virusdefinitionen dauerhaft angewandt werden, sollten Sie die Aktualisierung der Virusdefinitionen für Ihr Antivirus-Programm so terminieren, dass sie beginnt, *nachdem* Deep Freeze erfolgreich den Zeitraum im Zustand "aufgetaut" gestartet hat, und *endet*, bevor Deep Freeze den Zeitraum im Zustand "aufgetaut" beendet. Hierdurch wird sichergestellt, dass die vom Antivirus-Programm heruntergeladenen und aktualisierten Virusdefinitionen dauerhaft im System bleiben. Somit wird das System durch Anti-Virus und Deep Freeze umfassend geschützt.

Faronics Anti-Virus: Faronics Anti-Virus funktioniert gemeinsam mit Deep Freeze und benötigt für die Aktualisierung der Virusdefinitionen keine Aufgabe zur Einrichtung eines Zeitraums im Zustand "aufgetaut". Faronics Anti-Virus kann Virusdefinitionen selbst dann aktualisieren, wenn sich die über Deep Freeze verwalteten Computer im Zustand *gefroren* befinden.

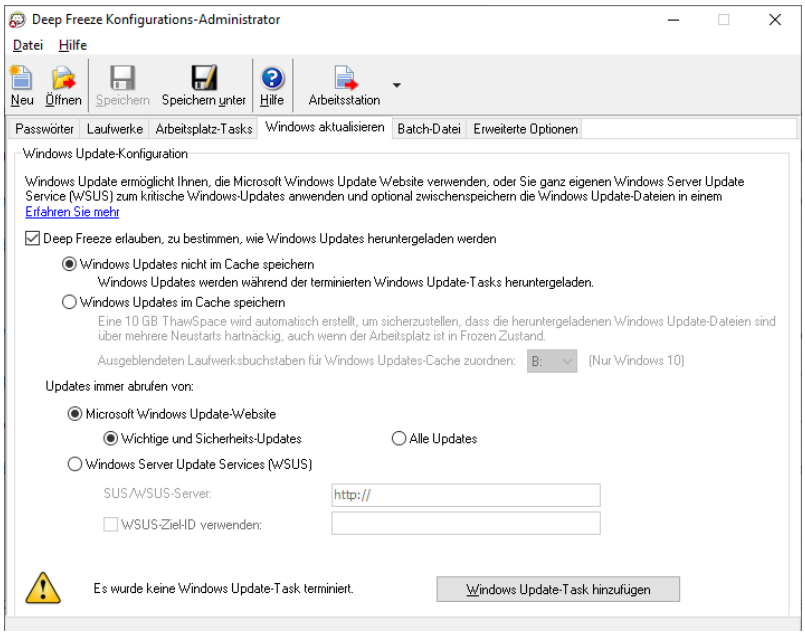


Andere Antivirus-Programme: Für alle anderen Antivirus-Programme wird zur Aktualisierung der Virusdefinitionen eine Aufgabe zur Einrichtung eines Zeitraums im Zustand "aufgetaut" benötigt. Für nähere Informationen über das Herunterladen von Virusdefinitionen ziehen Sie bitte das Benutzerhandbuch Ihres Antivirusprogramms zurate. Alternativ hierzu können Virusdefinitionen manuell angewandt werden, wenn sich die über Deep Freeze verwalteten Computer im Zustand *aufgetaut* befinden. Sie können auch eine Installation der neuesten Virendefinitionen *ohne Benutzereingriff* durch eine Stapeldateiaufgabe planen.

Registerkarte "Windows Update"

Die Registerkarte "Windows Update" dient zur Anpassung der Einstellungen für Windows Update. Wenn Sie zum ersten Mal eine Windows Update-Aufgabe erstellen, haben Sie die Option, die Standardeinstellungen in der Registerkarte "Windows Update" anzupassen. Eine Änderung der Standardeinstellungen ist nicht unbedingt erforderlich. Auch mit den Standardeinstellungen wird das Windows Update erfolgreich durchgeführt. Die Einstellungen auf der Registerkarte "Windows Update" werden für alle Windows Update-Aufgaben übernommen.

Die Einstellungen, die auf der Deep Freeze-Registerkarte "Windows Update" vorgenommen werden, haben Vorrang vor den Windows Update-Einstellungen der einzelnen Arbeitsplätze.



Die Einstellungen können folgendermaßen angepasst werden:

Deep Freeze erlauben, zu bestimmen, wie Windows Updates heruntergeladen werden: – Wählen Sie diese Checkbox aus, um es Deep Freeze zu erlauben, selbst zu bestimmen, wie Windows Updates heruntergeladen werden sollen. Die folgenden Optionen sind verfügbar:

- Wählen Sie die Download-Optionen für Windows Update aus:
  - Windows Updates nicht im Cache speichern – Wählen Sie diese Option aus, um Windows-Aktualisierungen ausschließlich im Rahmen der Windows Update-Aufgabe herunterzuladen.
  - Windows Updates im Cache speichern – Wählen Sie diese Option aus, um Aktualisierungen herunterzuladen, wenn sich der Arbeitsplatz im Zustand "gefroren" oder "aufgetaut" befindet, und diese dann über die Windows Update-Aufgabe zu installieren. Diese Option erstellt einen 10 GB großen

Auftauplatz, in dem Windows-Aktualisierungen gespeichert werden, um sicherzustellen, dass die Windows Update-Dateien auch bei mehreren Neustarts erhalten bleiben.

Nur für Windows 10-Systeme – Wenn die Option „Zwischenspeicherung von Windows-Updates" ausgewählt ist, ist die Dropdown-Liste für Laufwerksbuchstaben aktiviert. Wählen Sie in der Dropdown-Liste einen Laufwerksbuchstaben aus, um diesen als ausgeblendeten Laufwerksbuchstaben für den Windows Updates-Cache zuzuordnen. Der zugewiesene Laufwerksbuchstabe für den Windows Updates-Cache wird im Windows Explorer nicht sichtbar sein.



Der ausgeblendete Laufwerksbuchstabe ist auf den Arbeitsplätzen nicht sichtbar und steht nur für Windows 10-Systeme zur Verfügung.

- Updates immer abrufen von:
  - Microsoft Windows Update-Website – Wählen Sie diese Option, um Updates direkt von der Windows Update-Website herunterzuladen.

    Sie können bestimmen, ob nur *Wichtige und Sicherheits-Updates* oder *Alle Updates* heruntergeladen werden sollen.

    > Wichtige und Sicherheits-Updates – Wählen Sie diese Option aus, um nur kritische Updates, Sicherheits-Updates und Funktionsupdates herunterzuladen.



Wenn Sie die Option *Wichtige und Sicherheits-Updates* auswählen, installiert Deep Freeze auch verfügbare Funktionsupdates für Windows 10.

    > Alle Updates – Wählen Sie diese Option aus, um alle Updates herunterzuladen.

  - Windows Server Update Services (WSUS) – Wählen Sie diese Option aus, um Updates vom WSUS-Server herunterzuladen. Geben Sie den *SUS/WSUS-Server* an. Sie können auch *WSUS-Ziel verwenden* auswählen und dann das Ziel angeben. Der Microsoft SUS-Client und der SUS/WSUS-Server können unter folgender Adresse heruntergeladen werden: http://www.microsoft.com/wsus.

Pro Arbeitsplatz wird eine Protokolldatei erstellt, die lokal auf dem jeweiligen Arbeitsplatz gespeichert wird.

Der standardmäßige Name für die Deep Freeze Windows Update-Protokolldatei ist *DFWuLogfile.log*. Sie kann an folgendem Speicherort gefunden werden:

C:\Programme\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (auf 32-Bit-Systemen) und C:\Programme (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (auf 64-Bit-Systemen).



- Der Name und der Speicherort der Protokolldatei können vom Benutzer nicht geändert werden.
- Die Deep Freeze- und Windows Update-Protokolldateien (Speicherort c:\windows\windowsupdate.log) sind sehr nützlich für die Fehlersuche bezüglich Windows Updates.
- X ist ein inkrementeller Wert, der davon abhängt, wie oft Sie Deep Freeze bereits auf einem Arbeitsplatz installiert haben.

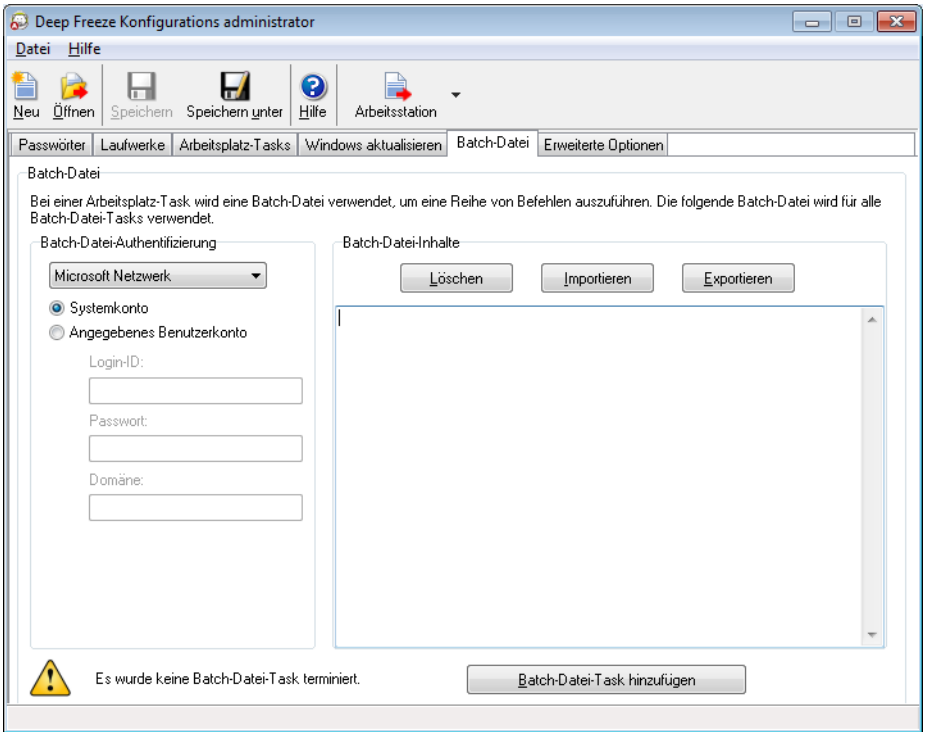
Wenden Sie sich bei Problemen mit der Datei DFWuLogfile.log an den technischen Support von Faronics (unter http://support.faronics.com).

Wenden Sie sich bei Problemen mit Windows Update an den technischen Support von Microsoft. (Siehe http://support.microsoft.com/kb/906602).

Siehe außerdem Microsoft KB 902093 *Interpretation der Windows Update-Protokolldatei* unter: http://support.microsoft.com/kb/902093/ oder besuchen Sie http://support.microsoft.com.

Registerkarte "Stapeldatei"

Die Registerkarte "Stapeldatei" dient zur Anpassungen der Einstellungen für Stapeldateiaufgaben. Wenn Sie eine Stapeldateiaufgabe über die Registerkarte "Arbeitsplatzaufgaben" planen, müssen Sie die Einstellungen auf der Registerkarte "Stapeldatei" konfigurieren.



Konfigurieren Sie die folgenden Einstellungen:

- Stapeldatei-Authentifizierung

  Wählen Sie Microsoft-Netzwerk aus, und geben Sie an, ob ein Systemkonto oder ein angegebenes Benutzerkonto verwendet werden soll. Wenn Sie ein angegebenes Benutzerkonto auswählen, geben Sie die Anmelde-ID, das Passwort und die Domäne an. Wählen Sie für Novell-Netzwerke die Option "Novell" aus, und geben Sie Anmelde-ID, Passwort, Baum, Kontext, und Server an.

  Die Standardkonfiguration unter Verwendung der Authentifizierung über das Microsoft-Netzwerk/Systemkonto muss vor der einer Verwendung alternativer Zugangsdaten getestet werden. Dieses Konto auf Maschinenebene ist häufig ausreichend, um die Aufgabe abzuschließen. Wenn die Stapeldatei einen Netzwerkzugriff auf sichere Ressourcen benötigt, muss möglicherweise ein spezielles Benutzerkonto verwendet werden.

- Stapeldatei-Inhalte

  Geben Sie eine benutzerdefinierte Stapeldatei ein, die während der Stapeldateiaufgabe ausgeführt werden soll. Die selbe Stapeldatei wird für alle Stapeldateiaufgaben verwendet. Die folgenden Optionen sind für die Ausführung benutzerdefinierter Stapeldateien verfügbar:

  - Klicken Sie auf *Löschen*, um die aktuelle Stapeldatei zu löschen

- Sie können eine vorhandene Datei laden, indem Sie auf *Importieren* klicken und zur Position der Datei navigieren.
- Sie können die Inhalte des Felds speichern, indem Sie auf *Exportieren* klicken und zur gewünschten Speicherposition wechseln.

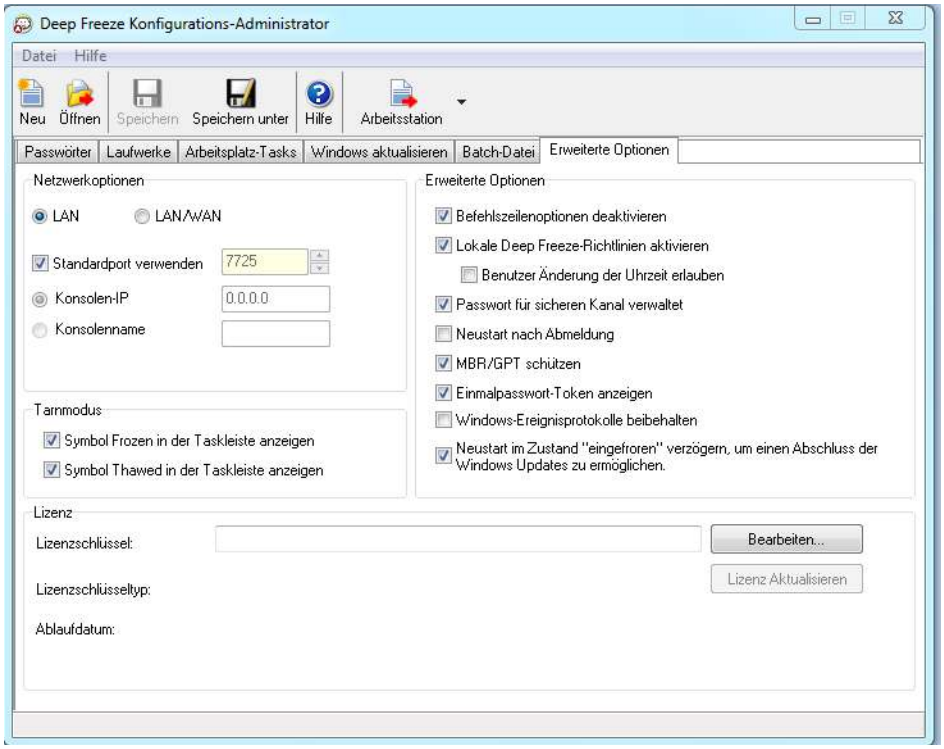
Bei der Stapeldatei kann es sich um einen beliebigen Befehl bzw. eine beliebige Serie von Befehlen handeln, die der Befehlsprozessor ausführen kann. Sie können benutzerdefinierte Scripts ausführen, die die Verwendung einer Scripting-Engine Dritter erfordern, indem Sie das Script aus der Stapeldatei heraus aufrufen, als würde es über die Befehlszeile ausgeführt.



Stapeldateien erlauben es Ihnen, VB-Scripts, PowerShell-Scripts, Ninite und andere Lösungen von Drittanbietern zu verwenden. Wenden Sie sich an Ihren Softwareanbieter oder lesen Sie im Benutzerhandbuch ihrer Drittlösung nach, wenn Sie Näheres über Scripting-Lösungen erfahren möchten, die Optionen *ohne Benutzereingriff* anbieten.

Registerkarte „Erweiterte Optionen“

Die Registerkarte „Erweiterte Optionen“wird verwendet, um die Netzwerkeinstellungen zu konfigurieren, die von den Computern verwendet werden, um mit der Konsole zu kommunizieren. Darüber hinaus werden diverse Sicherheitsoptionen konfiguriert und Lizenzschlüssel verwaltet.



Netzwerk

Für die Kommunikation zwischen der Deep Freeze Enterprise-Konsole und Computern, auf denen Deep Freeze installiert ist, können zwei unterschiedliche Modi verwendet werden: LAN-Modus oder LAN/WAN-Modus.

- LAN – Wählen Sie LAN aus, um Deep Freeze für eine Kommunikation innerhalb eines lokalen Netzwerks (Local Area Network, LAN) zu konfigurieren. Der LAN-Modus ist ein selbst konfigurierender Modus, für den nur eine Portnummer erforderlich ist. Der Standardport ist 7725. Die Portnummer kann geändert werden, wenn sie einen Konflikt mit anderen Programmen im LAN auslöst. Im LAN-Modus finden sich Deep Freeze-Zielcomputer und die Enterprise-Konsole durch UDP-Sammelaufrufe. Diese Sammelaufrufe finden nur statt, wenn Computer oder die Enterprise-Konsole gestartet sind, was sicherstellt, dass die Kommunikation zwischen den Zielcomputern und der Konsole nur geringen Datenverkehr im Netzwerk verursacht.
- LAN/WAN – Wählen Sie LAN/WAN aus, um Deep Freeze für eine Kommunikation sowohl innerhalb eines lokalen Netzwerks (Local Area Network, LAN) als auch innerhalb eines Fernnetzes (Wide Area Network, WAN) zu konfigurieren. LAN/WAN kann in entweder einer LAN- oder einer WAN-Umgebung verwendet werden, ebenso wie über das Internet. Dieser Modus verwendet eine IP-Adresse oder den

Computernamen zusammen mit einer Portnummer, um die Kommunikation zwischen der Konsole und den verwalteten Computern zu ermöglichen.

Die folgenden beiden Methoden sind verfügbar, um die Konsole zu identifizieren:

- Angabe der Konsolen-IP, die statisch sein muss
- Angabe des Konsolennamens, in welchem Fall die IP dynamisch sein kann (wenn als Teil der Domänenstruktur eine gültige DNS-Auflösung verfügbar ist).

Wenn sich die Enterprise-Konsole hinter einer Firewall oder einem NAT-Router (Network Address Translation-Router) befindet, muss die Firewall bzw. der Router so konfiguriert werden, dass Datenverkehr zur Enterprise-Konsole durchgelassen wird. In Abhängigkeit von der Firewall oder dem Router kann es erforderlich sein, Computer mit der IP-Adresse der Firewall zu konfigurieren, so dass Datenverkehr weitergeleitet werden kann.



Deep Freeze konfiguriert die erforderlichen Ausnahmen der Windows Firewall automatisch. Windows Firewall braucht nicht manuell konfiguriert werden.

Weitere Informationen über die Konfiguration und Verwendung von Deep Freeze in einer spezifischen Netzwerkumgebung finden Sie in Anhang B. Alternativ können Sie sich auch mit dem technischen Kundendienst in Verbindung setzen.

Wenn eine Portnummer verwendet wird, bei der es sich nicht um den Standardwert 7725 handelt (für Deep Freeze registriert), sollten Sie darauf achten, dass sichergestellt ist, dass keine Konflikte mit Anwendungen auftreten, die bereits auf dem Netzwerk laufen. Bekannte, häufig verwendete Ports (0–1023) sollten vermieden werden, und alle registrierten Ports (1024–49151) sollen vor Implementierung auf Konflikte überprüft werden.



Es wird empfohlen, Ports im nicht registrierten Bereich über 49152 zu verwenden. Sie können ein Labor oder ein Gebäude gemäß der Portnummer isolieren, indem Sie die Portsegementierung verwendet, und die entsprechende Portnummer an den Arbeitsplätzen und in der Deep Freeze Enterprise-Konsole konfigurieren. Durch diese Methode können Sie Verwaltungsfunktionen für eine bestimmte Arbeitsplatzgruppe, und nicht für die gesamte Organisation, festlegen. UDP- und TCP-Port-Ausnahmen müssen für diese Ports konfiguriert werden. Weitere Informationen hierzu finden Sie unter Beispiel 3 – Mehrere Ports, Fernzugriff auf Konsole.

Eine vollständige Liste der Ports, die verschiedenen Anwendungen zugeordnet sind, finden Sie auf der Website der Internet Assigned Numbers Authority unter http://www.iana.org/assignments/port-numbers.

Erweiterte Optionen

- Befehlszeilenoptionen deaktivieren – Diese Option ist standardmäßig ausgewählt. Durch Abwahl dieser Option wird eine weitere Anpassung des Deep Freeze-Installationsprogramms bei Verwendung des stillen Installationssystems ermöglicht. Die Auswahl dieser Option verhindert die Änderung vorher vorhandener Konfigurationsoptionen bei der Installation

- Lokale Deep Freeze-Richtlinien aktivieren – Zur Steigerung der Sicherheit entfernt Deep Freeze die folgenden lokalen Rechte: Debugging von Programmen, Änderung von Firmware und Änderung der Systemzeit; wählen Sie diese Option ab, um vorhandene Rechte zu nutzen.
- Benutzer Änderung der Uhrzeit erlauben – Wählen Sie diese Option aus, um es Benutzern eines Arbeitsplatzes im Zustand "gefroren" zu erlauben, die Systemuhr anzupassen. Aktivieren Sie diese Funktion während der Sommerzeit, um es Windows zu erlauben, die Zeit beim Wechsel zwischen Sommer- und Winterzeit automatisch zu aktualisieren.
- Passwort für sicheren Kanal verwalten – Das Passwort für den sicheren Kanal ist ein Element aller Windows-Betriebssysteme, das nur Anwendung findet, wenn das System in einer Windows Server-Domänenumgebung läuft. Das Passwort für den sicheren Kanal wird für eine sichere Kommunikation zwischen dem Server und den Arbeitsplätzen verwendet. Das Passwort für den sicheren Kanal wird automatisch auf Grundlage der Betriebssystemeinstellungen geändert. Bei der Verwendung von Deep Freeze geht ein geändertes Passwort für den sicheren Kanal beim Neustart verloren. Durch die Option *Passwort für sicheren Kanal verwalten* lässt sich diese Situation vermeiden. Die Deep Freeze-Funktion "Passwort für sicheren Kanal verwalten" verändert den Wert der Gruppenrichtlinie *Maximale Passwortgültigkeit des Maschinenkontos* auf Grundlage des Deep Freeze-Zustands (*gefroren* oder *aufgetaut*).
  - Wählen Sie die Option *Passwort für sicheren Kanal verwalten* aus, wenn Deep Freeze das Passwort für den sicheren Kanal verwalten soll.

    Wenn sich der Arbeitsplatz im Zustand "gefroren" befindet – Der Arbeitsplatz ändert das Passwort für den sicheren Kanal nicht. Hierdurch wird sichergestellt, dass eine sichere Kommunikation zwischen dem Server und dem Arbeitsplatz stets gewahrt wird.

    Wenn sich der Arbeitsplatz im Zustand "aufgetaut" befindet – Der Arbeitsplatz ändert das Passwort für den sicheren Kanal und synchronisiert das Passwort mit dem Server.
  - Wählen Sie die Option *Passwort für sicheren Kanal verwalten* nicht aus, wenn Deep Freeze das Passwort für den sicheren Kanal nicht verwalten soll.

    Wenn sich der Arbeitsplatz im Zustand "gefroren" befindet – Wenn das Passwort für den sicheren Kanal geändert und mit dem Server synchronisiert wird, wird das alte Passwort beim Neustart wiederhergestellt.

    Wenn sich der Arbeitsplatz im Zustand "aufgetaut" befindet – Wenn sich der Arbeitsplatz an dem Tag, an dem das Passwort für den sicheren Kanal geändert wird im Zustand *aufgetaut* befindet, wird das neue Passwort angenommen und der Arbeitsplatz mit dem Server synchronisiert.



Die Funktion "Passwort des sicheren Kanals verwalten" in Deep Freeze hat immer Vorrang vor der Gruppenrichtlinie *Maximale Passwortgültigkeit des Maschinenkontos*.

Richten Sie Folgendes in der Gruppenrichtlinie ein, damit die Funktion zur Verwaltung des Passworts des sicheren Kanals funktioniert:

Domänen-Controller: Passwortänderungen des Maschinenkontos ablehnen auf *Nicht definiert*

- Neustart nach Abmeldung – Wählen Sie diese Checkbox aus, um den Computer automatisch *neu zu starten*, wenn er abgemeldet wird. Wenn diese Option ausgewählt

ist, wird der Computer bei der Benutzerabmeldung im Zustand "gefroren" neu gestartet.

- MBR/GPT schützen – Markieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass der Master Boot Record durch Deep Freeze gesichert wird. Wenn diese Option ausgewählt ist, werden alle Änderungen am Master Boot Record bei jedem Neustart verworfen, wenn sich der Computer im Zustand *gefroren* befindet.
- Windows-Ereignisprotokolle beibehalten – Wählen Sie dieses Markierungsfeld aus, um Windows-Ereignisprotokolle beizubehalten. Deep Freeze erstellt einen Auftauplatz mit 100 MB und speichert alle Windows-Ereignisprotokolle, so dass diese beim Neustart nicht gelöscht werden, selbst wenn sich der Computer im Zustand „eingefroren" befindet. Die Protokolldatei wird recycelt, sobald sie eine Größe von 100 MB erreicht. Die Protokolldatei enthält Ereignisse, die sich auf Anwendungen, Hardware, das System und Sicherheit beziehen.
- Neustart im eingefrorenen Zustand verzögern, um Windows Updates abzuschließen – Wählen Sie diese Option aus, um einen Neustart im eingefrorenen Zustand zu verzögern, wenn im Rahmen einer Windows Update-Aufgabe noch Konfigurationen oder Installationsschritte für Windows Updates vorgenommen werden müssen. Wenn Sie diese Option auswählen und Windows-Updates (über einen anderen Mechanismus als Deep Freeze) durchführen, wird bei einem Neustart im eingefrorenen Zustand sichergestellt, dass sämtliche Installations- und Konfigurationsschritte für Windows Updates abgeschlossen werden, bevor ein Neustart im eingefrorenen Zustand erfolgt.



Wenn Sie *Neustart im eingefrorenen Zustand verzögern, um Windows Updates abzuschließen* auswählen und Deep Freeze installieren, prüft das Installationsprogramm, ob alle Windows Updates vollständig sind. Wenn die Windows Updates nicht vollständig sind, wird die Installation von Deep Freeze nicht fortgesetzt. Schließen Sie die Windows Updates ab, und versuchen Sie erneut, Deep Freeze zu installieren.

Wenn Sie die Option *Neustart im eingefrorenen Zustand verzögern, um Windows Updates abzuschließen* deaktivieren und Deep Freeze installieren, stellen Sie sicher, dass alle Windows Updates manuell durchgeführt werden. Wenn diese Option deaktiviert wird, kann dies zur Folge haben, dass der Computer aufgrund nicht abgeschlossener Windows Updates in einem Neustartzyklus hängenbleibt.

Beispiel

In einer Windows-Domänenumgebung mit Windows Server 2008 R2, der mehrere Arbeitsplätze verwaltet, wird das Passwort für den sicheren Kanal für die sichere Kommunikation zwischen dem Server und den Arbeitsplätzen verwendet.

Gehen Sie im Deep Freeze Enterprise-Konfigurationsadministrator auf die Registerkarte *Erweiterte Optionen*, und wählen Sie *Passwort für sicheren Kanal verwalten* aus. Erstellen Sie die Arbeitsplatzinstallationsdatei, und implementieren Sie sie auf dem Arbeitsplatz.

Richten Sie Folgendes in der Gruppenrichtlinie ein, damit die Funktion zur Verwaltung des Passworts des sicheren Kanals funktioniert:

Domänen-Controller: Passwortänderungen des Maschinenkontos ablehnen auf *Nicht definiert*

Domänenmitglied: Passwortänderungen des Maschinenkontos deaktivieren auf *Deaktiviert*

Wenn sich der Arbeitsplatz im Zustand „eingefroren“ befindet, wird das Passwort für den sicheren Kanal nicht verändert. Wenn sich der Arbeitsplatz im Zustand „aufgetaut“ befindet, wird das Passwort für den sicheren Kanal auf dem Arbeitsplatz geändert und mit dem Server synchronisiert.

Tarnmodus

- Symbol "gefroren" in der Taskleiste anzeigen – Wählen Sie diese Option aus, um das Symbol anzuzeigen, das angibt, dass Deep Freeze installiert ist und der Computer sich im Zustand "gefroren" befindet.
- Symbol "aufgetaut" in der Taskleiste anzeigen – Wählen Sie diese Option aus, um das Symbol anzuzeigen, das angibt, dass Deep Freeze installiert ist, der Computer sich jedoch im Zustand "aufgetaut" befindet.

Wenn die Optionen für die Anzeige eines Deep Freeze-Symbols in der Taskleiste nicht ausgewählt sind, muss der Tastaturbefehl STRG+ALT+UMSCHALTTASTE+F6 verwendet werden, um auf den Anmeldedialog zuzugreifen.

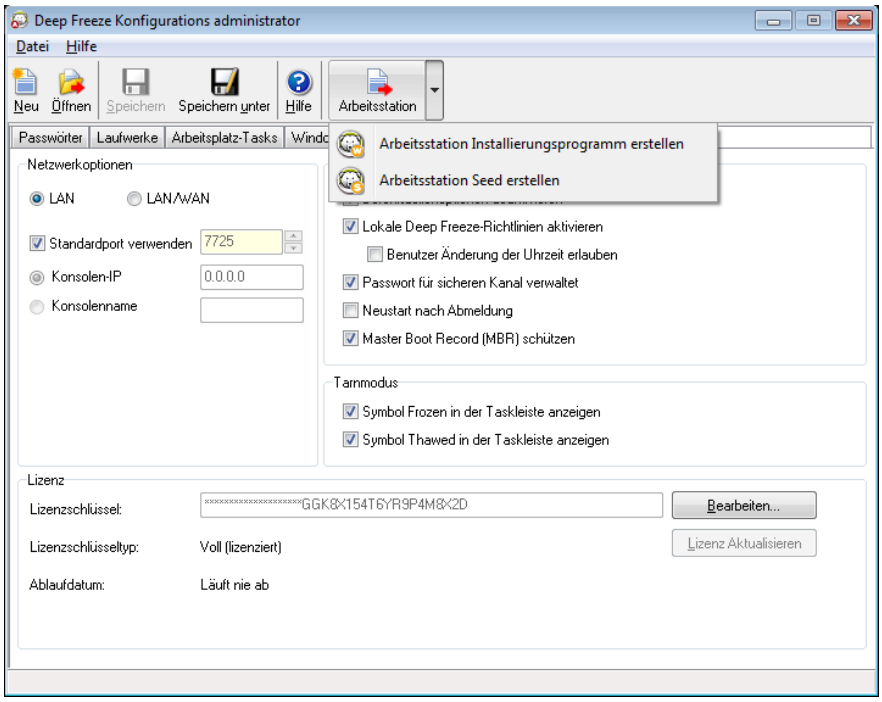
Lizenz

- Lizenzschlüssel – Klicken Sie auf Bearbeiten, und geben Sie den Lizenzschlüssel ein.
- Lizenzschlüsseltyp – Der Lizenzschlüsseltyp wird angezeigt. Dieses Feld zeigt an, ob es sich um eine Probe- oder eine Vollversion handelt.
- Ablaufdatum – Das *Ablaufdatum* für Deep Freeze wird angezeigt.

Sie haben die folgenden Möglichkeiten, den Lizenzschlüssel zu aktualisieren:

- Über die Arbeitsplatzinstallationsdatei – Der Lizenzschlüssel wird im Konfigurationsadministrator aktualisiert, und eine Arbeitsplatzinstallationsdatei wird erstellt. Der Lizenzschlüssel ist dann Teil der Arbeitsplatzinstallationsdatei.
- Über die Enterprise-Konsole – Der Lizenzschlüssel kann direkt über die Enterprise-Konsole aktualisiert werden. Wenn der Lizenzschlüssel in der Enterprise-Konsole aktualisiert wird, wird er automatisch auf allen verbundenen Computern aktualisiert. Weitere Informationen über die direkte Aktualisierung über die Enterprise-Konsole finden Sie im Abschnitt Lizenzen.
- Manuell auf jedem Computer – Der Lizenzschlüssel kann manuell auf jedem Computer einzeln aktualisiert werden. Weitere Informationen hierzu finden Sie im Abschnitt Registerkarte Status.

Arbeitsplatzinstallationsprogramm und Arbeitsplatz-Seed erstellen



Sie können angepasste Deep Freeze-Installationsprogrammdateien mit allen in den vorherigen Abschnitten konfigurierten Optionen erstellen, indem Sie in der Symbolleiste des Konfigurationsadministrators auf die Schaltfläche *Erstellen* klicken und *Arbeitsplatzinstallationsprogramm erstellen* auswählen.



Der Standarddateiname für dieses Programm ist DFWks.exe. Wie empfehlen Ihnen, diesen Namen beizubehalten; bei komplexeren Netzwerkstrukturen können Sie Ihm aber auch zusätzliche Buchstaben hinzufügen, die auf die Konfiguration des Programms hinweisen, z.B.: *DFwks_10gbThawSpace.exe* oder *DFWks_NoMaintenance.exe* oder *DFwks_Wed-5pmUpdates.exe* zur leichteren Organisation und Identifikation des Installationsprogramms und seiner Funktionen. Dieselbe Empfehlung gilt auch für *Deep Freeze-Konfigurationsdateien* (.rdx).

Diese Datei kann dann verwendet werden, um Deep Freeze auf Computern zu installieren. Hierfür sind folgende Optionen verfügbar:

- Überwachte Installation (Installation auf Basis von Benutzereingaben)
- Stilles Installationssystem – Installation, die den Benutzer nicht über den Fortschritt informiert und während der Installation keine Nachrichten bereitstellt. Für nähere Informationen zum Befehl "stille Installation", sehen Sie Stille Installation oder Deinstallation.

- Zielinstallation – Durch die Deep Freeze Enterprise-Konsole für Arbeitsplätze, die bereits ein Seed oder eine Vorgängerversion von Deep Freeze enthalten, die mit dem gleichen Anpassungscode erstellt worden ist.

Klicken Sie zur Erstellung eines Arbeitsplatz-Seeds in der Symbolleiste des Konfigurationsadministrators auf die Schaltfläche *Erstellen*, und wählen Sie *Arbeitsplatz-Seed erstellen* aus. Das Arbeitsplatz-Seed ist ein schlankes Programm, das es Administratoren erlaubt, Computer aus der Ferne über die Enterprise-Konsole zu installieren und zu steuern. Das Arbeitsplatz-Seed kann als Teil eines Master-Images installiert und dann über Imaging-Software implementiert werden. Alle Computer im LAN, auf denen das Arbeitsplatz-Seed installiert ist, werden in der Enterprise-Konsole angezeigt. Der Standarddateiname für dieses Programm ist *DFWksSeed.exe*.

Alle werden standardmäßig im Ordner *Deep Freeze Enterprise* > *Installationsprogramme* gespeichert. Es kann eine alternative Position ausgewählt werden, und der Dateiname kann bei Bedarf geändert werden. Um einen anderen Speicherort als standardmäßigen Speicherort einzurichten, wählen Sie den gewünschten Ort für die Speicherung von Installationsprogrammen und Arbeitsplatz-Seeds aus, und klicken Sie auf „Speichern". Aktivieren Sie das Kontrollkästchen Diesen *Ordner als Standardspeicherort festlegen*, wenn Sie dazu aufgefordert werden. Klicken Sie auf *OK*.

Es wird empfohlen, eine Namenskonvention zu verwenden, wenn Sie mehrere angepasste Installationsdateien erstellen.



Die Dateien *DFwks.exe*, *DFwksseed.exe* und *depfrz.rdx* können erstellt werden und (beliebig austauschbar) jedem Deep Freeze-Computer mit dem gleichen Anpassungscode bereitgestellt werden. Der Deep Freeze-Seed kann als Vorlage/Platzhalter verwendet werden, um sicherzustellen, dass grundlegende Elemente wie Passwörter, Netzwerkkonfiguration und standardisierte Arbeitsplatzaufgaben konsistent sind. Der Seed verwendet keine Konfigurationseinstellungen, speichert diese aber in der Datei. Um die Datei als Vorlage zu verwenden, öffnen Sie einfach *DFwksseed.exe* mit dem Konfigurationsadministrator und nehmen Sie die erforderlichen Änderungen vor. Um die Arbeitsplatzinstallation zu erstellen, klicken Sie dann auf *Arbeitsplatzinstallationsdatei* > *erstellen*.



Es wird empfohlen, die Verwendung des Konfigurationsadministrators in größeren Umgebungen aus Sicherheitsgründen einzuschränken. Um dies zu tun, können Sie den Deep Freeze-Administrator sichern oder Ihn unzugänglich machen, indem Sie die Datei DFadmin.exe aus dem Ordner *C:\Programme\Faronics\Deep Freeze Enterprise* entfernen. Diese Datei kann zum Beispiel auf den Arbeitsplatz des Domänenadministrators verschoben und von der Deep Freeze Enterprise-Konsole gelöscht werden. Um diese Datei wiederherzustellen, kann Sie aus einer andere Installation derselben Version des Programms wieder an den Zielort kopiert und durch das OTP-Passwort autorisiert werden, oder es kann Deep Freeze Enterprise mit dem gleichen Anpassungscode erneut installiert oder aktualisiert werden.



Deep Freeze Enterprise-Konsole verwenden

Dieses Kapitel beschreibt die Verwendung der Deep Freeze Enterprise-Konsole.

Themen

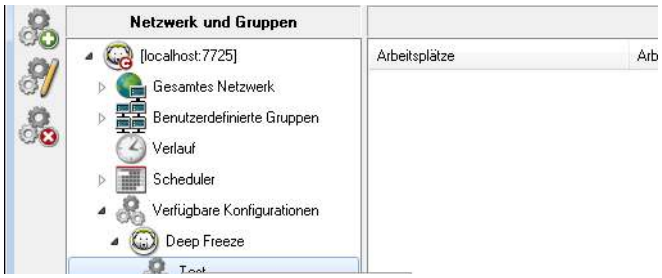
Deep Freeze-Konfiguration
Konfigurationsgenerator
Deep Freeze Enterprise-Konsole
Spalten anzeigen
Statusbasierte Auswahl
Die Kommunikation zwischen der Konsole und den Arbeitsplätzen verwalten
Remote-Konsolen
Verbindung zu einer Remote-Konsole herstellen
Deep Freeze mit der Konsole verwalten
Lizenzen
Deep Freeze-Aufgaben terminieren
Computer terminierten Tasks zuordnen
Netzwerk und Gruppen verwalten
Verlauf
Computer zu einer Gruppe hinzufügen
Benutzerdefinierte Aktionen konfigurieren
Konsolen-Customizer
Deep Freeze Enterprise-Konsole herunterfahren
Deep Freeze auf dem Arbeitsplatz installieren
Deep Freeze über die Konsole auf dem Arbeitsplatz installieren
Stille Installation oder Deinstallation
Nach Updates suchen

Deep Freeze-Konfiguration

Bei der Deep Freeze-Konfiguration handelt es sich um eine Gruppe von Einstellungen, die das Verhalten von Deep Freeze auf dem Arbeitsplatz definiert. Deep Freeze-Konfigurationen können über die Deep Freeze-Konsole erstellt und angewandt werden.

Führen Sie die folgenden Schritte aus, um eine Deep Freeze-Konfiguration zu erstellen:

1. Starten Sie die Deep Freeze-Konsole.
2. Gehen Sie auf *Netzwerk und Gruppen* > *Verfügbare Konfigurationen* > *Deep Freeze*.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Neue Konfiguration erstellen* aus.



4. Wählen Sie die Einstellungen auf den einzelnen Registerkarten aus bzw. geben Sie die entsprechenden Informationen an, wie unter Den Deep Freeze Enterprise-Konfigurationsadministrator verwenden beschrieben ist.
5. Geben Sie den Namen der Konfiguration an, und klicken Sie auf *OK*.
6. Optional können Sie in der Drop-Down-Liste *Exportieren als* > *Arbeitsplatz-Seed* oder *Exportieren als* > *Arbeitsplatz-Installationsdatei* auswählen, um die Konfiguration zu exportieren.
7. Klicken Sie auf *OK*.

Deep Freeze-Konfiguration anwenden

Nachdem eine Konfiguration erstellt wurde, kann sie auf mehrere Arbeitsplätze angewandt werden.

Führen Sie die folgenden Schritte aus, um die Deep Freeze-Konfiguration anzuwenden:

1. Wechseln Sie zum Teilfenster *Arbeitsplätze*.
2. Wählen Sie einen oder mehrere Arbeitsplätze aus.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Konfiguration aktualisieren* > *Deep Freeze* > *[Konfigurationsname]* aus.

Die Konfiguration wird auf den ausgewählten Arbeitsplatz bzw. die ausgewählten Arbeitsplätze angewandt.



Wenn Sie die Deep Freeze-Konfiguration für Passwörter, Arbeitsplatzaufgaben oder Neustart nach Abmeldung ändern und die Konfiguration anwenden, werden die Einstellungen sofort angewandt.

Wenn die Option *Bei Konfigurations-Update löschen* bei der Erstellung der Installationsdatei ausgewählt wurde, werden bestehende Auftauplätze und die Daten in den Auftauplätzen gelöscht, und die neuen Auftauplätze werden gemäß den Einstellungen erstellt, wenn die Konfiguration angewandt wird.

Alle anderen Einstellungen erfordern einen Neustart, bevor sie wirksam werden. Änderungen an *Befehlszeile deaktivieren* können durch die Anwendung von Konfigurationsänderungen nicht umgesetzt werden.

Deep Freeze-Konfiguration bearbeiten

Führen Sie die folgenden Schritte aus, um die Deep Freeze-Konfiguration zu bearbeiten:

1. Gehen Sie in der Enterprise Console zum Fenster Netzwerke und Gruppen.
2. Wählen Sie *Verfügbare Konfigurationen* > *Deep Freeze* > *[Konfigurationsname]* aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählte Konfiguration, und wählen Sie *Ausgewählte Konfiguration bearbeiten* aus.
4. Bearbeiten Sie die Einstellungen Ihren Anforderungen entsprechend.
5. Klicken Sie auf *OK*.

Deep Freeze-Konfiguration löschen

Führen Sie die folgenden Schritte aus, um die Deep Freeze-Konfiguration zu löschen:

1. Gehen Sie in der Enterprise Console zum Fenster Netzwerke und Gruppen.
2. Wählen Sie *Verfügbare Konfigurationen* > *Deep Freeze* > *[Konfigurationsname]* aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählte Konfiguration, und wählen Sie *Ausgewählte Konfiguration löschen* aus.
4. Klicken Sie auf *OK*.

Deep Freeze-Konfiguration exportieren

Führen Sie die folgenden Schritte aus, um die Deep Freeze-Konfiguration zu exportieren:

1. Gehen Sie in der Enterprise Console zum Fenster Netzwerke und Gruppen.
2. Wählen Sie *Verfügbare Konfigurationen* > *Deep Freeze* > *[Konfigurationsname]* aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählte Konfiguration, und wählen Sie *Exportieren als* aus.Es gibt drei Optionen:
   - Wählen Sie Arbeitsplatzinstallationsprogramm aus. Geben Sie einen Namen an, und klicken Sie auf *Speichern*.
   - Wählen Sie Arbeitsplatz-Seed aus. Geben Sie einen Namen an, und klicken Sie auf *Speichern*.
   - Wählen Sie Konfigurationsdatei aus. Geben Sie einen Namen an, und klicken Sie auf *Speichern*.

Konfigurationsgenerator

Deep Freeze Console bietet ein als Konfigurationsgenerator bezeichnetes Tool, um Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien auf der Basis der Parameter zu erstellen, die in einer CSV-Datei angegeben sind. Eine beispielhafte CSV-Datei wird bereitgestellt, die bearbeitet und auf eine unbegrenzte Anzahl von Einträgen ausgeweitet werden kann. Die Parameter für die Einstellungen in der CSV-Datei sind identisch mit den Einstellungen im Deep Freeze Enterprise-Konfigurationsadministrator. Der Spaltentitel der CSV-Datei stellt die jeweilige Einstellung dar, die Spalte stellt einen Eintrag für eine einzelne Deep Freeze-Konfigurations- bzw. Deep Freeze-Installationsdatei dar.

