

Microsoft® Windows Embedded Standard 2009
(WES) und Windows® XP Embedded (XPe)
Kurzreferenz
HP Thin Clients



© Copyright 2008, 2009 Hewlett-Packard Development Company, L.P.

Microsoft und Windows sind in den USA eingetragene Marken der Microsoft Corporation. Win32, Windows Internet Explorer und Windows Media Player sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Adobe und Acrobat sind Marken oder eingetragene Marken von Adobe Systems Incorporated.

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden.

Die einzigen Garantieansprüche für HP Produkte und Services sind in den Garantieerklärungen festgehalten, die diesen Produkten und Services beiliegen. Aus dem vorliegenden Dokument sind keine weiteren Garantieansprüche abzuleiten. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen.

Dieses Dokument enthält Informationen, die durch das Urheberrecht geschützt sind. Ohne schriftliche Genehmigung der Hewlett-Packard Company darf dieses Dokument weder kopiert noch in anderer Form vervielfältigt oder übersetzt werden.

Microsoft Windows Embedded Standard 2009 (WES) und Windows XP Embedded (XPe) Kurzreferenz

HP Thin Clients

Zweite Ausgabe (April 2009)

Erste Ausgabe (September 2008)

Teilenummer des Dokuments: 502961–042

Allgemeines

Dieses Handbuch ergänzt die Standarddokumente für Windows XPe der Microsoft Corporation. In diesem Dokument werden die Unterschiede, Erweiterungen und Zusatzfunktionen beschrieben, die im aktuellen Image dieses Terminals enthalten sind.

- △ **VORSICHT!** In dieser Form gekennzeichnete Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anweisungen hin.
- △ **ACHTUNG:** In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Beschädigungen der Geräte oder zum Verlust von Daten führen kann.
- 📝 **HINWEIS:** In dieser Form gekennzeichnete Text enthält wichtige ergänzende Informationen.

Inhaltsverzeichnis

1 Weitere Informationen und Updates

2 Einführung

Desktop	3
Benutzerdesktop	3
Administratordesktop	3
Anforderungen an die Serverumgebung	4
Sitzungsdienste	4
Citrix ICA	4
Microsoft RDP	5
Terminalemulationsunterstützung	5
Unterstützungsdienste	5
Altiris Deployment Server	5
HP Gerätemanager	5

3 Konfiguration

Anmeldung	6
Automatische Anmeldung	6
Manuelle Anmeldung	7
Zugriff auf die Anmeldung als Administrator	7
Abmeldung, Neustart und Herunterfahren des Thin Clients	8
Enhanced Write Filter	8
Energieverwaltung	9
Systemzeit	9
Lokale Laufwerke	10
Laufwerk Z	10
Laufwerk C und Flash-Laufwerk	10
Speichern von Dateien	11
Zuordnen von Netzlaufwerken	11
Servergespeicherte Profile	11
Benutzerkonten	11
Erstellen eines neuen Benutzerkontos	11
Benutzer-Manager	12
Benutzerprofile	12

Regions- und Sprachoptionen	14
Verwaltung	15

4 Anwendungen

Symantec EndPoint Protection Firewall	17
Informationen zum Agenten	17
Neue Leistungsmerkmale und Funktionen	18
Microsoft Windows-Firewall	18
Standardmäßige Aktivierung	18
Konfigurieren der Microsoft Windows-Firewall	18
Ermitteln von Konfigurationsinformationen	21
Beheben von Anwendungsproblemen	21
Fehlersymptome	21
Fehlerbehebung	22
Hinzufügen eines Programms	22
Hinzufügen eines Ports	23
Citrix Program Neighborhood und PN Agent	24
Remotedesktopverbindung	25
HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements	27
HP RGS-Empfänger (Remote Graphics Software)	27
HP Session Allocation Manager (SAM) Client	28
TeemTalk Terminal Emulation	29
VMWare View Manager	29
Altiris Client Agent	29
HP Management Agent	32
HP Client Automation Registration and Agent Loading Facility (RALF)	32
Microsoft Internet Explorer	33
Windows Media Player 11	33

5 Zusätzliche Optionen in der Systemsteuerung

Enhanced Write Filter Manager	36
Vorteile des Enhanced Write Filters	36
Enhanced Write Filter-Statusdienst	36
Enhanced Write Filter GUI	37
EWF-GUI – Schaltflächen	38
Befehle zum Starten des Tools über die DOS-Befehlszeile	39
Verwenden der Bootbefehle	39
HP RAMDisk	39
HP DHCP Settings Update Client	41
HP ThinState Capture	42
HP ThinState Deploy	45
HP FTP Image Update	46
Serveranforderungen	46

DHCP-Server	46
FTP-Server	46
Beschreibung	46
Hosteinstellungen	47
Auswahl des zu aktualisierenden Image	48

6 Verwaltung und Imageaktualisierungen

Altiris Deployment Solution-Software	50
HP Gerätemanager	50
Add-on-Erweiterungen	50
Imageaktualisierungen	51
HP FTP Image Update	51
HP ThinState Capture und Deploy	51
HP Compaq Thin Client Imaging Tool	51
HP Client Automation	51

7 Peripheriegeräte

Drucker	53
Hinzufügen von Druckern, die den generischen Druckertreiber für den unformatierten Ausdruck von Texten verwenden	54
Verwenden von herstellerspezifischen Druckertreibern	54
Add-on "HP Universal Print Driver for Thin Clients"	54
Audio	55

Index	56
--------------------	-----------

1 Weitere Informationen und Updates

HP stellt für Thin Client-Images Add-ons, Microsoft® QFE-Updates (Quick Fix Engineering) und regelmäßige Updates zur Verfügung. Informationen zu diesen Updates sowie wichtige Dokumentation mit speziellen Informationen für die jeweilige Imageversion finden Sie auf der Website des HP Supports unter <http://www.hp.com/support>. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen** oder **Treiber und Software zum Herunterladen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die [Eingabetaste](#).

2 Einführung

HP WES-basierte Thin Client-Modelle von HP verwenden das Betriebssystem Windows Embedded Standard 2009 (WES). HP XPe-basierte Thin Client-Modelle von HP verwenden das Betriebssystem Windows XP Embedded (XPe). Dieses Handbuch enthält Informationen, die sich auf die neuesten gelieferten Images für WES und XPe Service Pack 3 (SP3) beziehen. Diese Thin Clients eignen sich dank ihrer Flexibilität, Konnektivität, Sicherheit, Multimediafunktionalität und Peripherieunterstützung besonders für die Mainstream-Nutzung in Unternehmen:

- Flexibilität
 - Unterstützung von Win32®-basierten Anwendungen
 - Umfangreiche Unterstützung von Peripheriegeräten
- Konnektivität
 - Citrix XenApp Plugin for Hosted Apps, Microsoft Remote Desktop Protocol (RDP), VMware View Client, HP Session Allocation Client, HP Remote Graphics und HP TeamTalk
- Vertraute Benutzeroberfläche durch Ähnlichkeit mit Windows XP Professional
- Verbesserte Sicherheit
 - Symantec EndPoint Protection Firewall
 - Microsoft Firewall (Add-on)
 - Geschütztes Flash-Laufwerk mit eingeschränktem Zugriff
- Multimedia
 - Windows Media® Player
 - Windows Musical Instrument Digital Interface (MIDI) (Add-on)
- Internetbrowser
 - Windows Internet Explorer®
 - Adobe Acrobat® (Add-on)
- Umfassende MUI-Unterstützung: Englisch, Französisch, Deutsch, Spanisch, Niederländisch, Norwegisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Koreanisch und Japanisch

Dieser Client wird von HP so konfiguriert, dass er sofort einsatzbereit ist. Die häufigsten Benutzeranforderungen werden sofort erfüllt. Über das Applet „Software“ in der Systemsteuerung können Sie Komponenten sowie die auf der Website des HP Supports verfügbaren Add-ons hinzufügen, entfernen und an die jeweiligen Anforderungen anpassen.

In diesem Handbuch werden die Funktionen dieses Clients beschrieben, die nicht Bestandteil des normalen Betriebssystems Microsoft Windows XP sind.

Normalerweise wird ein Terminal lokal konfiguriert und als Vorlage für andere Terminals verwendet, die dann mit den entsprechenden Verwaltungstools lokal oder remote konfiguriert werden.

Desktop

Dieser Abschnitt enthält eine allgemeine Übersicht über die Komponenten und Funktionen des WES- und XPe-Desktops für Benutzer und Administratoren.

Benutzerdesktop

Nach der Anmeldung als Benutzer wird der WES- oder XPe-Standarddesktop angezeigt, der allerdings nur Symbole für Citrix Program Neighborhood, Microsoft RDP und Internet Explorer enthält. Diese Programme können auch über das Menü „Start“ ausgewählt werden. Sie können die Terminalemulationsanwendung (HP TeemTalk) über **Start > Programme > Hewlett-Packard** öffnen.

 **HINWEIS:** Außerdem ist es möglich, Verknüpfungen zu Remoteanwendungen, die über Citrix publiziert wurden, in das Menü „Start“ aufzunehmen oder als Symbole auf dem Desktop anzuzeigen. Entsprechende Informationen und Anweisungen finden Sie in der Dokumentation zu Citrix.

Informationen zur Funktion der normalen Elemente des WES- oder XPe-Desktops und des Menüs „Start“ finden Sie in der betreffenden Microsoft Dokumentation unter:

- WES – <http://msdn.microsoft.com/en-us/embedded/bb981920.aspx>
- XPe – <http://msdn2.microsoft.com/en-us/embedded/aa731409.aspx>

Weitere Informationen zu Citrix Program Neighborhood oder Citrix XenApp finden Sie unter <http://www.citrix.com>.

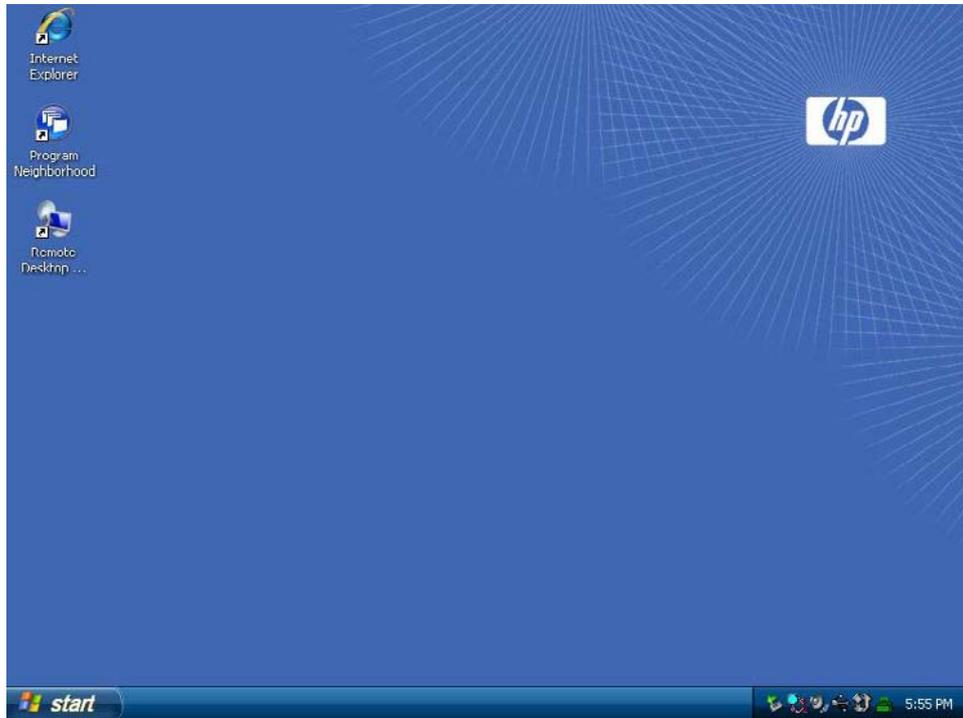
 **HINWEIS:** Die Systemsteuerung (über **Start > Systemsteuerung**) bietet Zugriff auf einige Ressourcen, mit denen die WES- oder XPe-Benutzereinstellungen geändert werden können. Wenn Sie auf alle Optionen und Dienstprogramme der Systemsteuerung zugreifen möchten, müssen Sie sich als Administrator anmelden.

Wenn Sie mit der rechten Maustaste auf den Hintergrund eines Benutzerdesktops klicken, wird kein Kontextmenü geöffnet.

Administratordesktop

Wenn Sie sich als Administrator anmelden, wird der normale Windows XP-Desktop angezeigt. Der Standardadministratordesktop umfasst die folgenden Symbole:

- Citrix Program Neighborhood
- Microsoft RDP
- Internet Explorer



 **HINWEIS:** Wenn Sie mit der rechten Maustaste auf den Hintergrund des Administratordesktops klicken, wird ein Kontextmenü geöffnet.

Anforderungen an die Serverumgebung

HP Thin Clients verwenden mehrere Dienste, die über ein Netzwerk zugänglich sind. Zu diesen Diensten zählen Sitzungs- und Produktunterstützungsdienste sowie Standardnetzwerkdienste wie DHCP und DNS. Für Thin Clients sind die folgenden Dienste erforderlich:

- Sitzungsdienste
- Unterstützungsdienste

Sitzungsdienste

In dem Netzwerk, an das der Thin Client angeschlossen ist, müssen die folgenden Sitzungsdienste vorhanden sein:

- Citrix ICA
- Microsoft RDP
- Terminalemulationsunterstützung

Citrix ICA

Citrix ICA (Independent Computing Architecture) kann im Netzwerk über Presentation Server und/oder XenApp für Microsoft Windows 2000/2003/2008 Server-Familie zur Verfügung gestellt werden.

Microsoft RDP

Der Terminaldienstclient des Thin Clients greift auf die Microsoft Terminaldienste zu. Sie können Microsoft RDP im Netzwerk über einen der folgenden Dienste zur Verfügung stellen:

- Microsoft Windows 2000/2003/2008 Server mit installierten Terminaldiensten
- Microsoft Windows 2000/2003/2008 Server

 **HINWEIS:** Wenn für beide Sitzungsdienste (ICA und RDP) Windows 2000/2003/2008-Server verwendet wird, muss sich im Netzwerk ein TSCAL-Server (Terminal Services Client Access Licenses, Clientzugriffslizenzen für Terminaldienste) befinden. Die Clientzugriffslizenzen gestatten es den Clients, die Terminal-, Datei-, Druck- und sonstigen Netzwerkdienste von Windows 2000/2003/2008 Server zu nutzen. Der Server erteilt den einzelnen Geräten temporäre Lizenzen, die 90 Tage gültig sind. Danach müssen Sie TSCALs erwerben und im TSCAL-Server installieren. Ohne eine temporäre oder permanente Lizenz kann keine Verbindung hergestellt werden.

Weitere Informationen zu den Microsoft Terminaldiensten finden Sie auf der Microsoft-Website unter <http://www.microsoft.com/windows2000/technologies/terminal/default.asp>.

Terminalemulationsunterstützung

Alle WES- oder XPe-basierten Thin Client-Modelle beinhalten eine Terminalemulationssoftware, die vorhandene, ältere Plattformen unterstützt. Die Terminalemulationssoftware verwendet für die Kommunikation mit der Computingplattform das Telnet-Protokoll.

Unterstützungsdienste

Altiris Deployment Server

Für das Thin Client-Netzwerk steht der Unterstützungsdienst Altiris Deployment Solution™ zur Verfügung. Dieser Dienst stellt ein benutzerfreundliches, integriertes Tool bereit, das eine Remoteverwaltung von Thin Clients im gesamten Lebenszyklus ermöglicht, z. B. erstmalige Bereitstellung, laufende Verwaltung und Softwareimplementierung.

Sie müssen Altiris Deployment Solution auf Windows 2000/2003/2008 Server oder einer Workstation installieren, die sich als Administrator einer Domäne anmelden kann, die die betreffenden Netzwerkdienste bereitstellt und auf ein Softwarerepository für den Thin Client zugreifen kann. Die Altiris Deployment Solutions-Software bietet die Möglichkeit, in einer PXE-Sitzung (Preboot Execution Environment) über das PXE-Protokoll ein neues Image zu erstellen oder den Thin Client wiederherzustellen. Die PXE-Aktualisierungsdienste sind Bestandteil von Altiris Deployment Solution.

Weitere Informationen zu Altiris Deployment Solution finden Sie auf der Altiris-Website unter <http://www.altiris.com/Support/Documentation.aspx> im Handbuch *Altiris Deployment Solution User Guide*.

HP Gerätemanager

Der HP Gerätemanager ist ein einfach zu installierendes und benutzerfreundliches Verwaltungstool für Thin Clients. Der HP Gerätemanager weist Ähnlichkeiten mit Altiris auf und bietet viele gleichartige Funktionen für die Verwaltung von Thin Clients. Der HP Gerätemanager bildet zusammen mit Altiris einen wesentlichen Teil des gesamten Verwaltungspakets von HP, sodass Kunden das Verwaltungstool auswählen können, das für die jeweilige Umgebung am besten geeignet ist.

3 Konfiguration

Anmeldung

Die Anmeldung am Thin Client kann automatisch oder manuell erfolgen.

Automatische Anmeldung

Die Anmeldung am WES- oder XPe-basierten Thin Client erfolgt standardmäßig automatisch. Der Administrator kann die automatische Anmeldung mit dem HP Windows Logon Configuration Manager in der Systemsteuerung aktivieren/deaktivieren sowie Benutzername, Kennwort und Domäne für die automatische Anmeldung ändern. Die Eigenschaften für die automatische Anmeldung können nur über das Administratorkonto geändert werden.



 **HINWEIS:** Zum Speichern der Änderungen müssen Sie während der aktuellen Bootsitzung den Schreibfiltercache deaktivieren oder mit der rechten Maustaste auf das grüne Schreibfiltersymbol klicken und den Befehl **commit** auswählen. Weitere Informationen zum Schreibfilter sowie Anweisungen zum Deaktivieren des Schreibfilters finden Sie unter [„Enhanced Write Filter Manager“ auf Seite 36](#). Aktivieren Sie den Schreibfilter, wenn Änderungen nicht mehr dauerhaft gespeichert werden sollen.