Führen Sie die folgenden Schritte aus, um über den Konfigurationsgenerator mehrere Deep Freeze-Installationsdateien zu erstellen:

1. Starten Sie die Deep Freeze-Konsole. Gehen Sie auf *Tools* > *Konfigurationsgenerator*. Alternativ hierzu können Sie diesen auch über den Deep Freeze Enterprise-Konfigurationsadministrator aufrufen, indem Sie auf *Datei* > *Konfigurationsgenerator* gehen.



2. Klicken Sie im Konfigurationsgenerator auf *Durchsuchen*.
3. Wählen Sie die Konfigurationsdatei (.csv-Datei) aus.
4. Klicken Sie auf *Generieren*.

Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien werden erstellt.

Wenn Sie den Konfigurationsgenerator das erste Mal verwenden, klicken Sie auf *Beispielhafte CSV-Datei*, um eine Vorlage der Datei herunterzuladen. Sie können die beispielhafte CSV-Datei mit den Werten aktualisieren, die für die Erzeugung der Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien benötigt werden. Es wird empfohlen, die Datei unter einem aussagekräftigeren Namen zu speichern.

Den Konfigurationsgenerator über die Befehlszeile verwenden

Sie können die Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien auch über die Befehlszeile erstellen. Starten Sie die Befehlszeile vom Deep Freeze-Installationsort, geben Sie die folgenden Parameter an, und drücken Sie die Eingabetaste:

32-Bit-Systeme:

```
[Systemlaufwerk]:\Programme\Faronics\Deep Freeze Enterprise\DFAdmin.exe
import [PFAD\Konfigurationsdatei.csv]
```

64-Bit-Systeme:

```
[Systemlaufwerk]:\Programme (x86)\Faronics\Deep Freeze
Enterprise\DFAdmin.exe import [PFAD\Konfigurationsdatei.csv]
```

Die Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien werden erzeugt und an der in der CSV-Datei angegebenen Position gespeichert.

Wenn Sie den Befehl im Synchronmodus ausführen, geben Sie den Befehl wie folgt an:

```
start /wait [Systemlaufwerk]:\Programme\Faronics\Deep Freeze
Enterprise\DFAdmin.exe import [PFAD\Konfigurationsdatei.csv]
```

Parameter der Konfigurationsdatei

Die folgende Tabelle erläutert die Parameter innerhalb der Konfigurationsdatei:

- Ändern Sie die Spaltenüberschriften nicht . Eine Änderung der Überschriften hat zur Folge, dass Deep Freeze die jeweiligen Zellwerte ignoriert. In diesem Fall werden die Standardwerte im Deep Freeze Enterprise-Konfigurationsadministrator verwendet.
- Fügen Sie für Parameter mit mehreren Einträgen mehrere Spalten hinzu. Passwörter, Auftauplätze, etc., können beispielsweise mehrere Spalten wie *Password1Enable, Password2Enable*, *ThawSpace1Drive*, *ThawSpace2Drive* haben.
- Wenn ein Eintrag leer gelassen oder eine ganze Spalte gelöscht wird, so wird der Standardwert im Deep Freeze Enterprise-Konfigurationsadministrator verwendet. Wenn die Pflichtfelder keine Werte enthalten oder wenn die Spalten, die Pflichtfelder darstellen, gelöscht werden, so werden keine Deep Freeze-Installations- bzw. Deep Freeze-Konfigurationsdateien erzeugt. Stattdessen wird eine Fehlermeldung erzeugt und in der Protokolldatei gespeichert. Klicken Sie im Konfigurationsgenerator auf den Link *Protokolldatei auf fehlerhafte Konfigurationen überprüfen*, um das Fehlerprotokoll aufzurufen.
- Verwenden Sie für den Namen des Parameters oder Werts kein Komma (,).
- Für Parameternamen und Werte braucht die Groß- und Kleinschreibung nicht beachtet zu werden.
- Felder, die ein Datum erfordern, verwenden das Format JJJJ/MM/TT.
- Felder, die die Uhrzeit erfordern, verwenden das Format hh:mm:ss (24-Stunden-Uhr).

Spalte / Parameter	Beschreibung
`FileName`	Geben Sie den Dateinamen sowie den Pfad an, an dem die Dateien gespeichert werden.

Spalte / Parameter	Beschreibung
`rdx`	Geben Sie 1 an, um die Deep Freeze-Konfigurationsdatei zu erzeugen. Geben Sie 0 an, um die Deep Freeze-Konfigurationsdatei nicht zu erzeugen.
`exe`	Geben Sie 1 an, um die Deep Freeze-Installationsdatei zu erzeugen. Geben Sie 0 an, um die Deep Freeze-Installationsdatei nicht zu erzeugen.
`Password1Enable`	Geben Sie 1 an, um Passwort 1 zu aktivieren. Geben Sie 0 an, um Passwort 1 zu deaktivieren.
`Password1Type`	Geben Sie Arbeitsplatz oder Befehlszeile an.
`Password1UserChange`	Geben Sie 1 an, wenn der Benutzer das Passwort ändern können soll. Geben Sie 0 an, wenn der Benutzer das Passwort nicht ändern darf.
`Password1`	Geben Sie das Passwort an.
`Password1TimeOut`	Geben Sie 1 an, wenn das Passwort zeitlich beschränkt ist. Geben Sie 0 an, wenn das Passwort zeitlich nicht beschränkt ist.
`Password1Activation`	Geben Sie das Datum der Passwortaktivierung an.
`Password1Expiration`	Geben Sie das Ablaufdatum des Passworts an.
`FrozenDrives`	Geben Sie die Buchstaben der Laufwerke im Zustand "eingefroren" in einer einzelnen Zeile an (Beispiel: CDEF).
`ThawSpace1Drive`	Geben Sie den Laufwerksbuchstaben für den Auftauplatz an.
`ThawSpace1Size`	Geben Sie die Größe des Auftauplatzes an.
`ThawSpace1SizeUnit`	Geben Sie an, ob als Einheit MB oder GB verwendet werden soll.
`ThawSpace1HostDrive`	Geben Sie den Host-Laufwerksbuchstaben für den Auftauplatz an.
`ThawSpace1Visibility`	Geben Sie 1 an, wenn der Auftauplatz sichtbar sein soll. Geben Sie 0 an, wenn der Auftauplatz nicht sichtbar sein soll.
`RetainExistingThawSpace`	Geben Sie 1 an, wenn der Auftauplatz beibehalten werden soll. Geben Sie 0 an, wenn der Auftauplatz gelöscht werden soll.
`HonorGPSettings`	Geben Sie 1 an, um Gruppenrichtlinieneinstellungen zu beachten. Geben Sie 0 an, um Gruppenrichtlinieneinstellungen nicht zu beachten.
`USB`	Geben Sie 1 an, um externe USB-Laufwerke im Zustand "aufgetaut" zu belassen. Geben Sie 0 an, um externe USB-Laufwerke im Zustand "eingefroren" zu belassen.
`FireWire`	Geben Sie 1 an, um externe FireWire-Laufwerke im Zustand "aufgetaut" zu belassen. Geben Sie 0 an, um externe FireWire-Laufwerke im Zustand "eingefroren" zu belassen.

Spalte / Parameter	Beschreibung
LAN_WAN	Geben Sie 1 an, wenn die Kommunikation zwischen dem Arbeitsplatz und der Deep Freeze Console im LAN-/WAN-Modus erfolgt. Geben Sie 0 an, wenn die Kommunikation zwischen dem Arbeitsplatz und der Deep Freeze Console nicht im LAN-/WAN-Modus erfolgt.
UseDefaultPort	Geben Sie 1 an, um den Standardport 7725 zu verwenden. Geben Sie 0 an, wenn der Standardport nicht verwendet werden soll.
Port	Geben Sie den Port an.
ConsoleIP_NAME	Geben Sie die Konsolen-IP, die statisch sein muss, oder den Namen an.
DisableCMD	Geben Sie 1 an, um die Befehlszeile zu deaktivieren. Geben Sie 0 an, um die Befehlszeile zu aktivieren.
EnableLocalPolicies	Geben Sie 1 an, um lokale Deep Freeze-Richtlinien zu aktivieren. Zur Steigerung der Sicherheit entfernt Deep Freeze die folgenden lokalen Rechte: Debugging für Programme durchführen, Firmware ändern und Systemzeit ändern. Geben Sie 0 an, um lokale Deep Freeze-Richtlinien zu deaktivieren.
AllowChangeClock	Geben Sie 1 an, um es Benutzern eines eingefrorenen Arbeitsplatzes zu erlauben, die Systemuhr anzupassen. Geben Sie 0 an, wenn Benutzer eines eingefrorenen Arbeitsplatzes die Systemuhr nicht anpassen dürfen.
ManageSCP	Geben Sie 1 an, um das Passwort für den sicheren Kanal zu verwalten. Geben Sie 0 an, um das Passwort für den sicheren Kanal zu deaktivieren.
RestartOnLogoff	Geben Sie 1 an, um den Arbeitsplatz beim Abmelden neu zu starten. Geben Sie 0 an, um den Neustart des Arbeitsplatzes beim Abmelden zu deaktivieren.
ProtectMBR	Geben Sie 1 an, um den Master Boot Record zu schützen. Geben Sie 0 an, wenn Deep Freeze den Master Boot Record nicht schützen soll.
ShowFrozenIcon	Geben Sie 1 an, um das Symbol "eingefroren" in der Taskleiste anzuzeigen. Geben Sie 0 an, um das Symbol "eingefroren" nicht in der Taskleiste anzuzeigen.
ShowThawedIcon	Geben Sie 1 an, um das Symbol "aufgetaut" in der Taskleiste anzuzeigen. Geben Sie 0 an, um das Symbol "aufgetaut" nicht in der Taskleiste anzuzeigen.
DelayFrozenReboot	Geben Sie 1 an, um den Neustart im Zustand "eingefroren" zu verzögern, um einen Abschluss der Windows Updates zu ermöglichen. Geben Sie 0 an, um die Verzögerung des Neustarts im Zustand "eingefroren" für einen Abschluss der Windows Updates zu deaktivieren.
BatchAuthentication	Geben Sie 1 für eine Massenauthentifizierung an. Geben Sie 0 für keine Massenauthentifizierung an.
UserAccount	Geben Sie 1 an, um ein Benutzerkonto zu verwenden. Geben Sie 0 an, um ein Systemkonto zu verwenden.
LoginID	Geben Sie die Anmelde-ID an.

Spalte / Parameter	Beschreibung
`Password`	Geben Sie das Passwort an.
`Domain`	Geben Sie die Domäne an.
`Tree`	Geben Sie die Baumstruktur an.
`Context`	Geben Sie den Kontext an.
`Server`	Geben Sie den Servernamen an.
`BatchFile`	Geben Sie die Inhalte der Stapeldatei an. Es wird nur 1 Zeile unterstützt.
`AllowWUDownload`	Geben Sie 1 an, um es Deep Freeze erlauben, zu bestimmen, wie Windows Updates heruntergeladen werden. Geben Sie 0 an, wenn Deep Freeze nicht bestimmen soll, wie Windows Updates herunterzuladen sind.
`CacheWU`	Geben Sie 1 an, um Windows Updates im Cache zu speichern. Geben Sie 0 an, wenn Windows Updates nicht im Cache gespeichert werden sollen.
`WSUS`	Geben Sie 1 an, um WSUS für Windows Updates zu verwenden. Geben Sie 0 an, wenn WSUS nicht für Windows Updates verwendet wird.
`UseWSUSTarget`	Geben Sie 1 an, um ein WSUS-Ziel zu verwenden. Geben Sie 0 an, wenn kein WSUS-Ziel verwendet werden soll.
`WSUSServer`	Geben Sie die URL für WSUS an.
`WSUSTarget`	Geben Sie das WSUS-Ziel an.
`Task1Enabled`	Geben Sie 1 an, um eine Arbeitsplatzaufgabe zu aktivieren. Geben Sie 0 an, um eine Arbeitsplatzaufgabe zu deaktivieren.
`Task1Type`	Geben Sie die Art der Aufgabe an – Neustart, Herunterfahren, Stapeldatei oder Windows Update.
`Task1Name`	Geben Sie den Namen der Aufgabe an.
`Task1Day`	Geben Sie den Tag an.
`Task1Start`	Geben Sie die Startzeit an.
`Task1End`	Geben Sie die Endzeit an.
`Task1AllowCancel`	Geben Sie 1 an, um es dem Benutzer zu erlauben, die Aufgabe abzubrechen. Geben Sie 0 an, wenn der Benutzer die Aufgabe nicht abbrechen darf.
`Task1ShutdownAfterTask`	Geben Sie 1 an, um den Arbeitsplatz nach der Aufgabe herunterzufahren. Geben Sie 0 an, wenn Deep Freeze den Arbeitsplatz nach der Aufgabe nicht herunterfahren soll.
`Task1DisableInput`	Geben Sie 1 an, um die Tastatur und die Maus zu deaktivieren. Geben Sie 0 an, wenn die Tastatur und die Maus nicht deaktiviert werden sollen.

Spalte / Parameter	Beschreibung
`Task1ShowMessageFor`	Geben Sie an, über wie viele Minuten hinweg die Nachricht angezeigt werden soll.
`Task1StartMessage`	Geben Sie die Nachricht an, die zu Beginn der Aufgabe angezeigt werden soll. Es wird nur 1 Zeile unterstützt.
`Task1DuringMessage`	Geben Sie die Nachricht an, die während der Aufgabe angezeigt werden soll. Es wird nur 1 Zeile unterstützt.

Deep Freeze Enterprise-Konsole

Die Deep Freeze Enterprise-Konsole zeigt den Status aller eingefrorenen und aufgetauten Computer, sowie der Zielarbeitsplätze im Netzwerk an, und ermöglicht es dem Administrator, spezifische Aufgaben auf diesen Computern auszuführen. Detaillierte Statusinformationen sind mit selektivem oder gruppiertem Berichtswesen verfügbar.

Die Enterprise-Konsole ermöglicht es Administratoren, die folgenden Aufgaben aus der Ferne durchzuführen:

- Sofort Zielinstallation auf Computern durchführen
- Einen oder mehrere Computer selektiv einfrieren, auftauen, oder aufgetaut sperren
- Ausgewählte Computer sperren oder entsperren
- Computer neu starten oder herunterfahren
- Terminierte Wartung stoppen
- Mit einer Wake-on-LAN-Netzwerkkarte ausgerüstete Arbeitsplätze hochfahren
- Deep Freeze-Software aktualisieren
- Tasks direkt über die Konsole terminieren
- Nachrichten an Computer senden
- Gruppen und Container aus Active Directory importieren
- Einmalige Passwörter generieren
- Aktionen terminieren
- Enterprise-Konsole anpassen
- Lizenzschlüssel aktualisieren

Die Enterprise-Konsole kann einen Computer im ausgeschalteten Zustand nur aufwecken, wenn der Computer entsprechend konfiguriert ist, um sich einzuschalten, wenn ein Wake-on-LAN-Paket empfangen wird.

Die Enterprise-Konsole starten

Die Enterprise-Konsole wird zusammen mit dem Deep Freeze Enterprise-Konfigurationsadministrator installiert. Öffnen Sie die Konsole, indem Sie den folgenden Pfad im Menü Start auswählen:

Start > *Programme* > *Faronics* > *Deep Freeze Enterprise* > *Deep Freeze -Konsole*

Die Enterprise-Konsole aktivieren

Als eine Sicherheitsfunktion von Deep Freeze Enterprise verhindert die OTP-Funktion eine unbefugte Nutzung der Deep Freeze Enterprise-Konsole. Wenn die Datei *DF6Console.exe* auf einen neuen Computer kopiert wird, muss die Konsole aktiviert werden. Wenn sie das erste Mal auf dem neuen Computer ausgeführt wird, wird ein Dialog mit einem OTP-Token angezeigt.

Der Netzwerkadministrator gibt diesen Token in das OTP-Generierungssystem des Konfigurationsadministrators ein. Ein OTP wird generiert. Geben Sie es in den Dialog ein, und die Konsole wird ausgeführt.

Der Computer, auf dem die Enterprise-Konsole installiert wird, darf nicht über eine Installation des Arbeitsplatz-Seeds (unter Verwendung desselben Ports) oder einer vollständigen Deep Freeze-Installation verfügen.

Statussymbole

Die Enterprise-Konsole zeigt den Status der Computer im lokalen Netzwerk an. In Abhängigkeit von der ausgewählten Ansicht werden die folgenden Symbole neben oder über dem Computernamen angezeigt:

Klassisches Erscheinungsbild	Modernes Erscheinungsbild	Definition
		Ziel: Computer, auf denen das Deep Freeze-Arbeitsplatz-Seed installiert ist, nicht jedoch Deep Freeze; auf Computern mit diesem Symbol kann Deep Freeze nur aus der Ferne installiert werden
		Computer, auf denen Deep Freeze installiert ist und die sich im Status „eingefroren“ befinden
		Computer, auf denen Deep Freeze installiert ist und die sich im Status „aufgetaut“ befinden
		Computer, auf denen Deep Freeze installiert ist und die sich im Status „aufgetaut und gesperrt“ befinden
		Computer, die derzeit ausgeschaltet sind
		Computer, die sich derzeit im Wartungsmodus befinden
		Computer, deren Kommunikation mit der Konsole unterbrochen wurde
		Gesperrte Computer

Klassisches Erscheinungsbild	Modernes Erscheinungsbild	Definition
		Computer, die sich über einen längeren als den in den Einstellungen für die Auftau-Warnmeldung definierten Zeitraum im Zustand „Thawed“ befinden
		Computer, die sich über einen längeren als den in den Einstellungen für die Auftau-Warnmeldung definierten Zeitraum im Zustand „Thawed und gesperrt“ befinden

Spalten anzeigen

Die Deep Freeze Enterprise Console bietet die Möglichkeit, die Spalten anzugeben, die im Teilfenster "Arbeitsplätze" angezeigt werden. Führen Sie die folgenden Schritte aus, um die gewünschten Spalten anzuzeigen:

1. Gehen Sie auf *Ansicht* > *Spalten*.
2. Wählen Sie die Spalten aus, die angezeigt werden sollen:
   - Konfiguration
   - Konfigurationsdatum
   - Ablaufdatum
   - Installationsdatei
   - IP-Adresse
   - Lizenzstatus
   - Anmeldename
   - MAC-Adresse
   - Betriebssystem
   - Port
   - Status
   - Aufgetaut seit
   - Freier Speicherplatz am Auftauplatz
   - Version
   - Arbeitsgruppe
   - Anti-Virus

Statusbasierte Auswahl

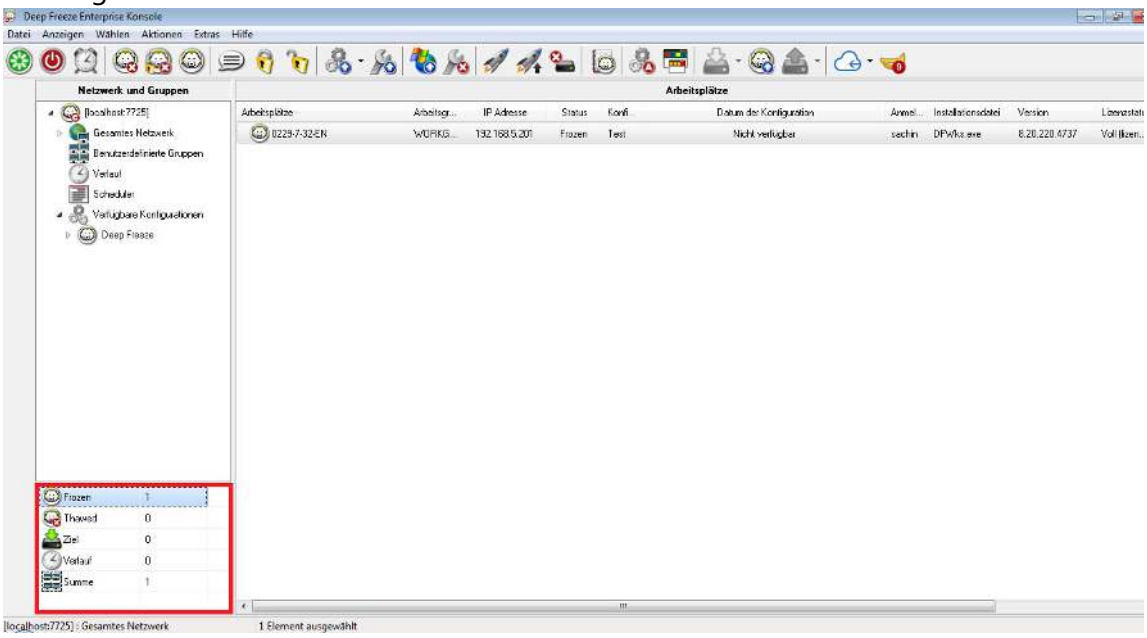
Sie können die Arbeitsplätze auf Basis des Deep Freeze-Status der verwalteten Arbeitsplätze auswählen. Die statusbasierte Auswahl erfolgt über das Menü *Auswahl* in der Deep Freeze Enterprise Console. Das Menü "Auswahl" bietet die folgenden Optionen:

- Alle im Zustand "eingefroren" auswählen – wählt die Arbeitsplätze aus, die sich im Zustand "eingefroren" befinden. Arbeitsplätze, die eingefroren und gesperrt sind, werden ebenfalls ausgewählt.
- Alle im Zustand "aufgetaut" auswählen – wählt die Arbeitsplätze aus, die sich im Zustand "aufgetaut" befinden. Arbeitsplätze, die aufgetaut und gesperrt sind, werden ebenfalls ausgewählt.
- Alle Ziele auswählen – wählt alle Zielcomputer aus, auf denen Deep Freeze installiert werden kann.
- Alle auswählen – wählt alle Arbeitsplätze aus.

Die folgenden Auswahloptionen sind auch über das Teilfenster "Status" verfügbar:

- Eingefroren – wählt die Arbeitsplätze aus, die sich im Zustand "eingefroren" befinden. Arbeitsplätze, die eingefroren und gesperrt sind, werden ebenfalls ausgewählt.
- Aufgetaut – wählt die Arbeitsplätze aus, die sich im Zustand "aufgetaut" befinden. Arbeitsplätze, die aufgetaut und gesperrt sind, werden ebenfalls ausgewählt.
- Ziele – wählt alle Zielcomputer aus, auf denen Deep Freeze installiert werden kann.
- Verlauf – zeigt den Verlauf an.
- Alle – wählt alle Arbeitsplätze aus.

Das Teilfenster "Status" der Deep Freeze Enterprise Console kann auch verwendet werden, um die Anzahl Arbeitsplätze für einen bestimmten Zustand auszuwählen und anzuzeigen.



Die Kommunikation zwischen der Konsole und den Arbeitsplätzen verwalten

Es gibt zwei Arten von Verbindungen von der Konsole zum Arbeitsplatz, bzw. von Konsole zu Konsole:

1. Lokale Verbindungen – Verbindungen, auf die nur die Enterprise-Konsole zugreifen kann, die als Host für diese Verbindungen fungiert.
2. Für Fernsteuerung aktivierte Verbindungen – Verbindungen, auf die sowohl über die Konsole zugegriffen wird, die als Host fungiert, als auch über andere Konsolen, die fern angebunden sind.



Der Server Service für Deep Freeze 6.5 führt keine automatische Aktualisierung des Server Service für Deep Freeze 6.4 oder niedriger durch. Beide Dienste können auf demselben Computer installiert werden, aber es kann immer nur ein Dienst auf einmal laufen.

Ein Computer kann aus den folgenden Gründen die Kommunikation mit der Konsole verlieren:

- Der Computer wird manuell ausgeschaltet oder wird ohne Warnung heruntergefahren
- Im Netzwerk ist ein starker Datenverkehr oder ein Ausfall zu verzeichnen
- Die Netzwerkeinstellungen des Computers werden geändert, um auf eine neue Konsole zu verweisen

In den meisten Fällen wird die Kommunikation mit dem Computer wiederhergestellt, wenn der Computer eingeschaltet wird, oder wenn die Bedingungen, die die Unterbrechung der Kommunikation ausgelöst haben, korrigiert werden. Es kann mehrere Minuten dauern, bis sich der Computer wieder mit der Konsole in Verbindung setzt und die Kommunikation wieder herstellt. Wenn die Kommunikation nicht wiederhergestellt werden kann, setzen Sie sich bitte mit dem Technischer Support in Verbindung, um Anweisungen für die Fehlerbehebung zu erhalten.

Den lokalen Dienst konfigurieren

Der lokale Dienst ist ein Dienst, der Verbindungen zu Computern einrichtet und aufrecht erhält.

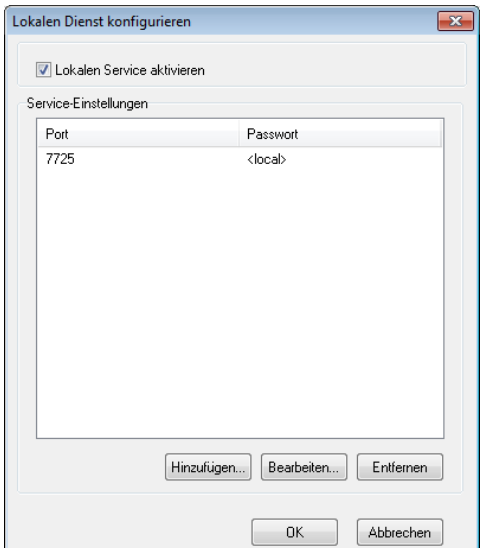
Den lokalen Dienst aktivieren

Der lokale Dienst wird standardmäßig installiert und aktiviert, wenn die Konsole das erste Mal ausgeführt wird.

Gehen Sie folgendermaßen vor, um den lokalen Dienst erneut zu aktivieren, wenn er deaktiviert (und/oder deinstalliert) wurde:

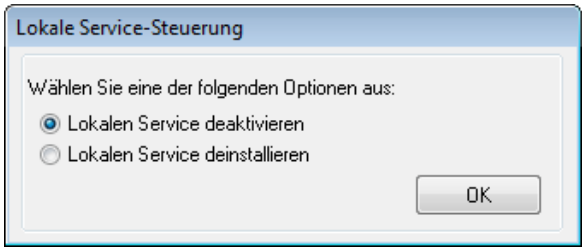
1. Wählen Sie *Tools* > *Netzwerkkonfiguration* aus.

2. Wählen Sie die Checkbox *Lokalen Dienst aktivieren* aus, um ihn zu aktivieren.



Den lokalen Dienst deaktivieren

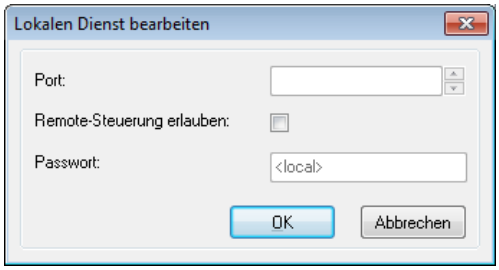
Wenn Sie die Markierung des Felds *Lokalen Dienst aktivieren* aufheben und auf *OK* klicken, wird die Option angezeigt, den lokalen Dienst entweder zu deaktivieren oder zu deinstallieren.



Eine Verbindung zu einem lokalen Dienst hinzufügen

1. Sie können eine Verbindung zu einem lokalen Dienst hinzufügen, indem Sie *Tools* > *Netzwerkkonfiguration* auswählen.
2. Um eine Verbindung hinzuzufügen, wählen Sie Hinzufügen aus, und geben Sie die Portnummer an (in diesem Fall *7725*).
3. Um die Konsole aus der Ferne steuern zu können, wählen Sie die Checkbox *Remote-Steuerung erlauben* aus, und geben Sie ein Passwort an.

Nachdem Sie *Hinzufügen* ausgewählt haben, wird in der Verbindungsliste des lokalen Diensts, sowie im Netzwerkfenster der Konsole eine Verbindung erstellt, die den Port *7725* bedient.



Eine Verbindung zu einem lokalen Dienst bearbeiten oder entfernen

Nachdem eine Verbindung zu einem lokalen Dienst hinzugefügt wurde, kann sie über die Option *Tools* > *Netzwerkkonfiguration* bearbeitet oder entfernt werden.

Führen Sie die folgenden Schritte aus, um eine Verbindung zu einem lokalen Dienst zu bearbeiten:

1. Stellen Sie sicher, dass die Option *Lokalen Dienst aktivieren* ausgewählt ist.
2. Wählen Sie einen Port aus der Liste von Verbindungen zu einem lokalen Dienst aus, und klicken Sie auf *Bearbeiten*.
3. Der Dialog Bearbeiten wird angezeigt, über den der Port aus der Ferne gesteuert und mit einem Passwort geschützt werden kann.
4. Um einen Port vom lokalen Dienst zu entfernen, wählen Sie den Port aus und klicken auf *Entfernen*. Hierdurch wird der Eintrag nicht aus dem Teilfenster *Netzwerk und Gruppen* in der Enterprise-Konsole gelöscht. Er wird lediglich aus der Verbindungsliste des lokalen Dienstes entfernt.
5. Um den Eintrag aus dem Netzwerkfenster in der Konsole zu entfernen, wählen Sie ihn aus, und klicken Sie auf das Symbol *Entfernen* in der Seitenleiste.

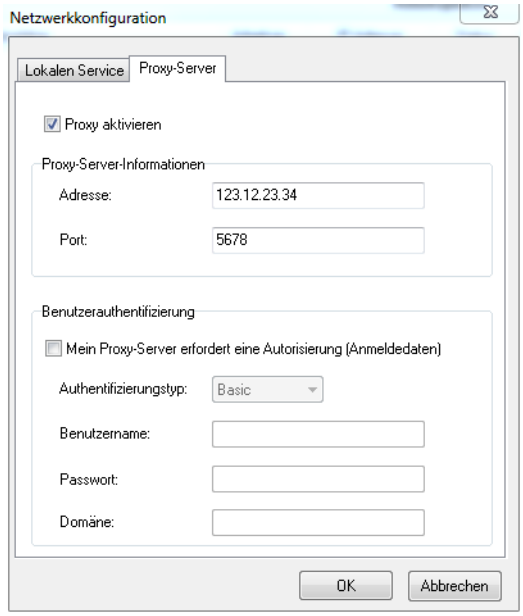
Die Proxy-Server-Verbindung konfigurieren

Wenn Sie für Verbindungen ins Internet einen Proxy-Server verwenden, müssen Sie die Proxy-Server-Einstellungen angeben, damit die folgenden Funktionen korrekt funktionieren:

- Nach Updates suchen
- Ankündigungen
- Lizenzaktivierung

Führen Sie die folgenden Schritte aus, um die Proxy-Server-Einstellungen anzugeben:

1. Wählen Sie *Tools* > *Netzwerkkonfiguration* aus.
2. Gehen Sie auf die Registerkarte "Proxy-Server".
3. Wählen Sie das Markierungsfeld *Proxy-Server aktivieren* aus, um diese Option zu aktivieren.



4. Geben Sie die folgenden Einstellungen für den Proxy-Server an:
   - Adresse – geben Sie die IP-Adresse des Proxy-Servers an.
   - Port – geben Sie die Portnummer für den Proxy-Server an.
5. Dieser Schritt ist optional. Führen Sie diesen Schritt nur dann aus, wenn Ihr Server eine Authentifizierung erfordert. Wählen Sie das Markierungsfeld *Mein Proxy-Server erfordert eine Autorisierung (Anmeldedaten)*aus, und geben Sie Werte für die folgenden Felder an:
   - Authentifizierungstyp – Wählen Sie den Authentifizierungstyp aus.
   - Benutzername – Geben Sie den Benutzernamen an.
   - Passwort – Geben Sie das Passwort an.
   - Domäne – Geben Sie die Domäne an.
6. Klicken Sie auf OK.

Remote-Konsolen

Eine Remote-Konsole ist eine Konsole, die als Host für eine oder mehrere Verbindungen fungiert, die es anderen Konsolen ermöglichen, eine durchgehende Verbindung herzustellen. Existierende Verbindungen müssen bearbeitet werden, so dass aus der Ferne auf diese zugegriffen werden kann.

Für Remote-Steuerung aktivierte Verbindungen einrichten

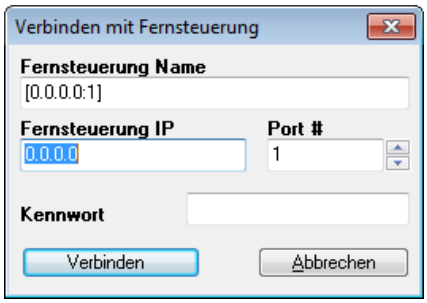
Führen Sie die folgenden Schritte aus, um eine Verbindung für einen Fernzugriff einzurichten:

1. Öffnen Sie *Tools* > *Netzwerkkonfigurationen*.
2. Wählen Sie die Checkbox *Lokalen Dienst aktivieren* aus.
3. Wählen Sie einen Port aus der Liste aus, und klicken Sie auf *Bearbeiten*.
4. Stellen Sie sicher, dass *Ferne Steuerung zulassen* ausgewählt ist.
5. Geben Sie ein Passwort an.
6. Klicken Sie auf *OK*.

Verbindung zu einer Remote-Konsole herstellen

Nachdem eine Remote-Konsole von der Host-Konsole eingerichtet wurde, kann von anderen Konsolen einer unterschiedlichen Maschine darauf zugegriffen werden.

1. Wählen Sie das Symbol *Verbindung zu Remote-Konsole herstellen* in der Seitenleiste aus, oder klicken Sie mit der rechten Maustaste auf das Netzwerkelement. Nach Auswahl wird der Dialog *Verbindung zu Remote-Konsole herstellen* angezeigt:



2. Geben Sie im Dialog *Verbindung zu Remote-Konsole herstellen* die Verbindungsdetails wie z.B. *Name der Remote-Konsole*, *IP der Remote-Konsole*, *Portnummer* und *Passwort* an. Diese Informationen werden vom Administrator der Host-Konsole bereitgestellt. Nachdem diese Informationen eingegeben wurden, können Sie abgerufen werden, indem Sie im Fenster *Netzwerk und Gruppen* mit der rechten Maustaste auf einen Port klicken und *Eigenschaften* auswählen.



Wenn die Verbindung zu einer Remote-Konsole unterbrochen wurde, kann die Verbindung durch einen Klick auf das Symbol *Verbindung zu Remote-Konsole wiederherstellen* in der Seitenleiste oder durch einen Rechtsklick auf einen Eintrag im Fenster *Netzwerk und Gruppen* wiederhergestellt werden.

Deep Freeze mit der Konsole verwalten

Die Enterprise Console enthält eine Symbolleiste am oberen Rand des Bildschirms, die einen schnellen Zugriff auf die Funktionen der Konsole ermöglicht.

Gehen Sie auf *Ansicht* > *Klassisches Erscheinungsbild*, um die Symbole im klassischen



Windows-Format anzuzeigen.

Gehen Sie auf *Ansicht* > *Modernes Erscheinungsbild*, um die Symbole im modernen Windows-Format anzuzeigen.



Auf diese Befehle kann, wie nachfolgend dargestellt, auch über das Kontextmenü zugegriffen werden, das angezeigt wird, wenn Sie mit der rechten Maustaste auf einen oder mehrere Computer klicken. Wenn eine bestimmte Aktion ausgewählt wird, führt der ausgewählte Computer diese Aktion aus, und die Statussymbole werden entsprechend aktualisiert. Wenn mehrere Computer ausgewählt werden, wird die Aktion nur auf die entsprechenden Computer angewandt. Wenn Sie beispielsweise Computer auswählen, die aufgetaut und eingefroren sind und die Aktion "Im Zustand „aufgetaut" neu starten" anwenden, werden nur die eingefrorenen Computer in den Zustand "aufgetaut" versetzt. Die Aktion wird nicht auf die Computer angewandt, die bereits aufgetaut sind.



Bestimmte Symbole sind deaktiviert, wenn der ausgewählte Computer diese Aktion nicht unterstützt. Ein Computer mit einem Symbol *Ziel* zeigt beispielsweise nicht die Option für ‚aufgetaut' oder ‚eingefroren' an, da das Programm noch nicht installiert wurde.

Eine vorgegebene Anzahl von Malen im Zustand „Thawed“/„Thawed und gesperrt“ neu starten

Sie können auswählen, dass ein Arbeitsplatz eine vorgegebene Anzahl von Malen im Zustand „Thawed“ oder „Thawed und gesperrt“ neu gestartet werden soll. Wenn diese Option ausgewählt wird, bleibt der Arbeitsplatz bei der vorgegebenen Anzahl von Neustarts im Zustand „Thawed“.

Führen Sie die folgenden Schritte aus:

1. Wählen Sie einen oder mehrere Arbeitsplätze aus.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie „Im Zustand „Thawed“ neu starten“ oder „Im Zustand „Thawed und gesperrt“ neu starten“ aus.
3. Wählen Sie die Option „Computer bei den nächsten X Neustarts in den Zustand „Thawed“ versetzen“ aus, und geben Sie die Anzahl der Neustarts vor.

   Wenn diese Option ausgewählt wird, wird der Arbeitsplatz bei der vorgegebenen Anzahl von Neustarts im Zustand „Thawed“ oder „Thawed und gesperrt“ neu gestartet.

   Wenn Sie beispielsweise „3“ als Anzahl von Neustarts vorgeben, bleibt der Arbeitsplatz bei den nächsten 3 Neustarts im Zustand „Thawed“ oder „Thawed und gesperrt“.

   Sie können den Arbeitsplatz maximal 99 Mal im Zustand „Thawed“ neu starten lassen.



Nachrichten an Computer senden

Führen Sie die folgenden Schritte aus, um eine Nachricht an einen oder mehrere Computer zu versenden:

1. Wählen Sie den bzw. die Computer aus, an die eine Nachricht versandt werden soll.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie im Kontextmenü *Nachricht senden* aus.
3. Geben Sie die Nachricht in den Dialog ein, der angezeigt wird, und klicken Sie auf *Senden*. Alternativ hierzu können Sie auch eine zuvor versandte Nachricht aus der Dropdown-Liste mit dem Verlauf senden. Ein Dialog wird angezeigt, der Sie auffordert, das Versenden der Nachricht an die ausgewählten Computer zu bestätigen.
4. Klicken Sie auf *OK*, um die Nachricht zu versenden, oder auf *Abbruch*, um den Dialog zu schließen, ohne die Nachricht zu versenden.

Eine Deep Freeze-Konfigurationsdatei aktualisieren

Führen Sie die folgenden Schritte aus, um die Konfiguration auf einem oder mehreren Computern mit den Einstellungen einer vorhandenen .rdx-Datei zu aktualisieren. (Eine .rdx-Datei ist eine Datei, die die Bedingungen enthält, die im Deep Freeze Enterprise-Konfigurationsadministrator angegeben sind.)

1. Klicken Sie mit der rechten Maustaste auf den oder die Computer, und wählen Sie *Mit RDX-Datei aktualisieren* aus.
2. Eine Nachricht wird angezeigt, die Sie dazu auffordert, eine vorhandene *.rdx*-Datei zu bestimmen.
3. Klicken Sie auf *OK*. Ein standardmäßiger Dialog *Datei Öffnen* wird angezeigt, in dem Sie eine .rdx-Datei aussuchen können.
4. Suchen Sie eine Datei, und klicken Sie auf *Öffnen*, um die Konfiguration auf dem ausgewählten Computer bzw. den ausgewählten Computern mit den Einstellungen der .rdx-Datei zu aktualisieren. Klicken Sie auf *Abbruch*, um die Aktualisierung der Konfiguration abzubrechen.

Windows Update ausführen

Windows Updates können bedarfsgerecht über das Kontextmenü angewandt werden.

Führen Sie die folgenden Schritte aus, um Windows Updates auf dem Arbeitsplatz auszuführen.

1. Klicken Sie mit der rechten Maustaste auf den oder die Computer, und wählen Sie *Windows Update ausführen* aus.
2. Klicken Sie auf *OK*.

Windows Updates werden auf den ausgewählten Arbeitsplatz bzw. die ausgewählten Arbeitsplätze angewandt. Die auf der Registerkarte Registerkarte "Windows Update" konfigurierten Einstellungen werden verwendet.

Windows Updates können nicht nur nach Bedarf über das Kontextmenü durchgeführt, sondern auch als Task terminiert werden. Nähere Informationen über die Planung einer Windows Updates-Aufgabe finden Sie unter Deep Freeze-Aufgaben terminieren.



Wenn die Netzwerkoptionen in der neuen Konfiguration geändert wurden, können die Computer die Kommunikation mit der vorhandenen Enterprise-Konsole verlieren. Wenn die Kommunikation mit den Computern unterbrochen wird, überprüfen Sie die Netzwerkeinstellungen der aktualisierten Computer, um sicherzustellen, dass sich die Portnummern und/oder die IP-Adresse der Konsole nicht geändert haben.



Änderungen an Passwörtern werden sofort wirksam. Alle anderen Änderungen werden wirksam, sobald ein Computer erneut gestartet wurde. Auftauplätze und/oder eingefrorene Laufwerke können durch die Aktualisierung der Konfigurationsdatei nicht geändert werden.

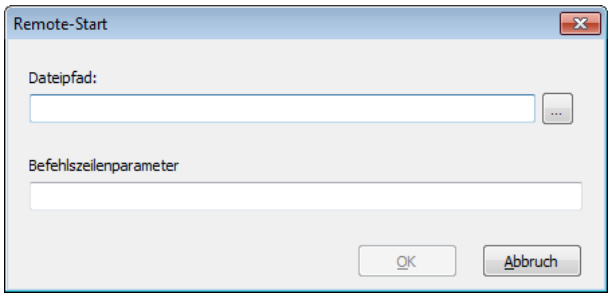
Remote-Ausführung

Diese Funktion erlaubt es IT-Administratoren, ausführbare Dateien auf verwalteten Arbeitsplätzen aus der Ferne auszuführen. Eine ausführbare Datei kann aus der Ferne auf mehreren von Deep Freeze verwalteten Arbeitsplätzen im Netzwerk installiert werden. Die Dateitypen .exe (ausführbare Dateien), .msi (MSI-Installationsdateien), .bat/.cmd Batch-Skript-Dateien), .vbs (VB script), und .ps1 (PowerShell). (werden unterstützt. Wenn eine MSI-Installationsdatei ausgewählt wird, führt Deep Freeze sie anhand von MSIEXEC aus.

Sie können auch eine Web-URL oder einen FTP-Speicherort für den Download und die Installation ausführbarer Dateien angeben. Die Datei wird automatisch vom angegebenen Speicherort heruntergeladen und auf dem Arbeitsplatz ausgeführt.

Führen Sie die folgenden Schritte aus, um ausführbare Dateien aus der Ferne auf Arbeitsplätzen auszuführen:

1. Sie haben die folgenden Möglichkeiten, um eine ausführbare Datei auf Arbeitsplätzen auszuführen:
   - Klicken Sie mit der rechten Maustaste auf einen oder mehrere Arbeitsplätze, und wählen Sie im Kontextmenü die Option *Remote-Ausführung* aus.
   - Über Deep Freeze-Aufgaben terminiert.
2. Geben Sie die Werte für die folgenden Felder an, oder wählen Sie als Alternative hierzu einen zuvor ausgewählten Wert aus der Dropdown-Liste mit dem Verlauf aus:



   - Dateiname und Pfad – geben Sie den Dateinamen und Pfad an, an dem sich die Datei auf dem Zielcomputer befindet. Alternativ hierzu können Sie auch blättern, um die ausführbare Datei auszuwählen. Oder geben Sie eine URL oder einen FTP-Speicherort an. Die Dateitypen .exe, .msi, .bat/.cmd, .vbs, und .ps1 werden unterstützt. MSI-Installationsdateien werden standardmäßig im Installationsmodus ausgeführt. Wenn die ausführbare Datei MeineAnwendung.exe beispielsweise unter C:/Anwendungsordner verfügbar ist, geben Sie *C:/Anwendungsordner/MeineAnwendung* an.
3. Geben Sie die Befehlszeilenparameter mit Umgebungsvariablen an (optional):
   - Argumente – geben Sie die Argumente an, die Sie mit dieser ausführbaren Datei anwenden möchten. Wenn die ausführbare Datei beispielsweise mit dem Befehl C:\Anwendungsordner\MeineAnwendung -o Protokolldatei.log über die Befehlszeilensteuerung ausgeführt wird, geben Sie als Argumente *-o Protokolldatei.log* an. Geben Sie für .msi-Dateien die Argumente an, die Sie normalerweise beim Start einer .msi-Datei mit MSIEXEC angeben würden. Wenn Sie für eine .msi-Datei kein Argument angeben, hängt Deep Freeze automatisch "/i" (installieren) an. Darüber hinaus ersetzt Deep Freeze bestehende Anzeigeoptionen mit /qn (still, keine UI).
4. Klicken Sie auf *OK*.