Wenn die automatische Anmeldung aktiviert ist, wird das Dialogfenster "Windows-Anmeldung" nicht angezeigt. Klicken Sie bei gedrückter **Umschalttaste** auf **Start > Herunterfahren > Abmelden**, wenn Sie sich bei aktivierter automatischer Anmeldung als anderer Benutzer anmelden möchten. Daraufhin wird das Dialogfenster "Windows-Anmeldung" angezeigt, in dem Sie die Anmeldeinformationen eingeben können.

Manuelle Anmeldung

Wenn die automatische Anmeldung deaktiviert ist, wird beim Start des Thin Clients das Dialogfenster "Windows-Anmeldung" angezeigt. Geben Sie die Anmeldeinformationen in die Textfelder **Benutzername** und **Kennwort** ein. Beachten Sie dabei Folgendes:

- Benutzername und Kennwort des Benutzerkontos sind werkseitig standardmäßig auf **Benutzer** eingestellt.
- Benutzername und Kennwort des Administratorkontos sind werkseitig standardmäßig auf **Administrator** eingestellt.
- Aus Sicherheitsgründen wird von HP empfohlen, die Standardwerte der Kennwörter zu ändern. Ein Administrator ist in der Lage, die Kennwörter zu ändern. Drücken Sie dazu **Strg+Alt+Entf**, um das Dialogfenster **Windows-Sicherheit** zu öffnen, und wählen Sie dann **Kennwort ändern** aus. Wenn Sie als Benutzer angemeldet sind, können Sie das Kennwort nicht ändern.
- Bei Kennwörtern wird im Gegensatz zu Benutzernamen Groß-/Kleinschreibung berücksichtigt.
- Der Administrator kann mit dem Dienstprogramm **Benutzermanager**, das in der Systemsteuerung unter der Option **Verwaltung** verfügbar ist, weitere Benutzerkonten erstellen. Weil der lokale Speicher begrenzt ist, sollte die Anzahl zusätzlicher Benutzer jedoch möglichst gering gehalten werden. Weitere Informationen finden Sie unter [„Benutzerkonten“ auf Seite 11](#).

Zugriff auf die Anmeldung als Administrator

So greifen Sie unabhängig vom jeweiligen Benutzermodus des Thin Clients auf die Anmeldung als Administrator zu:

- ▲ Halten Sie die **Umschalttaste** gedrückt, und klicken Sie auf **Start > Herunterfahren**. Halten Sie die **Umschalttaste** im Dialogfenster **Herunterfahren** weiterhin gedrückt, und wählen Sie **Abmelden** aus. Klicken Sie dann auf **OK**.

Daraufhin wird das Fenster für die Anmeldung als Administrator angezeigt.

 **HINWEIS:** Benutzername und Kennwort für das Administratorkonto sind standardmäßig auf **Administrator** eingestellt. Benutzername und Kennwort für das Benutzerkonto sind standardmäßig auf **Benutzer** eingestellt.

Mit HP Windows Logon Configuration Manager können Sie den Standardbenutzer für die Anmeldung dauerhaft ändern. Auf diese Anwendung in der Systemsteuerung kann nur der Administrator zugreifen.

Abmeldung, Neustart und Herunterfahren des Thin Clients

Klicken Sie auf **Start > Herunterfahren**, wenn Sie den Thin Client neu starten bzw. herunterfahren oder sich abmelden möchten. Wählen Sie im Dialogfenster **Herunterfahren** die gewünschte Aktion aus, und klicken Sie dann auf **OK**.



HINWEIS: Sie können sich auch im Dialogfenster "Windows-Sicherheit" abmelden oder den Thin Client herunterfahren. Drücken Sie **Strg+Alt+Entf**, um das Dialogfenster zu öffnen.

Wenn die automatische Anmeldung aktiviert ist und Sie sich beim Thin Client abmelden (ohne ihn herunterzufahren), wird vom Thin Client automatisch der Standardbenutzer angemeldet, der in der Windows Anmeldekonfiguration eingerichtet wurde. Anweisungen zum Anmelden als anderer Benutzer finden Sie unter [„Anmeldung“ auf Seite 6](#).

Abmeldung, Neustart bzw. Herunterfahren des Thin Clients wirkt sich auf die folgenden Dienstprogramme aus:

- Enhanced Write Filter
- Energieverwaltung
- Systemzeit

Enhanced Write Filter

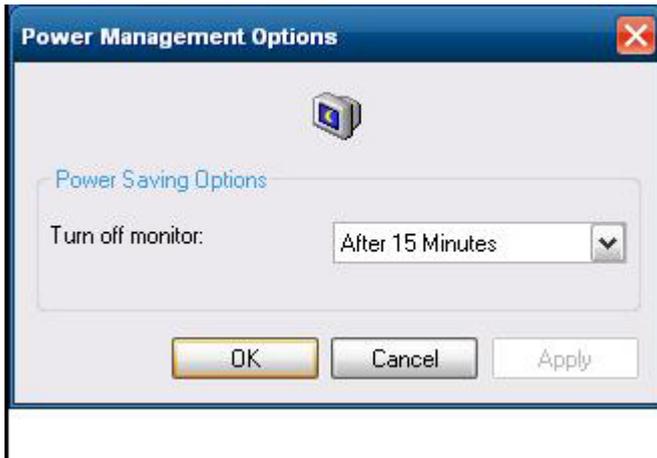
Ausführliche Informationen zu Enhanced Write Filter finden Sie unter [„Enhanced Write Filter Manager“ auf Seite 36](#). Zum Speichern von Änderungen der Systemkonfiguration müssen Sie den Schreibfiltercache in der aktuellen Bootsitzung deaktivieren oder den Befehl `-commit` ausführen. Andernfalls gehen die neuen Einstellungen verloren, wenn der Thin Client heruntergefahren oder neu gestartet wird. Aktivieren Sie den Schreibfilter, wenn Änderungen nicht mehr dauerhaft gespeichert werden sollen.

Der Inhalt des Schreibfiltercaches geht nicht verloren, wenn Sie sich abmelden und wieder als (gleicher oder anderer) Benutzer anmelden. Sie können den Schreibfiltercache nach der erneuten Anmeldung deaktivieren. Die Änderungen gehen dann nicht verloren.

Nur der Administrator verfügt über die Zugriffsrechte zum Deaktivieren des Schreibfilters.

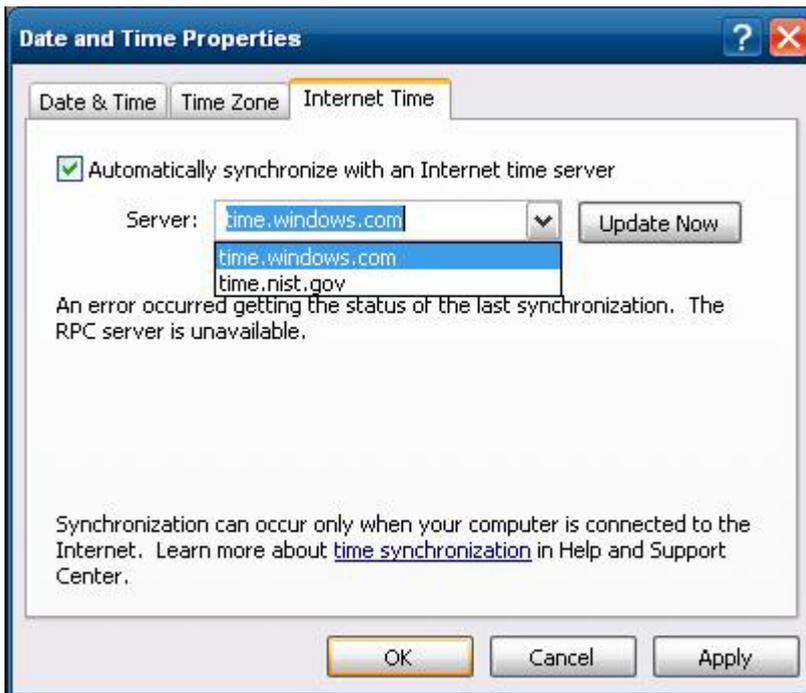
Energieverwaltung

Ein „Bildschirmschoner“ deaktiviert nach einer bestimmten Leerlaufzeit das Videosignal zum Monitor, sodass der Monitor in einen Energiesparmodus wechselt. Sie können Energiesparoptionen für den Monitor einstellen. Klicken Sie dazu mit der rechten Maustaste auf den Desktophintergrund, und wählen Sie **Eigenschaften** > **Bildschirmschoner** > **Energieverwaltung** aus.



Systemzeit

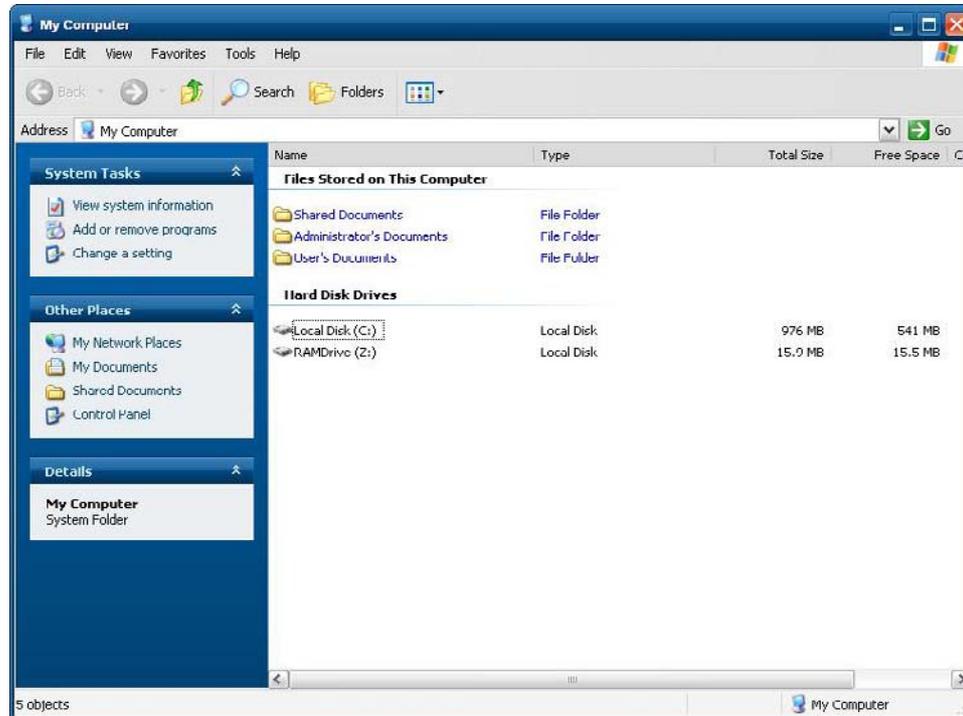
Nach dem Ausschalten bleibt die Uhrzeit erhalten, solange das Gerät an die Stromversorgung angeschlossen ist. Sie können die lokale Uhrzeit manuell festlegen oder das Dienstprogramm für die lokale Uhrzeit so einstellen, dass die Uhr des Thin Clients zu festgelegten Zeiten mit einem Zeitserver synchronisiert wird.



-  **HINWEIS:** Der Dienst "Windows-Zeitgeber" wird standardmäßig nicht gestartet. Sie können den Dienst in der Systemsteuerung über das Applet "Verwaltung" starten. Sie sollten den Dienst starten, damit die richtige Uhrzeit verwendet wird, da einige Anwendungen u. U. auf die lokale Uhrzeit des Thin Clients zugreifen müssen. Klicken Sie in der Taskleiste auf die Uhrzeit, um das Dialogfenster "Eigenschaften von Datum und Uhrzeit" zu öffnen, oder doppelklicken Sie in der Systemsteuerung auf das Symbol **Datum und Uhrzeit**.

Lokale Laufwerke

Die folgenden Abschnitte enthalten eine Beschreibung der lokalen Laufwerke des Thin Clients.



Laufwerk Z

Beim Laufwerk Z handelt es sich um den integrierten flüchtigen Speicher (MS-RAMDRIVE) des Thin Clients. Deshalb wird von HP empfohlen, auf diesem Laufwerk keine Daten zu speichern, die Sie behalten möchten. Anweisungen zur RAMDisk-Konfiguration finden Sie unter [„HP RAMDisk“ auf Seite 39](#). Informationen zur Verwendung des Laufwerks Z für servergespeicherte Profile finden Sie unter [„Servergespeicherte Profile“ auf Seite 11](#).

Laufwerk C und Flash-Laufwerk

Beim Laufwerk C handelt es sich um das integrierte Flash-Laufwerk. Von HP wird empfohlen, keine Daten auf dem Laufwerk C zu speichern, da dadurch der freie Speicherplatz auf dem Flash-Laufwerk verringert wird.

-  **ACHTUNG:** Wenn der verfügbare Speicherplatz auf dem Flash-Laufwerk weniger als 10 MB beträgt, wird der Thin Client instabil.

Vom Thin Client wird ein Schreibfilter verwendet, um die Sicherheit zu erhöhen und umfangreiche Schreibaktivitäten auf dem Flash-Laufwerk zu vermeiden. Damit die Änderungen der Thin Client-

Konfiguration beim Neustart des Thin Clients nicht verloren gehen, muss der Schreibfilter in der aktuellen Bootsitzung deaktiviert oder der Befehl `-commit` ausgeführt werden. Anweisungen zum Deaktivieren des Caches finden Sie unter [„Enhanced Write Filter Manager“ auf Seite 36](#). Aktivieren Sie den Schreibfilter, wenn Änderungen nicht mehr dauerhaft gespeichert werden sollen.

Speichern von Dateien

- △ **ACHTUNG:** Der Thin Client verwendet ein eingebettetes Betriebssystem mit einer bestimmten Flash-Speichergröße. Von HP wird empfohlen, Dateien, die Sie behalten möchten, auf einem Server und nicht auf dem Thin Client zu speichern. Sie müssen auf Anwendungen achten, die Daten auf das Laufwerk C schreiben, das sich im Flash-Speicher befindet (viele Anwendungen speichern Cachedateien standardmäßig auf dem Laufwerk C des lokalen Systems). Ändern Sie die Anwendungseinstellungen so, dass das Laufwerk Z verwendet wird, wenn Daten auf ein lokales Laufwerk geschrieben werden müssen. Aktualisieren Sie die Konfigurationseinstellungen (siehe Beschreibung unter [„Benutzerkonten“ auf Seite 11](#)), um Schreibvorgänge auf das Laufwerk C zu minimieren.

Zuordnen von Netzlaufwerken

Wenn Sie als Administrator angemeldet sind, können Sie Netzlaufwerke zuordnen.

Führen Sie die folgenden Schritte aus, damit die Zuordnungen nach einem Neustart des Thin Clients beibehalten werden:

1. Deaktivieren Sie den Schreibfiltercache in der aktuellen Bootsitzung, oder führen Sie den Befehl `-commit` aus.
2. Klicken Sie auf **Verbindung bei Anmeldung wiederherstellen**.

Da ein Benutzer den Schreibfiltercache nicht deaktivieren kann, muss sich der Benutzer abmelden (ohne den Thin Client herunterzufahren oder neu zu starten), sich danach als Administrator anmelden und dann den Schreibfilter deaktivieren, damit die Zuordnungen beibehalten werden.

Mithilfe eines Dienstprogramms „Benutzermanager“ können Sie auch ein Remote-Basisverzeichnis einrichten.

Servergespeicherte Profile

Speichern Sie serverseitige Profile auf dem Laufwerk C. Die Größe der Profile muss begrenzt sein. Die Profile gehen beim Neustart des Thin Clients verloren.

-  **HINWEIS:** Damit servergespeicherte Profile funktionieren und heruntergeladen werden können, muss genügend Flash-Speicher verfügbar sein. In einigen Fällen kann es notwendig sein, Softwarekomponenten zu entfernen, um Speicherplatz für servergespeicherte Profile zu schaffen.

Benutzerkonten

In diesem Abschnitt wird beschrieben, wie neue Benutzerkonten und Benutzerprofile erstellt werden.

Erstellen eines neuen Benutzerkontos

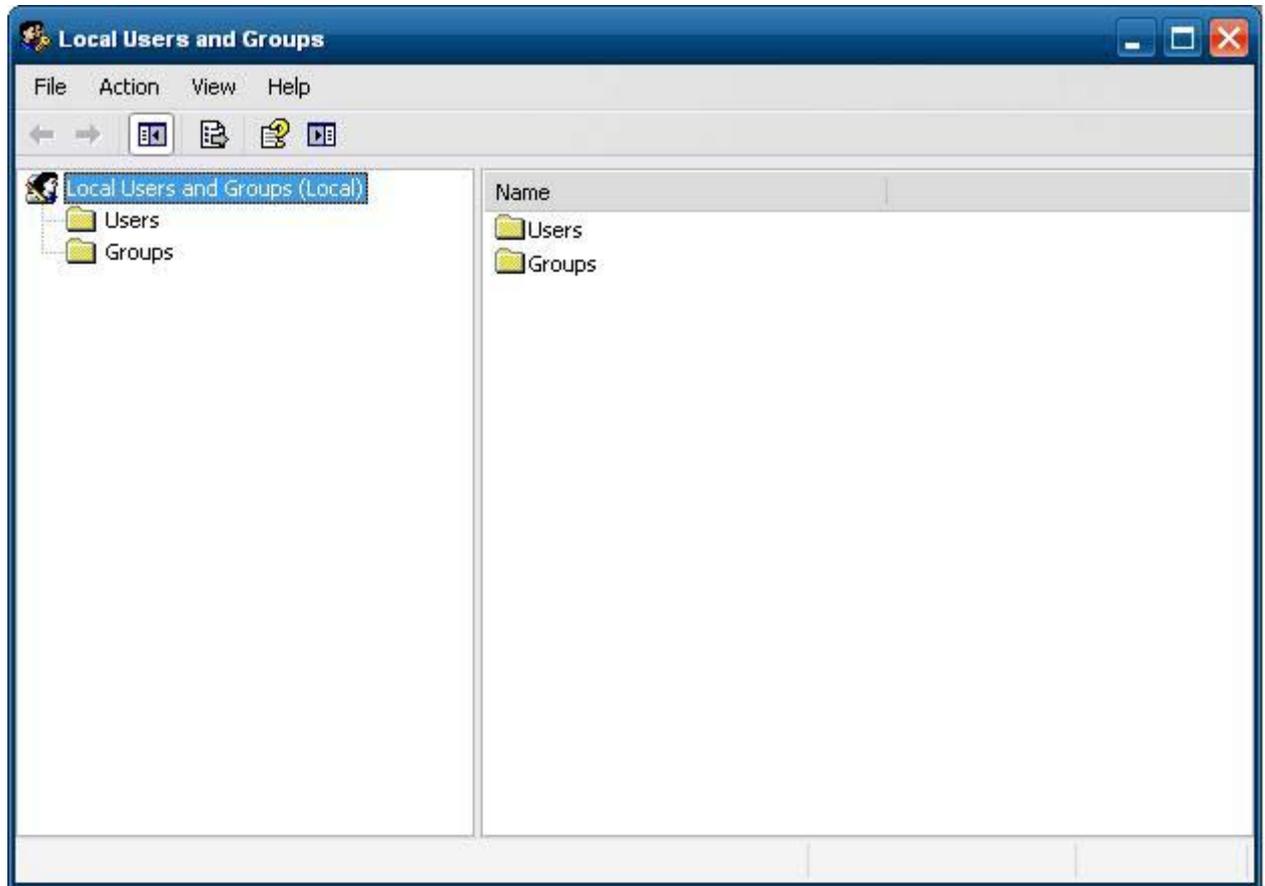
- △ **ACHTUNG:** Sie müssen den Schreibfiltercache in der Bootsitzung deaktivieren, in der ein neues Konto erstellt wird, und danach den Schreibfilter wieder aktivieren, nachdem alle permanenten Änderungen im Flash-Speicher gespeichert wurden.