Die Datei wird auf den ausgewählten Arbeitsplätzen aus der Ferne ausgeführt.

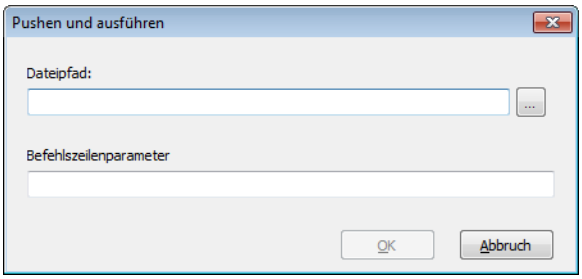
Pushen und ausführen

Diese Funktion erlaubt es IT-Administratoren, ausführbare Dateien auf verwaltete Arbeitsplätzen zu übertragen und dort auszuführen. Eine ausführbare Datei kann aus der Ferne auf mehreren von Deep Freeze verwalteten Arbeitsplätzen im Netzwerk installiert werden.

Sie können auch eine Web-URL oder einen FTP-Speicherort für den Download und die Installation ausführbarer Dateien angeben. Die Datei wird automatisch vom angegebenen Speicherort heruntergeladen und auf dem Arbeitsplatz ausgeführt.

Führen Sie die folgenden Schritte aus, um Dateien auf verwaltete Arbeitsplätze zu übertragen und dort auszuführen:

1. Sie haben die folgenden Möglichkeiten, um eine ausführbare Datei auf Arbeitsplätzen auszuführen:
   - Klicken Sie mit der rechten Maustaste auf einen oder mehrere Arbeitsplätze, und wählen Sie im Kontextmenü die Option *Pushen und ausführen* aus.
   - Über Deep Freeze-Aufgaben terminiert.
2. Navigieren Sie zum gewünschten Dateipfad oder geben Sie diesen an (oder wählen Sie als Alternative hierzu einen zuvor angegebenen Wert aus der Dropdown-Liste mit dem Verlauf aus):



   - Dateiname und Pfad – geben Sie den Dateinamen und Pfad an, an dem sich die Datei auf dem Konsolencomputer befindet. Alternativ hierzu können Sie auch blättern, um die ausführbare Datei auszuwählen. Oder geben Sie eine URL oder einen FTP-Speicherort an. Die Dateitypen .exe, .msi, .bat/.cmd, .vbs, und .ps1werden unterstützt. MSI-Dateien werden standardmäßig im Installationsmodus ausgeführt. Wenn die ausführbare Datei MeineAnwendung.exe beispielsweise unter C:/Anwendungsordner verfügbar ist, geben Sie *C:/Anwendungsordner/MeineAnwendung* an.
3. Geben Sie die Befehlszeilenparameter mit Umgebungsvariablen an (optional):
   - Argumente – geben Sie die Argumente an, die Sie mit dieser ausführbaren Datei anwenden möchten. Wenn die ausführbare Datei beispielsweise mit dem Befehl C:\Anwendungsordner\MeineAnwendung -o Protokolldatei.log über die Befehlszeilensteuerung ausgeführt wird, geben Sie als Argumente *-o Protokolldatei.log* an. Geben Sie für .msi-Dateien die Argumente an, die Sie normalerweise beim Start einer .msi-Datei mit MSIEXEC angeben würden. Wenn Sie für eine .msi-Datei kein Argument angeben, hängt Deep Freeze automatisch "/i" (installieren) an. Darüber hinaus ersetzt Deep Freeze bestehende Anzeigeoptionen mit /qn (still, keine UI).
4. Klicken Sie auf OK.

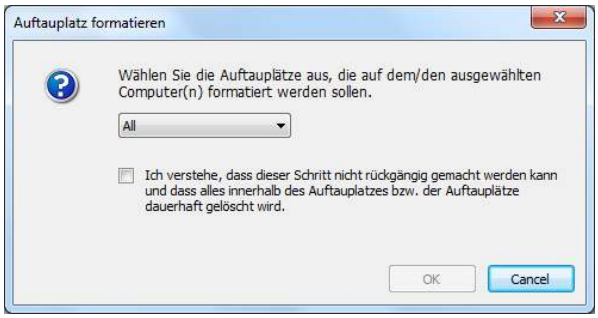
Die Datei wird auf den ausgewählten Arbeitsplatz übertragen und aus der Ferne auf den ausgewählten Arbeitsplätzen ausgeführt.

Auftauplatz formatieren

Die Deep Freeze Enterprise-Konsole bietet die Möglichkeit, einen bestimmten Auftauplatz oder alle Auftauplätze auf verwalteten Arbeitsplätzen zu formatieren.

Führen Sie die folgenden Schritte aus, um die Auftauplätze zu formatieren:

1. Wählen Sie einen oder mehrere Arbeitsplätze aus.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie *Auftauplätze* > *Auftauplatz formatieren* aus. Alternativ hierzu können Sie in der Symbolleiste auf das Symbol "Auftauplatz formatieren" klicken.
3. Der Dialog „Auftauplatz formatieren" wird angezeigt. Wählen Sie *Alle* aus, oder wählen Sie das Laufwerk aus, das formatiert werden soll.



4. Wählen Sie *Ich verstehe, dass dieser Schritt nicht rückgängig gemacht werden kann und dass alles innerhalb des Auftauplatzes bzw. der Auftauplätze dauerhaft gelöscht wird* aus.
5. Klicken Sie auf *OK*.

Der Befehl "Auftauplatz formatieren" löscht alle Daten der Auftauplätze. Die Daten können nach dem Löschen nicht wiederhergestellt werden. Erstellen Sie Sicherheitskopien wichtiger Dateien, bevor Sie den Auftauplatz formatieren.

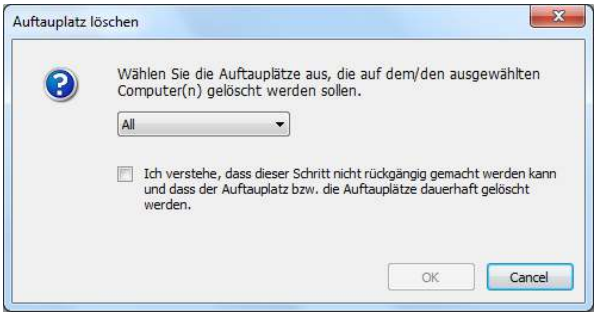
Auftauplatz löschen

Die Deep Freeze Enterprise-Konsole bietet die Möglichkeit, einen bestimmten Auftauplatz oder alle Auftauplätze auf verwalteten Arbeitsplätzen zu löschen.

Führen Sie die folgenden Schritte aus, um die Auftauplätze zu löschen:

1. Wählen Sie einen oder mehrere Arbeitsplätze aus.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie *Auftauplätze* > *Auftauplatz löschen* aus. Alternativ hierzu können Sie in der Symbolleiste auf das Symbol „Auftauplatz löschen" klicken.

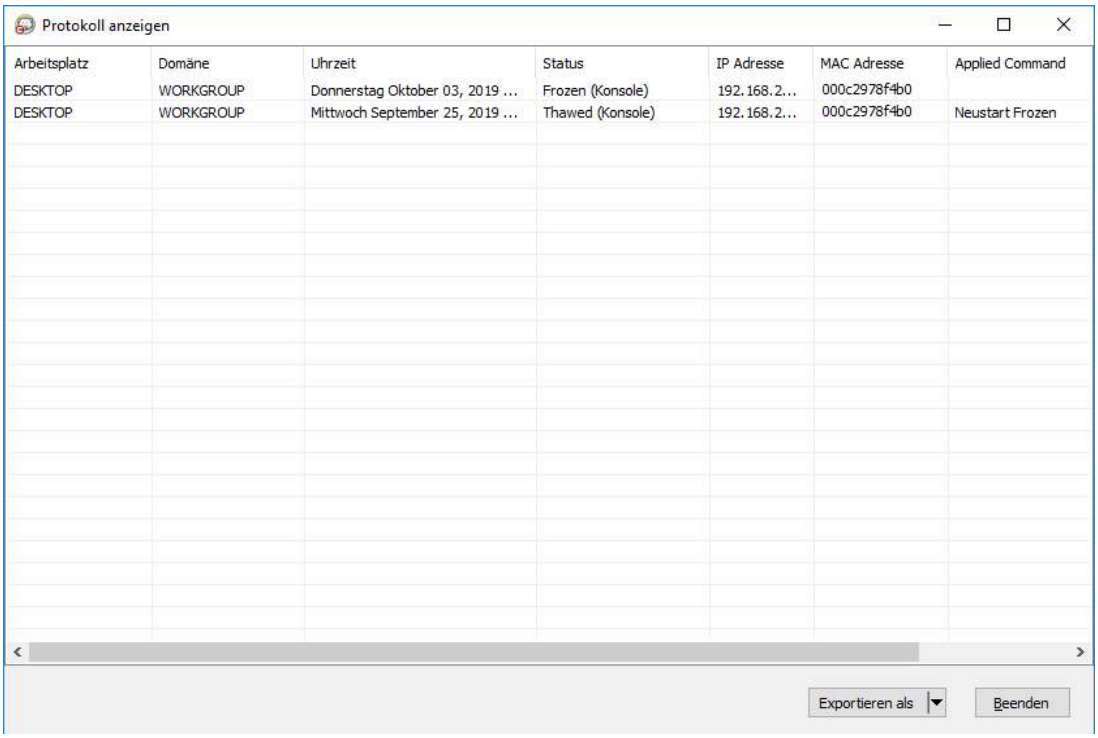
3. Der Dialog „Auftauplatz löschen" wird angezeigt. Wählen Sie *Alle* aus, oder wählen Sie das Laufwerk aus, das gelöscht werden soll.



4. Wählen Sie *Ich verstehe, dass dieser Schritt nicht rückgängig gemacht werden kann und dass der Auftauplatz bzw. die Auftauplätze dauerhaft gelöscht werden* aus.
5. Klicken Sie auf *OK*.

Die Konsolenprotokolldatei anzeigen

Die Enterprise Console führt ein Protokoll des Status- und Aktivitätsverlaufs aller verbundenen Computer. Das Protokoll speichert Informationen der letzten 7 Tage. Informationen, die älter als 7 Tage sind, werden automatisch aus dem Protokoll gelöscht.



- Um die Protokolldatei für einen oder mehrere Computer anzuzeigen, klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie *Protokoll anzeigen* aus.
- Sie können die Protokolldatei sortieren, indem Sie auf eine gewünschte Kopfzeile klicken. Die folgenden Spalten stehen zur Verfügung:
  - Arbeitsplatz
  - Domäne
  - Uhrzeit

- Status

  Die Spalte „Status“ zeigt den aktuellen Status des Computers sowie die Art und Weise an, in der der Computer neu gestartet wurde.

  Wenn der Computer beispielsweise über die Konsole im Zustand „Thawed“ neu gestartet wurde, wird als Status „Thawed (Konsole)“ angezeigt.
- IP-Adresse
- MAC-Adresse
- Angewandter Befehl (eingefroren, aufgetaut, neu starten, herunterfahren)
- Installationsdatei

- Sie können die Protokolldatei exportieren, indem Sie auf "Exportieren als" klicken, und "Text" oder "CSV" auswählen. Geben Sie den Namen der Datei an, und klicken Sie auf OK.

Zielinstallation von Deep Freeze

Führen Sie die folgenden Schritte aus, um eine vollständige Arbeitsplatzinstallation auf einem beliebigen Computer, auf dem ein Arbeitsplatz-Seed installiert ist, aus der Ferne durchzuführen.

1. Klicken Sie mit der rechten Maustaste auf einen oder mehrere Computer, und wählen Sie *Installieren* aus. Ein Dialog wird angezeigt, in dem Sie aufgefordert werden, die Installation zu bestätigen. Klicken Sie auf *OK*.
2. Ein Dialogfenster wird angezeigt, in dem Sie die Datei auswählen können, die auf dem Remote-Computer installiert werden soll.
3. Wählen Sie die Installationsdatei aus, die verwendet werden soll, und klicken Sie auf *Öffnen*.
4. Der Computer installiert Deep Freeze und wird neu gestartet.
5. Nach Abschluss der Installation gibt die Enterprise-Konsole die Änderung des Zustands des Computers wieder und zeigt diesen als *eingefroren* an.

Deep Freeze-Software aktualisieren

Führen Sie die folgenden Schritte aus, um Deep Freeze-Computer (auf denen Deep Freeze 7,7 oder höher installiert ist) mit einer neueren Version von Deep Freeze zu aktualisieren:

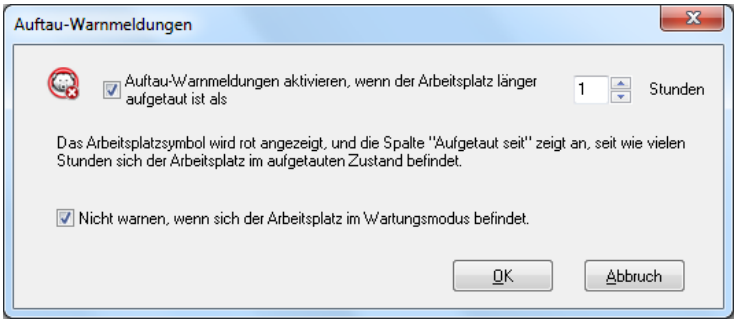
1. Wählen Sie in der Enterprise-Konsole die Computer aus, die aktualisiert werden sollen. Die Computer können sich entweder im Zustand "eingefroren" oder "aufgetaut" befinden.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie im Kontextmenü *Deep Freeze aktualisieren* aus.
3. Die ausgewählten Computer werden mit der neuen Version der Deep Freeze-Software aktualisiert, behalten jedoch alle Einstellungen der aktuellen Version bei. Die Computer werden zweimal neu gestartet, um die Aktualisierung abzuschließen.

Auftau-Warnmeldungen

Auftau-Warnmeldungen informieren den Administrator, wenn ein Computer über einen vorgegebenen Zeitraum hinweg im Zustand „aufgetaut" gelassen wurde. Die Deep Freeze Enterprise-Konsole zeigt das Arbeitsplatzsymbol rot an, und die Spalte *Aufgetaut seit* zeigt an, seit wie vielen Stunden sich der Arbeitsplatz im aufgetauten Zustand befindet.

Führen Sie die folgenden Schritte aus, um eine Auftau-Warnmeldung einzurichten:

1. Gehen Sie auf *Tools* > *Auftau-Warnmeldungen*.
2. Der Dialog „Auftau-Warnmeldung" wird angezeigt. Wählen Sie „Auftau-Warnmeldungen aktivieren, wenn der Arbeitsplatz länger als x Stunden aufgetaut ist" aus. Wählen Sie den Wert für x aus.



3. Wählen Sie *Nicht warnen, wenn sich der Arbeitsplatz im Wartungsmodus befindet* aus, wenn Sie nicht über Arbeitsplätze gewarnt werden wollen, bei denen gerade eine Wartung durchgeführt wird.
4. Klicken Sie auf *OK*.

Lizenzen

Der Lizenzschlüssel kann über die Deep Freeze Enterprise Console und aktualisiert werden, und die Workstation-Lizenzen können entweder automatisch oder manuell aktiviert werden.

Gehen Sie folgendermaßen vor, um die Workstation-Lizenzen für Deep Freeze automatisch zu aktivieren:

1. Starten Sie die *Deep Freeze Enterprise Console*.
2. Gehen Sie zu *Tools* > *Lizenzen*.
3. Der Dialog *Lizenzen* wird angezeigt.



4. Klicken Sie auf *Bearbeiten*, und geben Sie den Lizenzschlüssel in das Feld *Lizenzschlüssel* ein.
5. Klicken Sie auf *Lizenz aktualisieren*. Hierdurch wird Deep Freeze von einer *Probe*version in eine *lizenzierte* Version umgewandelt. Im Feld *Lizenzschlüsseltyp* wird der *Lizenzschlüssel* angezeigt. Das *Ablaufdatum* zeigt das Datum und die Uhrzeit an, zu der die Lizenz abläuft.

Deep Freeze aktiviert jede Arbeitsplatzlizenz automatisch über die Enterprise Console oder durch Herstellung einer direkten Verbindung zum Lizenzaktivierungsserver von Faronics.

Die Aktivierung Ihrer Produktlizenz ist erforderlich, um Ihre Kopie zu authentifizieren und ein Ablaufen des Produkts zu vermeiden. Deep Freeze-Arbeitsplätze, die nicht innerhalb von 30 Tagen aktiviert werden, können nicht in den Zustand "eingefroren" versetzt werden.

Sobald eine Internetverbindung verfügbar ist, stellt der Arbeitsplatz eine Verbindung entweder zur lokalen Konsole oder direkt zum Faronics-Aktivierungsserver her und überträgt bestimmte Informationen über Ihren Computer (u.a. Produktversion, Lizenzschlüssel, Rechner-ID, Version des Betriebssystems, MAC-Adresse, ID der CPU und ID des Konsolenrechners) an unsere sicheren Server.

Manuelle Aktivierung

Führen Sie zunächst die Schritte 1 bis 5 durch, um die Workstation-Lizenzen für Deep Freeze manuell zu aktivieren. Gehen Sie daraufhin folgendermaßen vor:

1. Klicken Sie auf *Jetzt aktivieren*. Es sind zwei Optionen verfügbar:



- Klicken Sie auf *Jetzt aktivieren*, um die Workstation-Lizenz für Deep Freeze über das Internet zu aktivieren. Die Lizenz für die Workstation wird durch Klicken auf *Weiter* aktiviert. Der Computer muss mit dem Internet verbunden sein, um eine Online-Aktivierung durchführen zu können.
- Wählen Sie *Offline aktivieren,* um die Deep Freeze-Workstation durch E-Mail oder Anruf an Faronics zu aktivieren. Klicken Sie auf *Weiter*. Der Bildschirm "Offline aktivieren" wird angezeigt.



2. Klicken Sie auf *Anforderungsdatei für Offline-Aktivierung erstellen* und dann auf *Speichern*. Senden Sie die Datei an activation@faronics.com, um eine Antwortdatei für die Aktivierung zu erhalten. Navigieren Sie zur *Antwortdatei für Aktivierung,* die Sie

von Faronics erhalten haben. Klicken Sie auf *Anforderungsdatei für Offline-Aktivierung anwenden*.



Der Lizenzschlüssel wird automatisch auf allen Computern aktualisiert, die mit der Enterprise-Konsole kommunizieren. Wenn ein Computer nicht erreicht werden kann (heruntergefahren oder vom Netzwerk getrennt), wird der Lizenzschlüssel aktualisiert, wenn der Computer mit der Enterprise Console kommuniziert.

Lizenzsymbol

Bei Workstations, deren Deep Freeze-Lizenzen noch nicht über den Faronics-Lizenzserver aktiviert worden sind, wird in der Symbolleiste ein Aktivierungssymbol angezeigt. Workstations können entweder online oder offline aktiviert werden.

Gehen Sie folgendermaßen vor, um die Workstations über das Aktivierungssymbol zu aktivieren.

1. Öffnen Sie das Dropdown-Menü durch Klicken auf das Aktivierungssymbol.



2. Wählen Sie *Alle Workstations online aktivieren*. Deep Freeze Console wird daraufhin den Faronics-Lizenzserver kontaktieren, um die Lizenzen zu aktivieren. Für die Online-Aktivierung ist eine Internetverbindung erforderlich.
3. Als Alternative können Sie auch die Option *Alle Workstations offline aktivieren* auswählen. Weitere Informationen über die Offline-Aktivierung finden Sie unter Manuelle Aktivierung.

Deep Freeze-Aufgaben terminieren

Deep Freeze Enterprise bietet zwei Arten von Deep Freeze-Aufgaben:

- Einzelaufgabe – enthält nur eine Deep Freeze-Aufgabe
- Kombinationsaufgabe – kann bis zu 5 Deep Freeze-Aufgaben für bis zu 20 Stunden enthalten. Eine Kombinationsaufgabe kann nicht sofort ausgeführt werden, sie kann nur terminiert werden.

Führen Sie die folgenden Schritte aus, um eine einzelne Deep Freeze-Aufgabe in der Enterprise-Konsole über den Assistenten für terminierte Aufgaben zu terminieren:

1. Öffnen Sie den *Assistenten für terminierte Aufgaben* auf eine der folgenden Arten:
   - Klicken Sie im Fenster *Netzwerk und Gruppen* auf *Scheduler*, und klicken Sie auf das Symbol *Aufgabe hinzufügen*
   - Klicken Sie im Fenster *Netzwerk und Gruppen* mit der rechten Maustaste auf *Scheduler*, und wählen Sie *Aufgabe hinzufügen* aus

Der folgende Bildschirm wird angezeigt:



2. Klicken Sie doppelt auf die gewünschte Aufgabe, oder wählen Sie die Aufgabe aus, und klicken Sie auf *Weiter*. Die folgenden Aufgaben sind für Deep Freeze verfügbar:
   - Neustart
   - Herunterfahren
   - Wake-On-LAN
   - Im Zustand „eingefroren" neu starten
   - Im Zustand „aufgetaut" neu starten
   - Im Zustand „aufgetaut und gesperrt" neu starten
   - Nachricht senden
   - Windows Updates ausführen
   - Remote-Ausführung

- Pushen und ausführen
- Aktualisieren
- Auftauplatz formatieren

3. Geben Sie im folgenden Bildschirm einen Namen für die Aufgabe ein, und wählen Sie den gewünschten Ausführungszeitplan für die Aufgabe aus: Täglich, Wöchentlich, Monatlich oder Nur einmalig. Aufgabennamen müssen eindeutig sein. Zwei Aufgaben dürfen nicht denselben Namen haben. Klicken Sie auf *Weiter*.



4. In Abhängigkeit von der ausgewählten Aufgabenausführung werden im Anschluss unterschiedliche Konfigurationsoptionen für Zeit und Datum angeboten. Klicken Sie auf *Weiter*.



5. Klicken Sie auf *Fertig stellen*, wenn die Konfiguration abgeschlossen ist.





Die Standardzeit für eine Task ist fünf Minuten nach der aktuellen Zeit.

Führen Sie die folgenden Schritte aus, um eine Kombinationsaufgabe in der Enterprise-Konsole über den Assistenten für terminierte Aufgaben zu terminieren:

1. Öffnen Sie den *Assistenten für terminierte Aufgaben* auf eine der folgenden Arten:
   - Klicken Sie im Fenster *Netzwerk und Gruppen* auf *Scheduler*, und klicken Sie auf das Symbol *Aufgabe hinzufügen*
   - Klicken Sie im Fenster *Netzwerk und Gruppen* mit der rechten Maustaste auf *Scheduler*, und wählen Sie *Aufgabe hinzufügen* aus

Der folgende Bildschirm wird angezeigt:



2. Wählen Sie „Kombinationsaufgabe“ aus, und klicken Sie auf *Weiter*.

3. Geben Sie im folgenden Bildschirm einen Namen für die Aufgabe ein, und wählen Sie den gewünschten Ausführungszeitplan für die Aufgabe aus – Täglich, Wöchentlich, Monatlich oder Nur einmalig. Aufgabennamen müssen eindeutig sein. Zwei Aufgaben dürfen nicht denselben Namen haben. Klicken Sie auf *Weiter*.



4. In Abhängigkeit von der ausgewählten Aufgabenausführung werden im Anschluss unterschiedliche Konfigurationsoptionen für Zeit und Datum angeboten. Klicken Sie auf *Weiter*.



5. Wählen Sie die Aufgabe aus der Dropdown-Liste aus, und geben Sie die Zeit an. Klicken Sie auf das „+"-Zeichen, um eine weitere Aufgabe hinzuzufügen. Wiederholen Sie den Prozess, um bis zu 5 Aufgaben für maximal 20 Stunden hinzuzufügen. Klicken Sie auf *Weiter*.



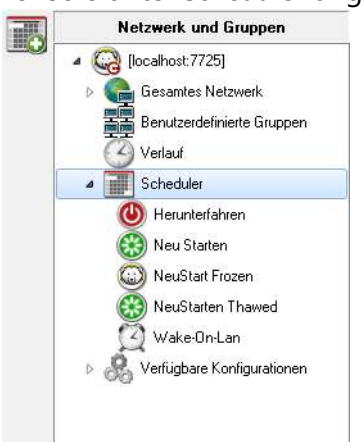
6. Prüfen Sie die Liste der Aufgaben, und klicken Sie auf *Fertig stellen*.

Geplante Aufgaben bearbeiten

Sie können geplante Aufgabe bearbeiten, indem Sie mit der rechten Maustaste darauf klicken und „Aufgabe bearbeiten" auswählen. Befolgen Sie die Schritte 1-5 im Abschnitt Deep Freeze-Aufgaben terminieren.

Computer terminierten Tasks zuordnen

Nachdem eine Task terminiert wurde, wird sie im Fenster *Netzwerk und Gruppen* der Konsole unter *Scheduler* angezeigt.



Sie können Computer einer Task zuordnen, indem Sie die gewünschten Computer im Teilfenster *Arbeitsplätze* der Konsole auswählen und auf die gewünschte Task ziehen. Sie können auch eine Gruppe auf eine Task ziehen.

Um zu sehen, welche Computer einer bestimmten Task zugeordnet sind, klicken Sie auf die Task. Die zugeordneten Computer werden im Teilfenster *Arbeitsplätze* angezeigt.

Um einen Computer aus einer Aufgabe zu löschen, klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie *Aus Aufgabe entfernen* aus.

Eine Aufgabe hinzufügen

Um eine Aufgabe hinzuzufügen, klicken Sie mit der rechten Maustaste auf „Scheduler", und wählen Sie „Aufgabe hinzufügen" aus.

Eine Aufgabe bearbeiten

Um eine Aufgabe zu bearbeiten, klicken Sie mit der rechten Maustaste darauf, und wählen Sie „Aufgabe bearbeiten" aus.

Eine Aufgabe anhalten

Um eine Aufgabe anzuhalten, klicken Sie mit der rechten Maustaste darauf, und wählen Sie „Aufgabe anhalten" aus.

Eine Aufgabe fortsetzen

Um eine Aufgabe fortzusetzen, klicken Sie mit der rechten Maustaste darauf, und wählen Sie „Aufgabe fortsetzen" aus.

Aufgaben löschen

Sie können eine Task löschen, indem Sie mit der rechten Maustaste auf die Task klicken und *Aufgaben löschen* auswählen.

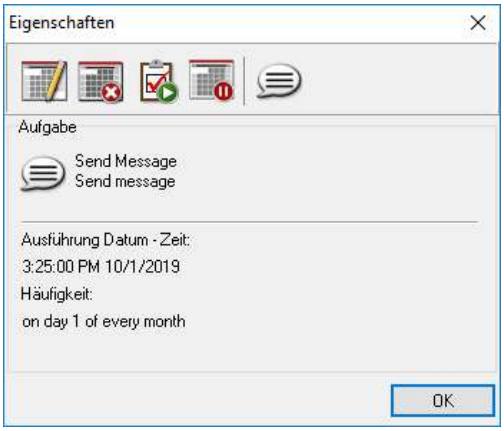
Eine Task sofort ausführen

Sie können eine Task sofort ausführen, indem Sie mit der rechten Maustaste auf die Task klicken und *Task ausführen* auswählen.

Eigenschaften von terminierten Tasks

Sie können die Eigenschaften einer Task anzeigen, indem Sie mit der rechten Maustaste auf den Aufgabennamen klicken und *Eigenschaften anzeigen* auswählen.

Der folgende Bildschirm wird angezeigt:



Terminierte Tasks werden auch ausgeführt, wenn die Enterprise-Konsole geschlossen ist, vorausgesetzt, der lokale Service ist aktiviert und die Netzwerkverbindungen werden beim Verlassen der Enterprise-Konsole nicht beendet.

Netzwerk und Gruppen verwalten

Die Enterprise-Konsole ordnet Computer automatisch nach Arbeitsgruppe oder Domäne an. Klicken Sie auf die entsprechende Arbeitsgruppe oder Domäne, um die Computer in dieser Arbeitsgruppe oder Domäne anzuzeigen.

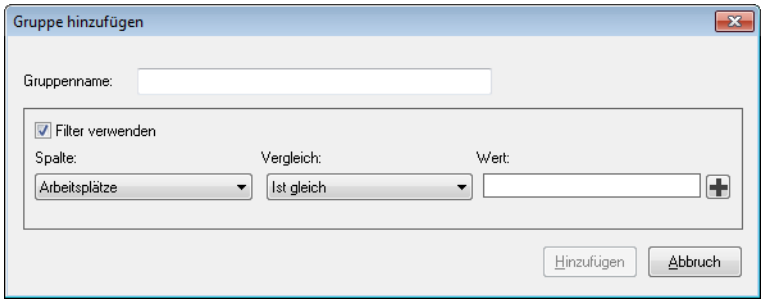
Die Enterprise-Konsole kann verwendet werden, um bestimmte Gruppen zu definieren, um Computer anzuordnen.

Eine Gruppe hinzufügen

Über den Dialog "Gruppe hinzufügen" können Sie mehrere Filter konfigurieren, um die Arbeitsplätze in verschiedene Gruppen einzuteilen. Dieser Filter aktualisiert die Liste der Arbeitsplätze automatisch auf der Grundlage der Änderungen der ausgewählten Parameter.

Führen Sie die folgenden Schritte aus, um eine Gruppe mit einem Filter hinzuzufügen:

1. Klicken Sie im Teilfenster *Netzwerk und Gruppen* mit der rechten Maustaste auf *Benutzerdefinierte Gruppen*.
2. Wählen Sie *Gruppe hinzufügen* aus. Der Dialog "Gruppe hinzufügen" wird angezeigt:



3. Geben Sie den *Gruppennamen* an.
4. Wählen Sie *Spalte* aus.
5. Wählen Sie *Vergleich* aus.
6. Wählen *Option* und/oder aus, ob Sie einen weiteren Filter hinzufügen.
7. Geben Sie *Wert* oder *Regulärer Ausdruck* an.
8. Klicken Sie auf *Hinzufügen*.

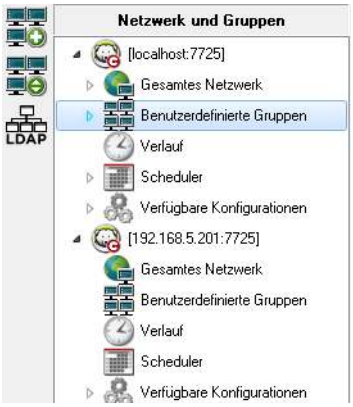
Die folgende Tabelle zeigt Spalte, Vergleich, Option und Werte.

Wählen Sie Spalte aus.	Wählen Sie Vergleich aus.	Wählen Sie Option aus.	Geben Sie Wert oder Regulärer Ausdruck an.
Arbeitsplätze	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Arbeitsgruppe	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
IP-Adresse	Ist gleich Ist größer als Ist größer als oder gleich Ist weniger als Ist weniger als oder gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Status	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Eingefroren Eingefroren und gesperrt Aufgetaut Aufgetaut und gesperrt Windows Update wird angewandt Batch-Datei wird angewandt Zeitraum im Status "aufgetaut" Wartungsmodus Lizenz abgelaufen Arbeitsplatz-Seed Unbekannt
Konfiguration	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.

Wählen Sie Spalte aus.	Wählen Sie Vergleich aus.	Wählen Sie Option aus.	Geben Sie Wert oder Regulärer Ausdruck an.
Konfigurationsdatum	Ist gleich Ist größer als Ist größer als oder gleich Ist weniger als Ist weniger als oder gleich Regulärer Ausdruck	Und Oder	Geben Sie das *Datum* an.
Installationsdatei	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Version	Ist gleich Ist größer als Ist größer als oder gleich Ist weniger als Ist weniger als oder gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Betriebssystem	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
MAC-Adresse	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Anmeldename	Ist gleich Ist nicht gleich Regulärer Ausdruck	Und Oder	Geben Sie den *Wert* oder *Regulären Ausdruck* an.
Aufgetaut seit	Ist gleich Ist größer als Ist größer als oder gleich Ist weniger als Ist weniger als oder gleich	Und Oder	Geben Sie den *Wert an.*

Eine benutzerdefinierte Gruppenstruktur erstellen

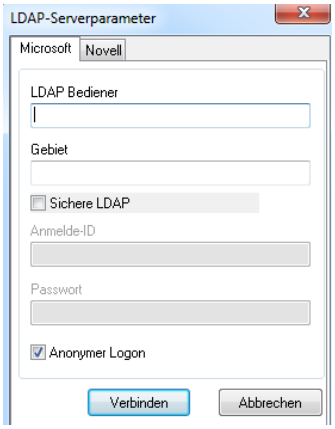
Nachdem eine Gruppe hinzugefügt wurde, können darunter eine oder mehrere Untergruppen hinzugefügt werden. Weiterhin kann eine unbegrenzte Menge von Untergruppen hinzugefügt werden, um zwischen Umgebungen zu unterscheiden, wie im nachfolgenden Beispiel dargestellt:



Gruppen aus Active Directory importieren

Wenn die Gruppenstruktur bereits innerhalb von Active Directory entworfen wurde, kann diese Struktur direkt in die Enterprise-Konsole importiert werden. Führen Sie die folgenden Schritte aus, um aus Active Directory zu importieren:

1. Wählen Sie *Tools* > *Grupppen aus Active Directory importireen* aus, oder klicken Sie in der Seitenleiste auf das Symbol *LDAP*.
2. Der folgende Dialog wird angezeigt – Wählen Sie entweder die Registerkarte *Microsoft* oder die Registerkarte *Novell* aus.



3. Geben Sie die Daten des LDAP-Servers in die Importposition ein. Es ist auch eine Option für eine anonyme Anmeldung verfügbar. Wenn diese Checkbox nicht ausgewählt wird, sind Benutzername und Passwort erforderlich.
4. Wählen Sie *Secure LDAP* aus, wenn Ihr Netzwerk Secure LDAP verwendet. (Nähere Informationen über Secure LDAP finden Sie unter https://support.microsoft.com/en-ca/kb/321051).
5. Klicken Sie auf *Verbinden*. Die *Active Directory*-Hierarchie wird angezeigt. Wählen Sie die erforderlichen Einträge aus, und klicken Sie auf *Importieren*.

Verlauf

Die Enterprise-Konsole speichert den Verlauf der Zielcomputer.

Wenn ein Computer vom Netzwerk getrennt ist, gerade heruntergefahren wird oder neu startet, wird in der Enterprise-Konsole neben dem entsprechenden Eintrag ein Ausrufezeichen (!) angezeigt. Wenn der Computer wieder online kommt, erlischt das Ausrufezeichen.

Wenn ein Computer permanent offline bleibt (z.B. permanent vom Netzwerk getrennt wurde), oder dieser nach dem Herunterfahren nicht neu gestartet wird, bleibt das Ausrufezeichen erhalten.

Gehen Sie in der Enterprise-Konsole auf *Datei* > *Beenden*. Wählen Sie die Option *Schließen und Netzwerkverbindungen beenden* und klicken Sie auf *OK*. Sobald Sie die Enterprise-Konsole erneut öffnen, werden die Computer, die mit einem Ausrufezeichen (!) versehen sind, im Verlauf angezeigt. Wenn der Computer ausgeschaltet ist, jedoch mit Hardware ausgestattet ist, die mit der Funktion "Wake-on-LAN" kompatibel ist, klicken Sie unter "Verlauf" mit der rechten Maustaste auf den entsprechenden Computer und wählen Sie "Wake-on-LAN", um den Computer erneut zu starten.

Optionen unter "Verlauf":

- Sie können den Verlauf anzeigen, indem Sie im Teilfenster *Netzwerke und Gruppen* auf *Verlauf* klicken.
- Sie können Computer aus dem Verlauf löschen, indem Sie die Computer auswählen, mit der rechten Maustaste darauf klicken und im Kontextmenü *Aus Verlauf entfernen* auswählen.
- Um einen oder mehrere Computer durch Wake-on-LAN zu starten, wählen Sie den/die Computer aus, klicken Sie mit der rechten Maustaste auf den jeweiligen Eintrag (die jeweiligen Einträge), und wählen Sie dann im Kontextmenü die Option *Wake-on-LAN* aus.

Computer zu einer Gruppe hinzufügen

Computer können zu einer Gruppe hinzugefügt werden, indem Sie sie vom Teilfenster *Arbeitsplätze* in die gewünschte Gruppe ziehen, oder indem Sie einen automatischen Filter verwenden, der bei der Erstellung der Gruppen eingestellt wird.

Über die automatische Gruppenfilterung können Computer automatisch zu benutzerdefinierten Gruppen hinzugefügt werden. Die Computer werden auf Basis ihrer Computernamen hinzugefügt.

Platzhalter (*, ?) können verwendet werden, um Computer auf Basis eines bestimmten Bestandteils des Namens hinzuzufügen.

Beispiel: *Lab1-** fügt alle Computer hinzu, deren Namen mit Lab1- beginnen.

Gruppen alphabetisch sortieren

Sie können die benutzerdefinierten Gruppen alphabetisch sortieren, indem Sie mit der rechten Maustaste auf *Benutzerdefinierte Gruppen* klicken, und *Gruppen alphabetisch sortieren* auswählen.

Arbeitsplätze aus einer benutzerdefinierten Gruppe entfernen

Sie können einen Computer aus einer Gruppe entfernen, indem Sie unter *Benutzerdefinierte Gruppen* auf den Computer klicken und *Aus Gruppe entfernen* auswählen.

Gruppen in eine Datei importieren oder exportieren

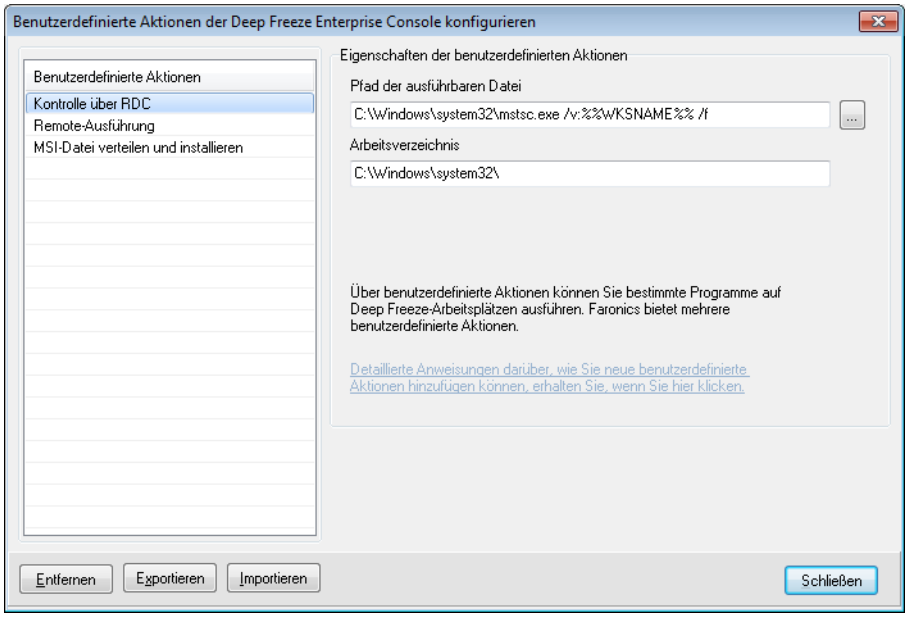
Um Gruppen aus einer Datei zu importieren oder in eine Datei zu exportieren, wählen Sie die gewünschte Option im Menü *Tools* aus.

Benutzerdefinierte Aktionen konfigurieren

Deep Freeze bietet die folgenden benutzerdefinierten Aktionen, auf die über das Menü *Aktionen* zugegriffen werden kann. Es können zusätzliche Aktionen erstellt werden, um auf individuelle Anforderungen einzugehen. Deep Freeze bietet drei Standardaktionen. Weitere benutzerdefinierte Aktionen können durch einen Import der entsprechenden *.xml*-Datei in die Deep Freeze-Konsole konfiguriert werden. Weitere Informationen über benutzerdefinierte Aktionen, die Struktur der Datei für benutzerdefinierte Aktionen und Detailinformationen über diverse Parameter finden Sie in Anhang E.

Kontrolle über RDC

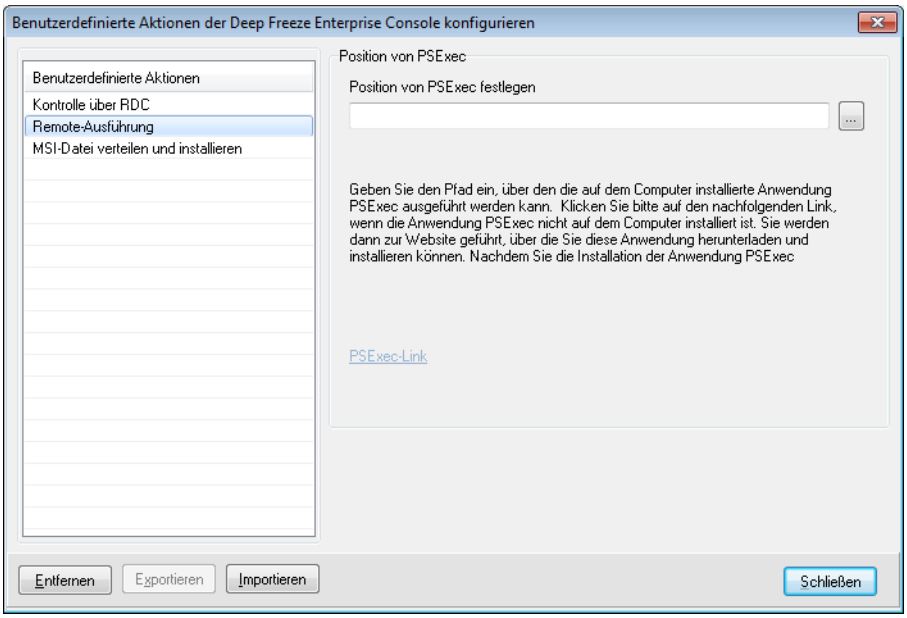
Dies ermöglicht eine Verbindung zum Computer über das Microsoft Remote Desktop Protocol. Die Remote-Desktopverbindung muss bereits auf den Zielmaschinen aktiviert sein.



1. Gehen Sie auf *Aktionsmenü* > *Benutzerdefinierte Aktionen*.
2. Wählen Sie *Kontrolle über RDC* aus.
3. Gebne Sie den *Pfad der ausführbaren Datei* ein, oder suchen Sie nach der Position, und wählen Sie sie aus.
4. Geben Sie das *Arbeitsverzeichnis* ein.
5. Klicken Sie auf *Anwenden*.

Remote-Ausführung

Über Remote-Ausführung können Sie eine ausführbare Datei auf einem Computer aus der Ferne ausführen. PsExec ist ein Tool, das verwendet werden kann, um eine ausführbare Datei auf einem Computer aus der Ferne auszuführen. PsExec muss heruntergeladen und auf dem Computer installiert werden. Weitere Informationen über PsExec finden Sie unter http://www.faronics.com/pstools.



Konfigurieren Sie

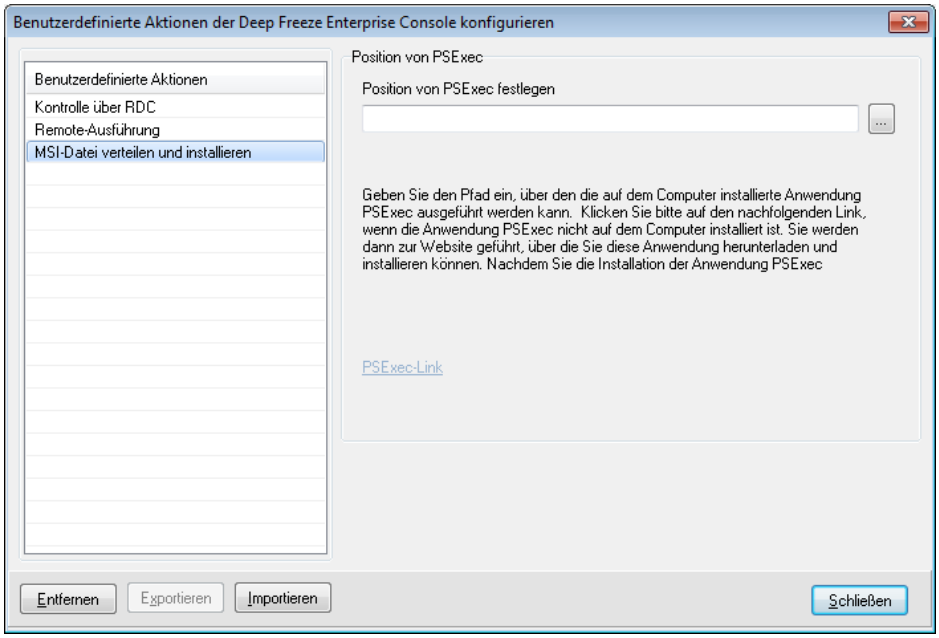
1. Gehen Sie auf *Aktion* > *Benutzerdefinierte Aktionen*.
2. Wählen Sie *Remote-Ausführung* aus.
3. Geben Sie den *PSExec-Pfad* ein, oder suchen Sie nach der Position, und wählen Sie sie aus.
4. Der *Pfad zur ausführbaren Datei* und das *Arbeitsverzeichnis* werden automatisch hinzugefügt. Der *Pfad zur ausführbaren Datei* und das *Arbeitsverzeichnis* können später noch verändert werden.
5. Klicken Sie auf *Schließen*.