Sie müssen sich als Administrator anmelden, um lokal oder remote Benutzerkonten erstellen zu können. Weil der lokale Flash-Speicher/Speicherplatz begrenzt ist, sollte die Anzahl zusätzlicher Benutzer möglichst gering gehalten werden.

Mit dem Dienstprogramm „Benutzermanager“ können Sie neue Benutzerkonten erstellen. Klicken Sie auf **Systemsteuerung > Verwaltung**, um auf dieses Dienstprogramm zuzugreifen.

Benutzer-Manager

Mit dem Dienstprogramm "Benutzer-Manager" kann der Administrator Benutzerkonten erstellen, löschen und verwalten.



Benutzerprofile

Das Profil eines neuen Benutzers basiert auf der Profilvorlage für Standardbenutzer, die Richtlinien enthält, die dem werkseitig definierten Benutzerkonto ähneln. Dieses neue Konto wird standardmäßig

als Mitglied in die lokale Benutzergruppe aufgenommen. Falls eine Änderung der Profileinstellungen des Standardbenutzers gegenüber den werkseitigen Einstellungen erfolgt, werden die geänderten Einstellungen automatisch auf das neue Benutzerprofil – lokal oder in der Domäne – angewendet. Lokale Konten, die vor den Änderungen am Profil für den Standardbenutzer erstellt wurden, bzw. Domänenkonten im Cache, die vor den Änderungen an diesem Gerät angemeldet wurden, bleiben von diesen Änderungen unberührt. Sie wirken sich nur auf Konten aus, die nach den Änderungen angemeldet oder zwischengespeichert werden.

Damit die Eigenschaften eines neuen Benutzers auf diejenigen des vordefinierten Benutzerkontos abgestimmt werden, muss der neue Benutzer zur Hauptbenutzergruppe hinzugefügt werden, da der neue Benutzer sonst keinen lokalen Drucker hinzufügen kann. Die Aktionsmöglichkeiten des Benutzers sind weiterhin begrenzt, obwohl er in der Hauptbenutzergruppe enthalten ist.

So erstellen Sie einen Benutzer:

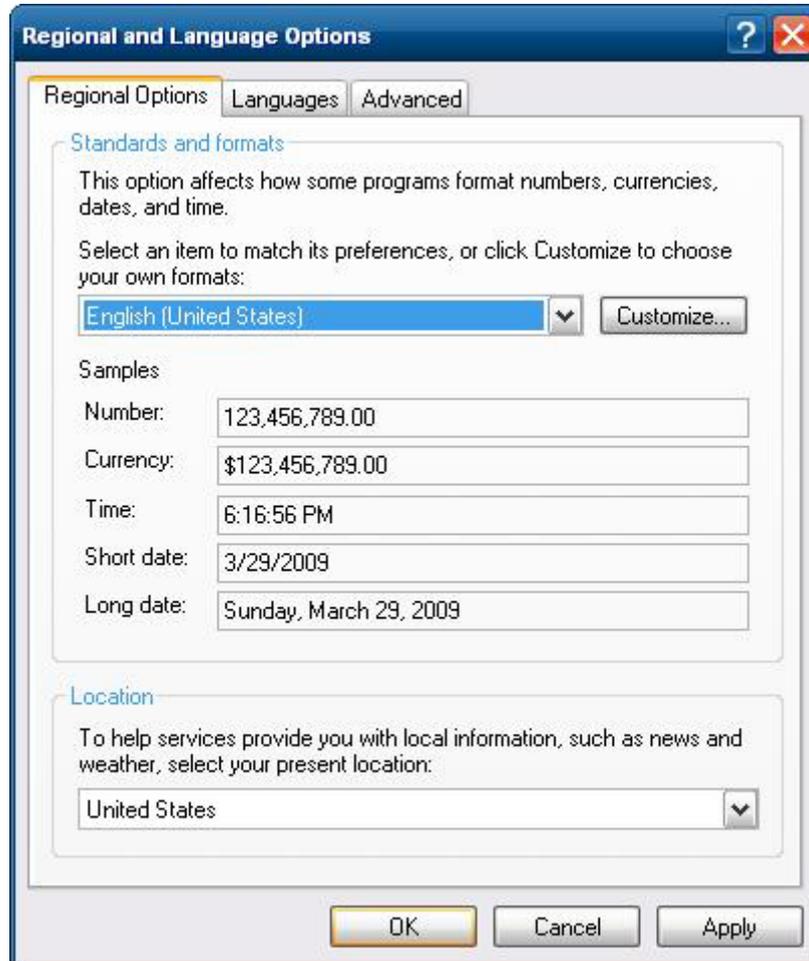
△ **ACHTUNG:** Da die Größe des Flash-Speichers begrenzt ist, wird von HP dringend empfohlen, andere Anwendungen, die neuen und vorhandenen Benutzern zur Verfügung stehen, entsprechend zu konfigurieren, um Schreibvorgänge im lokalen Dateisystem zu vermeiden. Aus dem gleichen Grund wird von HP ebenfalls empfohlen, die Konfigurationseinstellungen der werkseitig installierten Anwendungen mit äußerster Sorgfalt zu ändern.

1. Melden Sie sich als Administrator an.
2. Klicken Sie auf **Start > Systemsteuerung > Verwaltung**, um das Fenster **Verwaltung** zu öffnen.
3. Doppelklicken Sie auf **Benutzer-Manager**, um das Fenster **Lokale Benutzer und Gruppen** zu öffnen.
4. Doppelklicken Sie auf den Ordner **Benutzer**, um dessen Inhalt im rechten Fensterbereich anzuzeigen.
5. Klicken Sie in der Menüleiste auf **Aktion**, und wählen Sie **Neuer Benutzer** aus. Daraufhin wird das Dialogfenster **Neuer Benutzer** geöffnet.
6. Geben Sie Benutzernamen und Kennwort ein, und wählen Sie anschließend die gewünschten Attribute aus.
7. Klicken Sie auf **Erstellen** und anschließend auf **Schließen**.
8. Wählen Sie im linken Fensterbereich des Fensters **Lokale Benutzer und Gruppen** den Ordner **Benutzer** aus.
9. Doppelklicken Sie im rechten Teilfenster auf den Namen des soeben erstellten Benutzers. Daraufhin wird das Dialogfenster **Eigenschaften von [Benutzernamen]** geöffnet, das mehrere Registerkarten enthält.
10. Öffnen Sie die Registerkarte **Mitgliedschaft**.
11. Klicken Sie auf **Hinzufügen**. Daraufhin wird das Dialogfenster **Gruppen wählen** geöffnet.
12. Geben Sie in das Feld **Geben Sie die zu verwendenden Objektnamen ein** den Text `Hauptbenutzer` ein. Daraufhin wird die Befehlsschaltfläche **Namen überprüfen** aktiviert.
13. Klicken Sie auf **Namen überprüfen** und anschließend auf **OK**.

Der neu erstellte Benutzer ist jetzt Mitglied der beiden Gruppen „Hauptbenutzer“ und „Benutzer“ und sollte über die Berechtigungen des Standardbenutzerkontos verfügen.

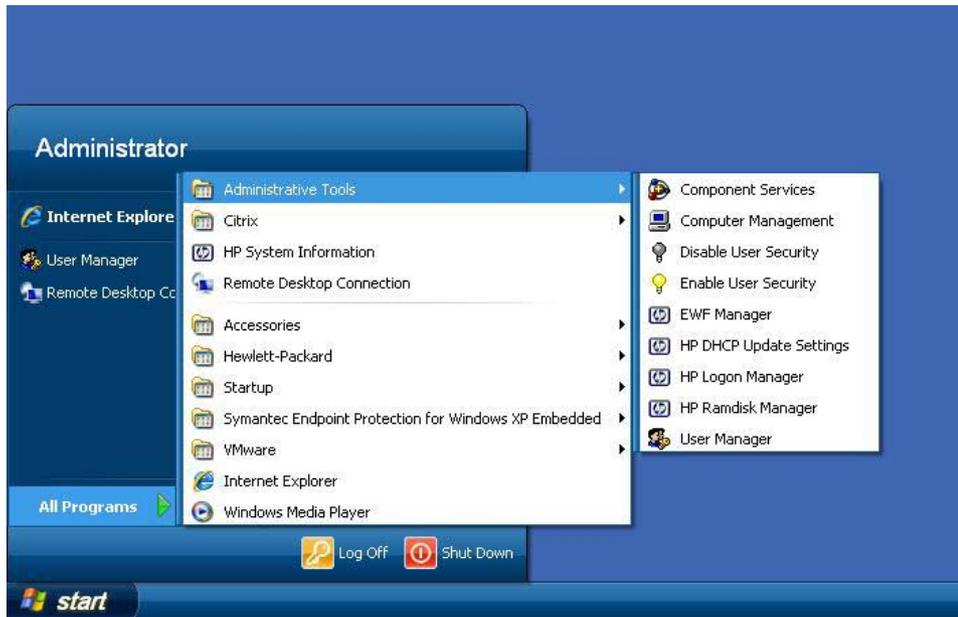
Regions- und Sprachoptionen

Die Optionen für die Tastatursprache sind werkseitig voreingestellt. Sollte eine Änderung erforderlich sein, kann die Tastatursprache in der Systemsteuerung über "Regions- und Sprachoptionen" ausgewählt werden. Mit diesem Programm können Sie die verwendete Tastatur sowie Layout-/IME-Einstellungen auswählen.



Verwaltung

Klicken Sie in der Systemsteuerung auf das Symbol **Verwaltung**, um auf die verfügbaren Verwaltungstools zuzugreifen:



4 Anwendungen

In den WES- und XPe-Images sind die folgenden vorinstallierten Anwendungen enthalten:

- [„Symantec EndPoint Protection Firewall“ auf Seite 17](#)
- [„Microsoft Windows-Firewall“ auf Seite 18](#)
- [„Citrix Program Neighborhood und PN Agent“ auf Seite 24](#)
- [„Remotedesktopverbindung“ auf Seite 25](#)
- [„HP Remote Desktop Protocol \(RDP\) Multimedia and USB Enhancements“ auf Seite 27](#)
- [„HP RGS-Empfänger \(Remote Graphics Software\)“ auf Seite 27](#)
- [„HP Session Allocation Manager \(SAM\) Client“ auf Seite 28](#)
- [„TeemTalk Terminal Emulation“ auf Seite 29](#)
- [„VMWare View Manager“ auf Seite 29](#)
- [„Altiris Client Agent“ auf Seite 29](#)
- [„HP Management Agent“ auf Seite 32](#)
- [„HP Client Automation Registration and Agent Loading Facility \(RALF\)“ auf Seite 32](#)
- [„Microsoft Internet Explorer“ auf Seite 33](#)
- [„Windows Media Player 11“ auf Seite 33](#)

Auf die folgenden Anwendungen können alle Benutzerkonten zugreifen:

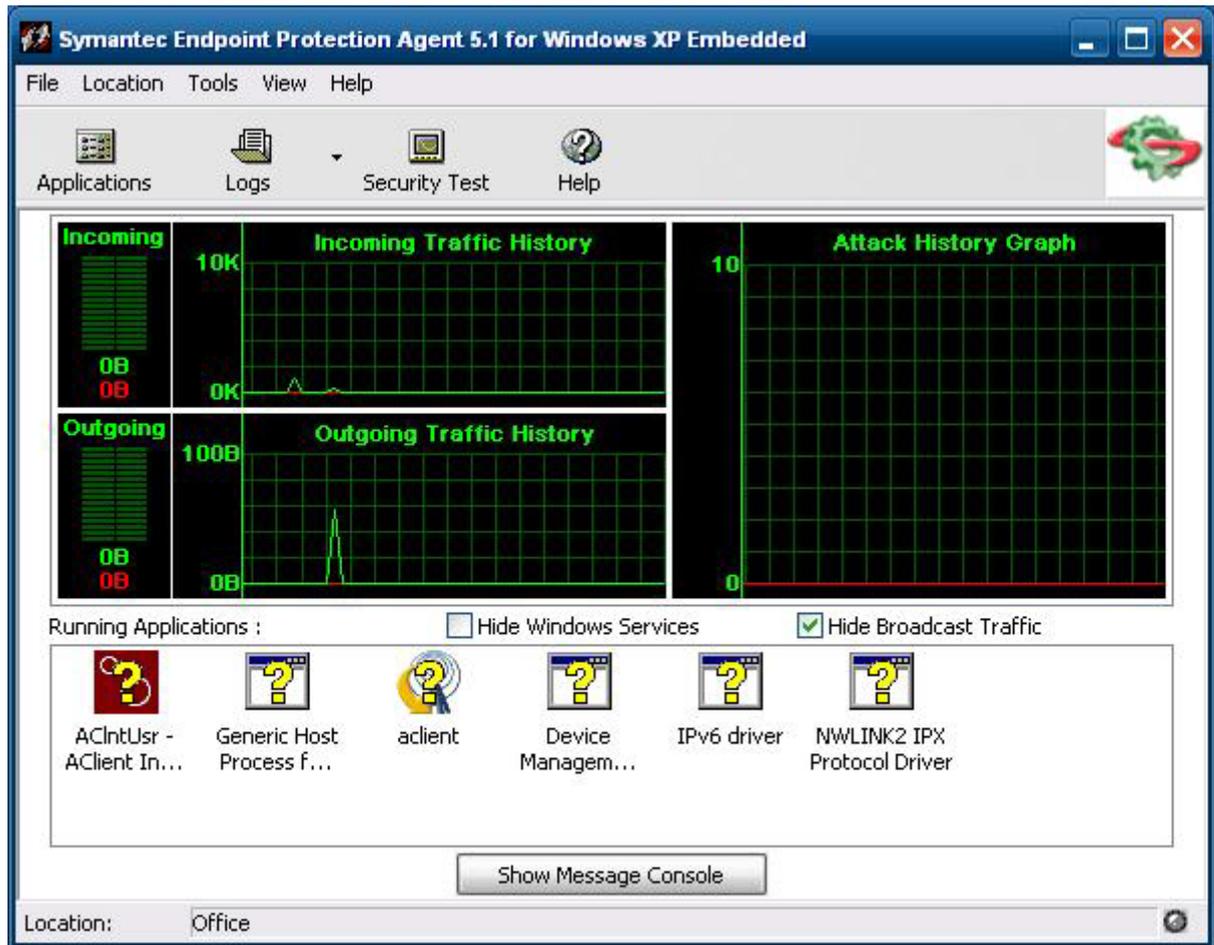
- [„Symantec EndPoint Protection Firewall“ auf Seite 17](#)
- [„Altiris Client Agent“ auf Seite 29](#)

Es besteht die Möglichkeit, weitere Anwendungen in der Form von Add-ons von der HP Website herunterzuladen.

Informationen zu diesen Anwendungen bzw. weitere wichtige Updates oder Dokumentation finden Sie auf der Website des HP Supports unter <http://www.hp.com/support>. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen** oder **Treiber und Software zum Herunterladen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die [Eingabetaste](#).

Symantec EndPoint Protection Firewall

Das HP Image enthält eine Symantec EndPoint Protection Agent Firewall.



Informationen zum Agenten

Der Symantec Endpoint Protection for Windows XPe Agent ist eine Sicherheitssoftware, die auf eingebetteten Endpunkten (z. B. HP Thin Clients) mit dem Betriebssystem WES oder XPe installiert wird.

Der Agent stellt eine anpassbare Firewall bereit, die den Endpunkt vor böswilligem oder unbeabsichtigtem Eindringen und Missbrauch schützt. Er erkennt und identifiziert bekannte Trojanische Pferde, Port-Scans und andere häufige Angriffe. Zur Abwehr werden Datenverkehr bzw. Netzwerkdienste, Anwendungen, Ports und Komponenten selektiv zugelassen oder blockiert.

Der Agent verwendet Sicherheitsrichtlinien, die Firewallregeln umfassen, sowie Sicherheitseinstellungen. Diese Richtlinien schützen einen einzelnen Endpunkt vor Netzwerkdatenverkehr und Viren, die Schäden verursachen können. Die Firewallregeln bestimmen, ob der Endpunkt ein- oder ausgehende Zugriffe von Anwendungen bzw. Diensten über die Netzwerkverbindung zulässt oder blockiert. Die Firewallregeln ermöglichen es dem Agenten, ein- oder ausgehende Anwendungen sowie Datenverkehr von oder zu bestimmten IP-Adressen und Ports zuzulassen oder zu blockieren. Die Sicherheitseinstellungen bieten die Möglichkeit, häufig

vorkommende Angriffe zu erkennen und zu identifizieren, nach einem Angriff entsprechende E-Mail-Nachrichten zu senden, anpassbare Meldungen anzuzeigen und andere zweckmäßige Sicherheitsaufgaben durchzuführen. Die Sicherheitsrichtlinien, die erweiterten Regeln, die Sicherheitseinstellungen sowie die Einstellungen des IPS-Moduls wurden von HP angepasst, um sowohl eine optimale Leistung als auch eine sichere Computingumgebung sicherzustellen.

Neue Leistungsmerkmale und Funktionen

- Alle Benutzerkonten können jetzt die Optionen und Einstellungen für den SEP-Agenten ändern. Zuvor konnte lediglich das Administratorkonto die Eigenschaften des Sygate-Agenten ändern. Der Zugriff von Benutzern auf die Firewall-Einstellungen kann jetzt durch ein Agentenkennwort eingeschränkt werden.
- Der bisherige Sygate-Richtlinieneditor wurde durch geänderte Verwaltungsoptionen für die Befehlszeile und eine Regelschnittstelle ersetzt. Regel- und Richtlinienänderungen, für die bisher ein eigenständiger Richtlinieneditor erforderlich war, können jetzt auf der Benutzeroberfläche des Agenten vorgenommen und anschließend mit neuen Befehlszeilenoptionen exportiert/importiert werden. Ein eigenständiger Richtlinieneditor für SEP steht nicht mehr zur Verfügung.

Weitere Informationen zur Symantec SEP Firewall stehen im *Symantec™ Endpoint Embedded Protection für Windows® XP Embedded Standard 2009 (WES) und Windows XP Embedded (XPe) Benutzerhandbuch* unter der folgenden Adresse zur Verfügung: <http://www.hp.com/support>. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die [Eingabetaste](#).

Microsoft Windows-Firewall

Von HP wird eine verbesserte Microsoft Windows-Firewall (zuvor Internetverbindungsfirewall genannt) als Add-on zur Verfügung gestellt. Die Firewall ist nach der Installation des Add-ons standardmäßig aktiviert.

Standardmäßige Aktivierung

Nach der Installation des Add-ons ist die Windows-Firewall standardmäßig für alle Netzwerkschnittstellen aktiviert. Durch die standardmäßige Aktivierung werden auch neue Netzwerkverbindungen geschützt, die zum System hinzugefügt werden. Dadurch kann die Kompatibilität von Anwendungen verloren gehen, wenn die Anwendung standardmäßig keine statusbehaftete Filterung unterstützt.

Konfigurieren der Microsoft Windows-Firewall

Um optimale Sicherheit und Benutzerfreundlichkeit zu gewährleisten, bietet die Windows-Firewall die Möglichkeit, Ausnahmen für Anwendungen und Dienste hinzuzufügen, damit sie eingehenden Datenverkehr empfangen können.

Sie können die Windows-Firewall in der **Systemsteuerung** konfigurieren. Der Zugriff auf die Firewallkonfiguration ist auf der Registerkarte **Erweitert** der Eigenschaften der Netzwerkverbindung möglich.

Das **Sicherheitscenter** ist nicht im Image enthalten. Das Systemsteuerungsapplet "FIREWALL.CPL" steht nach der Installation der Windows-Firewall nur dem Administratorkonto zur Verfügung.



 **HINWEIS:** Das Systemsteuerungsapplet steht nach der Installation des Windows-Firewall-Add-ons nur dem Administratorkonto zur Verfügung.

- Registerkarte **Allgemein:** Die Registerkarte **Allgemein** bietet Zugriff auf die folgenden drei Hauptkonfigurationsoptionen:
 - Aktiv (empfohlen)
 - Keine Ausnahmen zulassen
 - Inaktiv (nicht empfohlen)

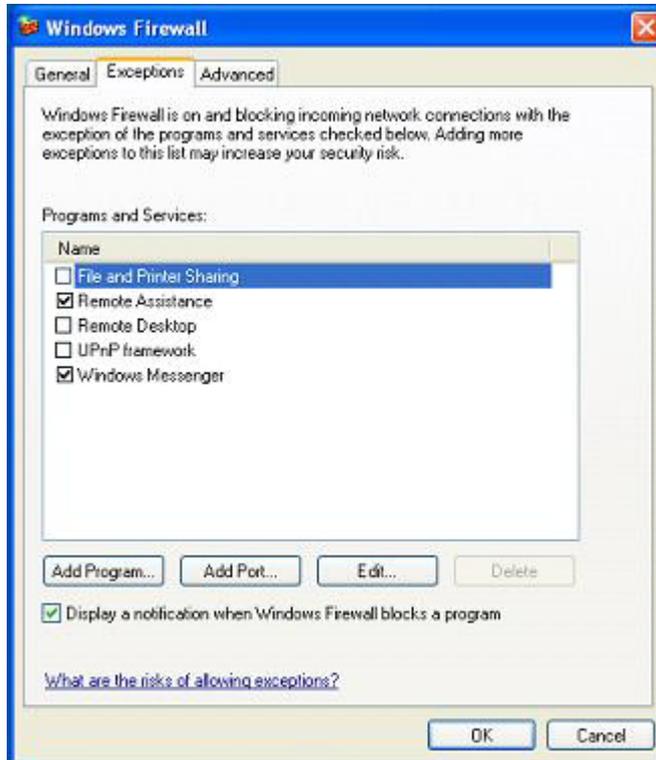
Bei Auswahl von **Keine Ausnahmen zulassen** blockiert die Windows-Firewall alle Verbindungsanforderungen an den Computer (einschließlich der Anforderungen von Programmen oder Diensten auf der Registerkarte **Ausnahmen**). Die Firewall blockiert außerdem die Datei- und Druckerfreigabe sowie die Suche nach Netzwerkgeräten.

Die Verwendung der Windows-Firewall ohne Ausnahmen ist sinnvoll, wenn Sie eine Verbindung zu einem öffentlichen Netzwerk verwenden. Mithilfe dieser Einstellung kann der Computer geschützt werden, da alle Verbindungsversuche zum Computer blockiert werden. Wenn Sie die Windows-Firewall ohne Ausnahmen verwenden, können Sie weiterhin Webseiten anzeigen, E-Mails senden und empfangen oder ein Instant Messaging-Programm verwenden.

- Registerkarte **Ausnahmen:** Auf dieser Registerkarte können Sie Ausnahmen für Programme und Ports hinzufügen, um bestimmten eingehenden Datenverkehr zuzulassen. Die Ausnahmeeinstellungen geben die Computer an, für die die betreffenden Ports/Programme geöffnet sind.

Sie können drei verschiedene Zugriffsmodi angeben:

- Alle Computer (einschließlich der im Internet)
- Nur für eigenes Netzwerk (Subnetz)
- Benutzerdefinierte Liste



Die Option "Benachrichtigen, wenn Programm durch Windows-Firewall geblockt wird" ist standardmäßig aktiviert.

Sie können für jede Ausnahme einen Bereich festlegen. Bei privaten und kleinen Netzwerken wird empfohlen, den Bereich nach Möglichkeit auf das lokale Netzwerk zu beschränken. Bei dieser Einstellung können Computer in einem Subnetz eine Verbindung mit dem Programm auf dem Computer herstellen. Der Datenverkehr von einem Remotenetzwerk wird jedoch gesperrt.

- Registerkarte **Erweitert**: Auf dieser Registerkarte können Sie die folgenden Funktionen konfigurieren.
 - **Netzwerkverbindungseinstellungen**: In diesem Abschnitt können Sie verbindungs-spezifische Regeln für die einzelnen Netzwerkschnittstellen auswählen.
 - **Sicherheitsprotokollierung**: Hier können Sie eine Protokolldatei für die Fehlerbehandlung erstellen.
 - **ICMP**: Mit dem Global Internet Control Message-Protokoll (ICMP) können Computer in einem Netzwerk Fehler- und Statusinformationen austauschen.
 - **Standardeinstellungen**: Hier können Sie die Standardkonfiguration der Windows-Firewall wiederherstellen.



Ermitteln von Konfigurationsinformationen

Mit dem folgenden Befehl können Sie die aktuelle Richtlinienkonfiguration der Windows-Firewall überprüfen: **netsh firewall show configuration**.

Beheben von Anwendungsproblemen

Probleme können am besten vermieden werden, wenn eine Anwendung so geändert wird, dass sie eine Firewall mit statusbehafteter Filterung verwendet. Dies ist allerdings nicht immer möglich. Die Firewall bietet daher die Möglichkeit, Ausnahmen für Ports und Anwendungen zu konfigurieren.

Fehlersymptome

Fehler in der Standardkonfiguration sind folgendermaßen erkennbar:

- Clientanwendungen können keine Daten von einem Server empfangen. Beispiele dafür sind FTP-Clients, Multimediasoftware sowie Benachrichtigungen über neue E-Mails in einigen E-Mail-Anwendungen.
- Serveranwendungen, die auf dem WES- oder XPe-basierten Computer ausgeführt werden, reagieren nicht auf Clientanforderungen. Beispiele dafür sind Webserver wie Internetinformationsdienste (IIS), Remotedesktop und Dateifreigabe.



-
-  **HINWEIS:** Fehler in Netzwerkanwendungen sind nicht auf Firewallprobleme beschränkt. Änderungen der RPC- oder DCOM-Sicherheit können ebenfalls Fehler verursachen. Daher muss festgestellt werden, ob für den Fehler eine Sicherheitswarnung der Windows-Firewall mit dem Hinweis angezeigt wird, dass eine Anwendung blockiert wurde.
-

Fehlerbehebung

Bei einem der oben genannten Fehler können Sie Ausnahmen zur Konfiguration der Windows-Firewall hinzufügen. Durch Ausnahmen wird die Firewall so konfiguriert, dass bestimmte eingehende Verbindungen zum Computer zugelassen werden.

-  **HINWEIS:** Von HP wird empfohlen, Programme und keine Ports hinzuzufügen. Das Hinzufügen eines Programms ist einfacher und sicherer als das Hinzufügen eines Ports, weil die genutzten Portnummern nicht bekannt sein müssen und der Port nur dann geöffnet ist, wenn das Programm auf eine eingehende Verbindung wartet. Der Port kann nur von der angegebenen Anwendung verwendet werden. Beim Öffnen eines Ports kann dieser von allen Anwendungen verwendet werden.
-

Hinzufügen eines Programms

Bei der Konfiguration der Firewall wird empfohlen, Programme zur Ausnahmeliste hinzuzufügen. Diese Lösung ermöglicht eine sehr einfache Konfiguration und bietet die Möglichkeit, dass die Firewall Portbereiche öffnet, die bei jeder Ausführung des Programms geändert werden können.

So fügen Sie eine Programmausnahme hinzu:

1. Öffnen Sie das Dialogfenster **Windows-Firewall**, und wählen Sie die Registerkarte **Ausnahmen** aus.
2. Klicken Sie auf das Kontrollkästchen neben dem Programm, wenn das Programm in der Liste enthalten ist, um die Ausnahme zu aktivieren. Klicken Sie auf **Programm**, wenn das Programm nicht in der Liste enthalten ist, um das Dialogfenster **Programm hinzufügen** zu öffnen.
3. Klicken Sie auf **Durchsuchen**, und wählen Sie das Programm aus, das als Ausnahme hinzugefügt werden soll. Klicken Sie anschließend auf **OK**.
4. Klicken Sie auf **Bereich ändern**, um den Bereich für das Programm anzuzeigen oder festzulegen, und klicken Sie anschließend auf **OK**.
5. Klicken Sie auf **OK**, um das Dialogfenster **Programm hinzufügen** zu schließen.
6. Klicken Sie auf das Kontrollkästchen, um das Programm zu aktivieren. Das Programm ist in der Liste standardmäßig nicht aktiviert.

Hinzufügen eines Ports

Wenn das Anwendungsproblem durch Hinzufügen des Programms zur Ausnahmeliste nicht behoben werden kann, können Sie manuell Ports hinzufügen. Sie müssen dazu die von der Anwendung verwendeten Ports kennen. Wenden Sie sich an den Hersteller der Anwendung, um die verwendeten Ports zu ermitteln. Dies ist die zuverlässigste Methode.

Wenn die Portnummern für den Prozess kleiner sind als 1024, ändern sich die Portnummern mit hoher Wahrscheinlichkeit nicht. Wenn die verwendeten Portnummern größer sind als 1024, verwendet die Anwendung u. U. einen Portbereich, sodass das Problem durch Öffnen einzelner Ports vermutlich nicht zuverlässig gelöst wird.

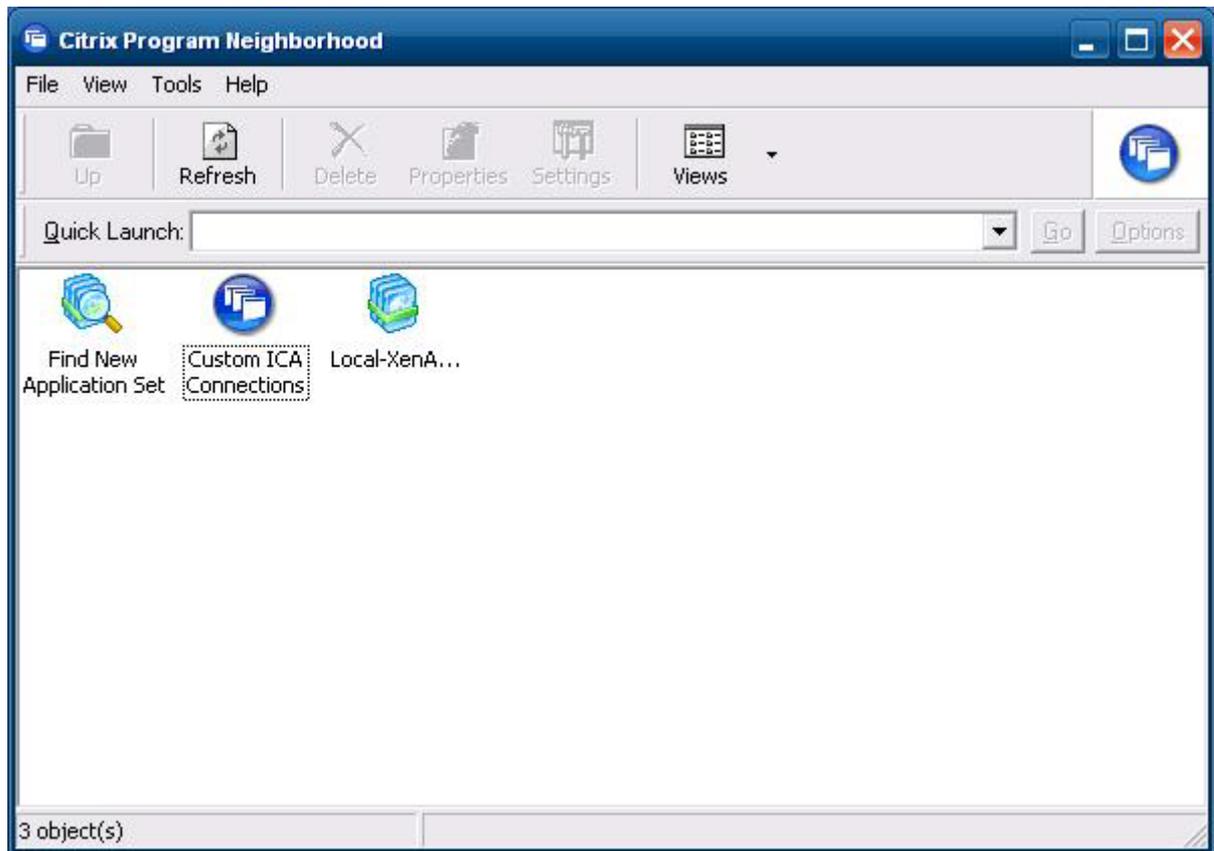
Fügen Sie eine Ausnahme für den betreffenden Port hinzu, nachdem Sie Portnummer und Protokoll ermittelt haben.

So fügen Sie eine Portausnahme hinzu:

1. Öffnen Sie das Dialogfenster **Windows-Firewall**, und klicken Sie auf die Registerkarte **Ausnahmen**.
2. Klicken Sie auf **Port**, um das Dialogfenster **Port hinzufügen** zu öffnen.
 - a. Geben Sie die **Portnummer** ein.
 - b. Wählen Sie das Protokoll **TCP** oder **UDP** aus.
 - c. Geben Sie in das Feld **Name** einen aussagekräftigen Namen für die Portausnahme ein.
3. Klicken Sie auf **Bereich ändern**, um den Bereich für die Portausnahme anzuzeigen oder festzulegen, und klicken Sie anschließend auf **OK**.
4. Klicken Sie auf **OK**, um das Dialogfenster **Port hinzufügen** zu schließen.
5. Klicken Sie auf das Kontrollkästchen neben dem entsprechenden Eintrag, um die Portausnahme zu aktivieren.

Citrix Program Neighborhood und PN Agent

Citrix Program Neighborhood ist eine Komponente von ICA, die mit MetaFrame 1.8 eingeführt wurde, mit der Benutzer Verbindungen zu MetaFrame- und WinFrame-Servern sowie veröffentlichten Anwendungen herstellen können. Program Neighborhood bietet eine umfassende administrative Kontrolle über die Zugriffsmöglichkeiten von Anwendungen und ermöglicht eine problemlose Desktopintegration.



Alternativ können Sie PN Agent verwenden, wenn Citrix Presentation Server oder XenApp über Web Interface implementiert ist. PN Agent ist von einer zentralen Konfigurationsdatei auf dem Web Interface-Server abhängig. Über diesen Client können Symbole auf den Desktop oder in das Menü „Start“ des Thin Client gestellt werden, um eine nahtlose Integration publizierter Anwendungen sicherzustellen.

Über den Citrix Ordner im Menü „Start“ können Sie auf PN Agent zugreifen und den PN Agent starten.