Ausführen

1. Wählen Sie die Computer im Teilfenster *Arbeitsplätze* aus.
2. Wählen Sie *Aktion* > *Remote-Ausführung* aus.
3. Der Dialog *Remote-Ausführung* wird angezeigt.
4. Geben Sie den *Benutzernamen*, das *Passwort* und den *Befehl* ein.
5. Klicken Sie auf *OK*.

MSI-Datei verteilen und installieren

Über die Option *MSI-Datei verteilen und installieren* können Sie eine *.msi*-Datei über die Enterprise-Konsole veteilen und auf einem Computer installieren.



Konfigurieren Sie

1. Gehen Sie auf *Aktion* > *Benutzerdefinierte Aktionen*.
2. Wählen Sie *MSI-Datei verteilen und installieren* aus.
3. Geben Sie den *PSExec-Pfad* ein, oder suchen Sie nach der Position, und wählen Sie sie aus.
4. Der *Pfad zur ausführbaren Datei* und das *Arbeitsverzeichnis* werden automatisch hinzugefügt. Der *Pfad zur ausführbaren Datei* und das *Arbeitsverzeichnis* können später noch verändert werden.
5. Klicken Sie auf *Schließen*.

Ausführen

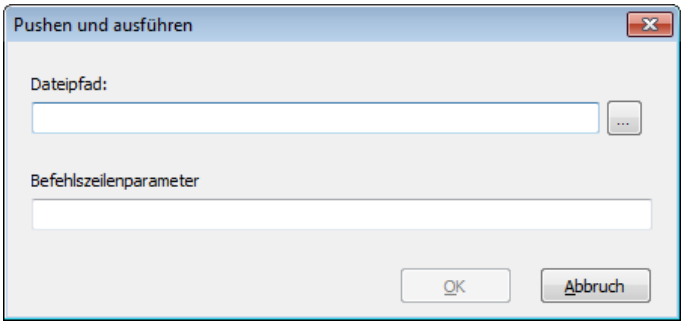
1. Wählen Sie die Computer im Teilfenster *Arbeitsplätze* aus.
2. Wählen Sie *Aktion* > *MSI-Datei verteilen und installieren* aus.
3. Der Dialog *MSI-Datei verteilen und installieren* wird angezeigt.
4. Geben Sie den *Benutzernamen*, das *Passwort*, den *Dateinamen* und den *Laufwerksbuchstaben* ein.
5. Klicken Sie auf OK.

Pushen und ausführen

Sie können Dateien auf verwaltete Arbeitsplätze übertragen (pushen) und dort ausführen.

Führen Sie die folgenden Schritte aus, um Dateien auf verwaltete Arbeitsplätze zu übertragen und dort auszuführen:

1. Wählen Sie im Teilfenster "Arbeitsplätze" einen oder mehrere Arbeitsplätze aus.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie *Aktionen* > *Pushen und ausführen* aus. Der Dialog "Pushen und ausführen" wird angezeigt:



3. Browsen Sie, um den Dateipfad auszuwählen, oder geben Sie den Dateipfad an.
   - Dateiname und Pfad – geben Sie den Dateinamen und Pfad an, an dem sich die Datei auf dem Konsolencomputer befindet. Alternativ hierzu können Sie auch blättern, um die ausführbare Datei auszuwählen. Die Dateitypen .exe (ausführbare Dateien) und .msi (MSI-Installationsdateien) werden unterstützt. MSI-Dateien werden standardmäßig im Installationsmodus ausgeführt. Wenn die ausführbare Datei MeineAnwendung.exe beispielsweise unter C:/Anwendungsordner verfügbar ist, geben Sie *C:/Anwendungsordner/MeineAnwendung* an.
4. Geben Sie die Befehlszeilenparameter mit Umgebungsvariablen an (optional):
   - Argumente – geben Sie die Argumente an, die Sie mit dieser ausführbaren Datei anwenden möchten. Wenn die ausführbare Datei beispielsweise mit dem Befehl C:\Anwendungsordner\MeineAnwendung -o Protokolldatei.log über die Befehlszeilensteuerung ausgeführt wird, geben Sie als Argumente *-o Protokolldatei.log* an. Geben Sie für .msi-Dateien die Argumente an, die Sie normalerweise beim Start einer .msi-Datei mit MSIEXEC angeben würden. Wenn Sie für eine .msi-Datei kein Argument angeben, hängt Deep Freeze automatisch "/i" (installieren) an. Darüber hinaus ersetzt Deep Freeze bestehende Anzeigeoptionen mit /qn (still, keine UI).
5. Klicken Sie auf OK.

Die Datei wird auf den ausgewählten Arbeitsplatz übertragen und aus der Ferne auf den ausgewählten Arbeitsplätzen ausgeführt.

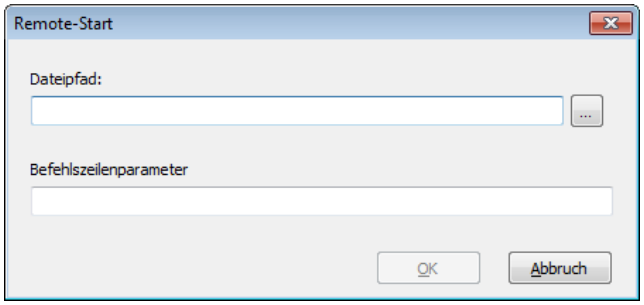
Remote-Ausführung

Sie können ausführbare Dateien auf verwalteten Arbeitsplätzen aus der Ferne ausführen.

Führen Sie die folgenden Schritte aus, um Dateien auf verwalteten Arbeitsplätzen aus der Ferne auszuführen:

1. Wählen Sie im Teilfenster "Arbeitsplätze" einen oder mehrere Arbeitsplätze aus.

2. Klicken Sie mit der rechten Maustaste, und wählen Sie *Aktionen* > *Remote-Ausführung* aus. Der Dialog "Remote-Ausführung" wird angezeigt.



3. Browsen Sie, um den Dateipfad auszuwählen, oder geben Sie den Dateipfad an.
   - Dateiname und Pfad – geben Sie den Dateinamen und Pfad an, an dem sich die Datei auf dem Konsolencomputer befindet. Alternativ hierzu können Sie auch blättern, um die ausführbare Datei auszuwählen. Die Dateitypen .exe (ausführbare Dateien) und .msi (MSI-Installationsdateien) werden unterstützt. MSI-Installationsdateien werden standardmäßig im Installationsmodus ausgeführt. Wenn die ausführbare Datei MeineAnwendung.exe beispielsweise unter C:/Anwendungsordner verfügbar ist, geben Sie *C:/Anwendungsordner/MeineAnwendung* an.
4. Geben Sie die Befehlszeilenparameter mit Umgebungsvariablen an (optional):
   - Argumente – geben Sie die Argumente an, die Sie mit dieser ausführbaren Datei anwenden möchten. Wenn die ausführbare Datei beispielsweise mit dem Befehl C:\Anwendungsordner\MeineAnwendung -o Protokolldatei.log über die Befehlszeilensteuerung ausgeführt wird, geben Sie als Argumente *-o Protokolldatei.log* an. Geben Sie für .msi-Dateien die Argumente an, die Sie normalerweise beim Start einer .msi-Dateie mit MSIEXEC angeben würden. Wenn Sie für eine .msi-Datei kein Argument angeben, hängt Deep Freeze automatisch "/i" (installieren) an. Darüber hinaus ersetzt Deep Freeze bestehende Anzeigeoptionen mit /qn (still, keine UI).
5. Klicken Sie auf OK.

Die Datei wird auf den ausgewählten Arbeitsplätzen aus der Ferne ausgeführt.

Benutzerdefinierte Aktionen löschen, importieren und exportieren

Benutzerdefinierte Aktionen löschen

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Aktionen zu löschen:

1. Gehen Sie auf *Aktionsmenü* > *Benutzerdefinierte Aktionen*.
2. Wählen Sie die benutzerdefinierte Aktion aus, die gelöscht werden soll.
3. Klicken Sie auf *Löschen*.

Benutzerdefinierte Aktionen importieren

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Aktionen zu importieren:

1. Gehen Sie auf *Aktionsmenü* > *Benutzerdefinierte Aktionen*.

2. Klicken Sie auf *Importieren*.
3. Blättern Sie, um die *.xml*-Datei, die importiert werden soll, zu suchen und auszuwählen.
4. Klicken Sie auf *Öffnen*, um die Datei zu importieren.

Benutzerdefinierte Aktionen exportieren

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Aktionen zu exportieren:

1. Gehen Sie auf *Aktionsmenü* > *Benutzerdefinierte Aktionen*.
2. Wählen Sie die benutzerdefinierte Aktion aus, die exportiert werden soll.
3. Klicken Sie auf *Exportieren*.
4. Der Dialog ‚Benutzerdefinierte Aktion in Datei exportieren' wird angezeigt.
5. Geben Sie einen *Dateinamen* an, und klicken Sie auf *Speichern*.

Konsolen-Customizer

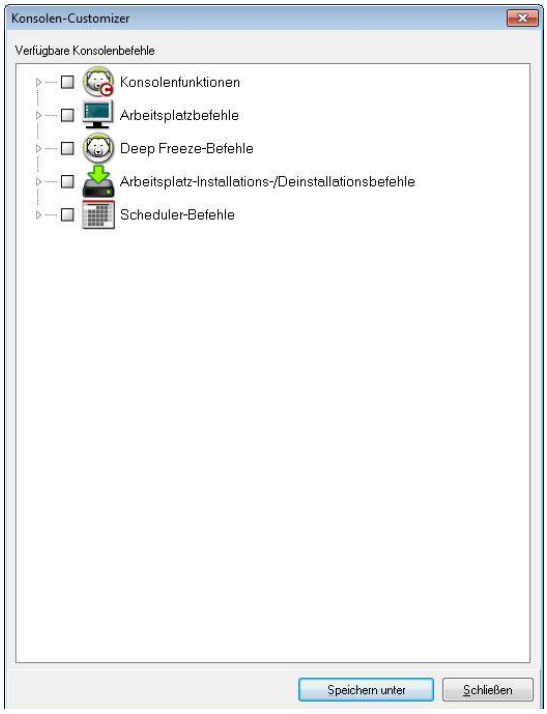
Über den Konsolen-Customizer können Sie festlegen, welche Funktionen und Befehle in der Konsole verfügbar sein sollen und das Ergebnis als neue Konsole speichern, die in Ihrer Organisation verteilt werden soll.

Die verfügbaren Einstellungen sind nach Kategorien gruppiert (Konsolenfunktionen, Arbeitsplatzbefehle, Deep Freeze-Befehle, Installations-/Deinstallationsbefehle für Arbeitsplätze und Scheduler-Befehle). Klicken Sie auf das Plussymbol (+) auf der linken Seite der einzelnen Kategorien, um die vollständige Liste der für diese Kategorie verfügbaren Einstellungen anzuzeigen.

Wählen Sie die einzelnen Checkboxes Ihrem Bedarf entsprechend aus oder ab. Alternativ können Sie auch ganze Kategorien auf einmal aus- oder abwählen. Abgewählte Einstellungen sind in der neuen Enterprise-Konsole, die Sie erstellen, nicht verfügbar. Ein Beispiel für die Verwendung des Konsolen-Customizers in einem praktischen Szenario finden Sie in Anhang D.

Führen Sie die folgenden Schritte aus, um Konsolen mit eingeschränkter Funktionalität zu erstellen:

1. Wählen Sie *Tools* > *Konsolen-Customizer* aus.
2. Der Konslen-Customizer wird angezeigt.



3. Wählen Sie die Funktionen aus, die in der neuen Konsole angezeigt werden sollen.
4. Klicken Sie auf *Speichern unter*, um die Konsole zu speichern. Geben Sie einen Namen für die Datei an.
5. Wenn Sie doppelt auf die neu erstellte *.exe*-Datei klicken, wird die Konsole mit der eingeschränkten Funktionalität gestartet.

Deep Freeze Enterprise-Konsole herunterfahren

Um die Deep Freeze-Konsole zu beenden, wählen Sie *Datei* > *Beenden* aus, oder klicken Sie auf die Schaltfläche ‚Fenster schließen'. Beim Beenden haben Sie die folgenden Auswahlmöglichkeiten:

- Konsole in die Taskleiste minimieren.

  Dies beendet die Konsole nicht, die Verbindungen bleiben erhalten. Das Symbol der Deep Freeze-Konsole wird in der Taskleiste angezeigt. Terminierte Tasks werden weiterhin ausgeführt. Um die Deep Freeze Enterprise-Konsole erneut zu öffnen, klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste, und wählen Sie *Deep Freeze-Konsole wiederherstellen* aus.

- Deep Freeze-Konsole schließen und Netzwerkverbindungen beibehalten

  Dies schließt die Konsole, die Verbindungen zu den Computern bleiben jedoch bestehen. Terminierte Tasks werden weiterhin ausgeführt.

- Deep Freeze-Konsole schließen und Netzwerkverbindungen beenden.

  Dies stoppt Konsolenprozesse, beendet die Verbindungen (einschließlich lokaler Dienst) und terminierte Tasks werden nicht gestartet. Terminierte Tasks, die bereits gestartet wurden, werden weiter ausgeführt.



Der Dialog wird in Zukunft beim Beenden nicht mehr angezeigt, wenn die Option *Als Standard festlegen* ausgewählt wurde. Sie können diese Einstellungen bearbeiten, indem Sie *Tools* > *Optionen beim Beenden* auswählen.

Deep Freeze auf dem Arbeitsplatz installieren

Nachdem über den Konfigurationsadministrator eine angepasste Installationsprogrammdatei erstellt wurde, kann Deep Freeze über eine Überwachte Installation, eine Zielinstallation, das Stille Installationssystem oder als Teil eines Imaging-Prozesses auf Computern implementiert werden.



Vor der Installation sollten alle im Hintergrund laufenden Dienstprogramme und Antivirensoftware deaktiviert und alle Anwendungen geschlossen werden. Diese Programme können die Installation beeinflussen und dazu führen, dass Deep Freeze nicht ordnungsgemäß funktioniert.

Der Computer wird nach Abschluss eines beliebigen Installationstyps erneut gestartet. Deep Freeze muss sich in einem aufgetauten Zustand befinden, damit eine Deinstallation erfolgreich sein kann.

Bei der Deinstallation wird vorhandener Auftauplatz gelöscht, wenn:

- Die Option, vorhandene Auftauplätze beizubehalten, im Konfigurationsadministrator nicht ausgewählt wurde.
- Der Auftauplatz nicht mit Deep Freeze Enterprise Version 5 oder höher erstellt wurde.

Überwachte Installation oder Deinstallation

Führen Sie die folgenden Schritte aus, um Deep Freeze zu installieren oder zu deinstallieren:

1. Führen Sie die Installationsprogrammdatei (*DFWks.exe*) auf dem Computer aus. Der folgende Bildschirm wird angezeigt:
2. Klicken Sie auf *Installieren* , um mit der Installation zu beginnen. Befolgen Sie die dargestellten Schritte, und lesen und akzeptieren Sie anschießend die Lizenzvereinbarung. Deep Freeze wird installiert, und der Computer wird neu gestartet.



Klicken Sie auf *Deinstallieren*, um Deep Freeze zu deinstallieren. Die Optin Deinstallieren wird nur angeboten, wenn Deep Freeze zuvor installiert wurde und sich der Computer derzeit im Zustand „aufgetaut" befindet. Wenn ein Auftauplatz vorhanden ist, zeigt Deep Freeze einen Dialog an, in dem Sie angeben müssen, ob er beibehalten oder gelöscht werden soll.



Wenn die Festplatte zu stark fragmentiert ist, können Auftauplätze nicht erstellt werden. Eine Nachricht wird angezeigt, in der Sie aufgefordert werden, die Installation abzubrechen oder Deep Freeze ohne Auftauplatz zu installieren.

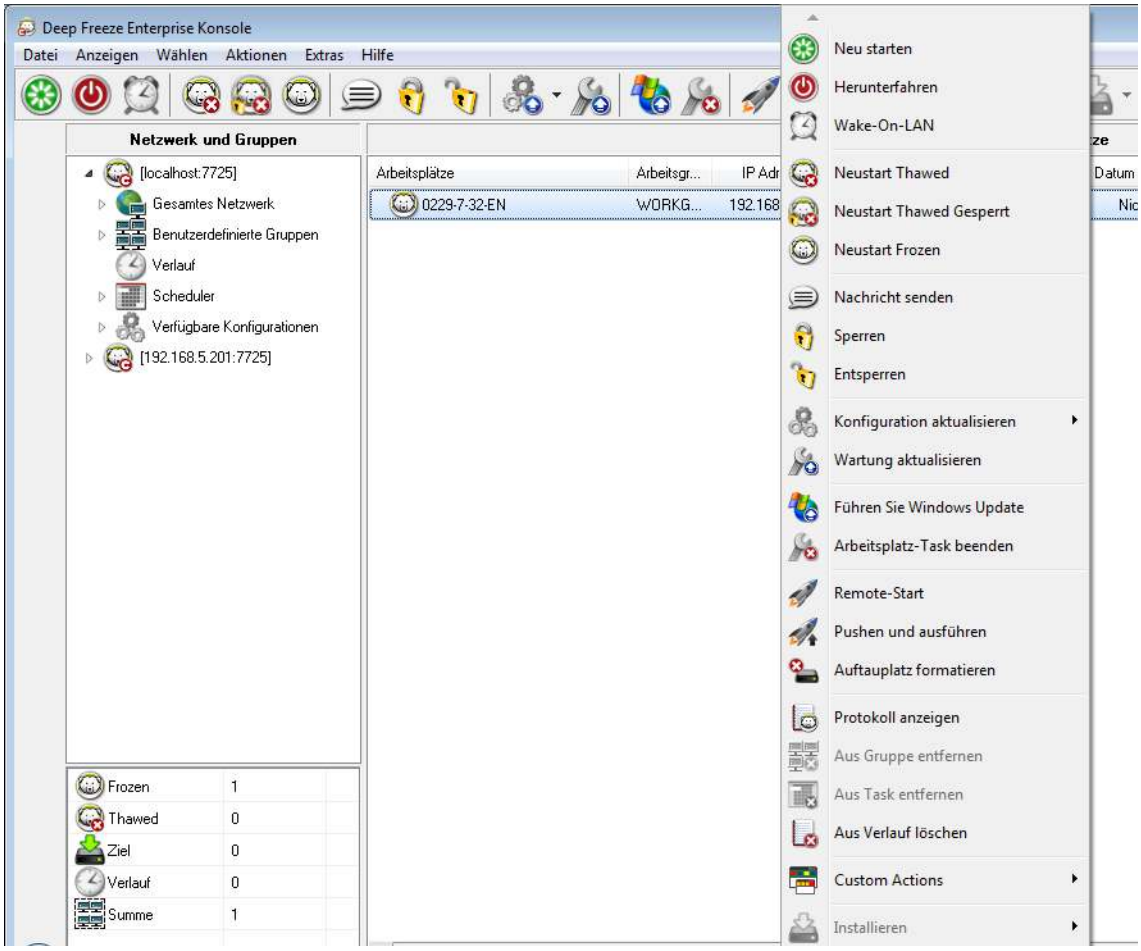


Wenn Sie *Neustart im eingefrorenen Zustand verzögern, um Windows Updates abzuschließen* (Registerkarte "Erweiterte Optionen" des Konfigurationsadministrators) auswählen und Deep Freeze installieren, prüft das Installationsprogramm, ob alle Windows Updates vollständig sind. Wenn die Windows Updates nicht vollständig sind, wird die Installation von Deep Freeze nicht fortgesetzt. Schließen Sie die Windows Updates ab, und versuchen Sie erneut, Deep Freeze zu installieren.

Wenn Sie die Option *Neustart im eingefrorenen Zustand verzögern, um Windows Updates abzuschließen* deaktivieren und Deep Freeze installieren, stellen Sie sicher, dass alle Windows Updates ohne Verwendung von Deep Freeze durchgeführt werden. Wenn diese Option deaktiviert wird, kann dies zur Folge haben, dass der Computer aufgrund nicht abgeschlossener Windows Updates in einem Neustartzyklus hängenbleibt.

Deep Freeze über die Konsole auf dem Arbeitsplatz installieren

Die Enterprise-Konsole kann verwendet werden, um Deep Freeze entweder vollständig zu deinstallieren, oder um Deep Freeze zu deinstallieren, das Arbeitsplatz-Seed jedoch beizubehalten. Ein Computer muss sich im aufgetauten Zustand befinden, um das Programm deinstallieren zu können.



Um Deep Freeze auf einem Computer zu deinstallieren und das Arbeitsplatz-Seed beizubehalten, klicken Sie mit der rechten Maustaste auf den entsprechenden Arbeitsplatz, und wählen Sie wie oben dargestellt *Deinstallation (Seed beibehalten)* aus. Oder klicken Sie auf das entsprechende Symbol in der Symbolleiste.

Um Deep Freeze und das Arbeitsplatz-Seed vollständig zu deinstallieren, wählen Sie den entsprechenden Computer aus, der deinstalliert werden soll, und klicken Sie in der Symbolleiste auf das Symbol *Deinstallieren*.

Der Computer muss sich im Zustand "aufgetaut" befinden, bevor Deep Freeze deinstalliert werden kann. Die Enterprise-Konsole fordert Sie auf, den Vorgang zu bestätigen. Nach Bestätigung der Deinstallation wird Deep Freeze deinstalliert und der Computer neu gestartet.

Stille Installation oder Deinstallation

Anhand des stillen Installationssystems kann Deep Freeze schnell auf zahlreichen Computern über ein Netzwerk installiert werden. Jedes beliebige Implementierungsdienstprogramm, das die Ausführung einer Befehlszeile auf einem fernen Computer ermöglicht, kann das stille Installationssystem implementieren. Nach Abschluss der stillen Installation wird der Computer sofort neu gestartet. Die Befehlszeile hat die folgenden Optionen:

Syntax	Beschreibung
`[/Install]`	Deep Freeze über die Installationsdatei installieren
`[/Install /Seed]`	Nur die angegebene Arbeitsplatz-Seed-Datei installieren
`[/Install /Thawed]`	Installieren Sie Deep Freeze anhand der Installationsdatei, und starten Sie den Computer im Zustand "aufgetaut".
`[/Uninstall]`	Deep Freeze deinstallieren
`[/Uninstall /Seed]`	Deep Freeze deinstallieren und Arbeitsplatz-Seed installiert lassen
`[/PW=password]`	Bei Installation ein Passwort einstellen*
`[/AllowTimeChange]`	Änderung der Systemuhr erlauben*
`[/Freeze=C,D,...]`	Nur aufgeführte Laufwerke einfrieren (alle anderen auftauen)*
`[/Thaw=C,D,...]`	Nur aufgeführte Laufwerke auftauen (alle anderen einfrieren)*
`[/USB]`	Externe USB-Festplatten vom Schutz ausschließen
`[/FireWire]`	Externe FireWire-Festplatten vom Schutz ausschließen

Beispiel Befehlszeile

```
DFWks.exe /Install /Freeze=C /PW=password
```

Im vorangehenden Beispiel hat die Deep Freeze-Installationsprogrammdatei den Namen *DFWks.exe*. Nur das Laufwerk C: wird eingefroren. Alle anderen Laufwerke des Computers werden aufgetaut. Wenn der Computer nur über ein Laufwerk C: verfügt, kann der Switch [/Freeze] ausgelassen werden. Ein Passwort (passwort) wird erstellt. Nach Ausführung des Befehls wird Deep Freeze installiert, der Computer wird neu gestartet und ist eingefroren und betriebsbereit.

Das stille Installationssystem funktioniert nicht ohne den Switch the [`/Install`] oder [`/Uninstall`] Deep Freeze muss aufgetaut sein, bevor [`/Uninstall`] verwendet werden kann.





Um die Optionen für die Konfiguration über die Befehlszeile auszuführen, darf die Option Befehlszeilenoptionen deaktivieren auf der Registerkarte ‚Erweiterte Optionen' nicht aktiviert sein.



*Diese Optionen sind standardmäßig deaktiviert.

Stille Installation oder Deinstallation über eine Verknüpfung

Durch Ausführung der folgenden Schritte kann Deep Freeze direkt auf einem Computer installiert werden, ohne das Installationsdialogfeld verwenden zu müssen.

1. Suchen Sie die Deep Freeze-Installationsprogrammdatei (*DFWks.exe*) auf dem Zielcomputer.
2. Klicken Sie mit der rechten Maustaste auf das Symbol, und wählen Sie *Verknüpfung erstellen* aus.
3. Klicken Sie mit der rechten Maustaste auf die Verknüpfung, und wählen Sie *Eigenschaften* aus.
4. Bearbeiten Sie den Pfad des Felds Ziel, indem Sie am Ende des Pfads `/install` oder `/uninstall` eingeben.

Beispiel für ein Verknüpfungsziel:

```
C:\Dokumente und Einstellungen\DFWks.exe /install
```

Wenn Sie auf die neue Verknüpfung doppelklicken, wird Deep Freeze sofort installiert oder deinstalliert. Der Computer wird daraufhin neu gestartet.

Deep Freeze muss sich im aufgetauten Zustand befinden, bevor `/uninstall` verwendet werden kann.



Wenn die Festplatte zu stark fragmentiert ist, können Auftauplätze nicht erstellt werden. Die Installation wurde abgebrochen.

Netzwerkinstallation für mehrere Computer

Das stille Installationssystem kann außerdem verwendet werden, um Deep Freeze über ein Netzwerk auf mehreren Computern zu installieren. Wenn die Arbeitsplätze im Netzwerk Anmeldescripts verwenden, können die Scripts verwendet werden, um Deep Freeze automatisch auf allen vernetzten Arbeitsplätzen zu installieren. Nach Abschluss der Installation werden alle Arbeitsplätze im aufgetauten Zustand erneut gestartet und sind betriebsbereit.

Verwenden Sie die folgende Befehlszeilensyntax, um eine Berichtsprotokolldatei für Installationsfehler zu erstellen:

```
\\Server Name\Share Name\DFWks.exe /Install >> my.log
```

Installation über vorhandene Deep Freeze-Versionen

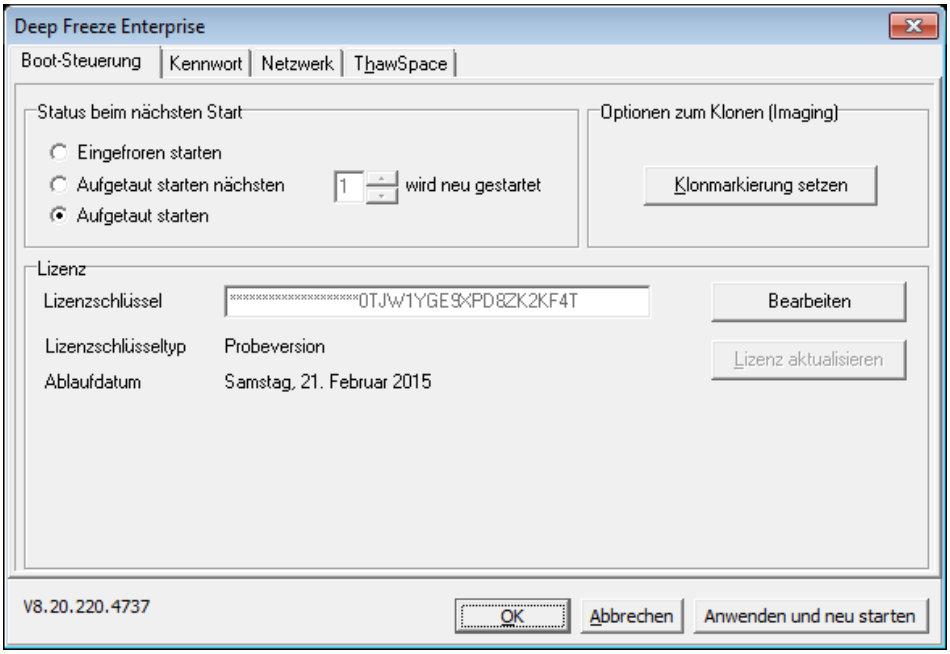
Wenn nicht die Funktion Deep Freeze-Software-Update (für Deep Freeze 6,5 und höher) verwendet wird, müssen alle vorhandenen Deep Freeze-Versionen deinstalliert werden, bevor eine neue Deep Freeze-Installation durchgeführt werden kann.

Installation über Imaging

Deep Freeze wurde entworfen, um mit allen bedeutenden Imaging- und Desktop-Management-Softwareprogrammen zu funktionieren. Verwenden Sie entweder eine überwachte oder eine stille Installation, um Deep Freeze auf einem Master-Image zu installieren.

Deep Freeze muss für die Implementierung vorbereitet werden, bevor ein Master-Image fertiggestellt werden kann. Führen Sie die folgenden Schritte aus, um das Master-Image für die Implementierung vorzubereiten:

1. Starten Sie den Computer erneut im Zustand *Thawed*.
2. Starten Sie Deep Freeze über das den Tastaturbefehl STRG+UMSCHALTTASTE+ALT+F6. Alternativ können Sie auch die *UMSCHALTTASTE* drücken und doppelt auf das Deep Freeze-Symbol in der Taskleiste klicken.
3. Geben Sie das Passwort ein, und klicken Sie auf *OK*.
4. Klicken Sie auf der Registerkarte *Boot-Steuerung* auf die Option *Klonmarkierung setzen*.
5. Die Nachricht *Die Markierung wurde erfolgreich gesetzt. Möchten Sie Ihren Computer jetzt neu starten?* wird angezeigt. Klicken Sie auf *Ja*, um den Computer sofort neu zu starten. Klicken Sie auf *Nein*, um den Computer später neu zu starten.







Der Befehl "Klonmarkierung setzen" ist für Imaging wichtig, da er die Computer im aufgetauten Zustand startet, wenn Deep Freeze nicht in der Lage ist, seine Konfigurationsdatei nach erfolgreicher Installation des Images zu lesen.

Wenn die Klonmarkierung nicht gesetzt wird und Deep Freeze nicht in der Lage ist, seine Konfigurationsdatei zu lesen, werden alle Laufwerke nach erfolgreicher Installation des Images in den Zustand "eingefroren" versetzt.



Wenn Sie Sysprep verwenden, achten Sie darauf, die Klonmarkierung nach Vorbereitung des Systems für Imaging und direkt vor der Durchführung von Sysprep zu setzen.

Nach dem Imaging müssen die Computer ein weiteres Mal neu gestartet werden, damit Deep Freeze die Änderungen an der Plattenkonfiguration korrekt bestimmen kann. Wenn das Imaging für die Computer in einem nicht überwachten Modus vorgenommen wird, sollten Schritte unternommen werden, um sicherzustellen, dass die Computer erneut gestartet werden, um die Aktualisierung der Konfiguration zu ermöglichen.

Um zum eingefrorenen Zustand zurückzukehren, nachdem das Imaging abgeschlossen wurde, stellen Sie Deep Freeze (im Master-Image) auf ‚Bei nächsten *n* Neustarts aufgetaut hochfahren', so dass der Computer nach *n* Neustarts automatisch eingefroren wird. Alternativ können sie die Deep Freeze-Befehlszeilensteuerung verwenden, um die ausgewählten Computer einzufrieren.

Zielinstallation

Deep Freeze kann auch über eine Zielinstallation von der Enterprise-Konsole aus implementiert werden.

Nach Updates suchen

Deep Freeze bietet die Möglichkeit, zu prüfen, ob neuere Versionen verfügbar sind.

Gehen Sie auf *Hilfe* > *Nach Updates suchen*. Hierdurch wird überprüft, ob neuere Versionen von Deep Freeze verfügbar sind.



Wenn eine neue Version verfügbar ist, klicken Sie auf *Aktuellste Version herunterladen*, um Deep Freeze zu aktualisieren.



Deep Freeze-Computer verwalten

Dieses Kapitel beschreibt die Verwaltung von Computern, auf denen Deep Freeze installiert ist.

Themen

Anmeldebildschirm
Registerkarte Status
Registerkarte "Passwort"
Registerkarte „Netzwerk"
Registerkarte „Auftauplatz"
Dauerhafte Softwareinstallationen, Änderungen oder Entfernungen

Anmeldebildschirm

Verwenden Sie eine der folgenden Arten, um auf Deep Freeze auf einem Computer zuzugreifen.

1. Wenn das Deep Freeze-Symbol in der Taskleiste angezeigt wird, halten Sie die UMSCHALTTASTE gedrückt, und klicken Sie doppelt auf das Deep Freeze-Symbol. Wenn Deep Freeze im Tarnmodus läuft und das Deep Freeze-Symbol nicht angezeigt wird, muss das Tastaturkürzel STRG+ALT+UMSCHALTTASTE+F6 verwendet werden, um auf den Anmeldedialog zuzugreifen.



2. Geben Sie das Administratorpasswort ein, und klicken Sie auf *OK* , um sich bei Deep Freeze anzumelden.

Als zusätzliche Sicherheitsfunktion verhindert Deep Freeze Brute Force-Attacken durch einen automatischen Neustart des Computers nach 10 erfolglosen Anmeldeversuchen.

Deep Freeze auf Touchscreen-Geräten starten

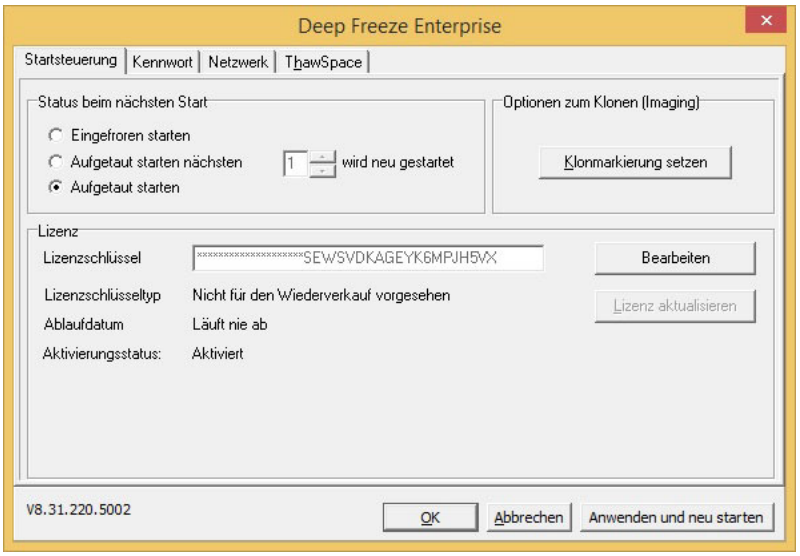
Sie können Strg+Alt+Umschalttaste+6 oder Strg+Alt+Umschalttaste+F6 verwenden, um Deep Freeze auf Touchscreen-Geräten zu starten. Sie müssen vor Verwendung der Tastenkombination jedoch die vollständige Tastatur aktivieren. Alternativ hierzu können Sie auch Taskleiste berühren und halten, um das Deep Freeze-Kontextmenü zu starten.

Registerkarte Status

Die Registerkarte *Status* bietet die folgenden Optionen:

Status beim nächsten Hochfahren

Die Registerkarte Status wird verwendet, um den Modus zu bestimmen, den Deep Freeze nach dem nächsten Neustart verwendet.



Wählen Sie eine der folgenden Optionen aus:

- Im Modus „eingefroren“ hochfahren,

  um sicherzustellen, dass der Computer nach dem nächsten Neustart eingefroren ist
- Im Modus „aufgetaut“ hochfahren, bei nächsten,

  um sicherzustellen, dass der Arbeitsplatz für die angegebene Anzahl von Neustarts im aufgetauten Zustand hochgefahren wird. Wenn die Anzahl von Neustarts erreicht ist, wird der Computer im eingefrorenen Zustand hochgefahren.
- Im Modus „aufgetaut“ hochfahren,

  um sicherzustellen, dass der Computer nach jedem Neustart aufgetaut ist

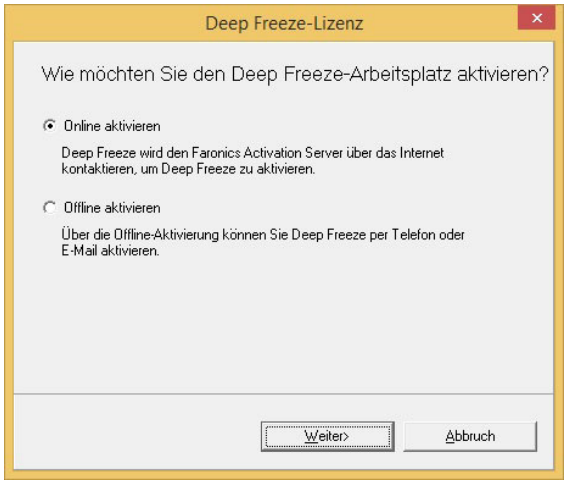
Wählen Sie das Optionsfeld neben der gewünschten Wahl aus, und klicken Sie auf *OK* , um Änderungen zu speichern. Durch einen Klick auf *Anwenden und neu starten* werden Änderungen gespeichert und der Computer wird sofort neu gestartet.

Klonen

Das Teilfenster *Klonen* wird verwendet, um Master-Images für den Implementierungsprozess vorzubereiten. Weitere Informationen hierzu finden Sie im Abschnitt Installation über Imaging.

Lizenz

1. Sie können den Lizenzschlüsse aktualisieren, indem Sie auf *Bearbeiten* klicken und den Lizenzschlüssel in das Feld *Lizenzschlüssel* eingeben.
2. Klicken Sie auf *Lizenz aktualisieren*. Hierdurch wird Deep Freeze von einer *Probe*version in eine *lizenzierte* Version umgewandelt. Im Feld *Lizenzschlüsseltyp* wird der *Lizenzschlüssel* angezeigt. Das *Ablaufdatum* zeigt das Datum und die Uhrzeit an, zu der die Lizenz abläuft.
3. Klicken Sie auf *Jetzt aktivieren*. Es sind zwei Optionen verfügbar:

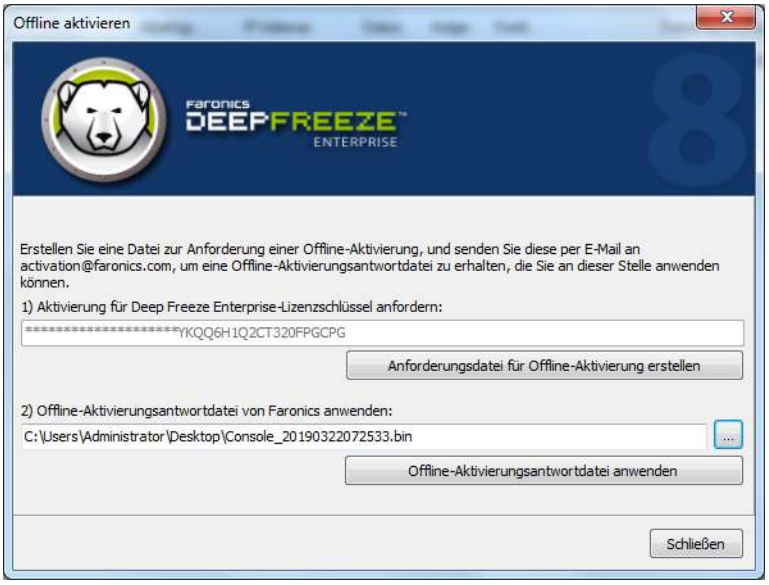


- Wählen Sie *Online aktivieren* aus, um die Deep Freeze-Lizenz online zu aktivieren. Diese Option ist mit Schritt 1 identisch. Klicken Sie auf *Weiter*, nachdem Sie diese Option ausgewählt haben. Deep Freeze wird online aktiviert, indem Sie auf *Weiter* klicken.
- Wählen Sie *Offline aktivieren* aus. Diese Option erlaubt es Ihnen, die Aktivierung telefonisch oder per E-Mail vorzunehmen. Klicken Sie nach der Aktivierung auf *Weiter*. Der Bildschirm "Offline aktivieren" wird angezeigt.



4. Senden Sie die *Aktivierungsdetails* telefonisch oder per E-Mail an den Aktivierungssupport von Faronics. Nachdem Sie den Aktivierungscode von Faronics

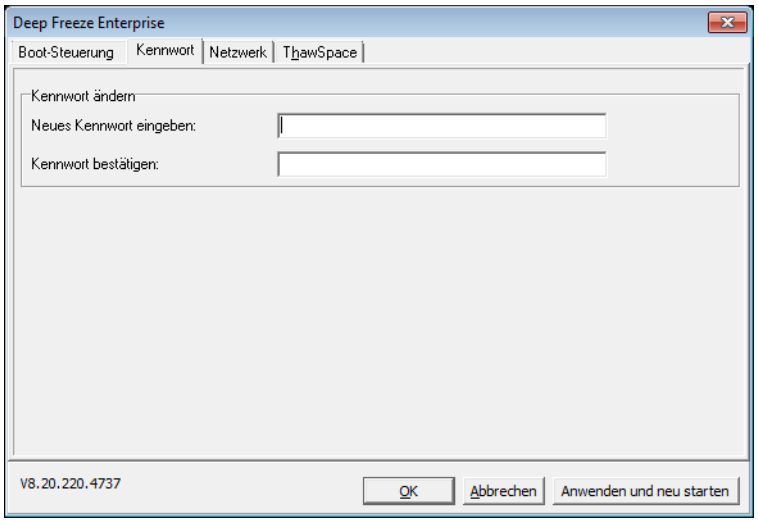
erhalten haben, geben Sie ihn in das Feld *Aktivierungscode* ein, und klicken Sie auf *Weiter*. Die Deep Freeze-Lizenz ist nun aktiviert.



Der Lizenzschlüssel wird automatisch auf allen Computern aktualisiert, die mit der Enterprise-Konsole kommunizieren. Wenn ein Computer nicht erreicht werden kann (heruntergefahren oder vom Netzwerk getrennt), wird der Lizenzschlüssel aktualisiert, wenn der Computer mit der Enterprise Console kommuniziert.

Registerkarte "Passwort"

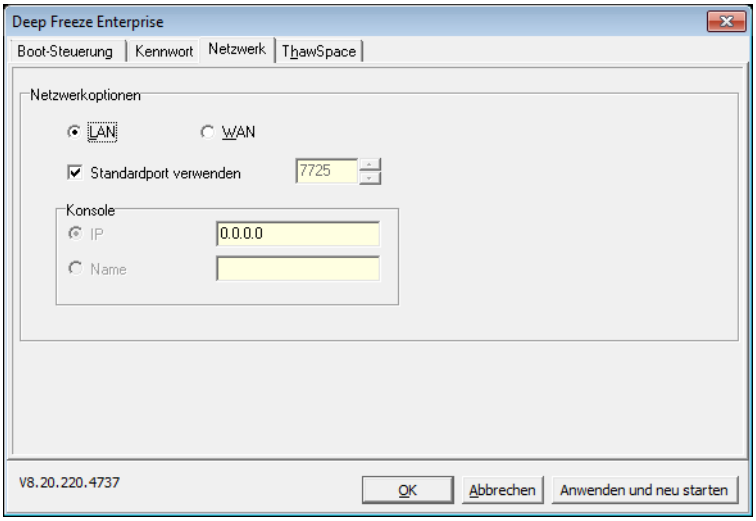
Über die Registerkarte *Passwort* können Sie das Passwort ändern.



1. Geben Sie im Feld *Neues Passwort eingeben* ein neues Passwort ein.
2. Bestätigen Sie das neue Passwort, indem Sie es erneut im Feld *Passwort bestätigen* eingeben.
3. Klicken Sie auf OK.
4. Das Passwort wird geändert, und ein Bestätigungsdialog wird angezeigt.