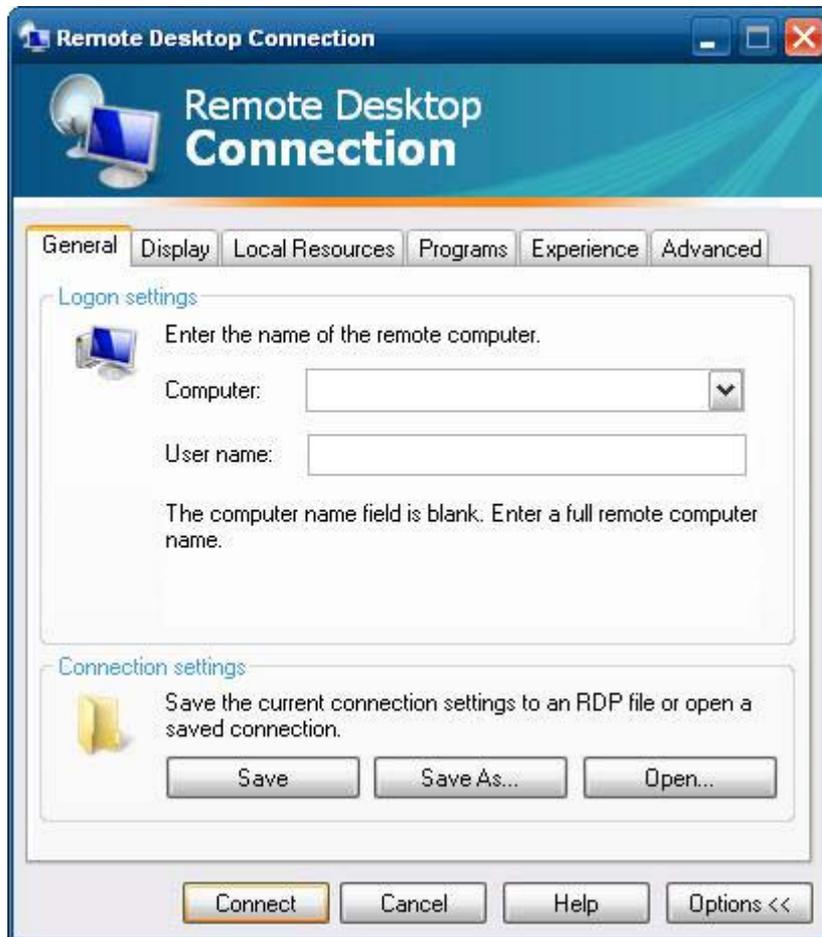


Die Dokumentation für die ICA-Clientanwendung steht auf der Website der Citrix Corporation unter www.citrix.com zur Verfügung.

Remotedesktopverbindung

Im Dialogfenster "Remotedesktopverbindung" können Sie mit Microsoft RDP Verbindungen zu einem Windows-Terminalserver herstellen oder auf Remoteanwendungen zugreifen.

Die Dokumentation mit ausführlichen Erklärungen und Anweisungen zur Verwendung von Microsoft RDC finden Sie auf der Microsoft Website.



HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements

Die Software „HP Remote Desktop Protocol (RDP) Multimedia and USB Enhancements“ erweitert die Virtualisierungsmöglichkeiten von Microsoft Remote Desktop Protocol. HP Remote Desktop Protocol Enhancements gestatten Benutzern eine über eine einzige Anmeldung initialisierte, virtuelle Desktop-Funktionsweise im Vollbildmodus (einschließlich Stereoklang). Die Software auf Clientseite, die in den neuesten WES- und XPe-Images enthalten ist, funktioniert nahtlos. Benutzer melden sich einfach am Thin Client an, um dessen Multimediafunktionen wie Schulungsvideos und USB-Geräteunterstützung zu nutzen. Weitere Informationen finden Sie unter <http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c01705352/c01705352.pdf>.

HP RGS-Empfänger (Remote Graphics Software)

HP Remote Graphics Software (RGS) ist ein leistungsstarkes Verbindungsprotokoll für Remotedesktops, das durch eine herausragende Funktionsweise für Remotedesktopbenutzer überzeugt. Es stellt vielfältige Benutzerumgebungen zur Verfügung, die Videos, Web-Flash-Animationen und grafikintensive Umgebungen umfassen. Alle Anwendungen werden nativ auf dem Remotesystem ausgeführt und nutzen die Computer- und Hardware-Grafikressourcen des sendenden Systems.

HP RGS erfasst den Desktop des Remotesystems und sendet ihn über eine Standardnetzwerkverbindung an ein Fenster auf einem lokalen Client (einem Empfänger). Dabei kommt eine neuartige Bildkomprimierungstechnologie zum Einsatz, die speziell für Text, digitale Bilder und Videoanwendungen mit hoher Framerate konzipiert wurde. Der Empfänger nutzt die Tastatur, die Maus und die USB-Geräte am Thin Client, um so mit den Anwendungen zu kommunizieren als würden sie physisch mit dem Sendersystem kommunizieren. Dadurch wird eine interaktive und leistungsstarke Desktopfunktionsweise mit mehreren Displays bereitgestellt.

Der RGS-Empfänger ist im neuesten HP Thin Client WES- und XPe-Image enthalten. Weitere Informationen zu Lizenzierung, Installation und Verwendung des RGS-Senders finden Sie unter <http://www.hp.com/go/rgs>.

HP Session Allocation Manager (SAM) Client

Die CCI-Lösung (Consolidated Client Infrastructure) von HP zentralisiert die Desktopcomputing- und Speicherressourcen in einfach zu verwaltenden, besonders sicheren Rechenzentren. Gleichzeitig ermöglicht sie den Endbenutzern ein einfaches Arbeiten in der vertrauten, traditionellen Desktopumgebung. Darüber hinaus wird in Unternehmen seit längerer Zeit die serverbasierte Verarbeitung eingesetzt, um auf einem Server virtuelle Instanzen von Desktopanwendungen zu erstellen, auf die mehrere Remotebenutzer zugreifen können. HP CCI bietet eine neue Alternative, um virtuelle Desktops zu erstellen.

Ein Bestandteil der CCI-Lösung ist der HP Session Allocation Manager (HP SAM), der eine Erweiterung des HP SAM-Clients bildet. Der HP SAM-Client ist im aktuellen HP Thin Client WES- und XPe-Image enthalten und kann über **Start > Programme** aufgerufen werden.



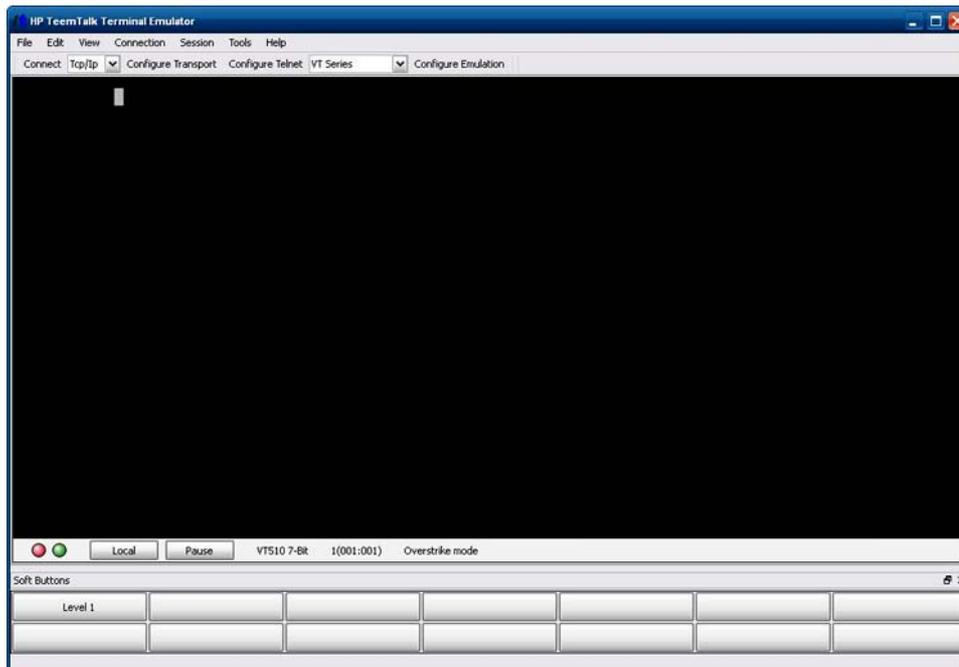
Mithilfe von HP SAM kann eine CCI-Implementierung gesteuert und verwaltet werden. Insbesondere besteht die Möglichkeit, die Zuordnung von Microsoft Remotedesktopverbindungen vom Gerät eines Benutzers (Thin Client) zu Remotedesktopsitzungen (Blade-PCs) zu verwalten. Unabhängig davon, ob die Sitzung von einem dedizierten physischen Bladesystem oder zusammen mit anderen Sitzungen von

einer virtuellen Hardwareplattform verwaltet wird, kann das HP SAM-System die betreffenden Desktopsitzungen bei Bedarf Benutzern zur Verfügung stellen.

Weitere Informationen zu HP SAM finden Sie unter <http://h71028.www7.hp.com/enterprise/cache/323204-0-0-225-121.html>.

TeemTalk Terminal Emulation

Alle WES- oder XPe-basierten Thin Client-Modelle beinhalten eine Terminalemulationssoftware, die vorhandene, ältere Plattformen unterstützt. Die Software verwendet für die Kommunikation mit der Computingplattform das Telnet-Protokoll. Entsprechende Anweisungen finden Sie in der Terminalemulationsdokumentation (nicht im Lieferumfang enthalten). Sie können TeemTalk Connection Wizard und TeemTalk Emulator standardmäßig über **Start > Alle Programme** aufrufen.



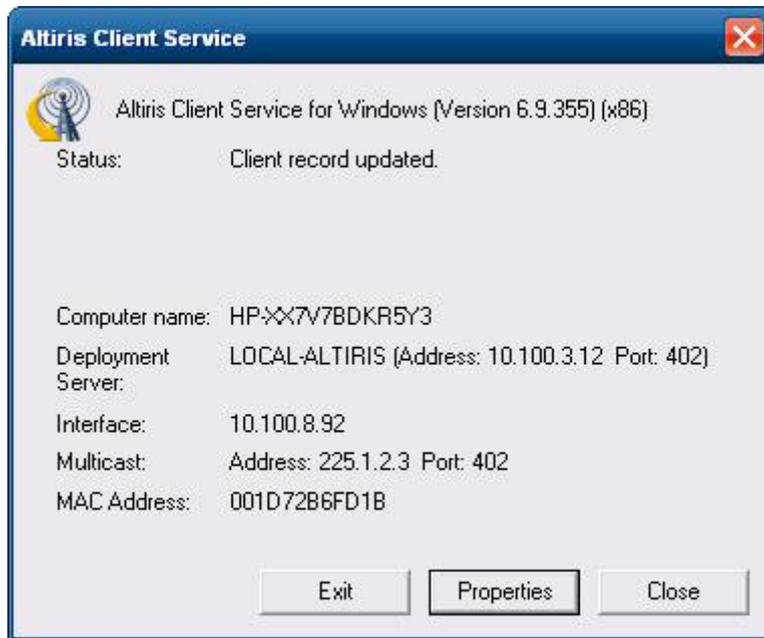
VMWare View Manager

Beim View Manager, einer Schlüsselkomponente von VMWare View, handelt es sich um eine Desktopverwaltungslösung der Unternehmensklasse, die die Verwaltung, die Bereitstellung und die Implementierung virtueller Desktops optimiert. Benutzer können über den View Manager sicher und bequem auf virtuelle Desktops, die in der VMWare Infrastruktur gehostet sind, Terminalserver, Blade-PCs und sogar physische Remote-PCs zugreifen.

Weitere Informationen zu VMWare View finden Sie unter <http://www.vmware.com/products/view>.

Altiris Client Agent

Mit dem Altiris Client Agent kann der Altiris-Server gültige Clients suchen, die zum Netzwerk hinzugefügt wurden. Der Agent sorgt für die Zuordnungen und meldet den Status der einzelnen Thin Clients an den Altiris-Server.



Altiris Client Service Properties [X]

Server Connection | Access | Security | Log File | Proxy | Startup/Shutdown

 Connect directly to this Deployment Server

Address/Hostname: Port:

Enable key-based authentication to Deployment Server

Key file:

Deployment Agent will require a key file in order to connect to Deployment Server.

Discover Deployment Server using TCP/IP multicast

If no Deployment Server is specified, the Deployment Agent will connect to the first Deployment Server it finds.

Server Name: Port:

Multicast Address: TTL:

Refresh connection after idle

Abort file transfers if rate is slower than Kbps

OK Cancel

HP Management Agent

Beim HP Management Agent handelt es sich um eine Softwarekomponente, die auf Thin Client-Geräten installiert ist, damit eine Interaktion zwischen dem HP Gerätemanager und den Geräten möglich ist. Der Agent ist im WES- und XPe-Standardimage des Thin Clients enthalten, damit der Gerätemanager ohne großen Aufwand Geräte verwalten kann (Agenten älterer Geräte müssen jedoch u. U. aktualisiert werden).

Weitere Informationen zum HP Gerätemanager und zum HP Management Agent sowie andere wichtige Aktualisierungen oder Dokumente finden Sie auf der Website des HP Supports: <http://www.hp.com/support>. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen** oder **Treiber und Software zum Herunterladen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die **Eingabetaste**.



HP Client Automation Registration and Agent Loading Facility (RALF)

Konfiguration und Betrieb von RALF

RALF ist bei Lieferung auf den neuesten HP Thin Client-Images (mit Ausnahme derjenigen, auf denen ThinConnect ausgeführt wird) vorinstalliert. RALF dient zur Registrierung auf einem HP Client Automation Server (HPCA), um den vollständigen HPCA-Agenten für den Client anfordern zu können, sodass sich der Thin Client über die HP Client Automation-Konsole verwalten lässt. RALF wird unter Verwendung eines Standardhostnamens für HPCA-Server konfiguriert, der als 'hpcaserver' definiert ist. Der HPCA-Server kann zwar diesem Namen entsprechend installiert werden, aber die übliche Vorgehensweise besteht darin, diesen Namen als DNS-Aliasnamen bei der Definition des tatsächlichen Hostnamens für den HPCA-Server zu verwenden. Bei HP Client Automation Standard, Starter und Enterprise Version 7.5 (oder höher) ist zusätzliche Dokumentation verfügbar, in der erläutert wird, wie sich RALF neu konfigurieren lässt, um einen anderen Hostnamen mithilfe der Befehlszeilenoptionen zu definieren. Weitere Informationen zu HP Client Automation finden Sie unter https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp.

Bei der Installation von RALF wird das Programm als Windows Dienst oder Linux Daemon ausgeführt, von dem regelmäßig geprüft wird, ob der HPCA-Server vorhanden ist. Diese Prüfung läuft 24 Stunden lang. Danach wird RALF heruntergefahren. Nach einem Neustart wird diese Prüfung erneut für 24 Stunden ausgeführt. Sobald eine Verbindung zum Server hergestellt wurde, wird das Gerät von RALF in der HPCA-Infrastruktur registriert. Danach wird auf die Bestätigung der Anforderung zum Installieren des HPCA-Agenten gewartet. Nach dem Installieren des HPDA-Agenten wird von RALF regelmäßig eine Verbindung zum Server hergestellt, und die Attribute der Geräteregistrierung werden überprüft.

Microsoft Internet Explorer

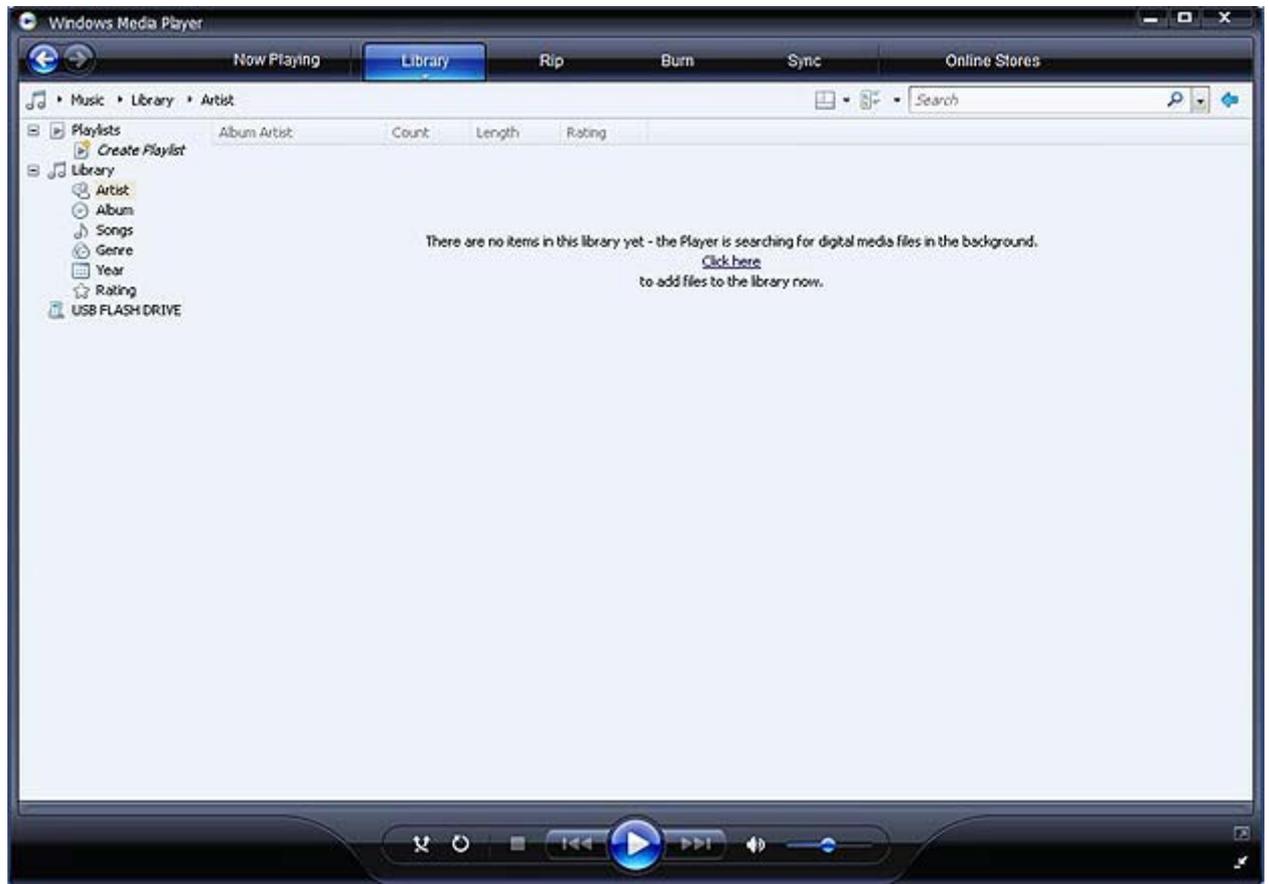
Auf dem Thin Client ist die Version 7.0 des Browsers Microsoft Internet Explorer installiert. Die Einstellungen für die Internetoptionen des Browsers wurden werkseitig vorkonfiguriert, um Schreibvorgänge in den Flash-Speicher zu begrenzen. Diese Einstellungen verhindern, dass der verfügbare, begrenzte Flash-Speicher verbraucht wird, und sollten daher nicht geändert werden. Sie können über ein ICA- oder RDP-Konto auf einen anderen Browser zugreifen, wenn zusätzliche Browserressourcen benötigt werden.

Microsoft Internet Explorer 7.0 ist wesentlich sicherer. Internet Explorer verfügt über weitere Steuerungsmöglichkeiten für die Ausführung aller Inhalte sowie über eine integrierte Funktion für die Verwaltung von Popup-Fenstern. Darüber hinaus verhindert Internet Explorer jetzt, dass Skripts Fenster und Statusleisten verschieben oder deren Größe ändern, um deren Anzeige zu verhindern oder andere Fenster zu verdecken.

Beim Internet Explorer 7 ist eine Funktion zum Blockieren der Übertragung unsicherer Dateien verfügbar. Eine Liste der Dateien, die üblicherweise als unsicher eingestuft werden, finden Sie unter *Informationen über die Liste „Nicht sichere Dateien“ in Internet Explorer 6* auf der Microsoft Website unter <http://support.microsoft.com/kb/291369>.

Windows Media Player 11

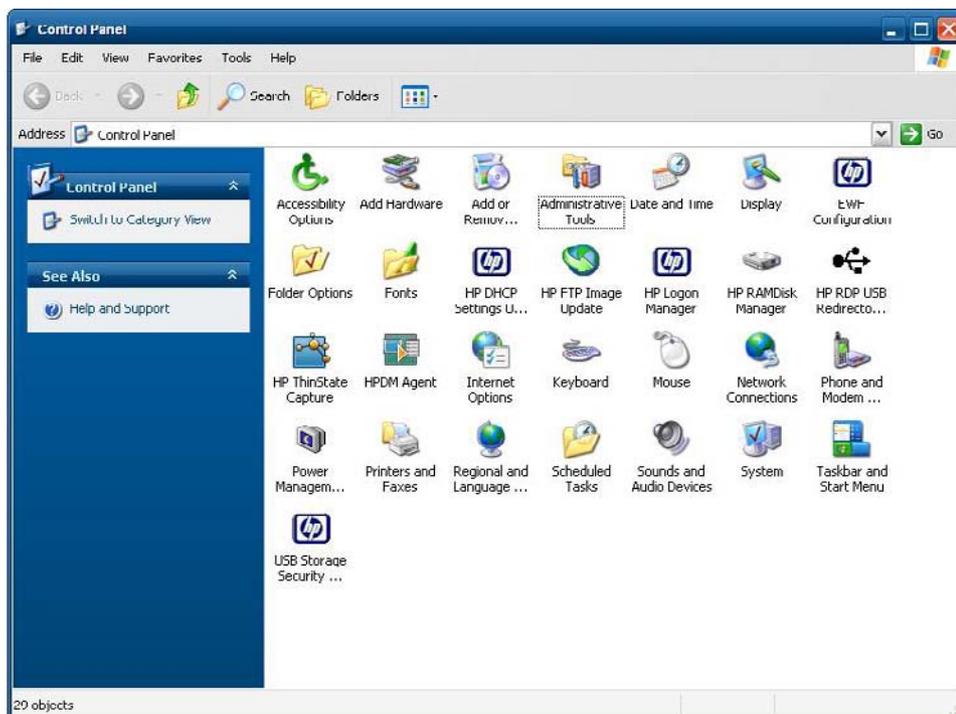
Die Version 11 von Windows Media Player umfasst Verbesserungen in den Bereichen Sicherheit, Leistung und Funktionalität. Weitere Informationen zu den Verbesserungen von Windows Media Player finden Sie auf der Windows Media Player-Homepage unter <http://www.microsoft.com/windows/windowsmedia/player/11/default.aspx>.



5 Zusätzliche Optionen in der Systemsteuerung

Sie können die Systemsteuerung über **Start > Systemsteuerung** aufrufen.

In den folgenden Abschnitten werden einige der zusätzlichen Optionen in der Systemsteuerung beschrieben.



Enhanced Write Filter Manager

WES und XPe umfassen die EWF-Konsolenanwendung (Enhanced Write Filter), Ewfmgr.exe, ein Tool, das über die Befehlszeile aufgerufen wird. Neben dem DOS-Befehlszeilentool beinhalten die WES- und XPe-Images eine Enhanced Write Filter GUI. Der EWF ermöglicht dem Betriebssystem (OS), von einem Datenträgervolume aus zu booten, das sich auf einem schreibgeschützten Medium oder einer schreibgeschützten Festplatte befindet, wobei Schreib-/Lesezugriff für das Betriebssystem angezeigt wird. Vom EWF werden alle Schreibvorgänge zu einer anderen Speicherposition, sog. Overlays, gespeichert. Am Overlay vorgenommene Änderungen werden nicht an den Flash-Speicher übertragen, sofern der EWF nicht deaktiviert wurde oder die Änderungen nicht ausdrücklich vom Benutzer übertragen werden.

Die EWF-Managerkonsolenanwendung kann verwendet werden, um eine Gruppe von Befehlen an den EWF-Treiber auszugeben sowie den Status der einzelnen geschützten Volume-Overlays und das Format der EWF-Konfigurationen insgesamt zu berichten.

Wenn Sie die EWF-Managerkonsolenanwendung in die Konfiguration aufnehmen und in das Echtzeit-Image integrieren, können Sie „Ewfmgr.exe“ und die entsprechenden Befehle nutzen.

Vorteile des Enhanced Write Filters

Der EWF stellt eine sichere Umgebung für das Thin Client-Computing zur Verfügung. Dazu wird der Thin Client vor unerwünschten Flash-Speicher-Schreibvorgängen geschützt. (Der Flash-Speicher ist der Bereich, in dem sich die Komponenten des Betriebssystems und der Funktionssoftware befinden.) Der Schreibfilter verlängert auch die Lebensdauer des Thin Client, da umfangreiche Schreibaktivitäten im Flash-Speicher verhindert werden. Durch einen Cache, der alle Flash-Schreibvorgänge abfängt und einen erfolgreichen Zugriff an den Prozess zurückmeldet, von dem die E/A-Operation angefordert wurde, wird ein Lese-/Schreibzugriff emuliert.

Die im Cache gespeicherten, abgefangenen Flash-Schreibvorgänge bleiben verfügbar, solange der Thin Client aktiv ist. Sie gehen jedoch verloren, wenn der Thin Client neu gestartet oder heruntergefahren wird. Damit die Ergebnisse von Schreibvorgängen für Registrierung, Favoriten, Cookies usw. erhalten bleiben, können die betreffenden Inhalte des Caches bei Bedarf mit der Altiris Deployment Solution-Software oder manuell mit dem Enhanced Write Filter Manager in den Flash-Speicher übertragen werden.

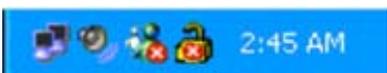
Nach dem Deaktivieren des Schreibfilters werden alle weiteren Schreibvorgänge während der aktuellen Bootsitzung bis zum nächsten Neustart ohne weitere Zwischenspeicherung in den Flash-Speicher geschrieben. Der Schreibfilter kann auch über die Befehlszeile aktiviert/deaktiviert werden. Aktivieren Sie den Schreibfilter stets, nachdem alle permanenten Änderungen erfolgreich vorgenommen wurden.

Beim EWF handelt es sich um ein leistungsstarkes Tool für alle Thin Client-Umgebungen, in denen mehrere Benutzer Zugriff auf das Gerät haben. Der EWF hindert Unbefugte daran, das Image zu ändern oder zu beschädigen.

Enhanced Write Filter-Statusdienst

Von diesem Dienst wird ein Symbol in der Taskleiste erstellt, das den Status des EWF anzeigt. Das EWF-Statussymbol erscheint als rotes 'Schloss', wenn der Filter deaktiviert ist, als grünes 'Schloss', wenn er aktiviert ist, und als gelbes 'Schloss', wenn festgelegt wurde, dass der Status beim nächsten Booten geändert werden soll.



Status	Beschreibung	Beispiel
Rot	Deaktiviert	
Grün	Aktiviert	
Gelb	Übertragungsmodus	
Gelb mit rotem 'X'	Schreibfilter beschädigt	

 **HINWEIS:** Bei einem beschädigten EWF muss der Thin Client mit dem Standardimage, das im Web zur Verfügung steht, neu geflasht werden.

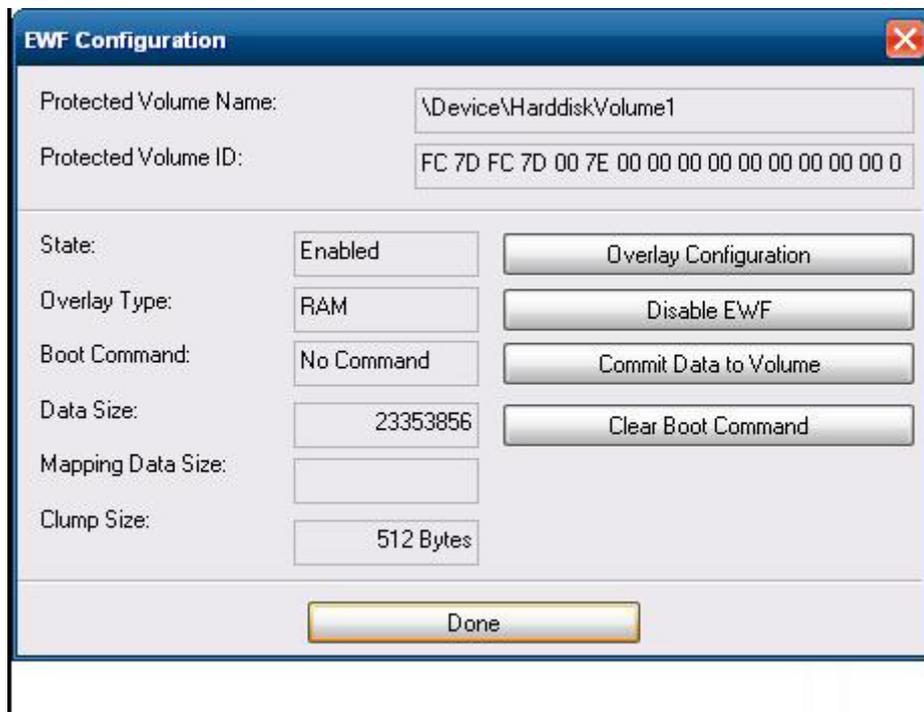
Wenn Sie als Administrator angemeldet sind, können Sie den Status des EWF ändern. Klicken Sie dazu mit der rechten Maustaste auf das Symbol, und wählen Sie den gewünschten EWF-Status aus.

 **HINWEIS:** Da das EWF Manager-Konsolendienstprogramm (ewfmgr.exe) und der EWF-Statusdienst getrennten Code ausführen, werden Statusänderungen durch „ewfmgr.exe“ nicht automatisch über das EWF-Statussymbol angezeigt.

Sie müssen mit der rechten Maustaste auf das Symbol klicken, um das Statussymbol nach Ändern des EWF mithilfe von ewfmgr.exe zu aktualisieren. (Danach können Sie auf eine beliebige Stelle der Anzeige klicken, um das Kontextmenü zu schließen.) Alle Operationen, die Sie über das Menü des EWF-Statussymbol ausführen, sind jedoch über die EWF-Manager-Konsolenanwendung sichtbar. Status und Änderungen am Enhanced Write Filter werden zwischen dem EWF-Statussymbol und der EWF-Manager-Applet in der Systemsteuerung synchronisiert.

Enhanced Write Filter GUI

Sie können über die Systemsteuerung oder die Option „Verwaltung“ auf die EWF-GUI zugreifen.



Gehen Sie wie folgt vor, um auf die EWF-GUI zuzugreifen:

1. Melden Sie sich als Administrator an.
2. Wählen Sie **Start > Systemsteuerung > Weitere Systemsteuerungsoptionen** oder **Start > Systemsteuerung > Verwaltung** aus.
3. Klicken Sie auf das Symbol **EWF Manager**.
4. In der EWF-GUI können Sie die Optionen für den Schreibfilter auswählen.

EWF-GUI – Schaltflächen

Die aktuelle Version der EWF-GUI umfasst die folgenden Schaltflächen:

Schaltfläche	Beschreibung
Enable EWF	Diese Schaltfläche entspricht funktional dem Befehl ewfmgr.exe c: -Enable in der DOS-Eingabeaufforderung.
Disable EWF	Diese Schaltfläche entspricht funktional dem Befehl ewfmgr.exe c: -Disable in der DOS-Eingabeaufforderung.
Overlay Configuration	Über diese Schaltfläche können Sie die Overlayinformationen anzeigen. Diese Informationen sind eine Kombination der Informationen, die über die Befehle ewfmgr.exe c: -Description und ewfmgr.exe c: -Gauge in der DOS-Eingabeaufforderung angezeigt werden.
Clear Boot Command	Diese Schaltfläche entspricht funktional dem Befehl ewfmgr.exe c: -NoCmd in der DOS-Eingabeaufforderung.
Commit Data to Volume	Diese Schaltfläche entspricht funktional dem Befehl ewfmgr.exe c: -Commit in der DOS-Eingabeaufforderung.

 **HINWEIS:** Mit dem Bootbefehl „Commit“ werden alle temporären Inhalte permanent in den Flash-Speicher geschrieben. Außerdem werden alle Inhalte, auf die nach Ausführen des Befehls „Commit“ aber vor einem Neustart des Systems zugegriffen wurde (und an denen Änderungen vorgenommen wurden) ebenfalls in den Flash-Speicher geschrieben. Dazu zählen auch Änderungen, die während einer beliebigen Anzahl an Anmelde-/Abmeldesitzungen vor dem nächsten Neustart vorgenommen wurden.

Befehle zum Starten des Tools über die DOS-Befehlszeile

In der folgenden Tabelle sind die unterstützten EWF-Boot-Befehle aufgelistet.

Bootbefehle	Beschreibung
All	Zeigt Informationen zu allen geschützten Volumes an und führt einen Befehl wie disable , enable und commit für die einzelnen Volumes aus (sofern angegeben).
Commit	Überträgt alle Daten der aktuellen Ebene im Overlay auf das geschützte Volume und setzt die aktuelle Overlayebene nach dem Herunterfahren auf 1 zurück.
Disable	Ermöglicht dem Benutzer, nach dem nächsten Neustart in das Image zu schreiben.
Enable	Hindert den Benutzer daran, nach dem nächsten Neustart in das Image zu schreiben.
Commitanddisable	Kombination der Befehle Commit und Disable . Über diesen Befehl werden Daten im Overlay nach dem Herunterfahren übertragen. Darüber hinaus wird der EWF nach jedem Systemneustart deaktiviert.

 **HINWEIS:** Mit dem Bootbefehl „Commit“ werden alle temporären Inhalte permanent in den Flash-Speicher geschrieben. Außerdem werden alle Inhalte, auf die nach Ausführen des Befehls „Commit“ aber vor einem Neustart des Systems zugegriffen wurde (und an denen Änderungen vorgenommen wurden) ebenfalls in den Flash-Speicher geschrieben. Dazu zählen auch Änderungen, die während einer beliebigen Anzahl an Anmelde-/Abmeldesitzungen vor dem nächsten Neustart vorgenommen wurden.

Verwenden der Bootbefehle

Geben Sie Befehle mit der folgenden Syntax in die Befehlszeile ein, um die Bootbefehle von EWF-Manager zu verwenden:

```
EWFMGR <Laufwerksbuchstabe> - [Bootbefehl]
```

 **HINWEIS:** Da die Befehle von EWF-Manager beim nächsten Neustart ausgeführt werden, muss das System neu gestartet werden, damit der Befehl wirksam wird.

HP RAMDisk

Der RAMDisk-Speicher ist ein flüchtiger Speicherbereich für die temporäre Speicherung von Daten. Er wird im Fenster "Arbeitsplatz" als Laufwerk Z angezeigt.



Im RAMDisk-Speicher werden die folgenden Objekte gespeichert:

- der Cache für Webseiten des Browsers
- der Browserverlauf
- Browsercookies
- Browsercache
- Temporäre Internetdateien
- Druckaufträge in der Warteschlange
- temporäre Benutzer-/Systemdateien

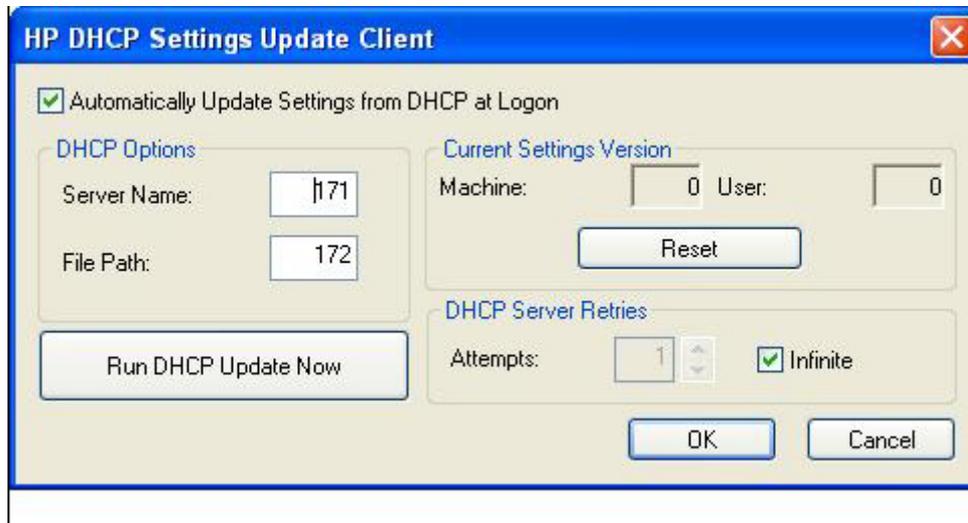
Im RAMDisk-Speicher können auch andere Daten temporär gespeichert werden (z. B. servergespeicherte Profile). Dies hängt von den Vorgaben des Administrators ab (siehe [„Lokale Laufwerke“ auf Seite 10](#)).