Registerkarte „Netzwerk“

Die Registerkarte *Netzwerk* kann verwendet werden, um die Netzwerkoptionen eines Computers zu konfigurieren.



Klicken Sie auf das gewünschte Optionsfeld, um zwischen den Kommunikationsmethoden *LAN* oder *WAN* auszuwählen.

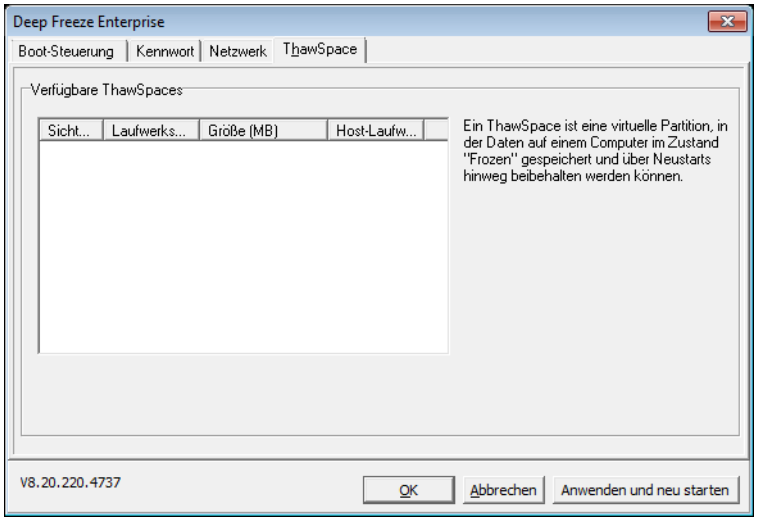
Die standardmäßige Portnummer kann geändert werden, indem Sie die Checkbox *Standardport verwenden* abwählen und die gewünschte Portnummer eingeben.

Weitere Informationen über die Netzwerkkonfiguration finden Sie unter Anhang B.

Registerkarte „Auftauplatz“

Ein *Auftauplatz* ist eine virtuelle Partition auf einem Computer, die verwendet werden kann, um Programme zu speichern, Dateien zu sichern oder dauerhafte Änderungen vorzunehmen. Alle im Auftauplatz gespeicherten Dateien bleiben nach einem Neustart erhalten, selbst wenn der Computer eingefroren ist.

Der Auftauplatz ist nur verfügbar, wenn im Deep Freeze Enterprise-Konfigurationsadministrator seine Erstellung eingestellt wurde.



Nach der Deinstallation von Deep Freeze werden alle Auftauplätze sichtbar gemacht. Wenn Deep Freeze erneut installiert wird, sind die den ursprünglichen Einstellungen auf der Registerkarte „Auftauplatz“ entsprechend entweder *Sichtbar* oder *Ausgeblendet*.

Ein vorhandener Auftauplatz wird bei einer Deinstallation gelöscht, wenn:

- Die Option, vorhandene Auftauplätze beizubehalten, im *Konfigurationsadministrator* nicht ausgewählt wurde
- Der Auftauplatz nicht mit Deep Freeze Version 5 oder höher erstellt wurde

Dauerhafte Softwareinstallationen, Änderungen oder Entfernungen

Computer müssen aufgetaut sein, damit dauerhafte Änderungen wirksam werden. Die Installation von Software erfordert häufig einen oder mehrere Neustarts, um die Installation abzuschließen.

Deep Freeze hilft Administratoren dabei, Herausforderungen bei der Beibehalten der Konfiguration ihrer Computer in einer Produktionsumgebung zu überwinden. Deep Freeze schützt Computer vor unbefugten Änderungen, Viren und Malware, die Computer in einen funktionsunfähig machen können. Deep Freeze bietet außerdem Funktionen, um Benutzerdaten zu speichern, ohne den Schutz des Computers zu beeinträchtigen.

Weitere Informationen darüber, wie Sie Deep Freeze implementieren können und dabei sicherstellen, dass die Benutzerdaten beibehalten werden, finden Sie unter *Deep Freeze – Verfügbare Benutzerdaten beibehalten* unter der Adresse http://www.faronics.com/library.



Anti-Virus verwalten

Dieses Kapitel beschreibt die Installation und Verwendung von Anti-Virus über die Enterprise Console.

Themen

Anti-Virus – Übersicht
Migration zum neuen Anti-Virus
Anti-Virus auf der Enterprise Console aktivieren
Den Anti-Virus Client auf dem Arbeitsplatz installieren
Anti-Virus-Konfiguration
Faronics Anti-Virus über die Enterprise Console verwenden
Anti-Virus-Aufgaben terminieren
Anti-Virus auf dem Arbeitsplatz verwenden
Nach Anti-Virus-Updates suchen
Faronics Anti-Virus aktualisieren
Den Anti-Virus-Client über die Enterprise Console deinstallieren
Faronics Anti-Virus über die Enterprise Console deaktivieren

Anti-Virus – Übersicht

Anti-Virus kann über die Enterprise Console installiert und verwendet werden. Die Verwendung von Anti-Virus ist optional. Deep Freeze Enterprise kann auch unabhängig ohne Anti-Virus verwendet werden.

Die folgenden Abschnitte werden erläutert:

- Anti-Virus auf der Enterprise Console aktivieren
- Den Anti-Virus Client auf dem Arbeitsplatz installieren
- Anti-Virus-Konfiguration
- Anti-Virus über die Enterprise Console verwenden
- Anti-Virus-Tasks terminieren
- Den Anti-Virus Client auf dem Arbeitsplatz verwenden
- Nach Updates suchen
- Faronics Anti-Virus aktualisieren
- Den Anti-Virus Client auf dem Arbeitsplatz deinstallieren
- Anti-Virus auf der Enterprise Console deaktivieren

Migration zum neuen Anti-Virus

Führen Sie die folgenden Schritte aus, um eine Migration zum neuen Anti-Virus durchzuführen:

1. Deinstallieren Sie das veraltete Anti-Virus.
2. Konfigurieren Sie die neue Anti-Virus-Richtlinie.
3. Installieren Sie das neue Anti-Virus.

Anti-Virus auf der Enterprise Console aktivieren

Anti-Virus ist jetzt Teil der Enterprise Console und kann aus dieser heraus aktiviert werden. Für Anti-Virus müssen Sie eine separate Lizenz erwerben.

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus zu aktivieren:

1. Starten Sie die *Deep Freeze Enterprise Console*
2. Gehen Sie auf *Tools* > *Lizenzen* > *Faronics Anti-Virus-Lizenz*.



3. Aktivieren Sie das Markierungsfeld *Ich möchte die Deep Freeze Console für die Verwaltung von Faronics Anti-Virus verwenden*.
4. Klicken Sie auf *Bearbeiten*.
5. Geben Sie den Lizenzschlüssel ein, und klicken Sie auf *Lizenz aktualisieren*.
6. Klicken Sie auf *Schließen*. Die Anti-Virus-Installationsdateien werden heruntergeladen. Die Anti-Virus-Spalten werden im Arbeitsplatzfenster angezeigt. Der Unterknoten "Anti-Virus" wird im Fenster "Netzwerk und Gruppen" unter *Verfügbare Konfiguration* hinzugefügt.

Den Anti-Virus Client auf dem Arbeitsplatz installieren

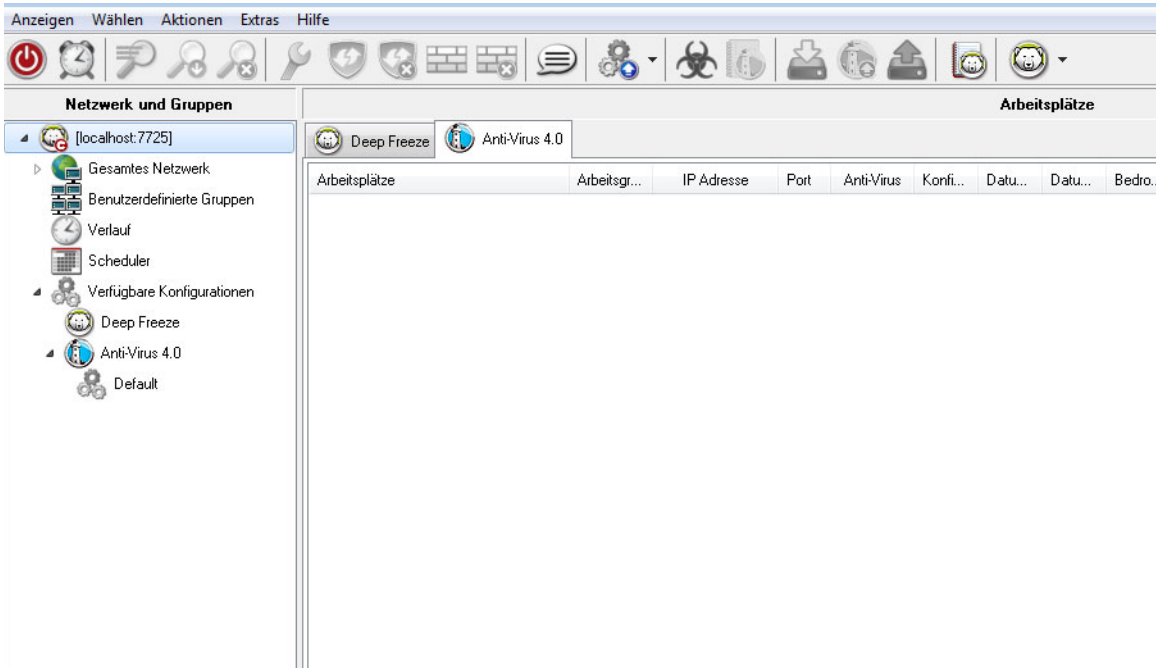
Bevor Sie Anti-Virus auf dem Arbeitsplatz installieren, stellen Sie sicher, dass die Deep Freeze-Arbeitsplatzinstallationsdatei oder der Deep Freeze-Seed auf dem Arbeitsplatz installiert wurde und dass sich der Arbeitsplatz im Zustand "aufgetaut" befindet.

Führen Sie die folgenden Schritte aus, um Anti-Virus auf dem Arbeitsplatz zu installieren:

1. Wählen Sie unter *Arbeitsplätze* > *Anti-Virus* einen einzelnen Arbeitsplatz oder mehrere Arbeitsplätze aus.
2. Klicken Sie in der Menüleiste auf das Anti-Virus-Symbol, und wählen Sie *Faronics Anti-Virus installieren* aus.
3. Aktivieren Sie das Markierungsfeld *Nicht kompatible Antivirus-Produkte vor der Installation von Faronics Anti-Virus entfernen*, um bestehende Antivirusprogramme zu entfernen.
4. Klicken Sie auf *OK*, um die Aktion zu bestätigen.

Der Arbeitsplatz wird neu gestartet, und der Anti-Virus-Client wird auf den Arbeitsplätzen installiert.

Die Anti-Virus-Optionen werden auf der Registerkarte Anti-Virus aktiviert.



Anti-Virus-Konfiguration

Eine Anti-Virus-Konfiguration enthält alle Einstellungen darüber, wie Anti-Virus auf dem Arbeitsplatz bzw. den Arbeitsplätzen läuft. Eine Konfiguration enthält die vom Programm durchgeführten Aktionen, den Zeitplan, den Proxy-Server, Fehlerberichte und die für den Benutzer auf dem Arbeitsplatz bzw. den Arbeitsplätzen zugängliche Funktionalität. Die folgenden Abschnitte erläutern die Erstellung und Anwendung einer Anti-Virus-Konfiguration.

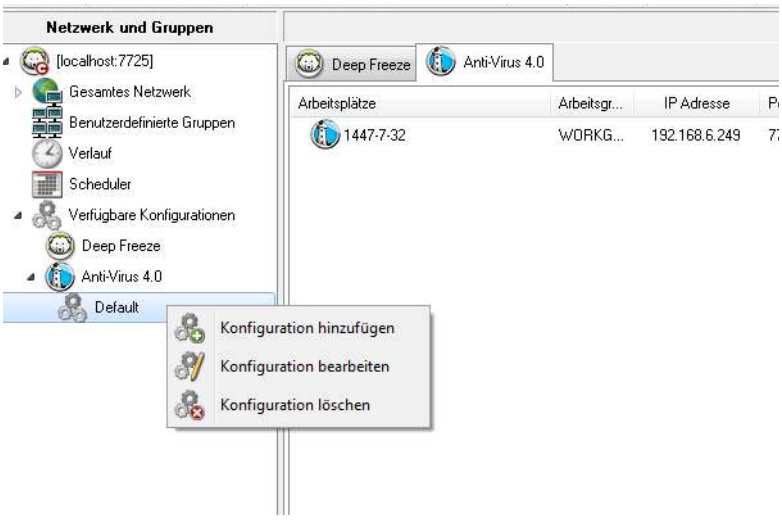


Anti-Virus enthält eine *Standard*konfiguration. Die Standardkonfiguration enthält die optimalen Konfigurationseinstellungen für die Verwaltung von Anti-Virus.

Anti-Virus-Konfiguration erstellen

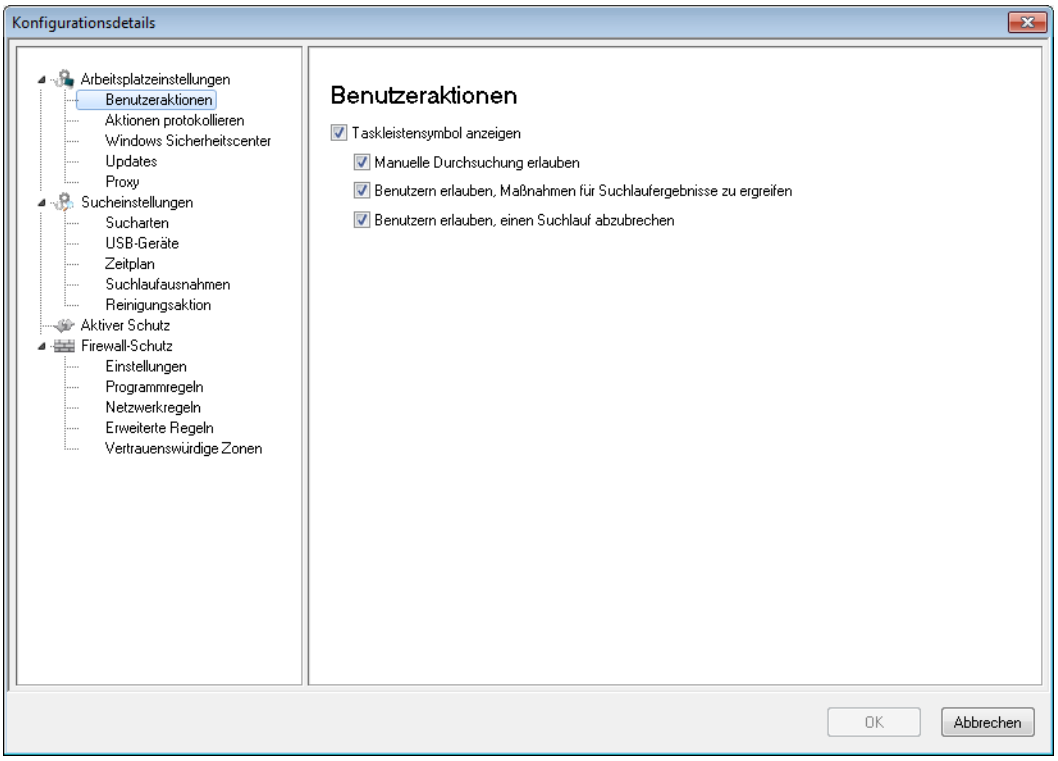
Führen Sie die folgenden Schritte aus, um eine neue Anti-Virus-Konfiguration zu erstellen:

1. Starten Sie die Enterprise Console.
2. Gehen Sie im Fenster *Netzwerk und Gruppen* auf *Verfügbare Konfigurationen* > *Anti-Virus*.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Neue Konfiguration erstellen* aus.



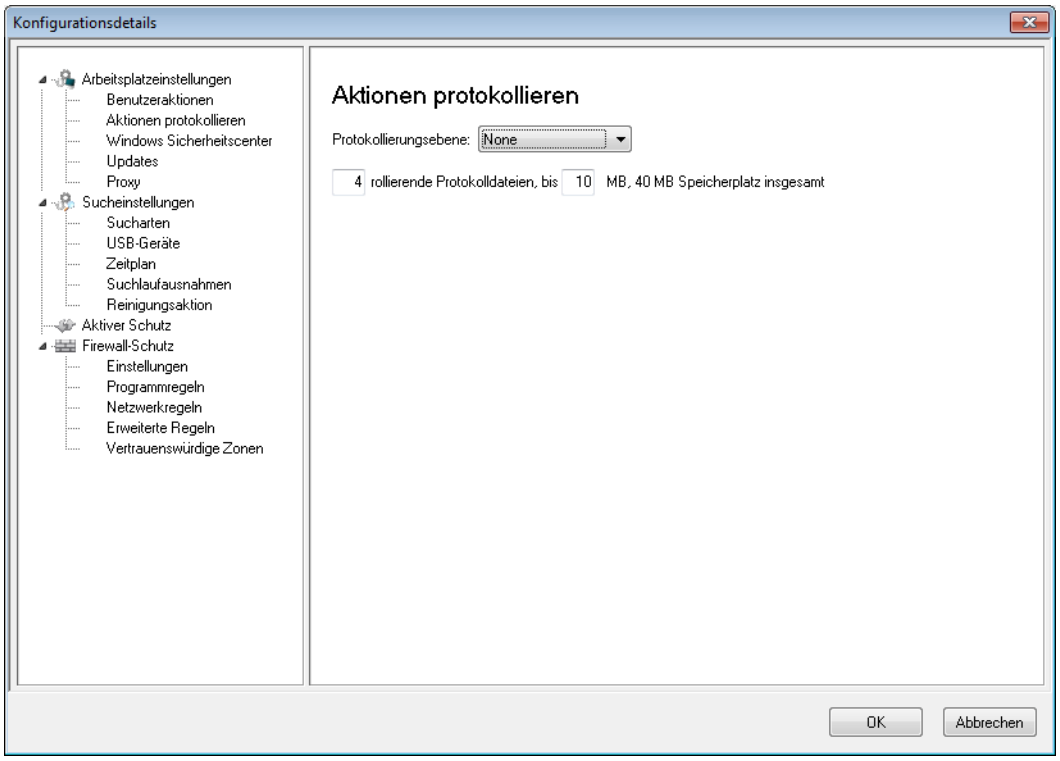
4. Geben Sie die Einstellungen unter dem Knoten *Arbeitsplatzeinstellungen* an:

- Teilfenster *Benutzeraktionen*



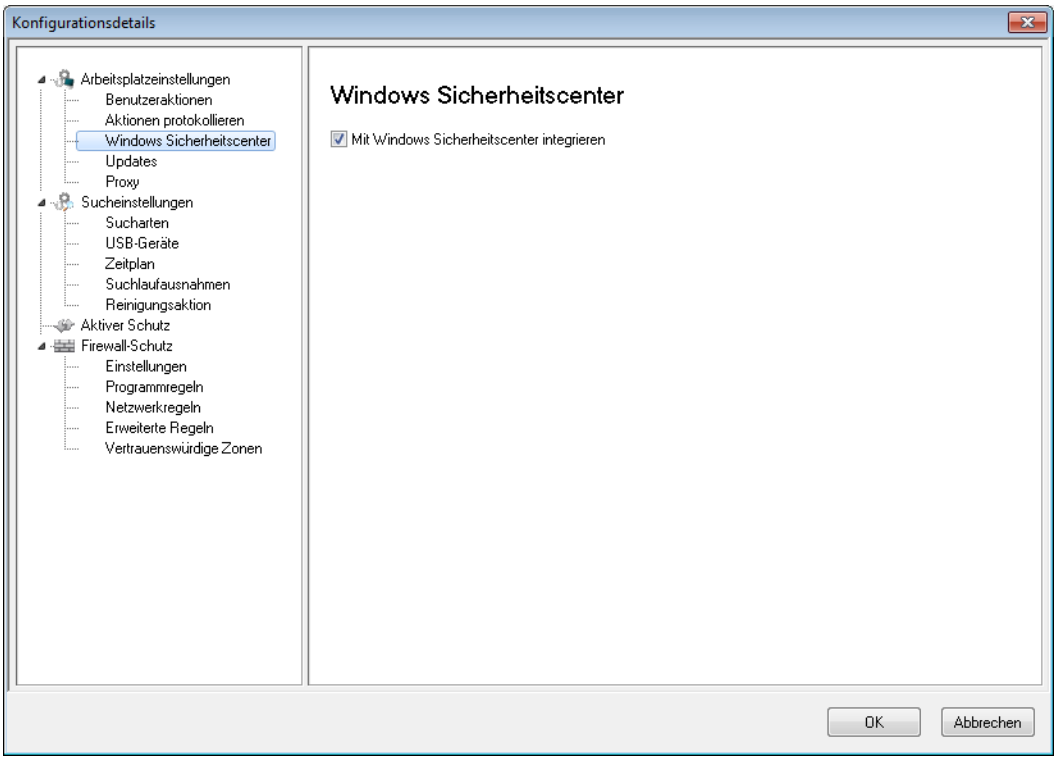
- Taskleistensymbol anzeigen – Wählen Sie dieses Markierungsfeld aus, um das Faronics Anti-Virus-Symbol in der Taskleiste des Arbeitsplatzes bzw. der Arbeitsplätze anzuzeigen. Wenn dieses Markierungsfeld nicht ausgewählt ist, wird Faronics Anti-Virus für den Benutzer ausgeblendet.
  - > Manuelle Durchsuchung erlauben – Wählen Sie dieses Markierungsfeld aus, um es Benutzern zu erlauben, einen Faronics Anti-Virus-Suchlauf auf dem Arbeitsplatz bzw. den Arbeitsplätzen manuell anzustoßen.
  - > Benutzern erlauben, Maßnahmen für Suchlaufergebnisse zu ergreifen – Wählen Sie dieses Markierungsfeld aus, um es Benutzern des Arbeitsplatzes zu erlauben, Maßnahmen für Suchlaufergebnisse zu ergreifen.
  - > Benutzern erlauben, einen Suchlauf lokal abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es Benutzern zu erlauben, den Suchlauf lokal auf dem Arbeitsplatz abzubrechen.

- Teilfenster *Aktionen protokollieren*



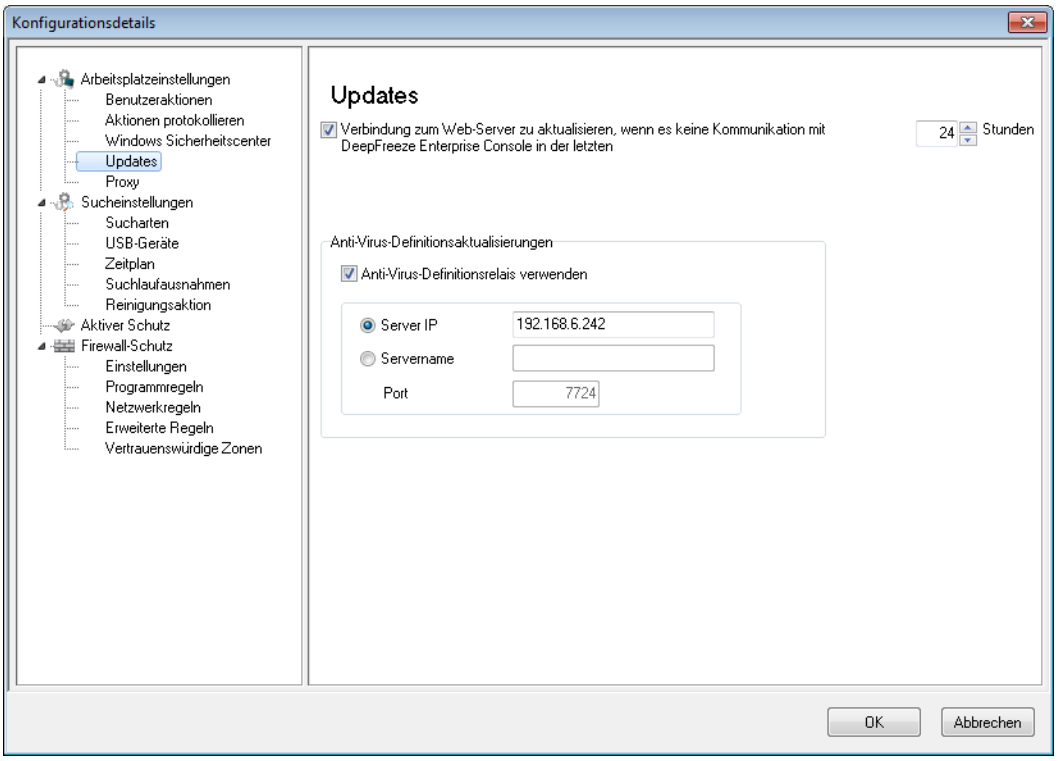
- Protokollierungsebene – Wählen Sie die Protokollierungsebene aus. Wählen Sie *Keine* aus, um keine Protokollierung einzustellen. Wählen Sie *Fehler* aus, um die Fehlermeldung zu protokollieren. Wählen Sie *Trace* für eine Nachverfolgung aus. Wählen Sie *Ausführlich* aus, um eine detaillierte Protokollierung zu erhalten.
- Anzahl Protokolldateien – Geben Sie die Anzahl der Protokolldateien an. Die Protokollinformationen werden seriell in den Dateien gespeichert. Wenn es beispielsweise drei Dateien A, B und C gibt, schreibt Faronics Anti-Virus die Fehlerprotokolle zunächst in Datei A. Wenn Datei A voll ist, werden die Protokolle in Datei B geschrieben, und schließlich in Datei C. Sobald Datei C voll ist, werden die Daten in Datei A gelöscht und mit neuen Protokolldaten überschrieben.
- Dateigröße – Wählen Sie die Größe der einzelnen Dateien in MB aus.

- Teilfenster *Windows Sicherheitscenter*



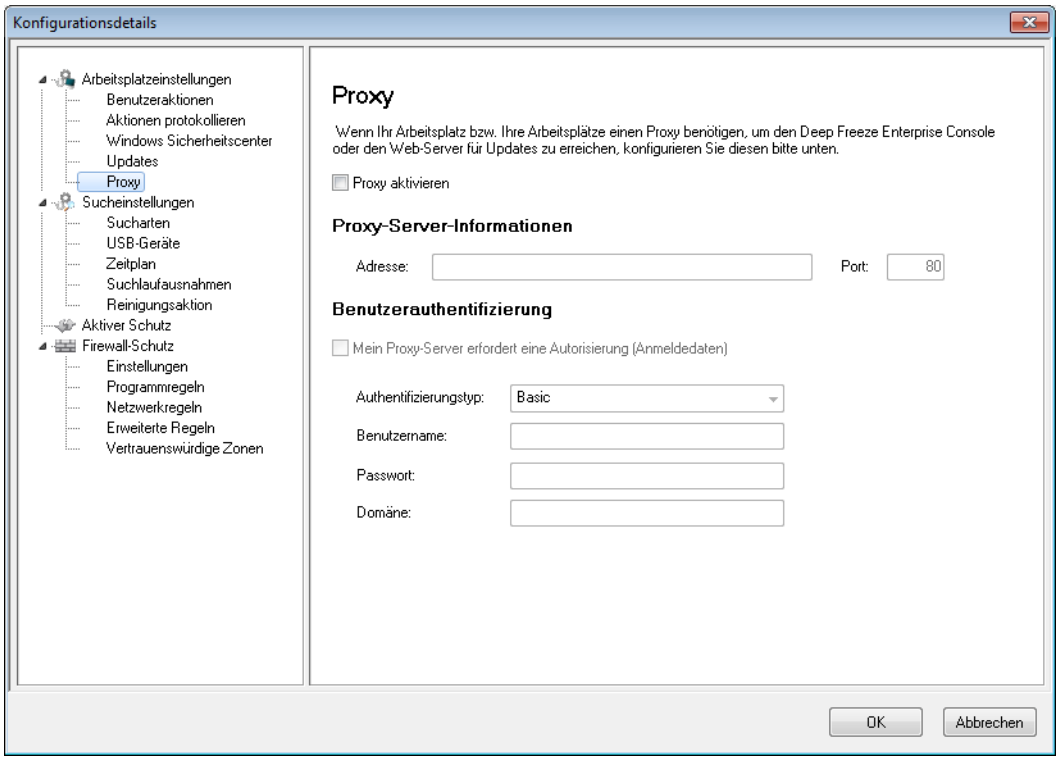
  - Mit Windows Sicherheitscenter integrieren – Wählen Sie dieses Markierungsfeld aus, um Faronics Anti-Virus mit dem Windows Sicherheitscenter zu integrieren. Das Windows Sicherheitscenter informiert Sie über die Taskleiste, ob Faronics Anti-Virus aktiv oder inaktiv ist.

- Teilfenster *Updates*



- Verbindung zum Web-Server für Updates herstellen, wenn es in den letzten x Stunden keine Kommunikation mit dem Faronics Core Server gab – Wählen Sie dieses Markierungsfeld aus, um eine Verbindung zum Web-Server für Updates herzustellen und Virusdefinitionen herunterzuladen, wenn der Kontakt zwischen dem Arbeitsplatz und dem Faronics Core Server unterbrochen wurde. Wenn Sie dieses Markierungsfeld nicht auswählen, werden die Virusdefinitionen nicht aktualisiert, wenn die Verbindung zwischen dem Arbeitsplatz und dem Faronics Core Server unterbrochen wird.

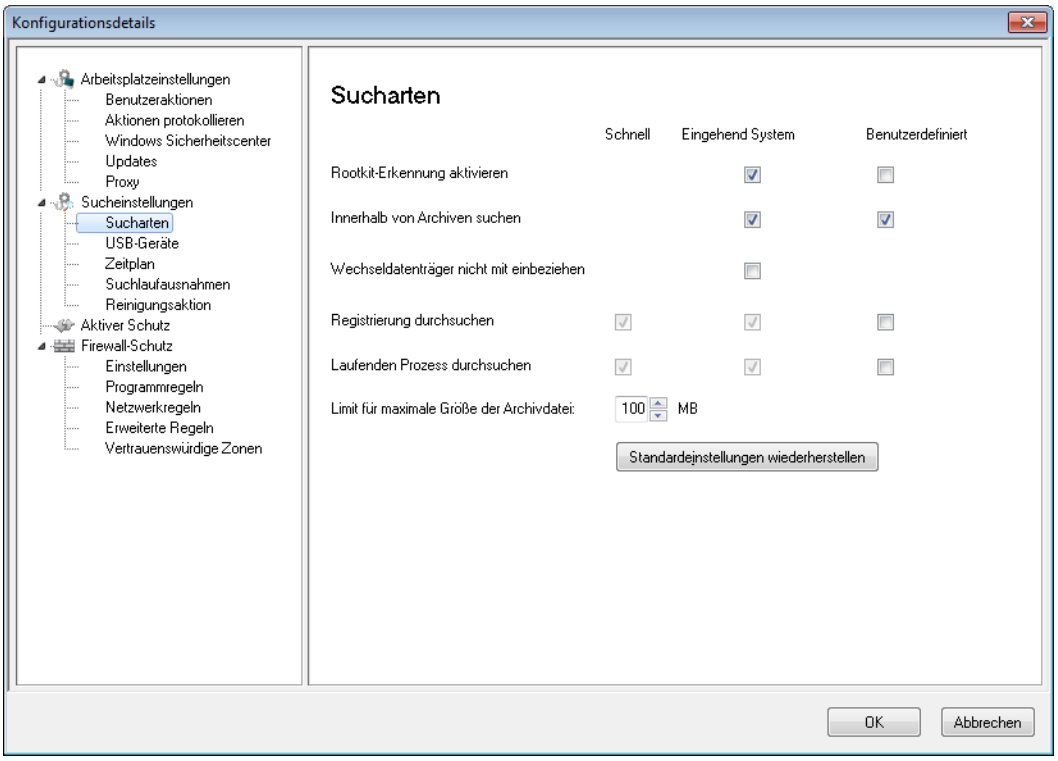
- Teilfenster *Proxy*



- Proxy aktivieren – Wählen Sie dieses Markierungsfeld aus, wenn der Arbeitsplatz bzw. die Arbeitsplätze einen Proxy benötigen, um den Faronics Core Server oder den Web-Server für Updates zu erreichen. Geben Sie die *Adresse* und den *Port* an.
- Mein Proxy-Server erfordert eine Autorisierung (Anmeldedaten) – Wenn der Server eine Authentifizierung erfordert, geben Sie Werte für die folgenden Felder an:
- Authentifizierungstyp – Wählen Sie den Authentifizierungstyp aus.
  - > Benutzername – Geben Sie den Benutzernamen an.
  - > Passwort – Geben Sie das Passwort an.
  - > Domäne – Geben Sie die Domäne an.

5. Geben Sie die Einstellungen unter dem Knoten *Suchlauf* an:

- Teilfenster *Sucheinstellungen* – Wählen Sie folgende Optionen für einen Schnellsuchlauf, eine eingehende Systemdurchsuchung und einen benutzerdefinierten Suchlauf aus:



Faronics Anti-Virus bietet drei Arten von Suchläufen:

- Schnellsuchlauf – Durchsucht die am häufigsten betroffenen Bereiche Ihres Computers. Die Dauer dieses Suchlaufs ist kürzer als die der eingehenden Systemdurchsuchung. Der Schnellsuchlauf verwendet außerdem weniger Speicherplatz als die eingehende Systemdurchsuchung.
- Eingehende Systemdurchsuchung – Führt einen gründlichen Suchlauf für alle Bereiche des Computers aus. Die für den Suchlauf in Anspruch genommene Zeit hängt von der Größe Ihrer Festplatte ab.
- Benutzerdefinierter Suchlauf – Führt einen Suchlauf auf der Basis der im Dialog *Richtliniendetails* ausgewählten Optionen durch.

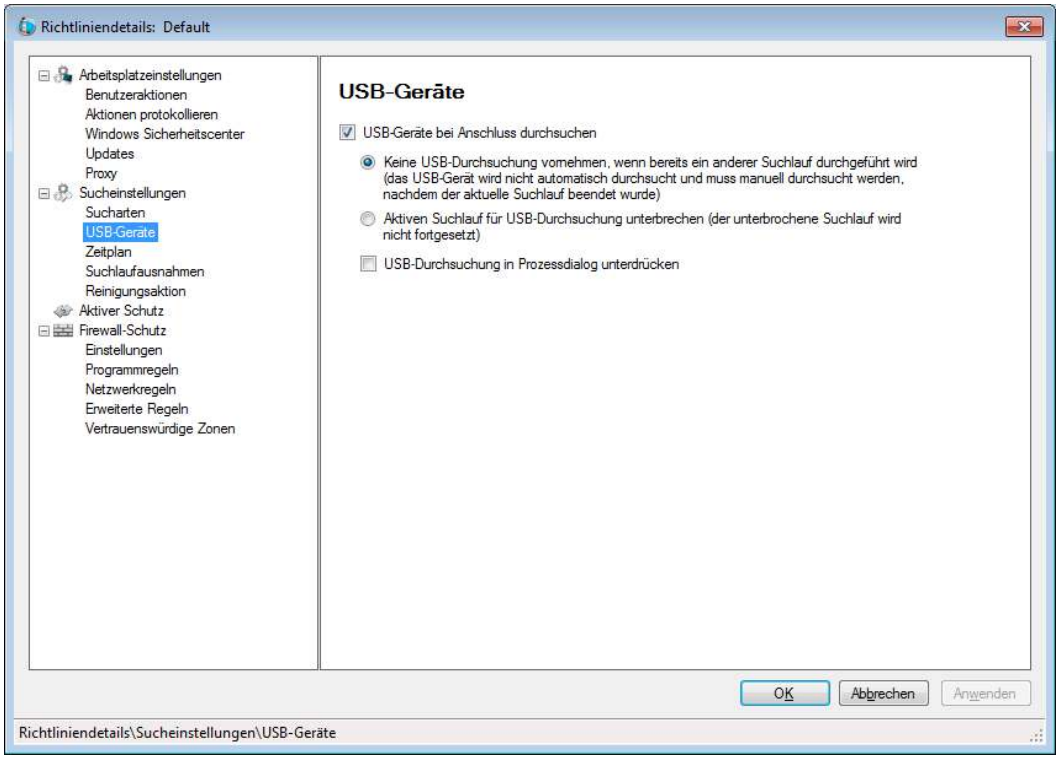
Wählen Sie für die einzelnen Sucharten die folgenden Optionen aus (manche Optionen sind, je nach Art des Suchlaufs, möglicherweise ausgeblendet):

- Rootkit-Erkennung aktivieren – Erkennt, ob der Computer mit einem Rootkit infiziert ist.
- Innerhalb von Archiven suchen – Durchsucht den Inhalt einer ZIP-Datei. Wenn Sie diese Option auswählen, berücksichtigt der Suchlauf auch Archivdateien wie .RAR- und .ZIP-Dateien. Wenn innerhalb einer .RAR-Datei eine infizierte Datei gefunden wird, wird die .RAR-Datei in Quarantäne gestellt. Wenn innerhalb einer .ZIP-Datei eine infizierte Datei gefunden wird, wird die infizierte Datei in Quarantäne gestellt und durch eine .TXT-Datei ersetzt, deren Text darauf hinweist, dass die Datei infiziert war und in Quarantäne gestellt wurde. Geben Sie die *Höchstgrenze für Dateigröße* an.
- Wechseldatenträger (z.B. USB) nicht mit einbeziehen – Schließt Wechseldatenträger aus dem Suchlauf aus. Externe Festplatten, USB-Laufwerke, etc. werden nicht

durchsucht.

- Registrierung durchsuchen – Durchsucht die Registrierung.
- Laufenden Prozess durchsuchen – Durchsucht alle laufenden Prozesse.

- Teilfenster *USB-Geräte* – Geben Sie die folgenden Einstellungen an:



USB-Laufwerke bei Anschluss durchsuchen – Wählen Sie dieses Markierungsfeld aus, um USB-Laufwerke bei Anschluss zu durchsuchen, und wählen Sie eine der folgenden Optionen aus:

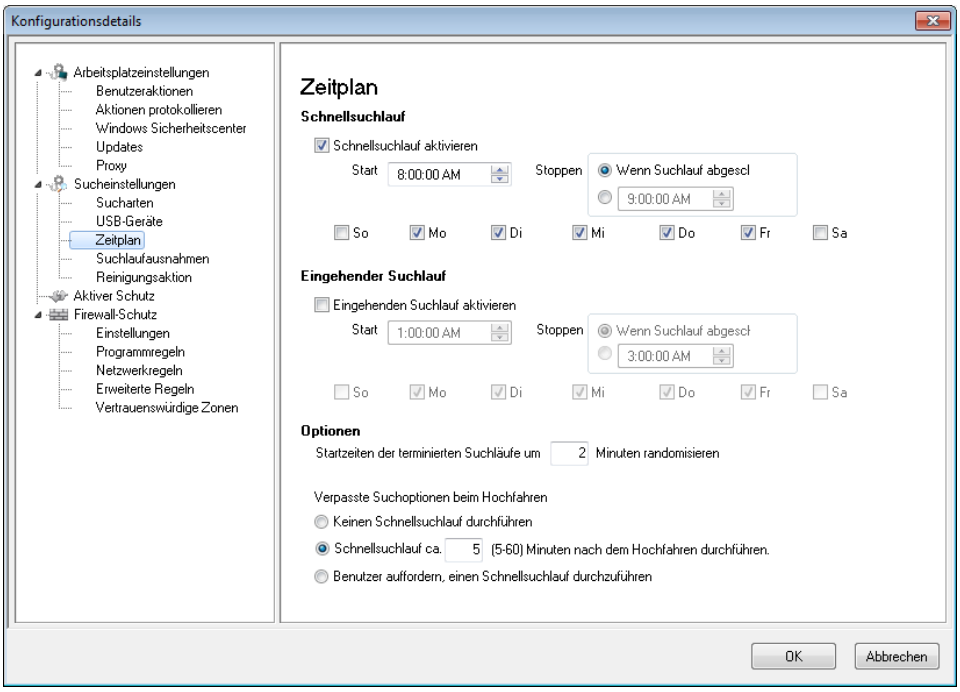
- Keine USB-Durchsuchung durchführen, wenn ein anderer Suchlauf bereits läuft – Wählen Sie diese Option aus, um sicherzustellen, dass ein aktiver Suchlauf nicht unterbrochen wird, wenn ein USB-Laufwerk angeschlossen wird. Das USB-Laufwerk muss manuell durchsucht werden, sobald der aktive Suchlauf abgeschlossen wurde.
- Aktiven Suchlauf für USB-Durchsuchung unterbrechen – Wählen Sie diese Option aus, um einen aktiven Suchlauf zu unterbrechen, um ein neu angeschlossenes USB-Laufwerk zu durchsuchen. Nachdem der aktive Suchlauf unterbrochen wurde, wird er nicht automatisch fortgesetzt und muss manuell neu gestartet werden.
- USB-Durchsuchung in Prozessdialog unterdrücken – Wählen Sie diese Option aus, um Anzeichen dafür, dass Anti-Virus USB-Geräte nach deren Anschluss durchsucht, auszublenden; es öffnet sich keine Anti-Virus-Benutzeroberfläche, und das Taskleistensymbol zeigt keine Tool-Tipps, die auf eine laufende Durchsuchung hindeuten. Benutzer werden am Ende eines Suchlaufs benachrichtigt, wenn ein Virus gefunden wurde. Wurden jedoch keine Viren erkannt, gibt es keine enachrichtigung über die Durchführung des Suchlaufs.

Beachten Sie, dass diese Option ignoriert wird, wenn die Option USB-Laufwerke bei Anschluss durchsuchen nicht ausgewählt ist.



Wenn das Markierungsfeld *Manuelle Durchsuchung erlauben* im Teilfenster *Benutzeraktionen* der Registerkarte *Arbeitsplatzeinstellungen* ausgewählt ist, wird das USB-Gerät automatisch durchsucht. Wenn das Markierungsfeld *Manuelle Durchsuchung erlauben* nicht ausgewählt ist, wird das USB-Gerät nicht automatisch durchsucht.

- Teilfenster *Zeitplan* – Geben Sie die folgenden Einstellungen an:



Schnellsuchlauf:

- Schnellsuchlauf aktivieren – Wählen Sie dieses Markierungsfeld aus, um den Schnellsuchlauf zu aktivieren.
- Start – Geben Sie die Startzeit an.
- Ende – Geben Sie die Endzeit an. Die maximale Dauer zwischen der *Startzeit* und der *Endzeit* beträgt *23:59* Stunden. Der Suchlauf endet, wenn vor Erreichen der *Endzeit* alle Dateien durchsucht wurden. Wenn der Suchlauf bis zur *Endzeit* nicht abgeschlossen ist, wird er zum *Endzeitpunkt* abgebrochen. Alternativ hierzu können Sie auch die Option *Wenn Suchlauf abgeschlossen ist* auswählen, um sicherzustellen, dass der Suchlauf abgeschlossen wird.
- Tage – Wählen Sie die Tage aus, an denen der terminierte Schnellsuchlauf durchgeführt werden soll.

Eingehender Suchlauf:

- Eingehenden Suchlauf aktivieren – Wählen Sie dieses Markierungsfeld aus, um den eingehenden Suchlauf zu aktivieren.
- Start – Geben Sie die Startzeit an.
- Ende – Geben Sie die Endzeit an. Die maximale Dauer zwischen der *Startzeit* und der *Endzeit* beträgt *23:59* Stunden. Der Suchlauf endet, wenn vor Erreichen der *Endzeit* alle Dateien durchsucht wurden. Wenn der Suchlauf bis zur *Endzeit* nicht

abgeschlossen ist, wird er zum *Endzeitpunkt* abgebrochen. Alternativ hierzu können Sie auch die Option *Wenn Suchlauf abgeschlossen ist* auswählen, um sicherzustellen, dass der Suchlauf abgeschlossen wird.

- Tage – Wählen Sie die Tage aus, an denen der terminierte eingehende Suchlauf durchgeführt werden soll.

Optionen:

- Startzeiten der terminierten Suchläufe um x Minuten randomisieren – Geben Sie die Anzahl der Minuten an. Die Startzeit der terminierten Suchläufe wird randomisiert, um die Auswirkungen auf den Datenverkehr im Netzwerk zu minimieren. Faronics Anti-Virus sendet eine Meldung an Faronics Core, wenn der Suchlauf beginnt. Dies kann zu einem erhöhten Datenaufkommen im Netzwerk führen, wenn der Suchlauf für mehrere Systeme gleichzeitig angestoßen wird.