Im Dialogfenster "RAMDisk Configuration" können Sie die RAMDisk-Größe konfigurieren. Wenn die RAMDisk-Größe geändert wird, muss der Thin Client neu gestartet werden, damit die Änderungen wirksam werden. Um die Änderungen permanent zu speichern, müssen Sie vor dem Neustart den Schreibfiltercache in der aktuellen Bootsitzung deaktivieren oder den Befehl -commit ausführen.

 **HINWEIS:** Standardmäßig ist die RAMDisk-Größe auf die optimale Größe von 16 MB eingestellt. Die maximale RAMDisk-Größe beträgt 64 MB. Die minimale Größe ist 2 MB.

HP DHCP Settings Update Client

Beim HP DHCP Settings Update Client handelt es sich um ein Dienstprogramm in der Systemsteuerung, mit dem ein IT-Administrator Einstellungen für das HP XP WES- oder XPe-Betriebssystem festlegen kann.



Die Einstellungen werden über eine INI-Datei festgelegt, die eine Teilmenge der Datei "sysprep.inf" von Microsoft sowie mehrere XPe/HP-spezifische Schlüssel verwendet. Es besteht die Möglichkeit, XPePrep durch Angabe einer INI-Datei, die lokal verarbeitet wird, oder in Verbindung mit DHCP- und FTP-Servern auszuführen, wenn die Einstellungen automatisch auf mehreren Clients im Netzwerk vorgenommen werden sollen.

Ausführliche Informationen finden Sie im Dokument *Using the HP DHCP Settings Update Client* auf der HP-Supportseite unter <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01444724/c01444724.pdf>.

HP ThinState Capture

Das Tool HP ThinState Capture ist ein sehr einfaches, assistentenbasiertes Tool, mit dem Sie ein WES- oder XPe-Image von HP Thin Clients erfassen können, das anschließend auf einem anderen HP Thin Client des gleichen Modells mit identischer Hardware implementiert werden kann.

Voraussetzungen

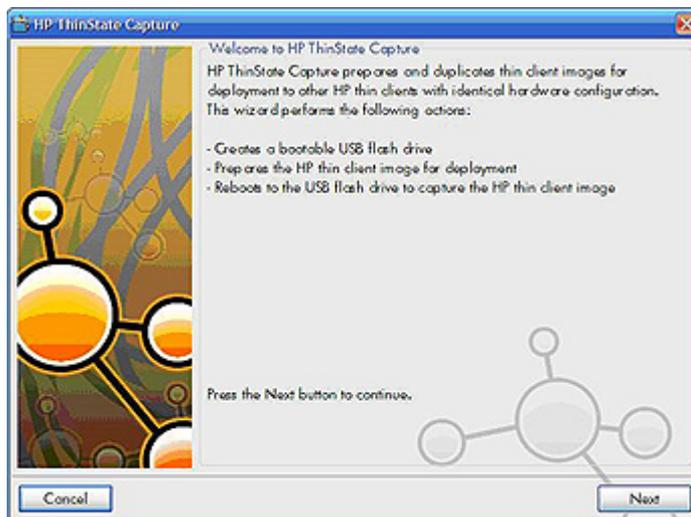
- Einen HP WES- oder XPe-basierten Thin Client, der über das neueste von HP bereitgestellte Image verfügt.
- Ein von HP zugelassenes USB-Flash-Laufwerk (USB-Stick). Informationen zu den aktuellen unterstützten USB-Flash-Laufwerken finden Sie in der Übersicht über die technischen Daten des Thin Clients t5630.

⚠ VORSICHT! Als erstes Startgerät im System-BIOS (F10) ist standardmäßig USB, dann ATA-Flash und schließlich das Netzwerk eingestellt. Wenn die Standardeinstellungen für die Startreihenfolge geändert wurden, müssen Sie vor der Verwendung des Tools HP ThinState Capture das erste Startlaufwerk im Abschnitt "Advanced BIOS Features" des System-BIOS (Aufruf über die Taste F10) auf "USB" einstellen.

📝 HINWEIS: Das Tool HP ThinState Capture ist kein eigenständiges Tool und kann im Thin Client-Image nur vom Administrator aufgerufen werden.

Speichern Sie alle Daten auf dem USB-Flash-Laufwerk, bevor Sie die folgenden Schritte ausführen.

1. Rufen Sie das Tool HP ThinState Capture in der Systemsteuerung auf. Daraufhin wird das folgende Fenster angezeigt.



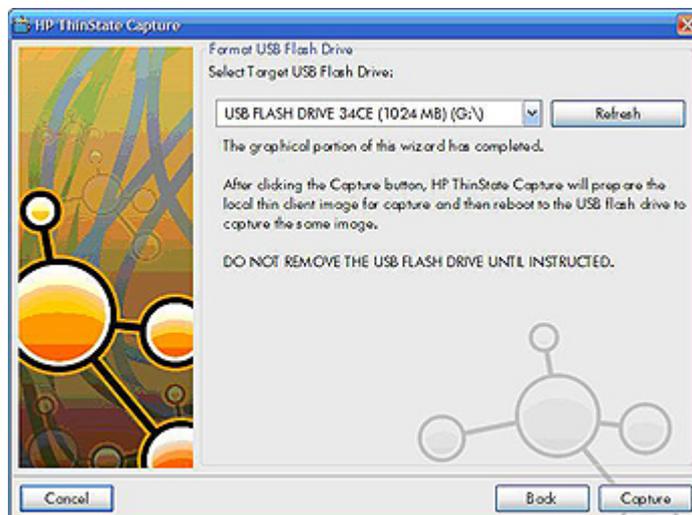
2. Klicken Sie auf **Next**.



Stecken Sie jetzt einen USB-Stick in das Gerät. Daraufhin werden der Buchstabe des USB-Laufwerks und dessen Größe angezeigt.

Der Speicher des USB-Sticks muss größer sein als der Flash-Datenträger des Geräts. Wenn der Thin Client über einen Flash-Speicher von 512 MB verfügt, muss das USB-Flash-Laufwerk daher mindestens 1 GB groß sein.

Nachdem ein USB-Stick der geeigneten Größe eingesteckt wurde, wird das folgende Fenster angezeigt.



3. Klicken Sie auf **Capture**. Daraufhin wird die folgende Warnung angezeigt.



4. Klicken Sie auf **Yes**. Das Tool HP ThinState Capture formatiert das USB-Flash-Laufwerk und aktiviert das Laufwerk als startfähigen Datenträger. Daraufhin wird das System neu gestartet.
5. Danach wird das folgende Fenster angezeigt. Befolgen Sie die angezeigten Anweisungen.



Sie können jetzt das USB-Flash-Laufwerk verwenden, um das erfasste Image auf einem anderen HP Thin Client desselben Modells mit identischer Hardware zu implementieren, das einen Flash-Speicher mit mindestens derselben Größe aufweist.

Die folgende Tabelle enthält eine Auflistung der unterstützten Erfassungs- und Implementierungsszenarien:

	Implementierung auf:		
	2 GB Flash-Speicher	1 GB Flash-Speicher	512 MB Flash-Speicher
Erfassung von:			
2 GB Flash-Speicher	X		
1 GB Flash-Speicher	X	X	
512 MB Flash-Speicher	X	X	X

HP ThinState Deploy

So führen Sie eine HP ThinState-Implementierung aus:

1. Legen Sie im System-BIOS (F10) als Startdatenträger **USB** fest.
2. Schließen Sie das USB-Flash-Laufwerk an das Thin Client-Gerät an, auf dem Sie das erfasste Image implementieren möchten, und schalten Sie das Gerät ein.
3. Befolgen Sie die angezeigten Anweisungen.

```
HP ThinState Deploy, Version x.xxx.xxx
Copyright <> 2006 Hewlett-Packard Development Company, L.P.

This utility will FORMAT your onboard thin client Flash disk and ERASE
ALL DATA currently on the disk. It will then RESTORE the operating
system software, device drivers, and other HP-provided software from
the USB Flash Disk.

Do you want to continue [Y/N]?

Are you sure that you want to run this utility [Y/N]?

Please do not power off your system during this process.

Validating the image...
Extracting the image...
Completed successfully! (xxx seconds)

Please remove the USB Flash Disk and power-cycle your system now.
```

Entfernen Sie das USB-Flash-Laufwerk, und schalten Sie das Gerät aus und wieder ein. Daraufhin wird das Image entbündelt. Dieser Vorgang kann 10-12 Minuten dauern. Schalten Sie das Gerät innerhalb dieses Zeitraums nicht aus.

Sie können das erfasste Image ("flash.ibr") auf dem USB-Flash-Laufwerk zusammen mit Altiris Deployment Solution oder dem HP Gerätemanager verwenden, um ein Image remote auf mehreren Thin Client-Geräten zu implementieren.

 **HINWEIS:** Sie müssen "flash.ibr" mit dem Dienstprogramm HP ThinState Deploy (z. B. "ibr.exe") verwenden. Das Image "flash.ibr" ist nicht mit den Altiris-Dienstprogrammen "rdeploy.exe" bzw. "rdeployt.exe" kompatibel. Weitere Informationen finden Sie im Whitepaper *HP Compaq Thin Client Imaging Tool* unter <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf>.

Weitere Informationen zu Altiris finden Sie unter <http://www.altiris.com/>.

HP FTP Image Update

Mit dem Dienstprogramm HP FTP Image Update Client können Sie ein Image von einem freigegebenen FTP-Verzeichnis auf einem HP Thin Client-System mit dem WES- oder XPe-Betriebssystem aktualisieren.

Serveranforderungen

DHCP-Server

Die Option 137 muss einen Zeichenfolgewert enthalten, der das freigegebene FTP-Verzeichnis angibt, in dem die WES- oder XPe-Images und das WinPE-Image gespeichert sind.

Wenn die XPe-Images und das WinPE-Image beispielsweise in "ftp://ftpserver/ftpordner" gespeichert sind, muss die DHCP-Option 137 die folgende Zeichenfolge enthalten:

- `ftp://benutzername:kennwort@ftpserver/ftpordner`
(wenn die FTP-Freigabe geschützt ist)
– oder –
- `ftp://ftpserver/ftpfolder`
(wenn ein anonymer Zugriff auf die FTP-Freigabe zulässig ist)

FTP-Server

Die WES- und XPe-Images (im .IBR-Format) und das von HP bereitgestellte WinPE-Image müssen sich im selben Ordner des FTP-Servers befinden.

Beschreibung

Der HP FTP Image Update Client kann nur von einem Administrator auf einem HP Thin Client-System ausgeführt werden, das für das WES- oder XPe-Betriebssystem lizenziert ist.

 **HINWEIS:** FTP Image Update ist nur auf den Thin Clients t5630, t5630w, t5730, t5730w, gt7720 und vc4820T mit dem aktuellen HP XPe-Image vorhanden (5.1.606 oder höher). Damit FTP Image Update einwandfrei funktioniert, muss auf dem Client mindestens der folgende Speicherplatz verfügbar sein: ca. 200 MB Flash-Speicher und ca. 250 MB RAM-Speicher. FTP Image Update über Funkverbindungen wird nicht unterstützt. Von HP wird mindestens 1 GB Flash-Speicher und 1 GB RAM-Speicher empfohlen, um die Flexibilität zu erhöhen und diese Funktion sowie alle anderen im aktuellen Image enthaltenen Funktionen optimal nutzen zu können.

Hosteinstellungen

Es gibt zwei Möglichkeiten, die Hosteinstellungen anzugeben:

1. Sie können die Einstellungen manuell eingeben, wenn Sie das Kontrollkästchen **Get Host Settings from DHCP server** deaktivieren und die entsprechenden Informationen in die Felder **Host ID**, **Path**, **User ID** und **Password** eingeben.

Wenn die FTP-Freigabe anonymen Lesezugriff gestattet, können Sie die Felder **User ID** und **Password** leer lassen.

Wenn die WES- oder XPe-Images und das WinPE-Image im Standardordner (Stammordner) des FTP-Servers gespeichert sind, können Sie das Feld **Path** leer lassen oder / in das Feld eingeben.

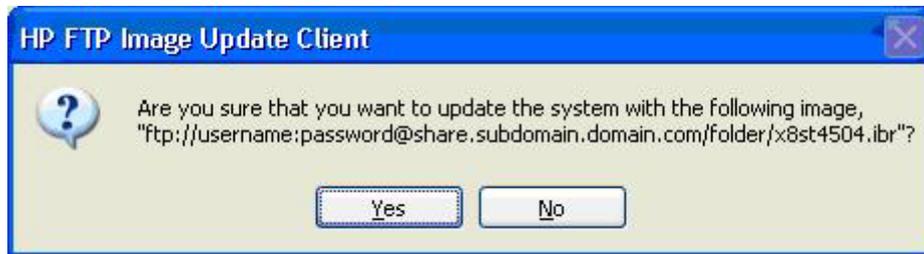
2. Die Einstellungen können automatisch über eine DHCP-Option abgerufen werden, wenn Sie das Kontrollkästchen **Get Host Settings from DHCP server** aktivieren.

Klicken Sie auf die Schaltfläche **Save Settings**, um die Hosteinstellungen zu speichern und festzuschreiben. Wenn das Applet erneut aufgerufen wird, werden die Einstellungen abgerufen und automatisch in die entsprechenden Steuerelemente eingetragen.

Auswahl des zu aktualisierenden Image

Klicken Sie auf die Schaltfläche **Refresh Image List**, nachdem die Hosteinstellungen eingegeben wurden (manuell oder automatisch über DHCP), damit das Applet die FTP-Freigabe nach allen XPe-Images abfragt, dessen BIOS-Zielfamilien mit der des aktuellen Thin Client-Systems übereinstimmen, und das Dropdown-Listefeld links neben der Schaltfläche entsprechend ausgefüllt wird. Sie können jedes Image in der Liste auswählen, um das Image des Systems zu aktualisieren bzw. ein Image zu erstellen.

Klicken Sie danach auf die Schaltfläche **Run Image Update Now**, um die Imageaktualisierung mit dem ausgewählten Image durchzuführen. Daraufhin wird ein ähnliches Bestätigungsdialogfenster wie in der folgenden Abbildung angezeigt.



Klicken Sie auf **No**, um den Vorgang abubrechen. Wenn Sie auf **Yes** klicken, wird vom HP FTP Image Update Client überprüft, ob auf dem Flash-Laufwerk mindestens 200 MB freier Speicherplatz für das WinPE-Image vorhanden sind. Andernfalls wird die folgende Fehlermeldung angezeigt.



Wenn der Flash-Datenträger genügend freien Speicherplatz aufweist, werden das WinPE-Image heruntergeladen, das Bootladeprogramm so geändert, dass beim nächsten Neustart des Systems WinPE geladen wird, und anschließend das System neu gestartet (WinPE-Phase).



Nachdem WinPE geladen wurde, wird IBRPE aufgerufen, um ein Image des Flash-Laufwerks mit dem Image zu erstellen, das von der FTP-Freigabe ausgewählt wurde. Nachdem das Image erstellt wurde, wird das System von IBRPE automatisch neu gestartet (FBA-Phase).

```
C:\Windows\System32\cmd.exe - \IBRPE\THINSTATE.CMD
HP Thin Client Imaging Tool, Version 6.00.2008.0519
Copyright (c) 2008 Hewlett-Packard Development Company, L.P.

This utility will FORMAT your flash disk and ERASE ALL DATA currently on the
disk. It will then RESTORE the original operating system software, device
drivers, and other HP-provided software that came with the computer.

Please do not power off your system during this process.

3% completed.
```

6 Verwaltung und Imageaktualisierungen

In diesem Abschnitt werden die Remoteverwaltungsmöglichkeiten und Firmwareaktualisierungsmethoden für den Thin Client beschrieben und erläutert.

Altiris Deployment Solution-Software

Die Altiris Deployment Solution-Software ist ein umfassendes Toolset für die Remoteverwaltung. Der Zugriff auf den Thin Client erfolgt über die Remoteagent- und PXE-Serverdienstprogramme von Altiris, die auf dem Thin Client installiert sind. Mithilfe der Altiris-Lösung können Sie die Thin Client-Verwaltungsfunktionen (einschließlich Firmwareaktualisierungen) ausführen, ohne dass ein Administrator die einzelnen Thin Client-Standorte aufsuchen muss.

Weitere Informationen zu Altiris finden Sie unter <http://www.altiris.com>.

HP Gerätemanager

Der HP Gerätemanager ist eine serverbasierte Anwendung, die zentrale Verwaltungsfunktionen für HP Thin Client-Geräte bereitstellt. Der Zugriff auf den Thin Client erfolgt über den HP Management Agent, der im WES- oder XPe-Standardimage des Thin Clients enthalten ist, damit der Gerätemanager ohne großen Aufwand Geräte verwalten kann (Agenten älterer Geräte müssen jedoch u. U. aktualisiert werden).

Weitere Informationen zum HP Gerätemanager und zum HP Management Agent sowie andere wichtige Aktualisierungen oder Dokumente finden Sie auf der entsprechenden Website des HP Supports: <http://www.hp.com/support>. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen** oder **Treiber und Software zum Herunterladen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die **Eingabetaste**.

Add-on-Erweiterungen

Wenn Sie ein Add-on-Modul installieren möchten, können Sie den Thin Client mit Altiris Deployment Solution oder dem HP Gerätemanager verwalten. Deaktivieren/aktivieren Sie ggf. den Schreibfilter, damit die Änderungen gespeichert werden.

△ **ACHTUNG:** Wenn der verfügbare Speicherplatz im Flash-Speicher auf unter 10 MB und/oder der verfügbare Systemspeicher auf unter 15 MB verkleinert wird, wird der Thin Client instabil.

📄 **HINWEIS:** Damit die Add-on-Module funktionieren und heruntergeladen werden können, muss genügend Flash-Speicher verfügbar sein. In einigen Fällen kann es notwendig sein, Softwarekomponenten zu entfernen, um Speicherplatz für Add-on-Module zu schaffen.

Imageaktualisierungen

Das Protokoll PXE (Preboot Execution Environment) von Intel definiert die Interaktion von TCP/IP, DHCP und TFTP, damit von einem Server eine Pre-Boot-Umgebung auf einen Client heruntergeladen werden kann. PXE ermöglicht den Start eines Clients von einem Server in einem Netzwerk, bevor das eingebettete Betriebssystem bzw. das Betriebssystem vom lokalen Flash-Modul gestartet wird. Mithilfe von PXE kann ein Netzwerkadministrator einen Thin Client remote aktivieren und verschiedene Verwaltungsaufgaben ausführen, z. B. das Betriebssystem und andere Software über das Netzwerk von einem Server auf dem Client laden. Der PXE-Client ist im Thin Client installiert. Die PXE-Serverkomponente ist Bestandteil der Altiris Deployment Solution-Suite.

 **HINWEIS:** Die automatische Aktualisierung von Citrix ICA funktioniert nicht mit dem ICA-Client, der im Thin Client installiert ist. Die Aktualisierungen werden über den Standardprozess für Firmwareaktualisierungen implementiert.

HP FTP Image Update

Mit dem Dienstprogramm HP FTP Image Update Client in der Systemsteuerung können Sie ein Image von einem freigegebenen FTP-Verzeichnis auf einem HP Thin Client-System mit dem WES- oder XPe-Betriebssystem aktualisieren. Weitere Informationen finden Sie unter „[HP FTP Image Update](#)“ auf Seite 46.

HP ThinState Capture und Deploy

Das Tool HP ThinState Capture ist ein sehr einfaches, assistentenbasiertes Tool, mit dem Sie ein WES- oder XPe-Image von HP Thin Clients erfassen können, das anschließend auf einem anderen HP Thin Client des gleichen Modells mit identischer Hardware implementiert werden kann. Weitere Informationen zum Tool HP ThinState Capture finden Sie unter „[HP ThinState Capture](#)“ auf Seite 42.

HP Compaq Thin Client Imaging Tool

Das HP Compaq Thin Client Imaging Tool ist Bestandteil des SoftPaq-Pakets, das das werkseitige Originalimage für den HP Thin Client enthält. Mit diesem Dienstprogramm können Sie das werkseitige Originalimage des Thin Clients wiederherstellen.

Mit diesem Dienstprogramm können Sie die folgenden Funktionen ausführen:

- Erstellen eines startfähigen Flash-Images auf einem USB-Flash-Laufwerk (USB-Stick).
- Entbündeln des Images in ein Verzeichnis, das in einem kundenspezifischen Implementierungsszenario oder einem PXE-Image genutzt werden kann.

Weitere Informationen zu diesem Dienstprogramm und dessen Einsatzmöglichkeiten finden Sie auf der HP Website unter <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00485307/c00485307.pdf>.

HP Client Automation

HP Client Automation ist eine unternehmensweite Lösung zur Clientverwaltung für physische und virtuelle Clients. Neben der vollständigen Verwaltung herkömmlicher Desktop- und Notebook-PCs kann HPCA auch zum Verwalten von Thin Client-Geräten und den virtuellen Back-End-Infrastrukturen verwendet werden, zu denen Verbindungen hergestellt werden. Das Programm führt zu einer

erheblichen Reduzierung der Herausforderungen und Schwierigkeiten in Zusammenhang mit der Verwaltung von Thin Client-Geräten und Client-Virtualisierungstechnologien. Dazu werden Automatisierungstools bereitgestellt, die zum Erstellen und Implementieren von Betriebssystem-Images und Software-Updates sowie zum Erfassen des Hardware-Inventars dienen. Da dieselbe Verwaltungskonsole und dieselben Verwaltungstools für alle Clientgeräte verwendet werden, hilft HPCA den Kunden, die Kosten zu senken und den Betrieb zu vereinfachen.

Weitere Informationen zu HP Client Automation finden Sie unter <http://www.hp.com/go/easydeploy>.

7 Peripheriegeräte

Abhängig von den verfügbaren Anschlüssen kann der Thin Client Dienste für USB- und PCI-Geräte sowie für serielle und parallele Geräte bereitstellen, sofern die entsprechende Software installiert ist. Im folgenden Abschnitt wird die werkseitig installierte Software beschrieben. Sobald entsprechende Add-ons für andere Dienste verfügbar werden, können Sie diese Dienste mit der Altiris Deployment Solution-Software oder dem HP Gerätemanager installieren. Weitere Informationen finden Sie unter „[Altiris Client Agent](#)“ auf Seite 29 und „[HP Management Agent](#)“ auf Seite 32.

Weitere Informationen zu den anschließbaren Peripheriegeräten finden Sie in der Übersicht über die technischen Daten des jeweiligen Modells unter <http://h10010.www1.hp.com/wwpc/us/en/sm/WF04a/12454-321959-89307-338927-89307.html>.

Wählen Sie das Modell aus, und klicken Sie dann auf **Specifications** und anschließend auf den Link **QuickSpec**.

Drucker

Im Thin Client ist ein generischer, universeller Druckertreiber installiert, der den unformatierten Ausdruck von Texten auf einem lokal angeschlossenen Drucker unterstützt. Um formatierte Texte und Grafiken auf einem lokal angeschlossenen Drucker drucken zu können, müssen Sie den vom Hersteller bereitgestellten Treiber installieren und die Anweisungen des Herstellers befolgen. Sie müssen dabei den Schreibfiltercache deaktivieren oder den Befehl "-commit" ausführen, um die Installation zu speichern. In ICA- und RDP-Anwendungen besteht außerdem die Möglichkeit, über die Druckertreiber auf den Servern Netzwerkdrucker zu verwenden.

Ausführliche Informationen finden Sie im Whitepaper *Printing and Imaging Support on HP Compaq Thin Clients* auf der HP-Supportseite unter <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00739537/c00739537.pdf>.

△ **ACHTUNG:** Wenn der verfügbare Speicherplatz im Flash-Speicher auf unter 10 MB und/oder der verfügbare Systemspeicher auf unter 15 MB verkleinert wird, wird der Thin Client instabil.

📄 **HINWEIS:** Um Druckertreiber herunterladen und verwenden zu können, muss genügend Flash-Speicherplatz vorhanden sein. In einigen Fällen kann es notwendig sein, Softwarekomponenten zu entfernen, um Speicherplatz für Druckertreiber zu schaffen.

Wenn Sie in einer ICA- oder RDP-Sitzung mit den Druckertreibern des Servers auf einem lokal angeschlossenen Drucker drucken, können Sie ebenfalls formatierte Texte und Grafiken ausdrucken. Dazu müssen der Druckertreiber auf dem Server und der Treiber für den unformatierten Ausdruck von Texten auf dem Thin Client installiert werden (siehe nächster Abschnitt).

Hinzufügen von Druckern, die den generischen Druckertreiber für den unformatierten Ausdruck von Texten verwenden

Führen Sie die folgenden Schritte aus, um einen Drucker hinzuzufügen, der den Druckertreiber für den unformatierten Ausdruck von Texten verwendet:

1. Schließen Sie den Drucker an den entsprechenden Anschluss an.
2. Wählen Sie **Start > Einstellungen > Drucker und Faxgeräte** aus.
3. Wählen Sie **Drucker hinzufügen** aus, um den **Druckerinstallations-Assistenten** zu öffnen.
4. Klicken Sie im ersten Fenster des Assistenten auf **Weiter**.
5. Wählen Sie **Lokaler Drucker, der an den Computer angeschlossen ist** aus.
6. Stellen Sie sicher, dass das Kontrollkästchen **Plug & Play-Drucker automatisch ermitteln und installieren** nicht markiert ist.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie **Folgenden Anschluss verwenden** aus.
9. Wählen Sie entsprechenden Anschluss in der Liste aus, und klicken Sie auf **Weiter**.
10. Wählen Sie den Hersteller und das Druckermodell aus, und klicken Sie auf **Weiter**.
11. Verwenden Sie den zugewiesenen Standardnamen oder einen anderen Namen für den Drucker, und klicken Sie dann auf **Weiter**.
12. Wählen Sie **Drucker nicht freigeben** aus, und klicken Sie auf **Weiter**.
13. Wählen Sie aus, ob eine Testseite gedruckt werden soll, und klicken Sie dann auf **Weiter**.
14. Klicken Sie auf **Fertig stellen**.

Verwenden von herstellerspezifischen Druckertreibern

Installieren Sie den vom Hersteller bereitgestellten Treiber und folgen Sie den Anweisungen des Herstellers. Sie müssen dabei den Schreibfiltercache deaktivieren oder den Befehl "-commit" ausführen, um die Installation zu speichern.

Add-on "HP Universal Print Driver for Thin Clients"

Von HP wurde ein Druck-Add-on für WES- und XPe-basierte Thin Clients entwickelt. Bei diesem Add-on handelt es sich um eine speziell für die Thin Client-Softwareumgebung überarbeitete Version des HP Universal Print Driver. Wegen des begrenzten Speicherplatzes ist die aktuelle Version beispielsweise nur in Englisch und ohne Hilfedateien verfügbar. Rufen Sie die Website <http://www.hp.com/support> auf. Wählen Sie Ihr Land auf der Karte aus, und wählen Sie dann **Treiber und Software zum Herunterladen** aus. Geben Sie das Thin Client-Modell in das Feld ein, und drücken Sie die **Eingabetaste**. Wählen Sie das Thin Client-Modell und das Betriebssystem aus. Laden Sie anschließend das Add-on herunter.

Ausführliche technische Daten, weitere Downloads sowie die Dokumentation der Originalversion des universellen Druckertreibers finden Sie unter <http://www.hp.com/go/upd>.

Weitere Informationen zum HP Universal Print Driver finden Sie im Whitepaper *Thin Client Printing with the HP Universal Print Driver* unter <http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c01237156/c01237156.pdf>.

Audio

Sie können das Audio von Anwendungen an die Audioanschlüsse des Thin Clients umleiten. Der Pegel wird extern gesteuert (z. B. mit einem 600-Ohm-Potentiometer). Für die Ansteuerung von Lautsprechern ist ein Verstärker erforderlich. Die Lautstärke können Sie über das Audiosymbol im Infobereich der Taskleiste anpassen. Wenn Sie auf dieses Symbol klicken, wird das Kontextmenü für die Lautstärkeregelung geöffnet; wenn Sie auf das Symbol doppelklicken, wird das Anwendungsdialogfenster "Lautstärkeregelung" geöffnet.

Index

- A**
 - Abmeldung 8
 - Add-on-Erweiterungen 50
 - Add-on-Module 50
 - Administrator
 - Anmelden 7
 - Desktop 3
 - Aktualisieren von Images 51
 - Aktualisierungen 50
 - Altiris
 - Client Agent 29
 - Deployment Server 5
 - Deployment Solution 50
 - Altiris Deployment Solution 5
 - Altiris-Website 5, 45
 - Ändern des Kennworts 7
 - Anforderungen
 - Server 4
 - USB-Stick 43
 - Anmelden
 - automatisch 6
 - manuell 7
 - Anmeldung als Administrator 7
 - Anwendungen 16
 - Audio 55
 - Automatische Anmeldung 6
- B**
 - Beheben,
 - Netzwerkanwendungsfehler 22
 - Beheben von
 - Anwendungsproblemen,
 - Microsoft Windows-Firewall 21
 - Benutzer
 - Konten 11
 - Profile 12
 - Benutzerdesktop 3
 - Benutzer-Manager 12
 - Bildschirmschoner 9
- C**
 - Citrix 24
 - Citrix ICA 4
 - Citrix-Website 25
 - Client Agent, Altiris 29
 - Client Automation 32, 51
- D**
 - Deployment Server, Altiris 5
 - Deployment Solution, Altiris 5
 - Desktop 3
 - Desktop, Administrator 3
 - Desktop, Benutzer 3
 - DHCP-Server 46
 - DHCP Settings Update Client 41
 - Dienste, Sitzung 4
 - Dienstprogramme
 - Client Automation 51
 - DHCP Settings Update Client 41
 - Systemzeit 9
 - Thin Client Imaging Tool 51
 - Universeller Druckertreiber 54
 - Drucker 53
 - Drucker, hinzufügen 54
 - Druckertreiber 54
 - Druckertreiber für den unformatierten Ausdruck von Texten 54
- E**
 - Empfänger, RGS 27
 - Emulation
 - TeemTalk Terminal Emulation 29
 - Terminal 5
 - Energieverwaltung 9
 - Enhanced Write Filter 8
 - Enhanced Write Filter Manager 36
 - Erstellen von Benutzerkonten 11
 - Erweiterungen, Add-on 50
 - EWf 8
- F**
 - Fehlerbehebung 22
 - Fehlersymptome, Microsoft Windows-Firewall 21
 - Filter
 - Enhanced Write Filter 8
 - Schreibfilter 10, 36
 - Firewall
 - konfigurieren 18
 - Microsoft Windows-Firewall 18
 - Symantec EndPoint Protection 17
 - Flash-Laufwerk 10
 - Flüchtiger Speicher 10
 - FTP Image Update
 - Hosteinstellungen 47
 - Imageauswahl 48
 - Serveranforderungen 46
 - FTP-Server 46
 - Funktionen, Thin Client 2
- G**
 - Gerätemananger 5, 32, 50
- H**
 - Herstellerspezifische Druckertreiber 54
 - Herunterfahren 8
 - Hinzufügen von Druckern 54
 - Hinzufügen von Ports, Microsoft Windows-Firewall 23
 - Hinzufügen von Programmen, Microsoft Windows-Firewall 22
 - Hosteinstellungen, FTP Image Update 47

HP Client Automation 32, 51
HP Compaq Thin Client Imaging Tool 51
HP DHCP Settings Update Client 41
HP FTP Image Update Hosteeinstellungen 47
Imageauswahl 48
Serveranforderungen 46
HP Gerätemanager 5, 32, 50
HP Management Agent 32
HP RALF 32
HP RAMDisk 39
HP Registration and Agent Loading Facility 32
HP SAM 28
HP SAM-Website 29
HP Session Allocation Manager 28
HP Supportwebsite 16
HP ThinState Capture 42, 51
HP ThinState Deploy 45, 51
HP Universal Print Driver 54

I

ICA 4
Imageaktualisierungen 50, 51
Imageauswahl, FTP Image Update 48
Imageerfassung 42
Imageerstellungstool 51
Imageimplementierung 45
Informationen, Websites 1
Internet 2
Internet Explorer 33
Internet Explorer, Liste unsicherer Dateien 33

K

Kennwort 7
Kennwort, ändern 7
Konfigurieren der Windows-Firewall 18
Konten
Benutzer 11
Erstellen von Benutzerkonten 11

L

Laufwerk C 10

Laufwerke
Laufwerk C und Flash-Laufwerk 10
Laufwerk Z 10
Laufwerk Z 10, 39
Liste unsicherer Dateien für Internet Explorer 33
Logon Configuration Manager 6
Lokale Laufwerke 10

M

Management Agent 32
Manuelle Anmeldung 7
Media Player 33
Microsoft Internet Explorer 33
Microsoft Internet Explorer, Liste unsicherer Dateien 33
Microsoft RDP 5, 27
Microsoft Windows-Firewall
Beheben von Anwendungsproblemen 21
Ermitteln von Konfigurationsinformationen 21
Fehlersymptome 21
Hinzufügen von Ports 23
Hinzufügen von Programmen 22 konfigurieren 18
Multimedia 2

N

Neustart 8

P

Peripheriegeräte 53
Peripheriegeräte, Website mit technischen Daten 53
PN Agent 24
Profile 12
Program Neighborhood 24
PXE 50

R

RALF 32
RAMDisk 39
RDP 5
Regions- und Sprachoptionen 14
Registration and Agent Loading Facility 32
Remote Desktop Protocol 27

Remotedesktopverbindung 25
Remote Graphics Software-Empfänger 27
RGS-Empfänger 27

S

SAM-Website 29
Schreibfilter 10, 36
Server
DHCP 46
FTP 46
Server, Altiris Deployment 5
Serveranforderungen 4
Serveranforderungen, FTP Image Update 46
Servergespeicherte Profile 11
Session Allocation Manager (SAM) 28
Sicherheit
Konfigurieren der Microsoft Windows-Firewall 18
Microsoft 17
Microsoft Windows-Firewall 18
Symantec EndPoint Protection Firewall 17
Sicherheitscenter 18
Sitzungsdienste 4
Speicher, flüchtig 10
Speichern von Dateien 11
Sprachoptionen 14
Standardkennwörter 7
Standardmäßige Aktivierung 18
Symantec EndPoint Protection 17
Systemsteuerung 35
Systemzeit 9

T

TeemTalk Terminal Emulation 29
Terminalemulation 5
Thin Client Imaging Tool 51
ThinState Capture 42, 51
ThinState Deploy 45, 51

U

Uhrzeit, Dienstprogramm 9
Universeller Druckertreiber 54
USB Enhancements 27
USB-Stick, Voraussetzungen 43

V

Verwaltung 15, 50
VMWare View Manager 29
Vorinstallierte Anwendungen 16

W

Website

Altiris 45
Citrix 25
HP SAM 29
HP Support 16
HP Thin Client Imaging Tool,
Whitepaper 45
Peripheriegeräte, Übersicht
über die technischen
Daten 53
Weitere Informationen 1
WES 3
Windows Media Player 33
Windows XPe 3
WES Website 3
Windows-Firewall 18
Windows Media Player 33
Windows Media Player-
Website 33
Windows XPe-Website 3

Z

Z, Laufwerk 39
Zuordnen von Netzlaufwerken 11
Zusätzliche Optionen,
Systemsteuerung 35