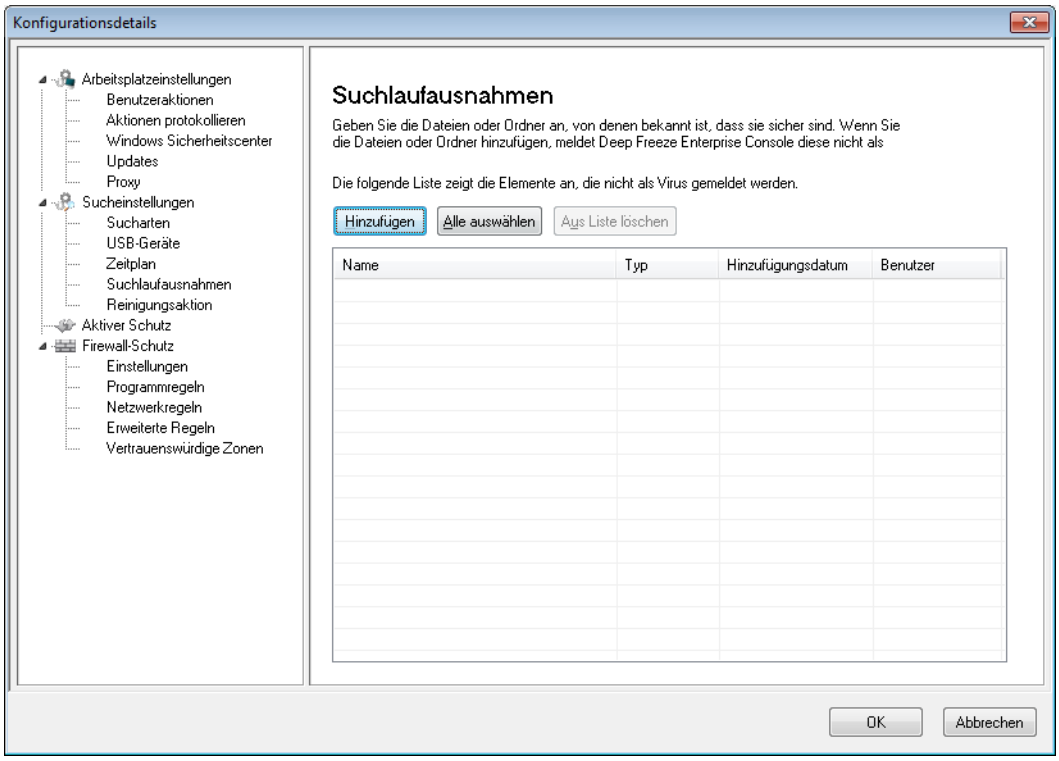
Optionen für verpasste Suchläufe beim Hochfahren – Wählen Sie eine der folgenden Optionen aus, die bestimmen, wie ein Suchlauf durchgeführt wird, wenn der Arbeitsplatz zum Zeitpunkt eines terminierten Suchlaufs nicht *eingeschaltet* war:

- Keinen Schnellsuchlauf durchführen – Wählen Sie diese Option aus, wenn Sie beim Hochfahren keinen Schnellsuchlauf durchführen möchten.
- Schnellsuchlauf ca. x Minuten nach dem Hochfahren durchführen – Geben Sie an, wie viele Minuten nach dem Hochfahren Faronics Anti-Virus einen Schnellsuchlauf durchführen soll.
- Benutzer auffordern, einen Schnellsuchlauf durchzuführen – Wählen Sie diese Option aus, um den Benutzer aufzufordern, einen Schnellsuchlauf durchzuführen.

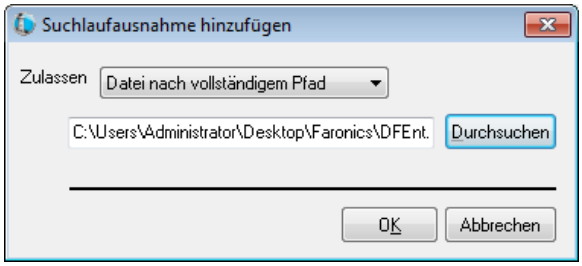
- Teilfenster *Suchlaufausnahmen* an:

  Ordner oder Dateien, von denen bekannt ist, dass sie sicher und infektionsfrei sind, können zur Registerkarte Suchlaufausnahmen hinzugefügt werden. Dateien, die zur Registerkarte Suchlaufausnahmen hinzugefügt werden, werden immer von Faronics Anti-Virus durchsucht. Faronics Anti-Virus meldet die Dateien jedoch niemals als schädlich oder infiziert. Diese Funktion ist nützlich, da Dateien und Ordner, von denen der Administrator weiß, dass sie sicher sind, nicht als schädlich gemeldet werden.

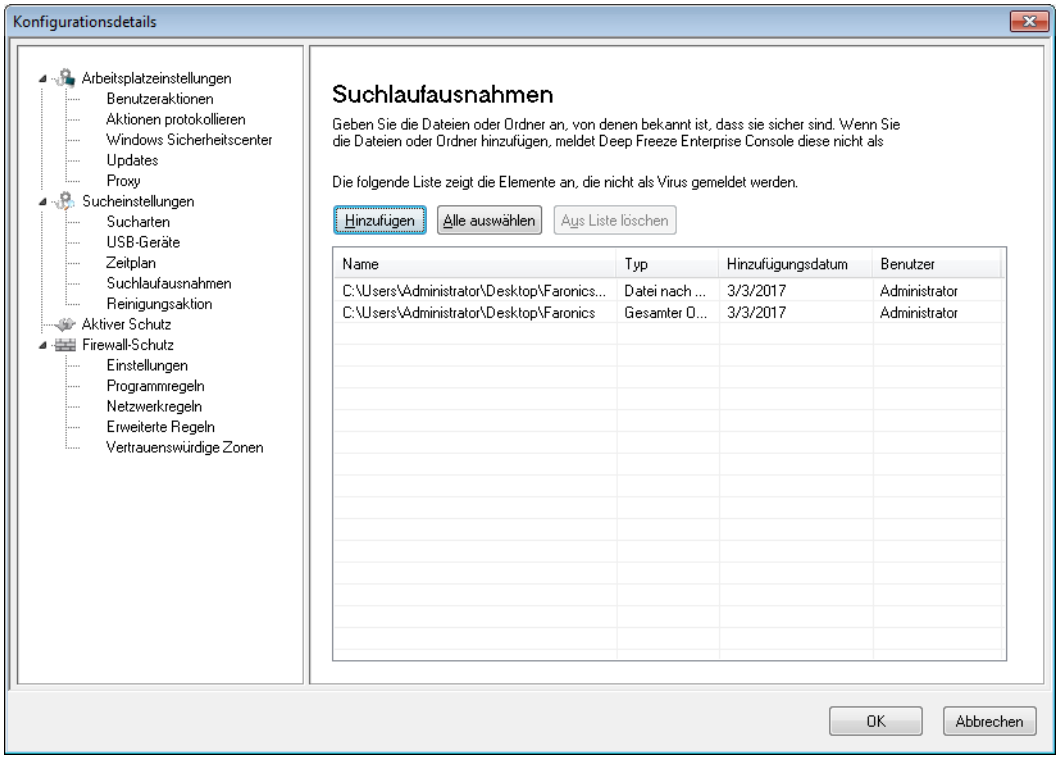
A. Klicken Sie auf *Hinzufügen*.



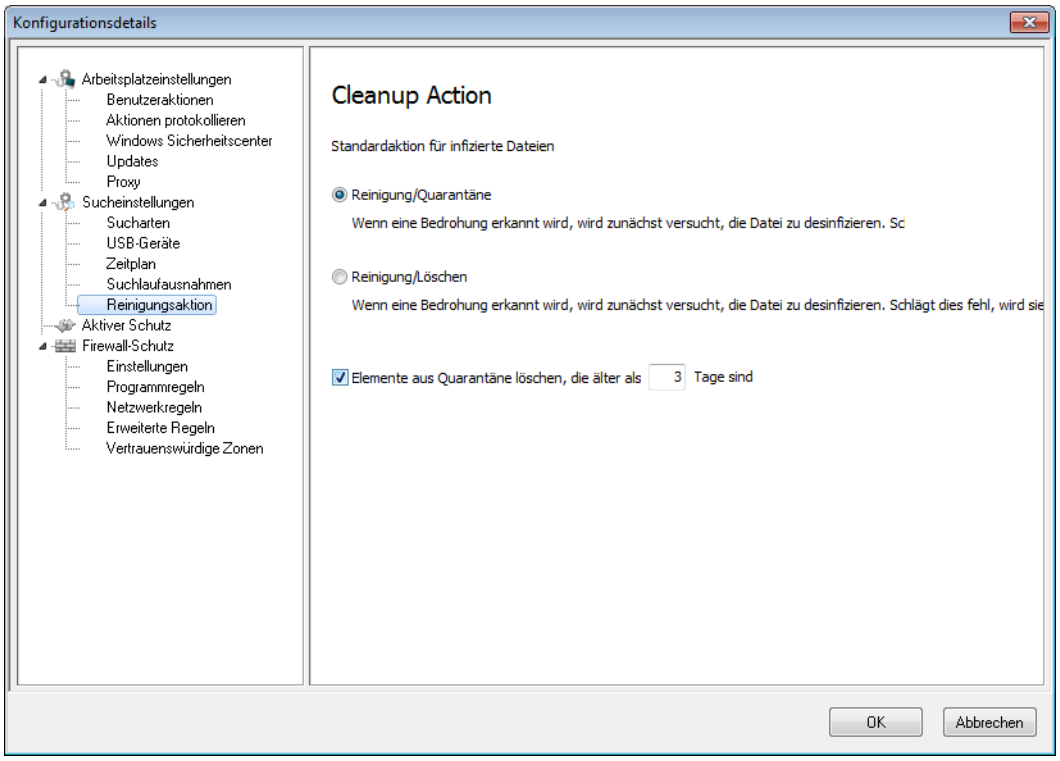
B. Wählen Sie im Dialog *Hinzufügen* entweder *Datei nach vollständigem Pfad*, oder *Gesamter Ordner* aus. Klicken Sie auf Durchsuchen, um die Datei oder den Ordner auszuwählen, und klicken Sie auf *OK*.



C. Die Option *Datei nach vollständigem Pfad* wird zum Teilfenster Suchlaufausnahmen hinzugefügt.



- Teilfenster *Reinigungsaktion* -Geben Sie die folgenden Einstellungen an:

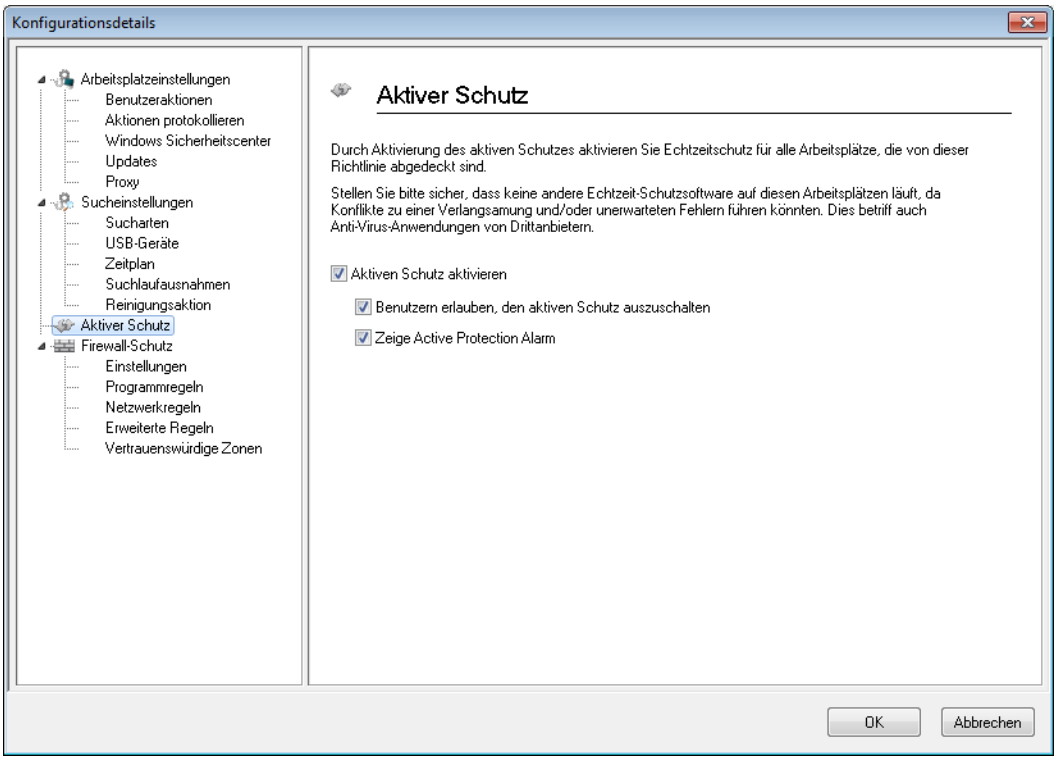


  - Reinigung/Quarantäne – Wenn eine Bedrohung erkannt wird, wird zunächst versucht, die Datei zu desinfizieren. Schlägt dies fehl, wird sie in Quarantäne

gestellt.

- Reinigung/Löschen – Wenn eine Bedrohung erkannt wird, wird zunächst versucht, die Datei zu desinfizieren. Schlägt dies fehl, wird sie gelöscht.
- Elemente aus Quarantäne löschen, die älter sind als – Geben Sie die Anzahl der Tage an, während derer Elemente in der Quarantäne vorgehalten werden sollen. Der Standardwert ist 3 Tage.

6. Geben Sie die Einstellungen im Teilfenster *Aktiver Schutz* an:

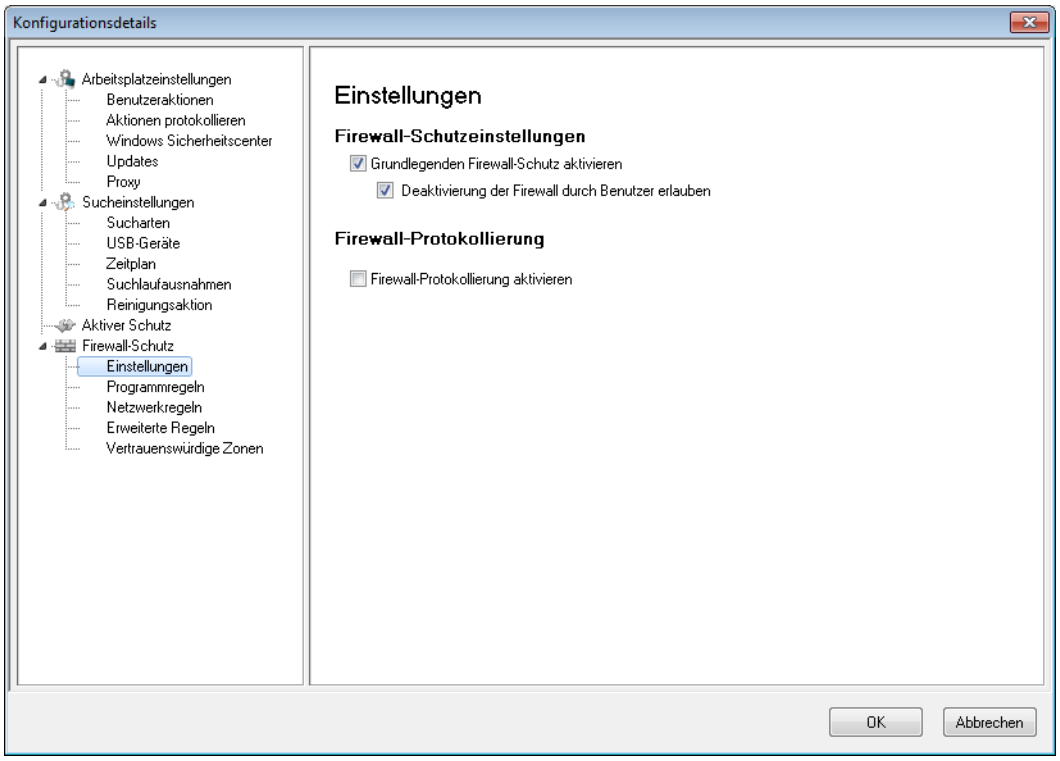


- Aktiven Schutz aktivieren – Wählen Sie diese Option aus, um Echtzeitschutz zu aktivieren. Der aktive Schutz ist die Echtzeitdurchsuchung, die Faronics Anti-Virus im Hintergrund ohne Auswirkungen auf die Systemleistung durchführt. Wenn das Risiko einer Echtzeitvirusinfektion über das Internet besteht, sollten Sie diese Option auswählen.
  - Benutzern erlauben, den aktiven Schutz auszuschalten – Wählen Sie diese Option aus, um es Benutzern zu erlauben, den aktiven Schutz auszuschalten. Wenn Benutzer Software installieren oder verwenden, die fälschlicherweise als Virus erkannt werden könnte (beispielsweise erweiterte Makros in Microsoft Office oder komplexe Batch-Dateien), wählen Sie diese Option aus.
  - Warnmeldung zum aktiven Schutz anzeigen – Wählen Sie diese Option aus, um eine Warnmeldung anzuzeigen, wenn während des aktiven Schutzes eine Bedrohung erkannt wird. Wählen Sie dieses Markierungsfeld nicht aus, wenn keine Warnmeldung angezeigt werden soll.

7. Geben Sie die Einstellungen unter dem Knoten *Firewall-Schutz* an:

   Der Knoten Firewall-Schutz bietet bidirektionalen Schutz und schützt Sie vor sowohl eingehendem als auch abgehendem Datenverkehr. Sie können individuell angepasste Regeln erstellen, um Ihr Netzwerk zu schützen. Sie können die Kommunikation entweder *Zulassen* oder *Blockieren*.

- Teilfenster *Einstellungen*



Firewall-Schutzeinstellungen

- Firewall-Schutz aktivieren – Wählen Sie dieses Markierungsfeld aus, um den Firewall-Schutz zu aktivieren. Der Firewall-Schutz hindert Hacker oder schädliche Software daran, sich über das Internet oder das Netzwerk Zugriff auf Ihren Computer zu verschaffen.

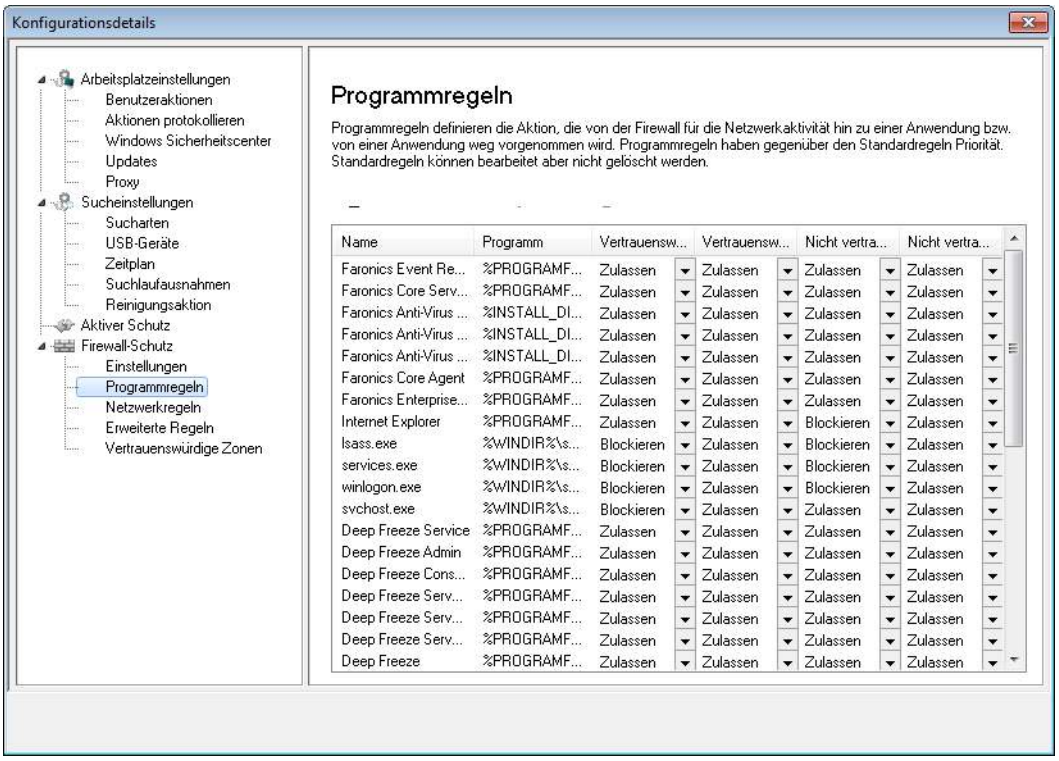
  > Deaktivierung der Firewall durch Benutzer erlauben – wählen Sie diese Option auf, um es Benutzern zu erlauben, die Firewall am Computer zu deaktivieren.

Firewall-Protokollierung

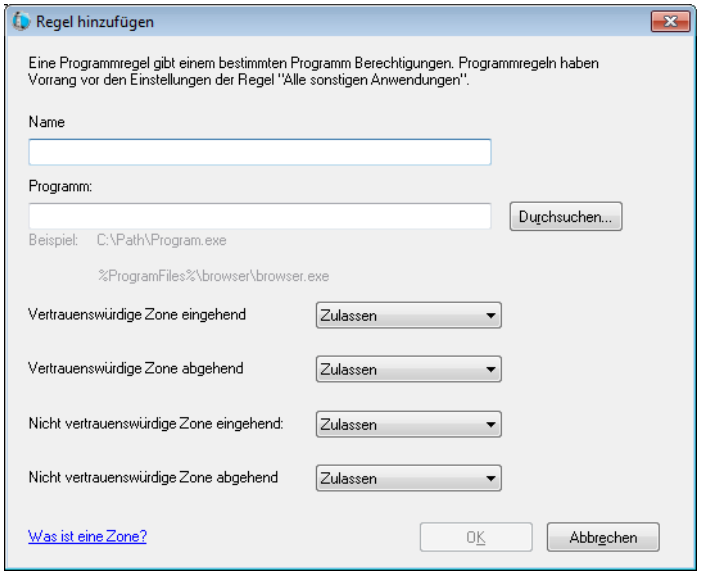
- Firewall-Protokollierung aktivieren – wählen Sie diese Option aus, um alle mit der Firewall zusammenhängenden Aktionen zu protokollieren.

- Teilfenster *Programmregeln*

Programmregeln definieren die Aktion, die von der Firewall für die Netzwerkaktivität hin zu einer Anwendung bzw. von einer Anwendung weg vorgenommen wird. Programmregeln haben gegenüber den Standardregeln Priorität. Standardregeln können bearbeitet aber nicht gelöscht werden.



Klicken Sie auf *Hinzufügen*, um eine neue Programmregel hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden angezeigt:

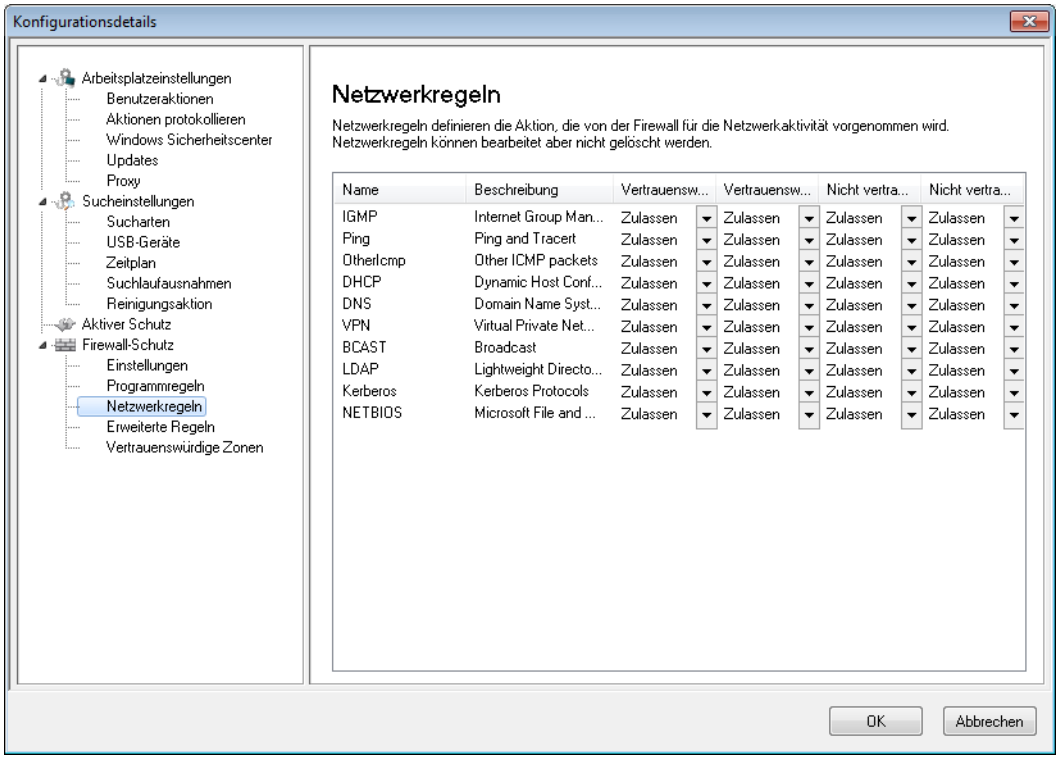


- Name – Name der Regel.
- Programm – Name des Programms, einschließlich des vollständigen Pfads und der Erweiterung.

- Vertrauenswürdige Zone eingehend – die Aktion wird für eingehende Kommunikation an das Programm in einer vertrauenswürdigen Zone vorgenommen (*Zulassen* oder *Sperren*).
- Vertrauenswürdige Zone abgehend – die Aktion wird für abgehende Kommunikation vom Programm in eine vertrauenswürdige Zone vorgenommen (*Zulassen* oder *Sperren*).
- Nicht vertrauenswürdige Zone eingehend – die Aktion wird für eingehende Kommunikation an das Programm in einer nicht vertrauenswürdigen Zone vorgenommen (*Zulassen* oder *Sperren*).
- Nicht vertrauenswürdige Zone abgehend – die Aktion wird für abgehende Kommunikation vom Programm in eine nicht vertrauenswürdige Zone vorgenommen (*Zulassen* oder *Sperren*).

- Teilfenster *Netzwerkregeln*

Netzwerkregeln definieren die Aktion, die von der Firewall für die Netzwerkaktivität vorgenommen wird. Netzwerkregeln können bearbeitet aber nicht gelöscht werden.



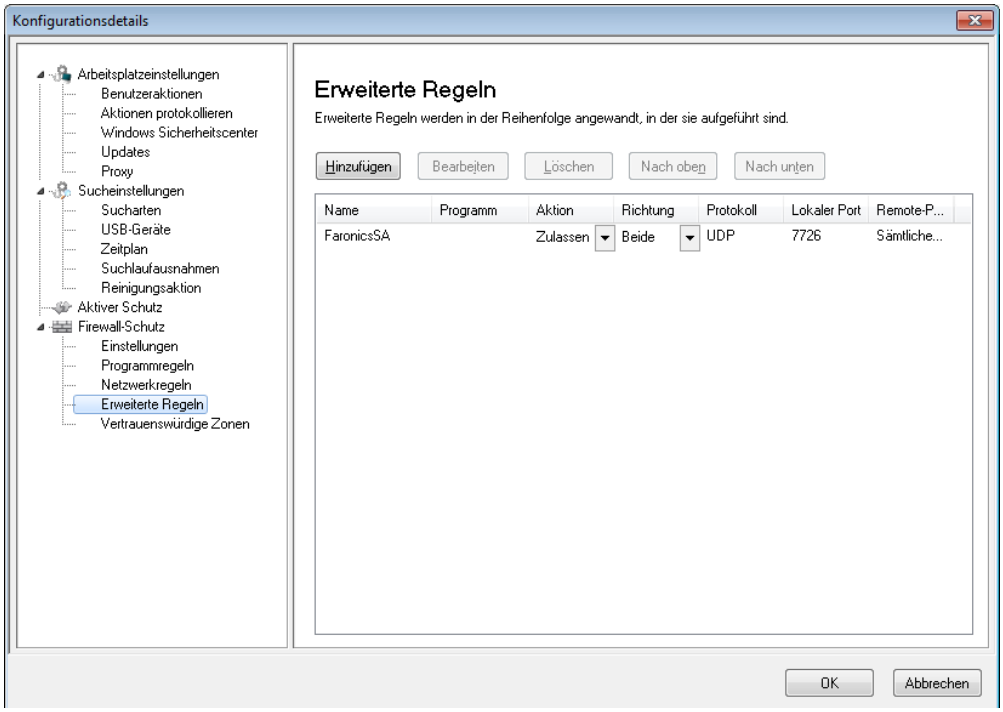
Wählen Sie für Folgendes die Netzwerkregeln aus:

Name	Beschreibung	Vertrauenswürdige Zone eingehend	Vertrauenswürdige Zone abgehend	Nicht vertrauenswürdige Zone eingehend	Nicht vertrauenswürdige Zone eingehend
IGMP	Internet Group Management Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus

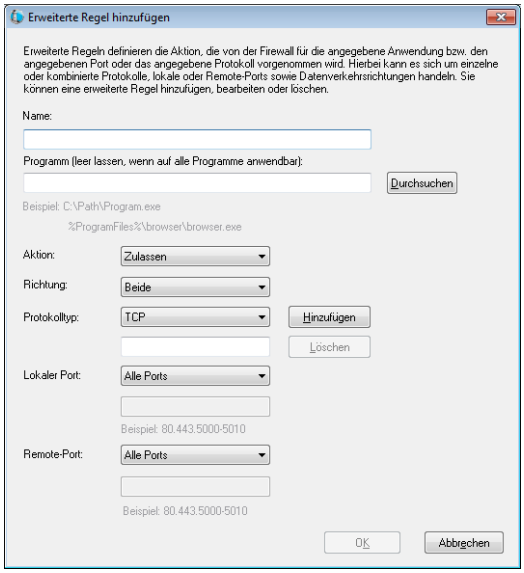
Name	Beschreibung	Vertrauenswürdige Zone eingehend	Vertrauenswürdige Zone abgehend	Nicht vertrauenswürdige Zone eingehend	Nicht vertrauenswürdige Zone eingehend
Ping	Ping und Tracert	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
OtherIcmp	Andere ICMP-Pakete	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
DHCP	Dynamic Host Configuration Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
DNS	Domain Name System	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
VPN	Virtual Private Network	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
BCAST	Broadcast	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
LDAP	Lightweight Directory Access Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
Kerberos	Kerberos-Protokolle	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
NETBIOS	Microsoft Gemeinsame Datei- und Druckernutzung	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus

- Teilfenster *Erweiterte Regeln*

Erweiterte Regeln definieren die Aktion, die von der Firewall für die angegebene Anwendung bzw. den angegebenen Port oder das angegebene Protokoll vorgenommen wird. Hierbei kann es sich um einzelne oder kombinierte Protokolle, lokale oder Remote-Ports sowie Datenverkehrsrichtungen handeln. Sie können eine erweiterte Regel hinzufügen, bearbeiten oder löschen.



Klicken Sie auf *Hinzufügen*, um eine neue erweiterte Regel hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden im Teilfenster Erweiterte Regeln angezeigt:

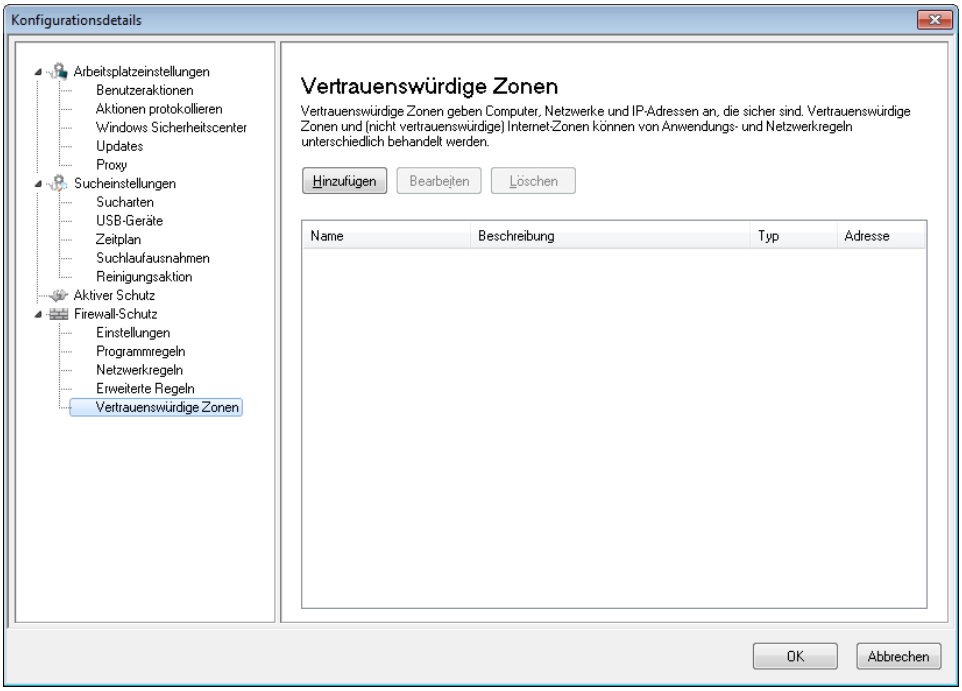


- Name – Name der Regel.
- Programm – Name des Programms und Pfad.

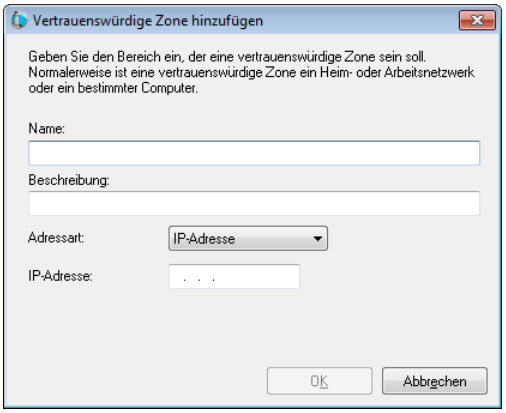
- Aktion – die von der Firewall für Kommunikation von der angegebenen Anwendung bzw. dem angegebenen Port oder Protokoll ergriffene Maßnahme (*Zulassen*, *Blockieren* oder *Benutzeraufforderung*).
- Richtung – die Richtung der Kommunikation (Beides, Eingehend, oder Abgehend).
- Protokoll – der Name des Protokolls.
- Lokaler Port – Details des lokalen Port.
- Remote-Port – Details des Remote-Port.

- Knoten *Firewall-Schutz* > Teilfenster *Vertrauenswürdige Zonen*

Vertrauenswürdige Zonen geben Computer, Netzwerke und IP-Adressen an, die vertrauenswürdig sind. Vertrauenswürdige Zonen und (nicht vertrauenswürdige) Internet-Zonen können von Programm- und Netzwerkregeln unterschiedlich behandelt werden.



Klicken Sie auf *Hinzufügen*, um eine neue vertrauenswürdige Zone hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden angezeigt:



- Name – Name der vertrauenswürdigen Zone.
- Beschreibung – Beschreibung der vertrauenswürdigen Zone.
- Art – Art der vertrauten Zone (IP-Adresse, oder Netzwerk).

8. Klicken Sie auf *OK*. Die neue Richtlinie *Neue Richtlinie 1* wird unterhalb des Knotens *Anti-Virus* angezeigt.

Anti-Virus-Konfiguration anwenden

Führen Sie die folgenden Schritte aus, um die Anti-Virus-Konfiguration anzuwenden:

1. Wechseln Sie zum Teilfenster *Arbeitsplätze*.
2. Wählen Sie einen oder mehrere Arbeitsplätze aus.
3. Klicken Sie mit der rechten Maustaste auf einen Arbeitsplatz bzw. auf mehrere Arbeitsplätze, und wählen Sie *Konfiguration aktualisieren* > *Anti-Virus* > *[Konfigurationsname]* aus.

Die Konfiguration wird auf den ausgewählten Arbeitsplatz bzw. die ausgewählten Arbeitsplätze angewandt.



Konfigurationsänderungen werden automatisch auf die erreichbaren Arbeitsplätze angewandt. Wenn die Arbeitsplätze nicht erreichbar sind, werden die Konfigurationsänderungen angewandt, sobald die Arbeitsplätze wieder erreichbar sind.

Anti-Virus-Konfiguration bearbeiten

Führen Sie die folgenden Schritte aus, um die Anti-Virus-Konfiguration zu bearbeiten:

1. Gehen Sie in der Enterprise Console zum Fenster Netzwerke und Gruppen.
2. Wählen Sie *Verfügbare Konfigurationen* > *Anti-Virus* > *[Konfigurationsname]* aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählte Konfiguration, und wählen Sie *Ausgewählte Konfiguration bearbeiten* aus.
4. Bearbeiten Sie die Einstellungen Ihren Anforderungen entsprechend.
5. Klicken Sie auf *OK*.

Anti-Virus-Konfiguration löschen

Führen Sie die folgenden Schritte aus, um die Anti-Virus-Konfiguration zu löschen:

1. Gehen Sie in der Enterprise Console zum Fenster Netzwerke und Gruppen.
2. Wählen Sie *Verfügbare Konfigurationen* > *Anti-Virus* > *[Konfigurationsname]* aus.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählte Konfiguration, und wählen Sie *Ausgewählte Konfiguration löschen* aus.
4. Klicken Sie auf *OK*.

Faronics Anti-Virus über die Enterprise Console verwenden

Nachdem der Faronics Anti-Virus-Client auf dem Arbeitsplatz installiert wurde, können über die Deep Freeze Console verschiedene Aktionen auf dem Arbeitsplatz ausgeführt werden.

Anti-Virus-Befehle

Es gibt zwei Möglichkeiten, um Befehle über die Deep Freeze Console einzugeben:

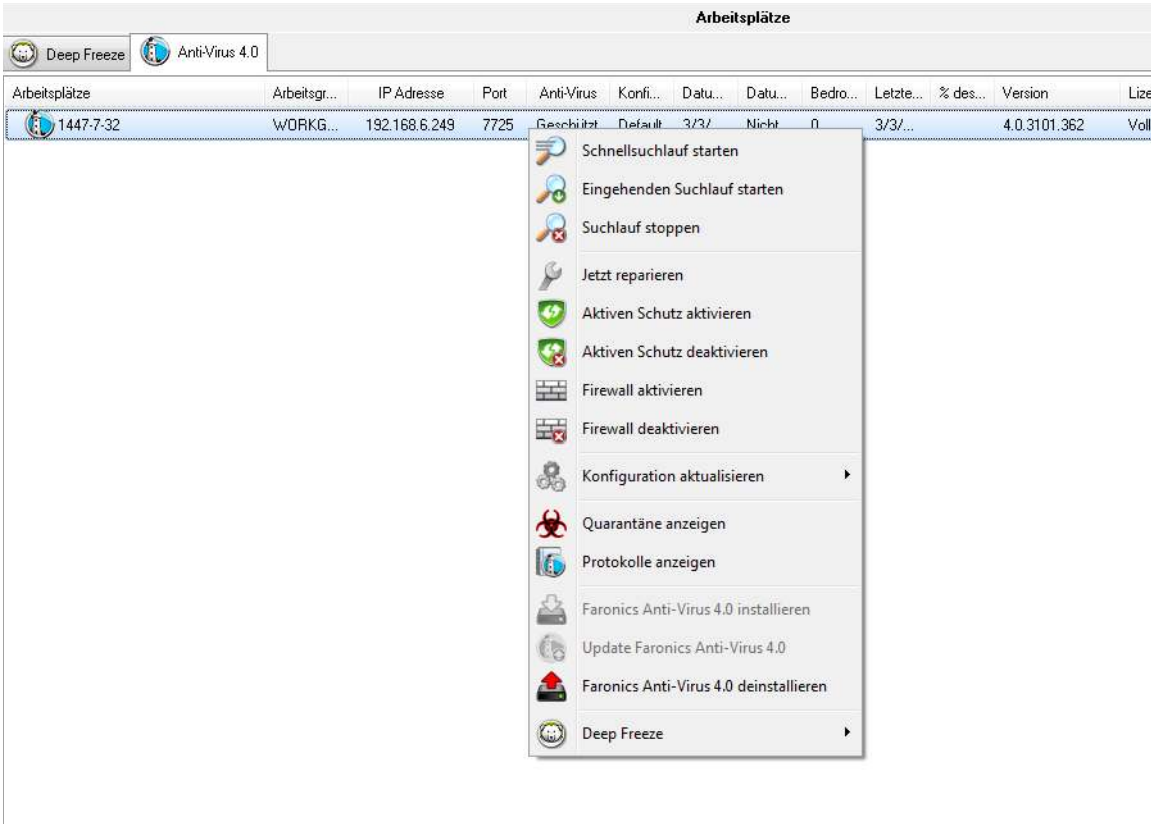
- Anti-Virus-Menü (in der Menüleiste)
- Anti-Virus-Kontextmenü (bei Rechtsklick)

Die Menübefehle werden in diesem Abschnitt näher erläutert.

Die folgenden Befehle sind im Anti-Virus-Menü verfügbar:



Dieselben Befehle sind auch über das Kontextmenü der Registerkarte *Anti-Virus* im Fenster *Arbeitsplätze* verfügbar:



Schnellsuchlauf

Der Schnellsuchlauf durchsucht die am häufigsten betroffenen Bereiche Ihres Computers. Die Dauer dieses Suchlaufs ist kürzer als die der eingehenden Systemdurchsuchung. Der Schnellsuchlauf verwendet außerdem weniger Speicherplatz als die eingehende Systemdurchsuchung.

- Einen Schnellsuchlauf starten

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf starten* aus.

- Einen Schnellsuchlauf stoppen

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf stoppen* aus.

- Einen Schnellsuchlauf anhalten

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf anhalten* aus.

- Einen Schnellsuchlauf fortsetzen

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf fortsetzen* aus.

Eingehender Suchlauf

Die eingehende Systemdurchsuchung führt einen gründlichen Suchlauf für alle Bereiche des Computers aus. Die für den Suchlauf in Anspruch genommene Zeit hängt von der Größe Ihrer Festplatte ab.

- Einen eingehenden Suchlauf starten

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Eingehenden Suchlauf starten* aus.

- Einen eingehenden Suchlauf stoppen

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Eingehenden Suchlauf stoppen* aus.

- Einen eingehenden Suchlauf anhalten

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf anhalten* aus.

- Einen eingehenden Suchlauf fortsetzen

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Schnellsuchlauf fortsetzen* aus.

Jetzt reparieren

Die Option Jetzt reparieren lädt die aktuellsten Virusdefinitionen herunter und führt einen Schnellsuchlauf auf dem Arbeitsplatz aus.

- Jetzt reparieren

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Jetzt reparieren* aus.

Aktiver Schutz

Der aktive Schutz ist eine Echtzeitmethode für die Erkennung von Malware. Der aktive Schutz läuft still im Hintergrund, während Sie arbeiten oder im Internet surfen und überwacht kontinuierlich die Dateien, die ausgeführt werden, ohne ihr System spürbar zu verlangsamen.

- Den aktiven Schutz aktivieren

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Aktiven Schutz aktivieren* aus.

- Den aktiven Schutz deaktivieren

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Aktiven Schutz deaktivieren* aus.

Firewall

Eine Firewall bietet bidirektionalen Schutz und schützt Sie vor sowohl eingehendem als auch abgehendem Datenverkehr. Eine Firewall schützt Ihr Netzwerk vor unbefugten Eindringlingen.

- Die Firewall aktivieren

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Firewall aktivieren* aus.

- Die Firewall deaktivieren

  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Firewall deaktivieren* aus.

Nachricht senden

Die Option Nachricht senden wird verwendet, um Nachrichten an Online-Arbeitsplätze zu senden.

- Eine Nachricht versenden

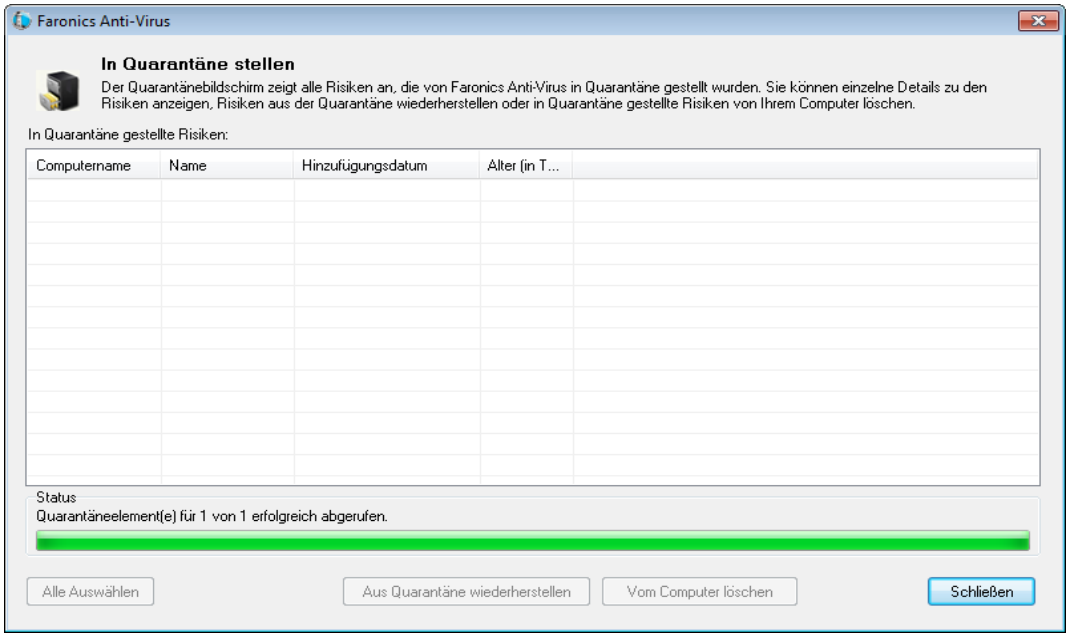
  Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Nachricht senden* aus.

Quarantäne-Informationen anzeigen

Der Quarantänebereich ist ein sicherer Bereich auf Ihrem Computer, den Faronics Anti-Virus verwendet, um Malware oder infizierte Dateien, die nicht desinfiziert werden konnten, zu speichern. Wenn sich Ihr Computer bzw. eine Datei auf Ihrem Computer nicht normal verhält, nachdem ein Element hier hinterlegt wurde, haben Sie die Möglichkeit, die Details eines Risikos zu überprüfen, es näher zu untersuchen und aus dem Quarantänebereich zu entfernen. Es wird dann an seiner ursprünglichen Position auf dem Computer wiederhergestellt. Sie können die riskanten Elemente auch dauerhaft aus der Quarantäne entfernen.

- Die Quarantäne-Informationen anzeigen

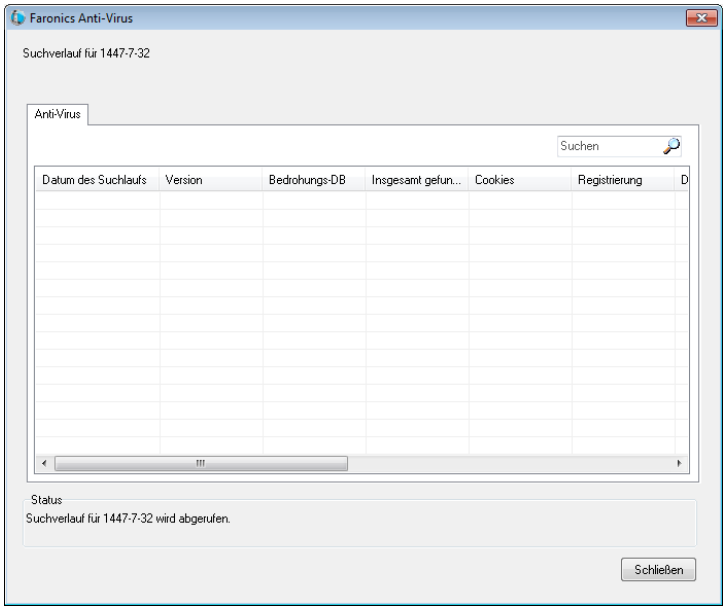
Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Faronics Anti-Virus* > *Quarantäne-Informationen abrufen* aus.



Suchverlauf anzeigen

Der Suchverlauf von Faronics Anti-Virus zeigt alle Aufgaben an, die von Faronics Anti-Virus auf dem Arbeitsplatz durchgeführt werden.

Wählen Sie einen einzelnen Arbeitsplatz aus, klicken Sie mit der rechten Maustaste darauf, und wählen Sie „Suchverlauf anzeigen" aus, um die Protokollinformationen anzuzeigen.



Anti-Virus-Aufgaben terminieren

Die folgenden Anti-Virus-Aufgaben können auf Basis eines vordefinierten Zeitplans über die Deep Freeze Console ausgeführt werden.

- Aktiven Schutz deaktivieren
- Aktiven Schutz aktivieren
- Schnellsuchlauf starten
- Eingehenden Suchlauf starten

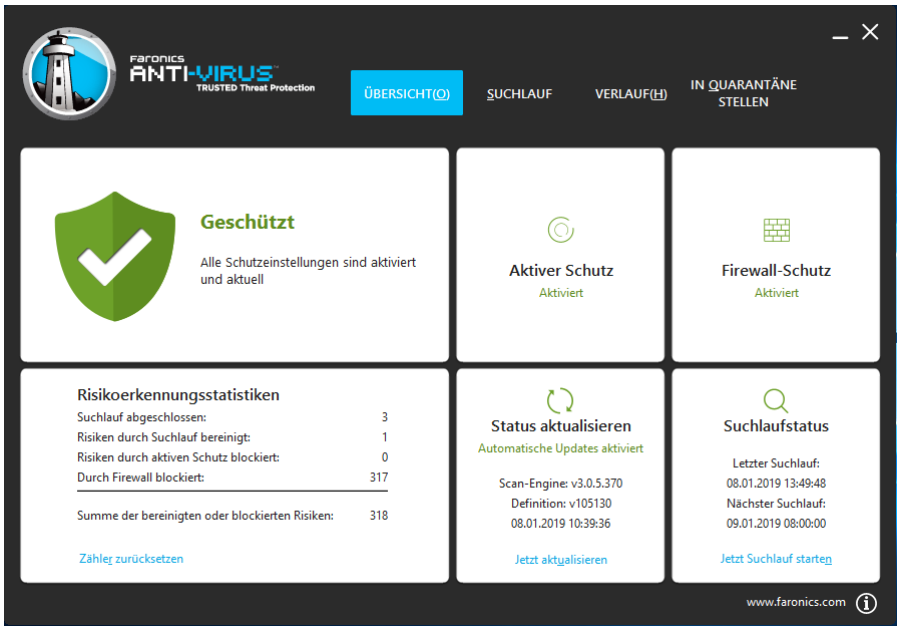
Das Verfahren für die Terminierung von Tasks ist im Abschnitt Deep Freeze-Aufgaben terminieren detailliert beschrieben.

Anti-Virus auf dem Arbeitsplatz verwenden

Die über Anti-Virus auf dem Arbeitsplatz verfügbaren Funktionen hängen voll und ganz von den in der Anti-Virus-Konfiguration ausgewählten Einstellungen ab. Weitere Informationen über die Anti-Virus-Konfiguration finden Sie unter Anti-Virus-Konfiguration.

Anti-Virus auf dem Arbeitsplatz starten

Gehen Sie auf *Start* > *Programme* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



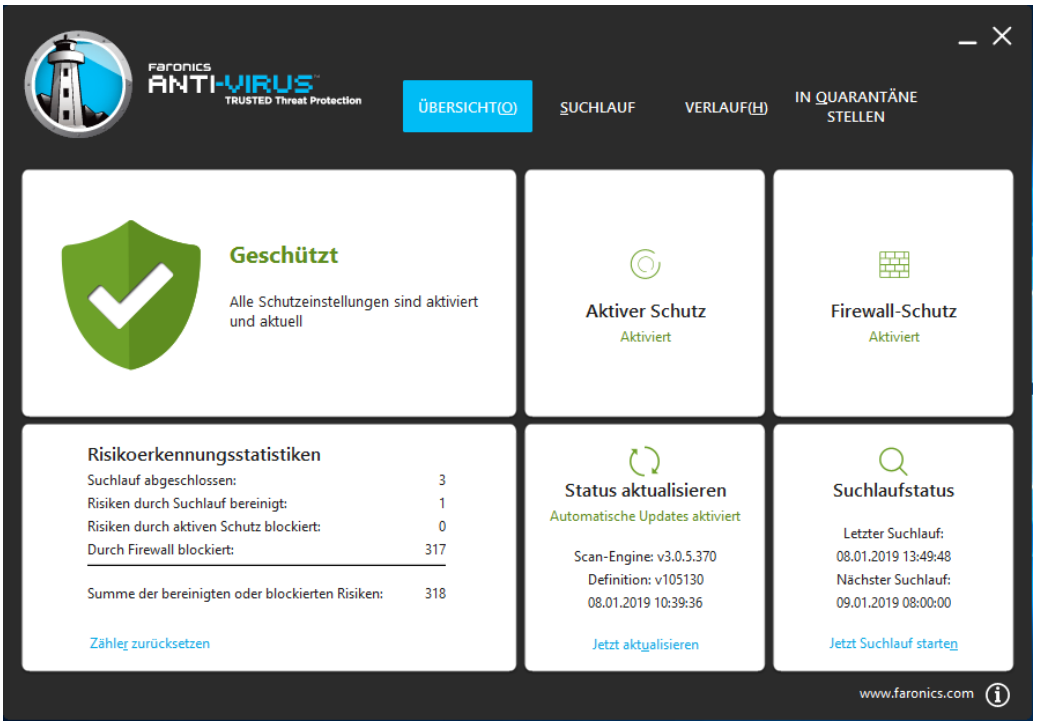
Die folgenden Teilfenster zeigen dem Benutzer wichtige Informationen an.

- *Geschützt* oder *Nicht geschützt* wird angezeigt, um anzugeben, ob der Computer geschützt ist oder nicht. Wenn „Nicht geschützt" angezeigt wird, klicken Sie auf die Schaltfläche *Jetzt reparieren* unter der Anzeige *Nicht geschützt*.
- *Suchlaufstatus* zeigt an, wann der letzte Suchlauf durchgeführt wurde. Sie können sofort einen Suchlauf durchführen, indem Sie auf den Link *Jetzt Suchlauf starten* klicken.
- *Update-Status* zeigt an, wann das letzte Update durchgeführt wurde. Sie können die Virusdefinitionen aktualisieren, indem Sie auf den Link *Jetzt aktualisieren* klicken.
- *Aktiver Schutz* zeigt an, ob der Echtzeitschutz aktiviert ist.
- *Firewall-Schutz* wird angezeigt, wenn der Arbeitsplatz durch die Firewall geschützt ist.
- *Risikoerkennungsstatistiken* zeigt die Statistiken für die von Faronics Anti-Virus ergriffenen Maßnahmen an. Klicken Sie auf *Zähler zurücksetzen*, um die Zähler auf null zurückzusetzen.

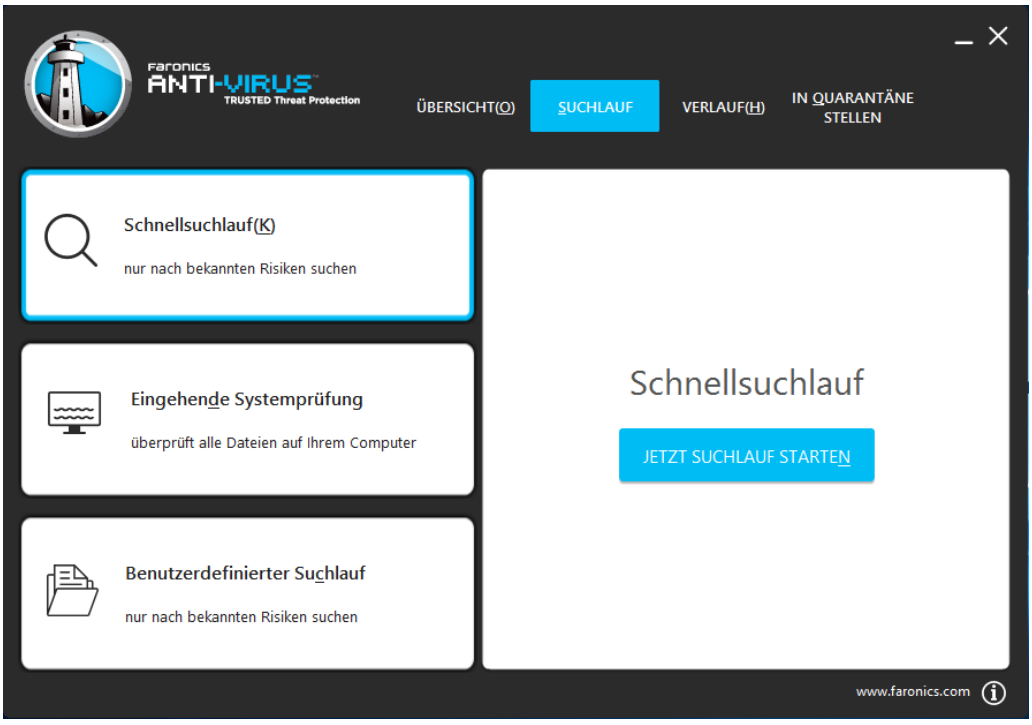
Den Arbeitsplatz durchsuchen

Führen Sie die folgenden Schritte aus, um einen Arbeitsplatz zu durchsuchen:

1. Gehen Sie auf *Start* > *Programme* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



2. Klicken Sie im Teilfenster *Suchlaufstatus* auf *Jetzt Suchlauf starten*. Die Registerkarte *Suchlauf* wird angezeigt. Alternativ hierzu können Sie auch auf die Registerkarte *Suchlauf* klicken.



3. Wählen Sie eine der folgenden Optionen aus:
   - Schnellsuchlauf – Sucht nur nach bekannten Bedrohungen.
   - Eingehende Systemdurchsuchung – Ein detaillierter Suchlauf aller Dateien auf dem Arbeitsplatz.
   - Benutzerdefinierter Suchlauf (Wählen Sie eine der folgenden Optionen aus):
     > Laufende Prozesse durchsuchen – Durchsucht die auf dem Arbeitsplatz laufenden Prozesse.
     > Registrierung durchsuchen – Durchsucht die Registrierungsdatenbank.
     > Geben Sie Laufwerke und Ordner an, die durchsucht werden sollen – Klicken Sie auf *Durchsuchen*, um die Ordner auszuwählen.
4. Klicken Sie auf *Jetzt Suchlauf starten*. Das sich drehende Symbol weist darauf hin, dass derzeit ein Suchlauf durchgeführt wird. Nach Beendigung des Suchlaufs werden die Suchlaufergebnisse angezeigt.
5. Wenn Sie eine Datei auswählen, stehen die folgenden Optionen zur Verfügung:
   - Wählen Sie *Reinigungsmaßnahme ändern* > *Empfohlene Maßnahme* aus, um die von Faronics Anti-Virus empfohlenen Maßnahmen umzusetzen.
   - Wählen Sie *Reinigungsmaßnahme ändern* > *In Quarantäne stellen/Desinfizieren* aus, um die Datei in Quarantäne zu stellen oder zu desinfizieren.
   - Wählen Sie *Reinigungsmaßnahme ändern* > *Löschen* aus, um die Datei zu löschen.
   - Wählen Sie *Reinigungsmaßnahme ändern* > *Zulassen* aus, um die Datei zuzulassen.
   - Klicken Sie auf *Alle auswählen,* um alle in den *Suchlaufergebnissen* angezeigten Dateien auszuwählen.
   - Klicken Sie auf *Details*, um die Details des Risikos anzuzeigen.
   - Klicken Sie auf *Abbrechen*, um den Dialog zu schließen, ohne Maßnahmen durchzuführen.
   - Klicken Sie auf *Bereinigen*, um die Datei zu entfernen und den Dialog zu schließen.

Eine Datei bzw. einen Ordner per Rechtsklick durchsuchen

Dateien oder Ordner (einzelne oder mehrere) können leicht auf Viren untersucht werden. Wenn Faronics Anti-Virus auf einem Arbeitsplatz installiert ist, wird die Option „Nach Viren durchsuchen“ zum Rechtsklickmenü hinzugefügt.

Führen Sie die folgenden Schritte aus, um eine Datei oder einen Ordner auf dem Computer zu durchsuchen:

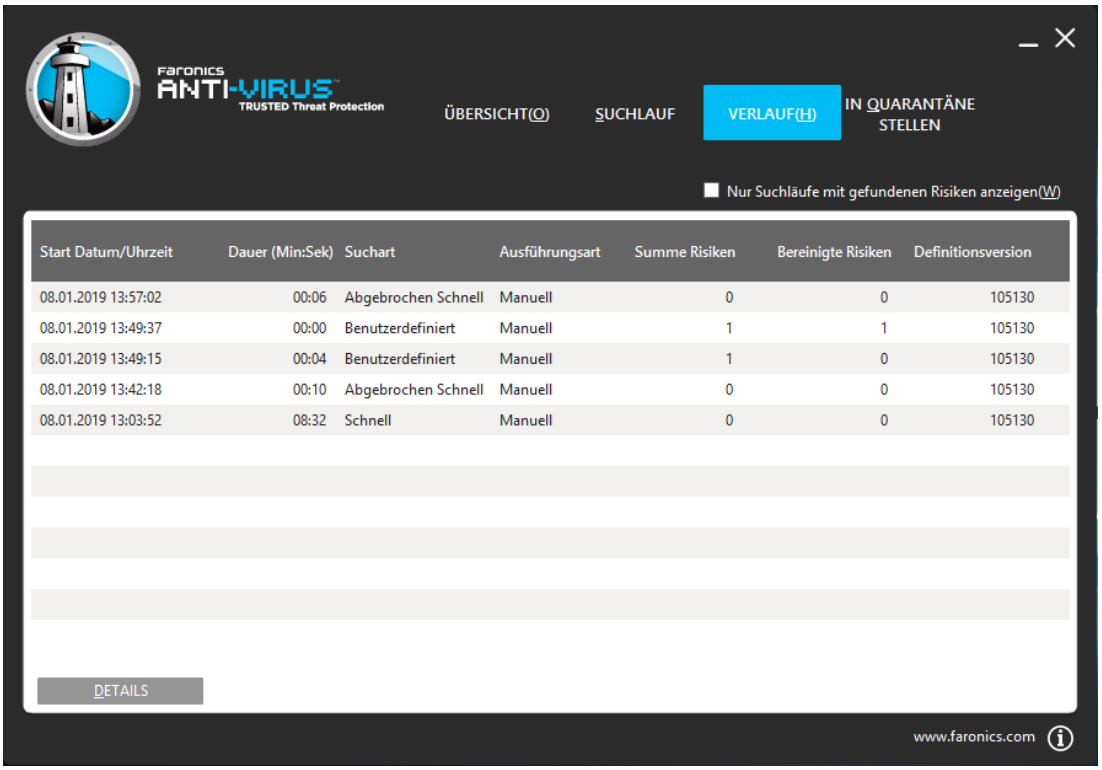
1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner.
2. Wählen Sie *Nach Viren durchsuchen* aus.

Der Suchlauf wird durchgeführt, und die Ergebnisse werden angezeigt.

Suchverlauf anzeigen

Führen Sie die folgenden Schritte aus, um den Suchverlauf anzuzeigen:

1. Gehen Sie auf *Start* > *Programme* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.
2. Klicken Sie auf die Registerkarte *Verlauf*.



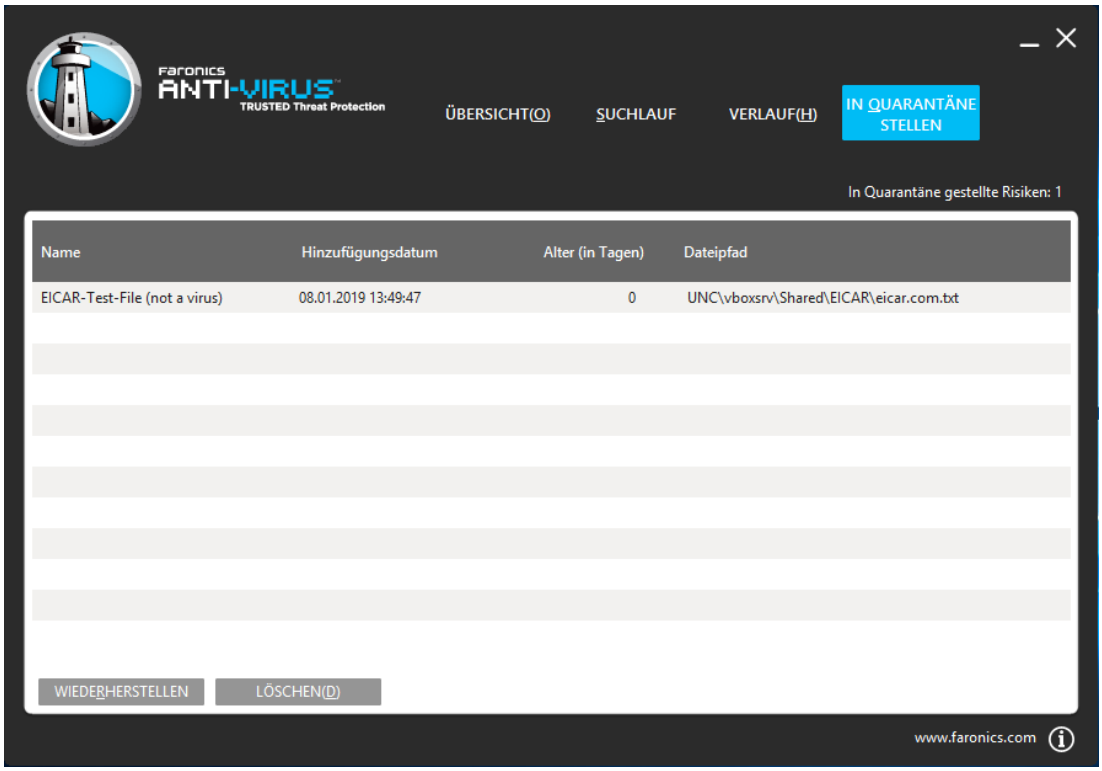
3. Wählen Sie die folgenden Aktionen aus:
   - Nur Suchläufe mit gefundenen Risiken anzeigen – Wählen Sie diese Option aus, um die diejenigen Suchläufe anzuzeigen, bei denen Risiken erkannt wurden.
   - Details – Wählen Sie einen Eintrag aus, und klicken Sie auf "Details", um detaillierte Informationen zum Suchlauf anzuzeigen.

In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen

Führen Sie die folgenden Schritte aus, um die Quarantäne anzuzeigen:

1. Gehen Sie auf *Start* > *Programme* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.

2. Klicken Sie auf die Registerkarte *Quarantäne*.

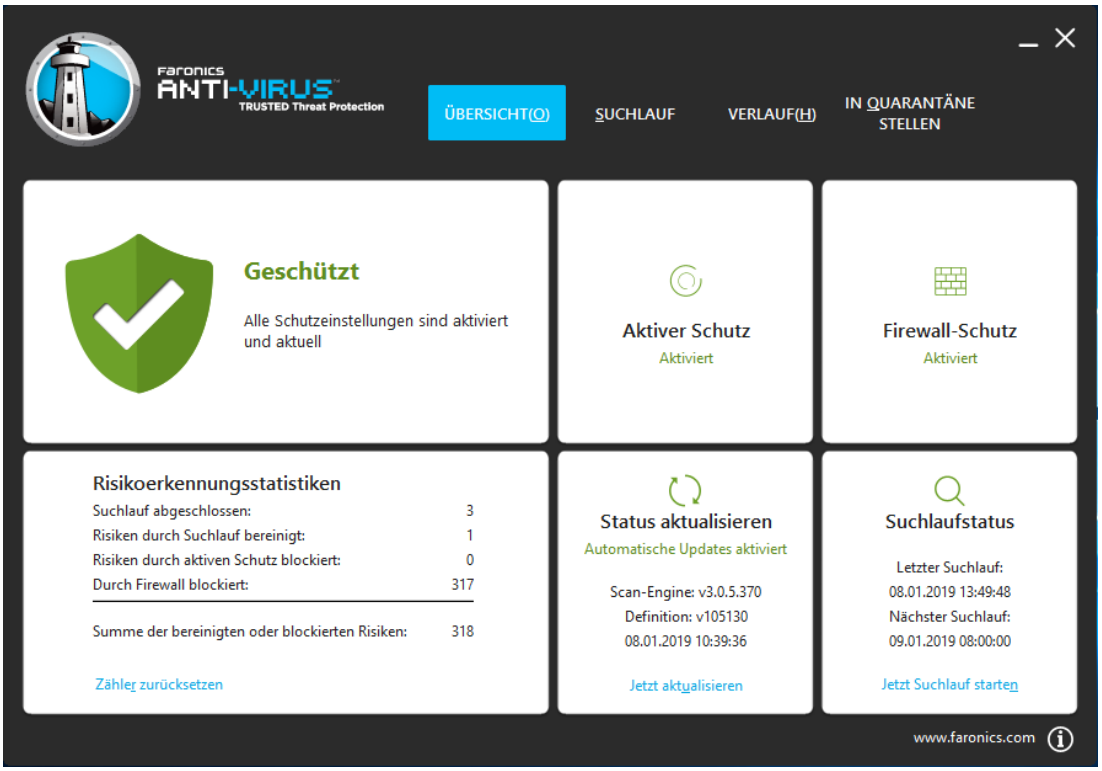


3. Klicken Sie auf *Risikodetails*. Die folgenden Informationen zu den einzelnen infizierten Dateien werden angezeigt:
   - Name
   - Hinzufügungsdatum
   - Alter (in Tagen)
4. Wählen Sie die folgenden Aktionen aus:
   - Details – Wählen Sie eine Datei aus, und klicken Sie auf *Details*, um die Details der infizierten Datei anzuzeigen. Hierdurch wird außerdem die empfohlene Aktion angezeigt.

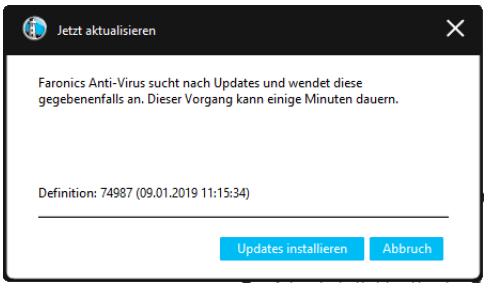
Antivirus-Definitionen auf dem Arbeitsplatz aktualisieren

Führen Sie die folgenden Schritte aus, um Anti-Virus-Definitionen auf dem Arbeitsplatz bzw. den Arbeitsplätzen zu aktualisieren:

1. Gehen Sie auf *Start* > *Programme* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



2. Klicken Sie im Teilfenster *Update-Status* auf *Jetzt aktualisieren*. Der Dialog *Jetzt aktualisieren* wird angezeigt.



3. Klicken Sie auf *Updates installieren*. Die Virusdefinitionen werden auf dem Arbeitsplatz aktualisiert.

Anti-Virus über die Taskleiste auf dem Arbeitsplatz verwalten

Faronics Anti-Virus kann auf dem Arbeitsplatz über ein Menü verwaltet wird, das in der Taskleiste angeboten wird.

Klicken Sie mit der rechten Maustaste auf das Faronics Anti-Virus-Symbol in der Tastleiste. Die folgenden Optionen sind verfügbar:

- Faronics Anti-Virus öffnen – Startet Faronics Anti-Virus auf dem Arbeitsplatz.
- Aktiver Schutz
  - Aktiver Schutz > Aktiven Schutz aktivieren – aktiviert den aktiven Schutz.
  - Aktiver Schutz > Aktiven Schutz deaktivieren > [Option auswählen] – Wählen Sie aus, wie lange der aktive Schutz deaktiviert werden soll. Wählen Sie 5 Minuten, 15 Minuten, 30 Minuten, 1 Stunde, Bis zum Neustart oder Dauerhaft aus. Diese Option

wird nur angezeigt, wenn sie in der Antivirenrichtlinie ausgewählt wurde.

- Jetzt Suchlauf starten > [Option auswählen] – Wählen Sie Suchlauf abbrechen, Schnellsuchlauf oder Eingehender Suchlauf aus. Diese Option wird nur angezeigt, wenn sie in der Antivirenrichtlinie ausgewählt wurde.
- Firewall-Schutz > Aktivieren oder Deaktivieren

Nach Anti-Virus-Updates suchen

Die Deep Freeze Console bietet die Möglichkeit, zu prüfen, ob neuere Versionen von Faronics Anti-Virus verfügbar sind.

Gehen Sie auf *Hilfe* > *Nach Updates suchen*. Hierdurch wird geprüft, ob eine neue Version von Faronics Anti-Virus verfügbar ist.

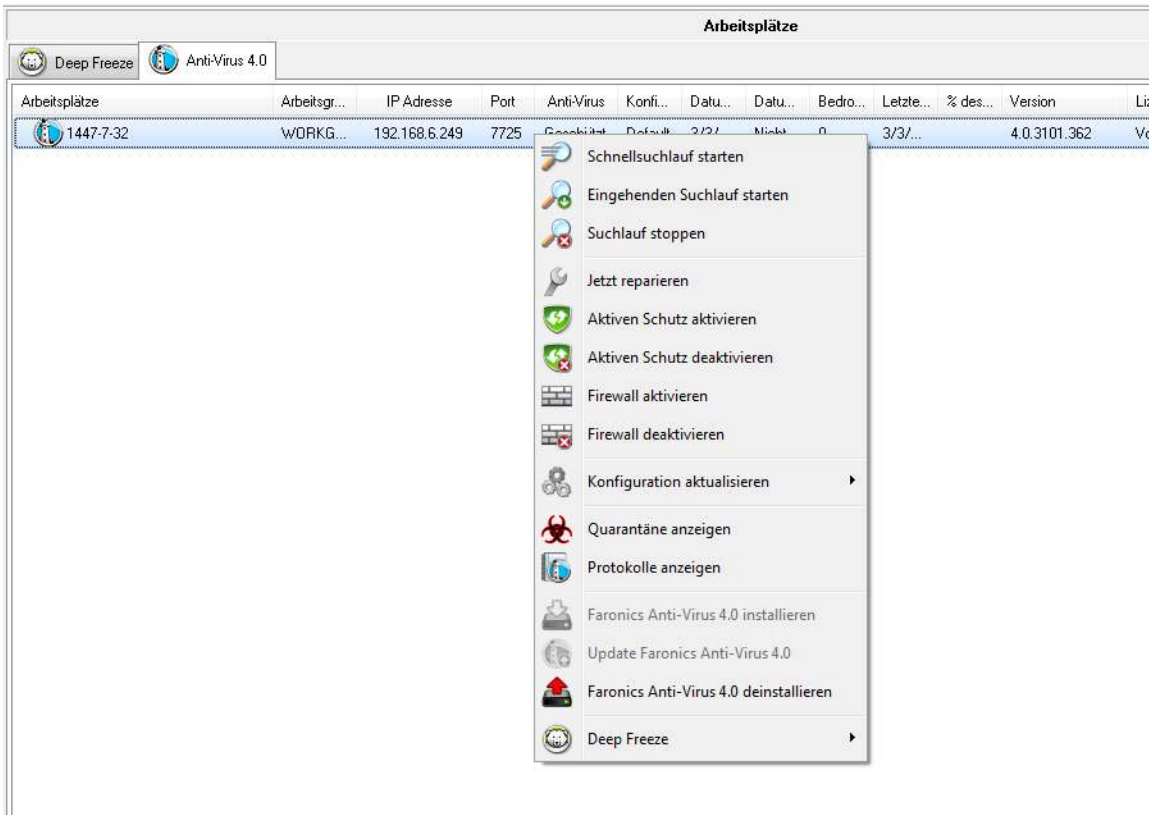


Wenn eine neue Version verfügbar ist, klicken Sie auf *Aktuellste Version herunterladen*, um Faronics Anti-Virus zu aktualisieren.

Faronics Anti-Virus aktualisieren

Wenn Sie nach Updates gesucht haben und eine neue Version verfügbar ist, führen Sie die folgenden Schritte aus, um eine neue Version auf dem Arbeitsplatz zu aktualisieren:

1. Gehen Sie im Fenster *Arbeitsplätze* auf die Registerkarte *Anti-Virus*.
2. Wählen Sie einen Arbeitsplatz (bzw. mehrere Arbeitsplätze) aus.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Faronics Anti-Virus aktualisieren* aus.



4. Klicken Sie auf *OK*, um die Aktion zu bestätigen.

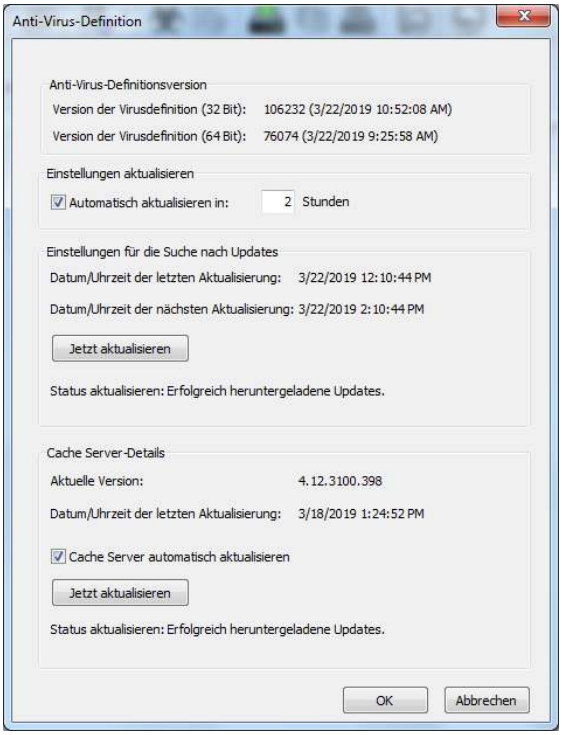
Der Arbeitsplatz wird neu gestartet, und der Faronics Anti-Virus-Client wird auf dem Arbeitsplatz bzw. den Arbeitsplätzen aktualisiert.

Anti-Virus-Definitionen aktualisieren

Der Anti-Virus-Definitionsserver wird zusammen mit Faronics Anti-Virus auf demselben Computer installiert, auf dem auch die Deep Freeze Console installiert ist. Der Anti-Virus-Definitionsserver lädt die neuesten Virusdefinitionen herunter und verteilt diese an die von Deep Freeze verwalteten Arbeitsplätze.

Führen Sie die folgenden Schritte aus, um Virusdefinitionen zu aktualisieren:

1. Starten Sie die Deep Freeze Console.
2. Gehen Sie auf *Tools* > *Anti-Virus-Definition*.
3. Die folgenden Einstellungen und Aktionen sind verfügbar:



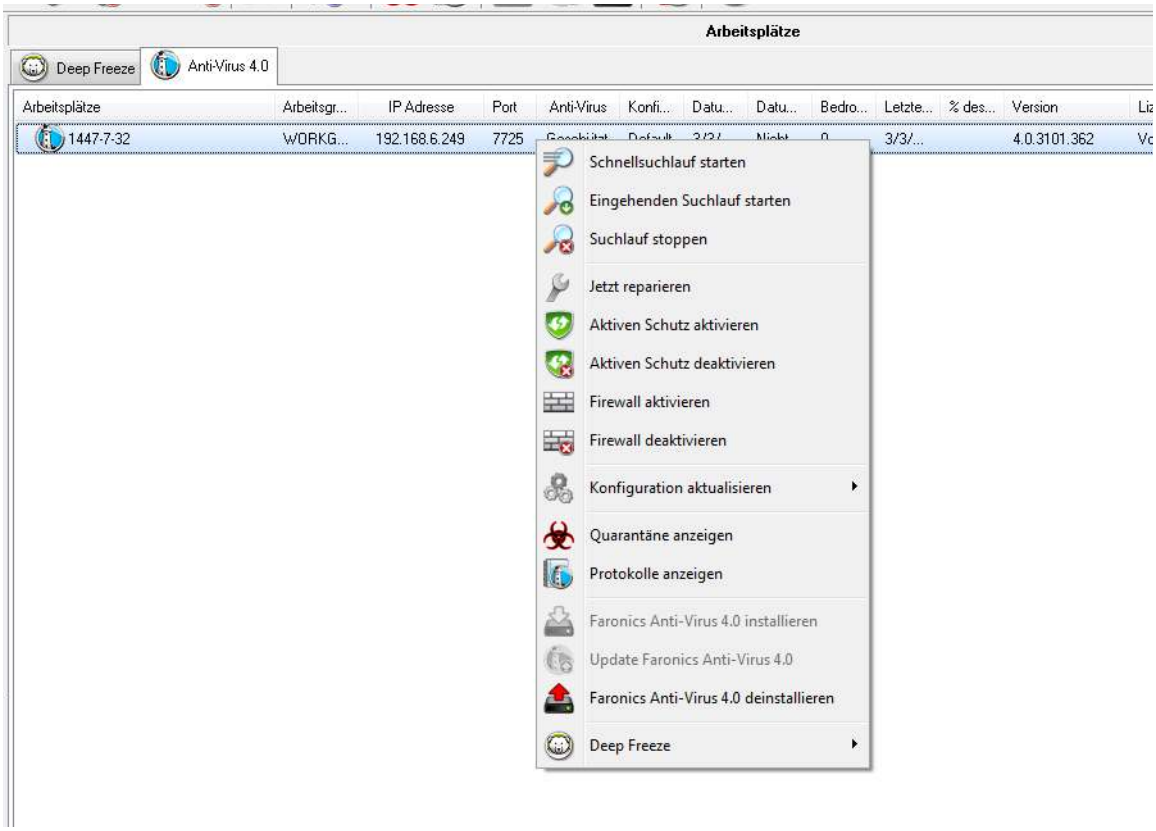
- Anti-Virus-Definitionsversion – die aktuelle Version der Anti-Virus-Definition wird angezeigt.
- Update-Einstellungen – wählen Sie das Markierungsfeld Automatisch aktualisieren in aus, und geben Sie einen Wert in Stunden ein.
- Einstellungen für die Suche nach Updates – Datum/Uhrzeit der letzten Aktualisierung sowie Datum/Uhrzeit der nächsten Aktualisierung werden angezeigt. Klicken Sie auf Jetzt aktualisieren, um die Virusdefinitionen sofort zu aktualisieren. Der Update-Status wird angezeigt.
- Cache Server-Details – die aktuelle Version und das Datum bzw. die Uhrzeit der letzten Aktualisierung werden angezeigt. Wählen Sie das Markierungsfeld Cache Server automatisch aktualisieren aus, um die neuesten Definitionen automatisch herunterzuladen und den Cache Server entsprechend zu aktualisieren. Klicken Sie auf Jetzt aktualisieren, um den Cache Server sofort zu aktualisieren.

4. Klicken Sie auf OK.

Den Anti-Virus-Client über die Enterprise Console deinstallieren

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus über die Enterprise Console auf dem Arbeitsplatz zu deinstallieren:

1. Gehen Sie im Fenster *Arbeitsplätze* auf die Registerkarte *Anti-Virus*.
2. Wählen Sie einen Arbeitsplatz (bzw. mehrere Arbeitsplätze) aus.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Faronics Anti-Virus deinstallieren* aus.



4. Klicken Sie auf *OK*, um die Aktion zu bestätigen.

Der Arbeitsplatz wird neu gestartet, und der Faronics Anti-Virus-Client wird auf dem Arbeitsplatz bzw. den Arbeitsplätzen deinstalliert.

Wenn der Anti-Virus-Client auf dem Arbeitsplatz deinstalliert wird, wird der Deep Freeze Seed beibehalten.

Der Deep Freeze Seed kann nicht deinstalliert werden, wenn der Anti-Virus-Client auf dem Arbeitsplatz installiert ist.

Faronics Anti-Virus über die Enterprise Console deaktivieren

Anti-Virus kann über die Deep Freeze Console deaktiviert werden, wenn es nicht verwendet werden soll.

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus über die Deep Freeze Console zu deaktivieren:

1. Gehen Sie auf *Tools* > *Lizenzen* > *Faronics Anti-Virus-Lizenz*.
2. Deaktivieren Sie die Checkbox *Ich möchte die Deep Freeze Console für die Verwaltung von Faronics Anti-Virus verwenden*.



3. Klicken Sie auf *Schließen*.
4. Starten Sie die Enterprise Console erneut, damit die Einstellungen übernommen werden.

Deep Freeze Befehlszeilensteuerung

Dieses Kapitel beschreibt die Verwendung der Deep Freeze-Befehle.

Themen

Deep Freeze Befehlszeilensteuerung (DFC.EXE)
Deep Freeze Befehlszeilensyntax
Befehlszeilensyntax für Faronics Anti-Virus

Deep Freeze Befehlszeilensteuerung (DFC.EXE)

Die Deep Freeze Befehlzeilensteuerung (DFC) bietet Netzwerkadministratoren eine erhöhte Flexibilität bei der Verwaltung von Deep Freeze-Computern. DFC funktioniert in Kombination mit Enterprise-Management-Tools Dritter und/oder zentralen Management-Lösungen. Diese Kombination ermöglicht es Administratoren, Computer spontan und nachfragegetrieben zu aktualisieren.

Es ist wichtig, zu beachten, dass DFC keine eigenständige Anwendung ist. DFC lässt sich reibungslos mit Lösungen integrieren, die Script-Dateien ausführen können, einschließlich standardmäßiger Anmelde-Scripts für eine einmalige Ausführung.

DFC-Befehle benötigen ein Passwort mit Befehlszeilenrechten. OPTs können nicht verwendet werden.

Sie erhalten eine Liste aller Befehle, wenn Sie DFC ohne Parameter aufrufen.

Die Dateien werden kopiert nach (32 Bit)

```
<WINDOWS>\system32\DFC.exe
```

Die Dateien werden kopiert nach (64 Bit)

```
<WINDOWS>\syswow64\DFC.exe
```

DFC-Rückgabewerte

Nach der Ausführung von DFC-Befehlen gibt DFC die folgenden Werte zurück:

Syntax	Beschreibung
`0`	ERFOLG oder Boolesches FALSCH, für Befehle, die ein Boolesches Ergebnis zurückgeben
`1`	Boolesches WAHR
`2 FEHLER`	Der Benutzer verfügt nicht über Administratorrechte
`3 FEHLER`	Der DFC-Befehl ist für diese Installation nicht gültig
`4 FEHLER`	Ungültiger Befehl
`5 – *FEHLER`	Interner Fehler bei der Ausführung des Befehls

Deep Freeze Befehlszeilensyntax

In Deep Freeze sind Passwörter auf maximal 63 Zeichen beschränkt. Wird ein längeres Passwort eingegeben, so wird der Befehl nicht erfolgreich ausgeführt.

Syntax	Beschreibung
`DFC password /BOOTTHAWED`	Startet den Computer erneut in einem aufgetauten Zustand; funktioniert nur bei eingefrorenen Computern
`DFC password /THAWNEXTBOOT`	Stellt den Computer für einen Start im aufgetauten Zustand bei nächstem Neustart ein; funktioniert bei eingefrorenen Computern und zwingt Computer nicht zu einem Neustart
`DFC password /BOOTFROZEN`	Startet den Computer erneut in einem eingefrorenen Zustand; funktioniert nur bei aufgetauten Computern
`DFC password /FREEZENEXTBOOT`	Stellt den Computer für einen Start im eingefrorenen Zustand bei nächstem Neustart ein; funktioniert bei aufgetauten Computern und zwingt Computer nicht zu einem Neustart
`DFC get /ISFROZEN`	Fragt Computer ab, ob er eingefroren ist. Gibt Fehlerebene 0 zurück, wenn er aufgetaut ist. Gibt 1 zurück, wenn er eingefroren ist.
`DFC get /CLONE`	Setzt die Klonmarkierung für Imaging-Zwecke.
`DFC password /CFG=[pfad] depfrz.rdx`	Ersetzt Deep Freeze-Konfigurationsinformationen. Funktioniert mit aufgetauten oder eingefrorenen Computern. Passwortänderungen sind sofort wirksam. Für andere Änderungen ist ein Neustart erforderlich.
`DFC get /version`	Zeigt die Versionsnummer von Deep Freeze an.
`DFC password /UPDATE=[Pfad zu Installationsdatei]`	Richtet den Computer für einen Neustart im aufgetauten Zustand und Installation eines Deep Freeze-Updates ein
`DFC password /LOCK`	Deaktiviert Tastatur und Maus des Computers. Funktioniert für eingefrorene oder aufgetaute Computer und erfordert keinen Neustart.

Syntax	Beschreibung
`DFC password /UNLOCK`	Aktiviert Tastatur und Maus des Computers. Funktioniert für eingefrorene oder aufgetaute Computer und erfordert keinen Neustart.
`DFC password /THAWLOCKNEXTBOOT`	Richtet den Computer ein, um in einem aufgetauten Zustand mit deaktivierter Tastatur und Maus neu zu starten; funktioniert nur mit eingefrorenen Computern
`DFC password /BOOTTHAWEDNOINPUT`	Startet den Computer erneut in einem aufgetauten Zustand mit deaktivierter Tastatur und Maus; funktioniert nur mit eingefrorenen Computern
`DFC get /LICENSESTATUS`	Zeit den Status und gegebenenfalls das Ablaufdatum der Lizenz an. Die folgenden unterschiedlichen Lizenztypen und entsprechenden Rückgabecodes sind möglich: 111: Nicht lizenziert – Deep Freeze ist nicht lizenziert und läuft 30 Tage ab Installation im *Probemodus*. 112: Bewertung – Für Bewertungszwecke mit einem festgelegten Ablaufdatum lizenziert. 113: Lizenziert – Ohne Ablaufdatum lizenziert. 114: Abgelaufen – Der Probezeitraum ist abgelaufen.
`DFC get /LICENSETYPE`	Zeit den Status und gegebenenfalls das Ablaufdatum der Lizenz an. Die folgenden unterschiedlichen Lizenztypen und entsprechenden Rückgabecodes sind möglich: 111: Keiner (nicht lizenziert) – Deep Freeze ist nicht lizenziert und läuft 30 Tage ab Installation im *Probemodus*. 112: Bewertung – Für Bewertungszwecke mit einem festgelegten Ablaufdatum lizenziert. 113: Standard (lizenziert) – Ohne Ablaufdatum lizenziert. 114: Nicht für Wiederverkauf – Ohne Ablaufdatum lizenziert. 115: Subskription 116: Probesubskription 117: Subskription nicht für den Wiederverkauf vorgesehen

Syntax	Beschreibung
`DFC passwort /LICENSE=lizenzschlüssel`	Ändert den Lizenzschlüssel. *passwort* ist das Deep Freeze-Administratorpasswort. *lizenzschlüssel* ist der Lizenzschlüssel für Deep Freeze. Wenn ein Fehler auftritt, werden die folgenden Fehlercodes angezeigt: 101: Der Lizenzschlüssel ist ungültig 102: Der eingegebene Lizenzschlüssel ist bereits abgelaufen.
`DFC password /ACTIVATE`	Aktiviert den Arbeitsplatz nach Abgleich mit dem Lizenzaktivierungsserver von Faronics.
`DFC get /ACTIVATION`	Zeigt den Aktivierungsstatus der Deep Freeze-Lizenz an. Gibt die folgenden Werte zurück: 0: Aktivierung steht noch aus 1: Aktiv 2: Autorisiert 3: Deaktiviert 4: Nicht autorisiert
`DFC password /WU [/UNLOCK] [/NOMSG | /NOMESSAGE] [/THAW]`	Windows-Updates werden heruntergeladen und auf dem Arbeitsplatz installiert. [/UNLOCK] Optionaler Parameter zur Aktivierung der Tastatur und der Maus während Windows-Updates. [/NOMSG | /NOMESSAGE] Optionaler Parameter zur Unterdrückung aller Informations-/Warnmeldungen von Deep Freeze während Windows-Updates. [/THAW] Optionaler Parameter, um den Rechner nach Abschluss des Windows-Updates wieder in den Zustand "aufgetaut" zu versetzen.
`DFC password /ENDTASK`	Beendet die laufende Arbeitsplatzaufgabe und startet den Computer im Zustand "eingefroren" neu. Stapeldateiaufgaben und Aufgabe zur Einrichtung eines Zeitraums im Zustand "aufgetaut" werden sofort beendet. Die Windows Update-Aufgabe ist abgeschlossen.

Syntax	Beschreibung
`DFC password /ENDTASK [/SHUTDOWN]`	Beendet die laufende Arbeitsplatzaufgabe und startet den Computer im Zustand "eingefroren" neu. Stapeldateiaufgaben und Aufgabe zur Einrichtung eines Zeitraums im Zustand "aufgetaut" werden sofort beendet. Die Windows Update-Aufgabe ist abgeschlossen. `[/SHUTDOWN]` Optionaler Parameter, um den Arbeitsplatz herunterzufahren.
`DFC password /FORMATTHAWSPACE`	Formatiert alle Auftauplätze auf dem Arbeitsplatz. An den Auftauplätzen gespeicherte Daten werden dauerhaft gelöscht.
`DFC password /DELETETHAWSPACE`	Löscht alle Auftauplätze auf dem Arbeitsplatz. An den Auftauplätzen gespeicherte Daten werden dauerhaft gelöscht.

Befehlszeilensyntax für Faronics Anti-Virus

Führen Sie die folgenden Schritte aus, um die Befehle für Faronics Anti-Virus auszuführen:

1. Gehen Sie auf dem Arbeitsplatz über die Eingabeaufforderung zu *<Systemverzeichnis>:\Programme\Faronics\Faronics Anti-Virus Enterprise*
2. Geben Sie `AVECLI\[Befehl]` ein.

Die folgenden Befehle stehen zur Verfügung:

Syntax	Beschreibung
`definitionversion`	Zeigt die Version der Virusdefinition an.
`scanengineversion`	Zeigt die Version der Scan Engine an.
`updatedefs`	Aktualisiert Virusdefinitionen und wendet diese an.
`fixnow`	Lädt die aktuellste Virusdefinition herunter. Aktiviert den aktiven Schutz sowie E-Mail-Schutz. Führt den standardmäßigen eingehenden Suchlauf durch.
`scanquick`	Startet einen Schnellsuchlauf.
`scandeep`	Startet einen eingehenden Suchlauf.
`enableap`	Aktiviert den aktiven Schutz.
`applydefs [Pfad zu Definitionen]`	Wendet Definitionsdatei vom Speicherort aus an.
`fixnow /quick`	Führt gegebenenfalls einen *Schnellsuchlauf* durch.
`setlicense[Schlüssel]`	Wendet einen angegebenen Lizenzschlüssel an.

Syntax:

```
AVECLI/definitionversion
```



Anhang A Ports und Protokolle

Der Schlüssel für die Einrichtung der Deep Freeze-Architektur besteht darin, zu wissen, welche Ports verwendet werden sollen. Der wesentliche Faktor ist die Bestimmung, welche Ports im Netzwerk verwendet werden, und die Verwendung von Ports, die keinen Konflikt mit diesen verursachen. Der Standardport 7725 wurde offiziell für Deep Freeze registriert.

Die Deep Freeze-Architektur besteht aus den folgenden drei Komponenten:

- Client (mit installiertem Seed)
- Remote-Konsole (lokaler Service aktiviert)
- Konsole (stellt Verbindung zu Remote-Konsole her)

Solange die Verbindung zwischen den Clients und der fernen Konsole denselben Port verwenden, dürfte es keinen Portkonflikt zwischen den unterschiedlichen Komponenten geben:



Ports können auch verwendet werden, um die Clients aufzuteilen. Wenn der lokale Service so eingerichtet ist, dass er auf drei Ports läuft (7725, 7724 und 7723) können Enterprise-Konsolen Verbindungen zu drei unterschiedlichen Ports herstellen und unter jedem Port eine andere Gruppe von Clients sehen.

Im voranstehenden Diagramm verwenden die Clients sowohl TCP- als auch UDP-Protokolle, um mit der fernen Konsole zu kommunizieren. Die Konsole, die eine Verbindung zur fernen Konsole herstellt, verwendet nur das TCP-Protokoll, um mit der fernen Konsole zu kommunizieren. Es ist wichtig, zu wissen, welche Ports und Protokolle verwendet werden, um eine Blockierung dieser durch Firewalls, Switches oder Router zu verhindern.



Anhang B Netzwerkbeispiele

Die folgenden Beispiele zeigen unterschiedliche Szenarien, die einen lokalen Service oder eine ferne Konsole betreffen.

- Beispiel 1 – Einzelnes Subnet
- Beispiel 2 – Mehrere Subnets, ein lokaler Dienst
- Beispiel 3 – Mehrere Ports, Fernzugriff auf Konsole
- Beispiel 4 – Mehrere Subnets, mehrere lokale Services

Jedes Beispiel erklärt, wie unterschiedliche Deep Freeze-Komponenten in unterschiedlichen Netzwerkumgebungen interagieren.

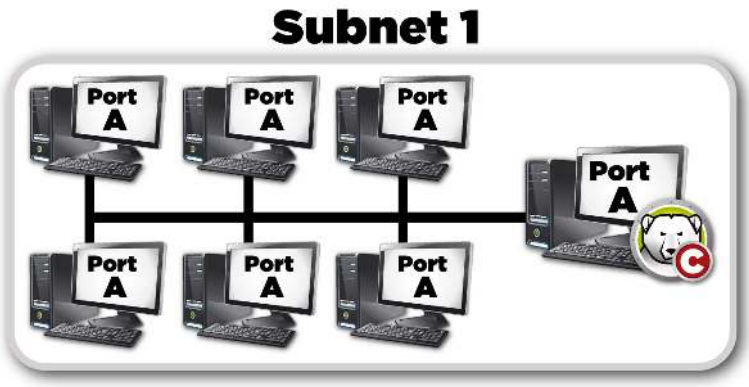


In den folgenden Beispielen ist auf den Client-Maschinen entweder die Deep Freeze-Arbeitsplatzinstallation oder das Arbeitsplatz-Seed installiert. Beide Installationen enthalten die Kommunikationskomponente, die mit der Konsole / der fernen Konsole kommuniziert. Der Unterschied zwischen der Arbeitsplatzinstallation und dem Arbeitsplatz-Seed besteht darin, dass die Arbeitsplatzinstallation Deep Freeze tatsächlich installiert, während das Seed nur die Kommunikationskomponente enthält.

Beispiel 1 – Einzelnes Subnet

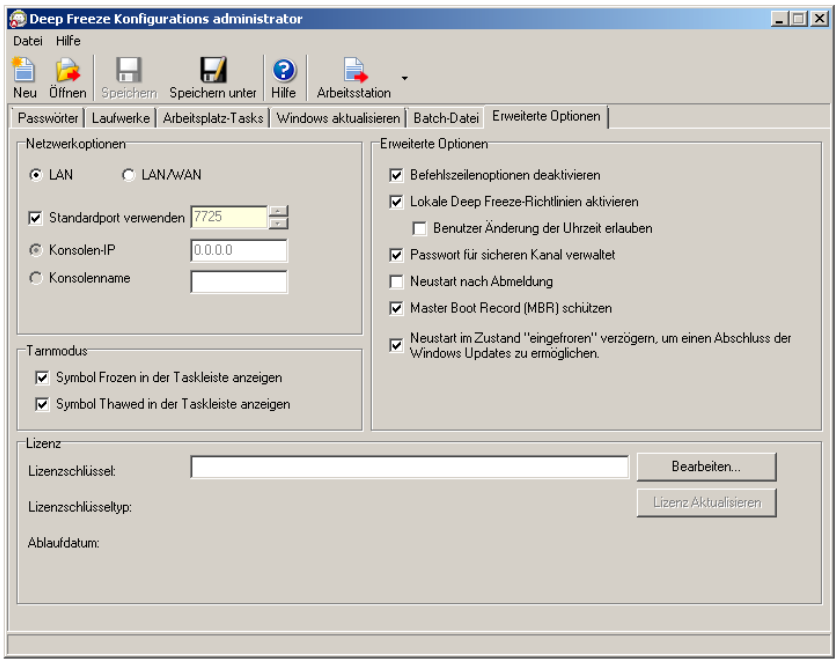
In dieser Umgebung sind alle Client-Maschinen in demselben Subnet enthalten, das auch die Konsolenmaschine enthält. Diese Umgebung erfordert keine ferngesteuerte Konsole, die jedoch auch verwendet werden könnte. In diesem Beispiel wird die ferne Konsole nicht verwendet. Dies ist die einfachste Netzwerkumgebung. Sie lässt sich auch am leichtesten konfigurieren.

Das folgende Diagramm zeigt die Netzwerktopologie:



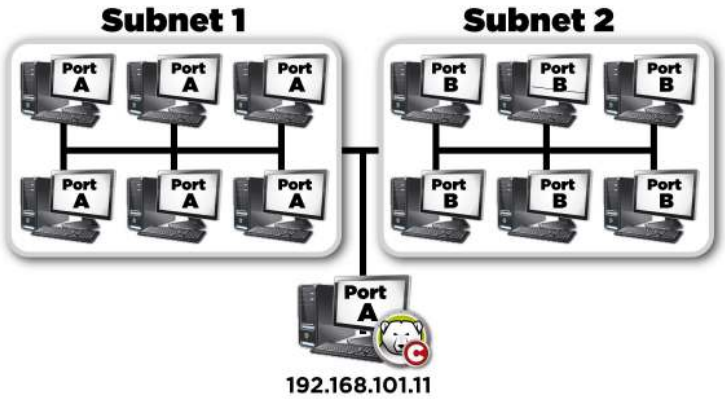
Die Client-Maschinen, hier durch Computersymbole dargestellt, befinden sich im selben Subnet wie die Maschine der Deep Freeze Enterprise-Konsole, die durch das Deep Freeze-Konsolensymbol dargestellt ist.

In diesem Szenario verwenden Clients Port A, während die Konsole eine Verbindung zu einem lokalen Dienst für denselben Port eingerichtet hat. Dieser Port wird vor Erstellung der Arbeitsplatzinstallationsdatei oder Arbeitsplatz-Seeds auf der Registerkarte *Erweiterte Optionen* konfiguriert.



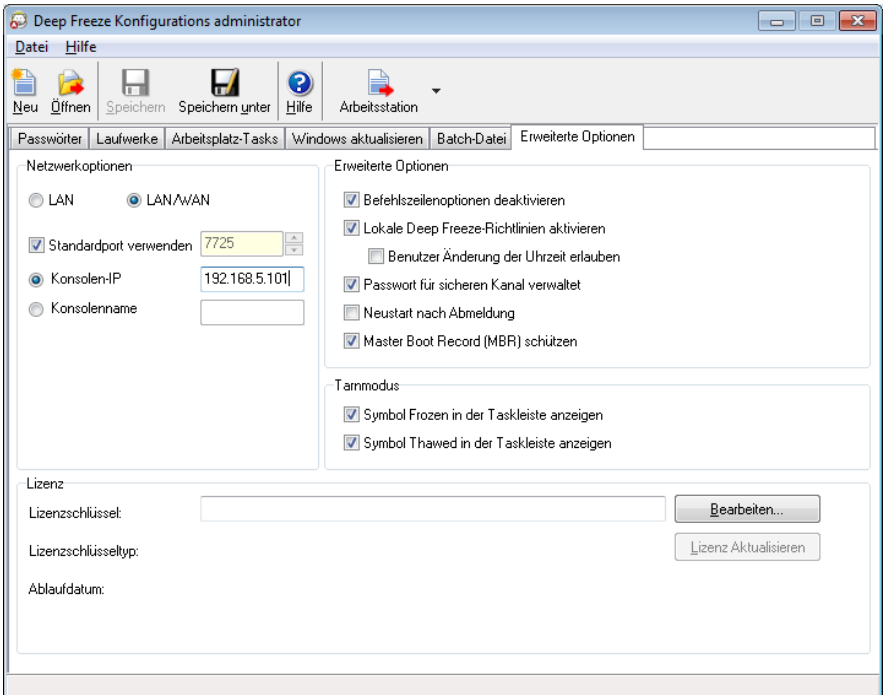
Beispiel 2 – Mehrere Subnets, ein lokaler Dienst

In dieser Umgebung befinden sich die Clients in mehr als einem Subnet. Es wird auch weiterhin nur eine Konsole verwendet. Diese Umgebung erfordert keine ferne Konsole, die jedoch auch verwendet werden könnte. Das folgende Diagramm zeigt die Netzwerktopologie:



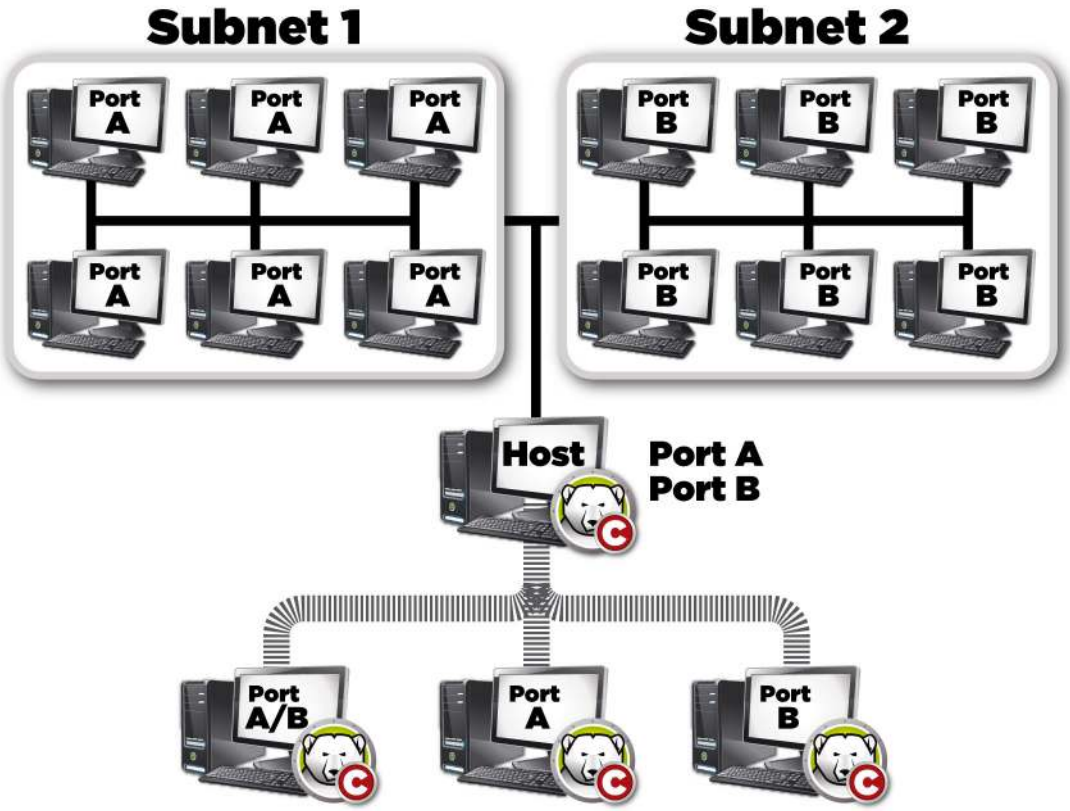
In diesem Szenario (ähnlich wie Beispiel 1 – Einzelnes Subnet) verwenden sowohl die Clients als auch die von der Konsole gehosteten Verbindung denselben Port. Dieser Port wird im Deep Freeze Enterprise-Konfigurationsadministrator vor Erstellung der Arbeitsplatzinstallationsdatei oder Arbeitsplatz-Seeds auf der Registerkarte *Erweiterte Optionen* konfiguriert.

Damit die Clients sichtbar werden, müssen Sie für die Verwendung einer LAN/WAN-Verbindung konfiguriert werden. Wenn die LAN/WAN-Option ausgewählt ist, wird ein Feld *Konsolen-IP* angezeigt. Geben Sie die IP der Maschine an, auf der die Enterprise-Konsole ausgeführt wird. Ein Beispiel für diese Einstellungen finden Sie nachfolgend auf der Registerkarte *Erweiterte Optionen* :



Beispiel 3 – Mehrere Ports, Fernzugriff auf Konsole

In diesem Umfeld befinden sich die Clients wieder an mehreren Ports. In diesem Fall wird mehr als eine Konsole verwendet. Über einen lokalen Dienst, dessen Administrator (Host) die Verbindungsinformationen freigegeben hat, wird auf mehrere Konsolen zugegriffen. Das folgende Diagramm zeigt die Netzwerktopologie:



In diesem Szenario hat der Host eine Verbindung anhand des lokalen Services eingerichtet. Wenn Sie das obenstehende Diagramm betrachten, stellen Sie fest, dass drei andere Konsolen eine Verbindung zum Host herstellen, um die Clients ihren Ports entsprechend zu sehen. Die Konsolen müssen nicht Teil einzelner Subnets sein, solange sie den Host sehen können.

Genaugenommen kann die Konsole, die über Port A/B verbunden ist, die Host-Konsole sehen, sowie sämtliche Computer, die Ports A und B zugeordnet sind. Die anderen Konsolen, die über Port B verbunden sind, sehen den Host und nur die Computer, die Port B zugeordnet sind.

Beispiel 4 – Mehrere Subnets, mehrere lokale Services

In diesem Beispiel gibt es zwei unterschiedliche Standorte.

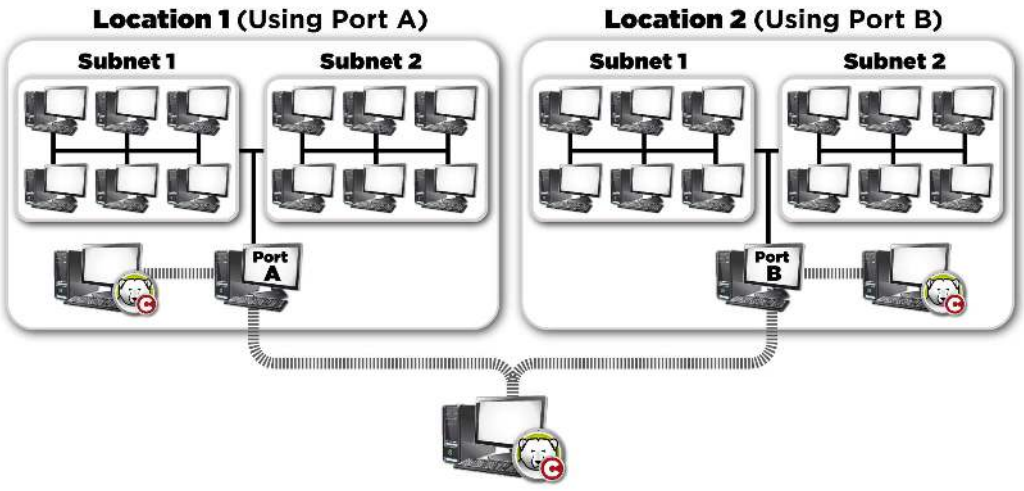
Nachfolgend eine Liste von Annahmen, die bezüglich dieses bestimmten Beispiels getroffen werden:

- Die Standorte sind verteilt und haben nur eine minimale Verbindung zu einander
- An jedem Standort gibt es einen Netzwerkadministrator, der für die Verwaltung von Deep Freeze an diesem Standort verantwortlich ist
- beide Standorte müssen von einem dritten Standort aus verwaltet werden

In diesem Beispiel sind die fernen Konsolen an den einzelnen Standorten eingerichtet und ein lokaler Dienst wird verwendet:

- Standort 1 (ein Computerlabor an einer Universität) verwendet Port A, um mit den Clients zu kommunizieren. Die Verbindungen werden von der Konsole gehostet. Die Computer der Universitätsbibliothek verwenden Port B. Die Konsole in der Abteilung für technischen Support verwendet die Verbindungen, die von sowohl der Labor- als auch der Bibliothekskonsole gehostet werden.
- Auf Konsolen, die nicht direkt mit einem Computer kommunizieren, sollte der lokale Service ausgeschaltet sein.

Das folgende Diagramm zeigt die Netzwerktopologie:



Der Vorteil dieser Struktur besteht darin, dass alle Pakete, die von Clients an Standort 1 versandt werden, an diesem Standort enthalten sind. Je geringer die Strecke ist, die ein Paket transportiert werden muss, desto geringer ist die Wahrscheinlichkeit, dass das Paket fehlschlägt.

Der Administrator im Labor kann eine Verbindung zum lokalen Service am selben Standort 1 herstellen, nicht jedoch zum lokalen Service in der Bibliothek. Der Grund hierfür besteht darin, dass der Laboradministrator das Passwort für den Zugriff auf den lokalen Service für die Bibliothek nicht kennt. Dasselbe gilt für den Administrator in der Bibliothek. Wenn der technische Support das Passwort für beide lokalen Services kennt (sowohl Labor als auch Bibliothek), kann eine Verbindung zum lokalen Service beider Standorte hergestellt werden, um alle Clients zu verwalten.



Anhang C Fehlerbehebung für eine Verbindung zur Remote-Konsole

Keine Clients in der Konsole

Nachfolgend einige häufige Gründe, warum Clients nicht in der Konsole angezeigt werden.

1. Die Konsole und die Clients enthalten nicht die richtigen Netzwerkeinstellungen.

Wenn die Konsole für die Verwendung eines bestimmten Ports eingestellt ist und die Clients einen anderen Port verwenden, sind sie jeweils für einander nicht sichtbar. Wenn die Computer außerdem für LAN/WAN konfiguriert sind, muss die IP der IP der Maschine entsprechen, auf der die Konsole läuft.

Die standardmäßige LAN-Einrichtung funktioniert, sofern alle Maschinen, auf denen Computer und Konsolen laufen, im selben Subnet enthalten sind. Wenn jedoch ein VLAN verwendet wird, oder wenn der Client in mehreren Subnets vorhanden ist, muss die Computerinstallation so konfiguriert werden, dass sie unter den LAN/WAN-Einstellungen läuft.

2. Irgendetwas im Netzwerk blockiert den Port, der zwischen der Konsole und den Clients verwendet wird.

Verwenden Sie ein Ping, um nach einer Verbindung zu suchen. Die Clients sind nicht in der Lage, Pakete zur Konsole bzw. zur fernen Konsole zu senden, weil es keine Route zum Host zu geben scheint. Ein Versuch, die IP der Konsole bzw. der fernen Konsole zu pingen scheint nicht zu funktionieren. Stellen Sie zur Lösung dieses Problems sicher, dass die beiden Maschinen eine Verbindung zueinander herstellen können.

Wenn ein Server, Router oder Switch im Netzwerk den Port blockiert, sind die Clients nicht sichtbar. Standardmäßig wird als Port 7725 verwendet.

3. Die Arbeitsplätze wurden mit einem unterschiedlichen Anpassungscode als die Konsole erstellt.

Wenn der Deep Freeze Enterprise-Konfigurationsadministrator erstmalig ausgeführt wird, wird der Benutzer aufgefordert, einen Anpassungscode einzugeben. Dieser Code ist sehr wichtig, da er die Software verschlüsselt. Dies bedeutet, dass alle Arbeitsplätze, die erstellt werden, mit diesem Anpassungscode verschlüsselt werden. Wenn eine Konsole unter Verwendung eines anderen Administrators erstellt wurde, der mit einem unterschiedlichen Anpassungscode installiert wurde, kann sie Arbeitsplätze, die mit dem ursprünglichen Code erstellt wurden, nicht sehen. Die Arbeitsplätze und die Konsole müssen mit einem Konfigurationsadministrator erstellt werden, der unter Verwendung desselben Anpassungscodes installiert wurde.

Fehler ‘Port wird verwendet’ bei Start der Konsole

Bei dem Versuch, die Konsole zu starten, wird die Fehlernachricht *Konsole kann nicht gestartet werden: Port wird verwendet* angezeigt. Es gibt mehrere Gründe, warum diese Fehlernachricht angezeigt werden könnte:

1. Es gibt eine Deep Freeze-Arbeitsplatzinstallation oder ein Arbeitsplatz-Seed, das unter demselben Port bzw. auf demselben Computer installiert ist, wie die Konsole.

Es kann sein, dass Deep Freeze im Tarnmodus installiert wurde (das Symbol wird nicht in der Taskleiste angezeigt). Das Seed zeigt kein Symbol an. Der beste Test besteht in der Ausführung einer Arbeitsplatzinstallationsdatei auf dem Computer. Wenn die Option Deinstallieren angezeigt wird, ist die Arbeitsplatzinstallationsdatei oder das Arbeitsplatz-Seed installiert und kann deinstalliert werden. Wenn die Option Deinstallieren nicht angezeigt wird, ist die Arbeitsplatzinstallationsdatei bzw. das Arbeitsplatz-Seed nicht installiert.

Die einfachste Lösung wäre, zunächst den lokalen Dienst auszuschalten und dann eine Verbindung zu einer Konsole herzustellen, auf die aus der Ferne zugegriffen werden kann.

2. Ein anderes Programm bzw. ein anderer Service verwendet den Port auf dieser Maschine.

In diesem Fall kann ein Port-Sniffer für die entsprechende Maschine eingesetzt werden, um zu sehen, welche Ports offen sind. Im Web sind mehrere Tools verfügbar, um diese Aktion auszuführen. Die Anwendung *netstat.exe*, die in Windows enthalten ist, sollte anzeigen, ob der Port, den Deep Freeze verwendet, bereits verwendet wird.

3. Das Netzwerkkabel ist nicht verbunden.

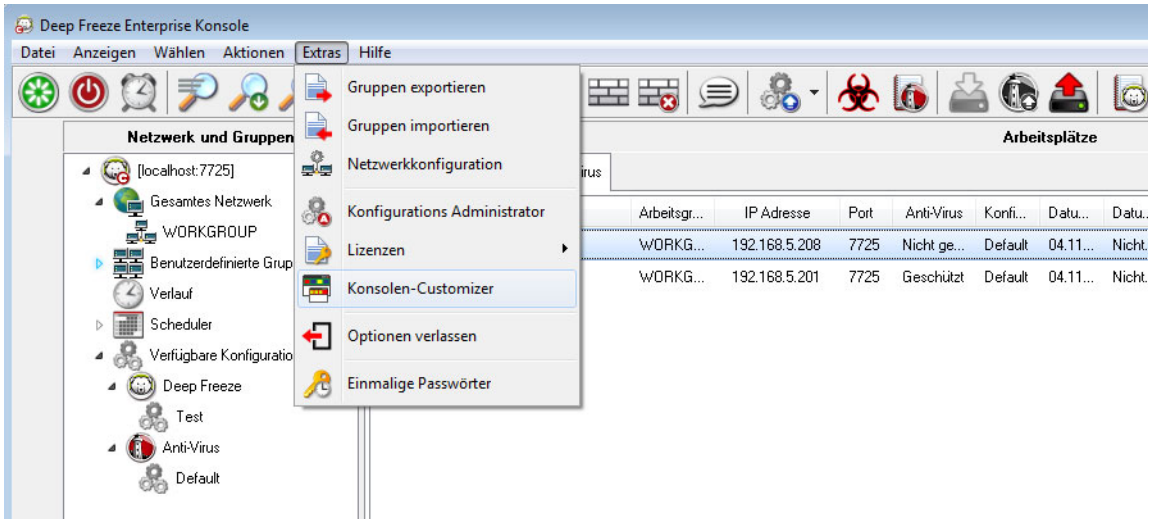
Diese Nachricht kann auftreten, wenn die Maschine über keine Netzwerkmaschine verfügt.

Anhang D Eine angepasste Deep Freeze Enterprise-Konsole erstellen

Die Deep Freeze Enterprise-Konsole umfasst die Möglichkeit, eine neue Enterprise-Konsole mit eingeschränkter Funktionalität zu erstellen. Eine angepasste, eingeschränkte Konsole kann in Ihrer Organisation eingeführt werden, um bestimmten Benutzer die Durchführung gewünschter Aufgaben zu ermöglichen, ohne ihnen vollen Zugang zu den vollständigen Funktionen der Enterprise-Konsole zu bieten.

In diesem Beispiel erstellen wird eine eingeschränkte Konsole erstellt, die einem Lehrer oder einem Ausbilder in einem Computerraum zur Verfügung gestellt werden kann. In diesem Szenario sollen Lehrer in der Lage sein, Rechner neu zu starten, bei Bedarf Tastatur und Maus zu sperren und Nachrichten an die Schüler zu senden. Der Lehrer soll jedoch nicht in der Lage sein, die Rechner in einem aufgetauten Zustand hochzufahren, Deep Freeze zu deinstallieren oder andere Aufgaben durchzuführen, die der IT-Abteilung vorbehalten sind.

Der Konsolen-Customizer kann über *Tools* > *Konsolen-Customizer* gestartet werden.



Die Option *Konsolenfunktionen* > *Aktivierung* bleibt ausgewählt. Hierdurch wird sichergestellt, dass bei Verlagerung der neuen Konsole auf einen anderen Computer ein einmaliges Passwort auf dem Computer eingegeben werden muss, auf den die Konsole übertragen wird. Wenn diese Sicherheitsmaßnahme in Ihrer Umgebung nicht erforderlich ist, brauchen Sie diese Option nicht auszuwählen.

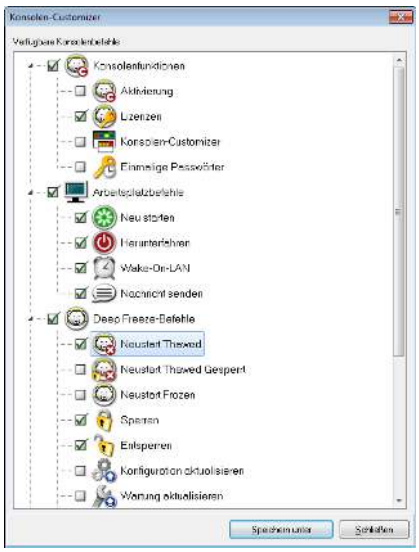
Konsolenfunktionen > *Einmaliges Passwort* wird nicht ausgewählt, da der Lehrer unter keinen Umständen in der Lage sein soll, den Computer im Zustand „aufgetaut" hochzufahren. Wenn ein Lehrer den Computer im Zustand „aufgetaut" hochfährt, können Schüler unnötige Software auf dem Computer installieren, die selbst nach einem Neustart dort verbleibt.

Alle Optionen unter *Arbeitsplatzbefehle* bleiben ausgewählt, da der Lehrer in der Lage sein soll, Nachrichten an Schüler zu senden und Computer nach Bedarf herunterzufahren, neu zu starten und hochzufahren.

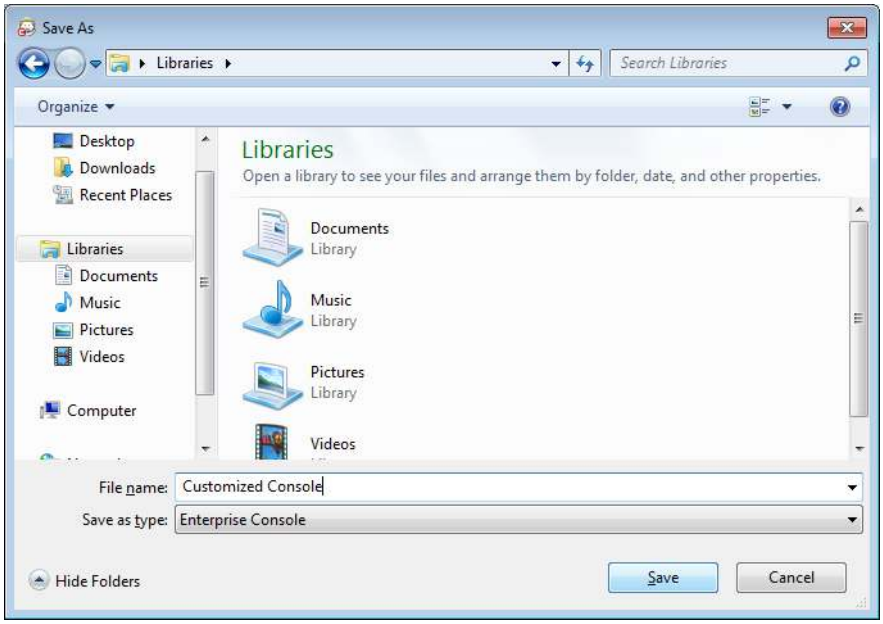
Von den Deep Freeze-Befehlen bleiben nur drei Optionen ausgewählt. *Entsperren*, *Sperren* und *Im Modus „eingefroren" neu starten*. Hierdurch ist der Lehrer in der Lage, die Tastatur

und die Maus auf Schülercomputern nach Bedarf zu sperren (und zu entsperren) und Computer im Modus *eingefroren* neu zu starten (sollte ein Computer versehentlich von einem Mitarbeiter der IT-Abteilung im Modus *aufgetaut* gelassen worden sein). Durch Abwahl aller anderen Optionen wird sichergestellt, dass ein Lehrer nicht in der Lage ist, einen Computer dauerhaft zu verändern.

Schließlich werden noch alle *Installations-/Deinstallationsbefehle für Arbeitsplätze* und alle *Scheduler-Befehle* abgewählt, da der Lehrer diese Optionen nicht verwenden können soll.



Nachdem alle Optionen ausgewählt wurden, klicken Sie auf *Speichern unter*, um die neue Enterprise-Konsole zu speichern. Ein standardmäßiger Dialog *Speichern unter* wird angezeigt.



Speichern Sie die neue eingeschränkte Enterprise-Konsole, und verteilen Sie sie an die gewünschten Benutzer.

Anhang E Deep Freeze-Aktionsdateien – RDC-Beispiel

Deep Freeze-Aktionsdateien

Eine Deep Freeze-Aktionsdatei ist eine XML-Datei, über die Administratoren zusätzliche Funktionalität für die Deep Freeze Enterprise-Konsole definieren können. Eine Aktionsdatei definiert eine Methode für den Aufruf einer externen Stapeldatei und die Übergabe von Informationen (beispielsweise IP-Adressen von Rechnern, Computernamen) an die Stapeldatei oder das Skript.

Aktionsdateien rufen lediglich ein externes Programm oder Skript auf. Daher können alle Skripterstellungssprachen, die über die Befehlszeile aufgerufen werden können, verwendet werden.

Beispiel für eine Aktionsdatei

Die Struktur der verwendeten Deep Freeze-Aktionsdatei ist nachfolgend dargestellt. Die Datei *DFEntConsoleCustomActions.xml* ist unter *C:\Programme\Faronics\Deep Freeze Enterprise* verfügbar. Die Datei kann bearbeitet werden, um weitere Aktionen (wie beispielsweise nachfolgend beschrieben wird) hinzuzufügen:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Deep Freeze standardmäßige angepasste Aktionsdatei-->
<CUSTOMDEFINEDACTIONS>
 <ACTION1>
  <CAPTION>
   <ENGLISH>Kontrolle über RDC</ENGLISH>
   <GERMAN>Kontrolle über RDC Deutsch</GERMAN>
   <JAPANESE>Kontrolle über RDC Japanisch</JAPANESE>
   <SPANISH>Kontrolle über RDC Spanisch</SPANISH>
   <FRENCH>Kontrolle über RDC Französisch</FRENCH>
   <CHINESE>Kontrolle über RDC Chinesisch</CHINESE>
</CAPTION>
  <FILEMENU>Y</FILEMENU>
  <POPUPMENU>Y</POPUPMENU>
  <SILENT>Y</SILENT>
  <SUBITEMS/>
  <PARAMS/>
  <SYNC/>
  <LOG/>
  <EXECUTE>C:\Windows\system32\mstsc.exe /v:%%WKSNAME%% /f</EXECUTE>
  <WORKDIR>C:\Windows\system32\</WORKDIR>
```

Im voranstehenden Beispiel enthält die angepasste Aktionsdatei den Befehl für die Ausführung des Remote-Desktops auf dem Konsolencomputer und die Herstellung einer Verbindung zum über den Parameter `%%WKSNAME%%` angegebenen Remote-Computer.

Die Datei *DFEntConsoleCustomActions.xml* enthält 3 Beispiele:

- Kontrolle über RDC
- Remote-Ausführung
- MSI-Datei verteilen und installieren

Weitere Informationen über die Verwendung der voranstehenden Beispiele finden Sie im Abschnitt Benutzerdefinierte Aktionen konfigurieren. Sie können die Datei *DFEntConsoleCustomActions.xml* Ihren Anforderungen entsprechend bearbeiten.

Struktur von Deep Freeze-Aktionsdateien

Das folgende XML-Schema skizziert die angepassten definierten Aktionen, die dem Benutzer zur Verfügung stehen. In Abhängigkeit von der Anzahl erforderlicher Befehle können mehrere XML-Dateien gespeichert werden. Alle Dateien müssen im Konsolenordner gespeichert werden, und das Attribut ‚schreibgeschützt' darf nicht ausgewählt sein.

Wenn Änderungen durchgeführt werden, muss die Deep Freeze-Konsole neu gestartet werden, damit die Änderungen übernommen werden.

Parameter	Nutzung
`<?xml version="1.0" encoding="UTF-8"?>`	
`<CUSTOMDEFINEDACTIONS>`	
`<CAPTION>`	Text, der im Dateimenü oder –untermenü angezeigt wird
`<ENGLISH>Caption</ENGLISH>`	Text in verschiedenen Sprachen
`<GERMAN>Caption</GERMAN>`	Text in verschiedenen Sprachen
`<JAPANESE>Caption</JAPANESE>`	Text in verschiedenen Sprachen
`<SPANISH>Caption</SPANISH>`	Text in verschiedenen Sprachen
`<FRENCH>Caption</FRENCH>`	Text in verschiedenen Sprachen
`<CHINESE>Caption</CHINESE>`	Text in verschiedenen Sprachen
`<FILEMENU>y</FILEMENU>`	Definiert, ob diese Aktion im Dateimenü enthalten ist
`<POPUPMENU>y</POPUPMENU>`	Definiert, ob diese Aktion im Kontextmenü (bei Rechtsklick) enthalten ist

Parameter	Nutzung
<SILENT>y</SILENT>	Definiert, ob ein Benutzer eine Bestätigungsaufforderung erhält
<SUBITEMS>	In den Unterelementen kann ein Element, das diesem Element untergeordnet ist, definiert werden
</SUBITEMS>	Wenn die Unterelemente definiert werden, wird die Aktion für diese Elemente ignoriert
<SYNC>y</SYNC>	Gibt an, ob Befehle synchron oder asynchron ausgeführt werden
<PARAMS>	Bei Auswahl dieser Aktion wird der Benutzer aufgefordert, individuelle Parameter einzugeben
<PASSWORD>	Name des Parameters
<VAR>%PARAM1%</VAR>	Name einer Variable, die mit EXECUTE verwendet wird
<ENGLISH>USERNAME Param (ENGLISH)</ENGLISH>	Text in verschiedenen Sprachen
<GERMAN>USERNAME Param (GERMAN)</GERMAN>	Text in verschiedenen Sprachen
<JAPANESE>USERNAME Param (JAPANESE)</JAPANESE>	Text in verschiedenen Sprachen
<SPANISH>USERNAME Param (SPANISH)</SPANISH>	Text in verschiedenen Sprachen
<FRENCH>USERNAME Param (FRENCH)</FRENCH>	Text in verschiedenen Sprachen
<CHINESE>USERNAME Param (CHINESE)</CHINESE>	Text in verschiedenen Sprachen
</CAPTION>	
</USERNAME>	
</PARAMS>	
<LOG>	Definiert das Verhalten der Protokolldatei
<APPEND>y</APPEND>	Definiert, ob die Protokolldatei angehängt oder neu erstellt wird
<FILENAME>c:\a1command.log</FILENAME>	Definiert den Dateinamen
<EXECUTE>c:\windows\vpn.exe %%IP%% %USERNAME% %PASSWORD% %%WKSNAME%%</EXECUTE>	Definiert den Befehl, der ausgeführt werden soll. Hier können Parameter und/oder Konsolenelemente verwendet werden

Parameter	Nutzung
<WORKDIR>c:\windows</WORKDIR>	Definiert das Arbeitsverzeichnis

Konsolenparameter

Die folgenden Konsolenparameter können von der Enterprise-Konsole an die ausgeführte Anwendung bzw. das Skript übergeben werden.

Parameter	Nutzung
%%WKSNAME%%	Arbeitsplatzname
%%DOMAIN%%	Arbeitsplatzdomäne
%%IP%%	Arbeitsplatz-IP
%%PORT%%	Arbeitsplatzport
%%STATUS%%	Arbeitsplatzstatus
%%CFGDATETIME%%	Datum/Uhrzeit der Arbeitsplatzkonfiguration
%%MAC%%	MAC-Adresse des Arbeitsplatzes
%%DFVERSION%%	Deep Freeze-Version des Arbeitsplatzes
%%CFGNAME%%	Arbeitsplatzkonfigurationsname
%%LOGGEDONUSER%%	Am Arbeitsplatz angemeldeter Benutzer
%%DFINSTALLATIONFILE%%	Arbeitsplatzinstallationsdatei
%%LICENSESTATUS%%	Arbeitsplatzlizenzstatus
%%LICENSEEXPIRYDATETIME%%	Datum und Uhrzeit für den Ablauf der Arbeitsplatzlizenz
%%AVSTATUS%%	Anti-Virus-Status des Arbeitsplatzes
%%OSVERSION%%	Arbeitsplatz-Betriebssystemversion