Registerkarte "Zugriffsrechte bearbeiten"

Gibt an, wie Internet Explorer alle Inhalte und Berechtigungen behandeln soll, die von signierten und unsignierten Java-Applets angefordert werden.

Die Einstellungen für unsignierte und signierte Berechtigungen wirken sich auf die folgenden Berechtigungen aus:

Zugriff zu allen Dateien

Zugriff zu allen Netzwerkadressen

Ausführen

Dialoge

Systeminformation

Drucken

Geschützter Arbeitsbereich

Benutzerdefinierter Dateizugriff

Nicht signierten Inhalt ausführen

Sie können Berechtigungen einzeln angeben, indem Sie **Nicht signierten Inhalt ausführen** auf **In geschützter Umgebung (Sandbox) ausführen** setzen. Anschließend können Sie jede Berechtigung einzeln auf **Deaktivieren** oder **Aktivieren** zurücksetzen. Wenn Sie **Deaktivieren** oder **Aktivieren** unter **Nicht signierten Inhalt ausführen** angeben, verwenden alle Berechtigungen unter **Zusätzliche nicht signierte Zugriffsrechte** diese Einstellung.

Wählen Sie eine der folgenden Einstellungen für **Nicht signierten Inhalt ausführen** aus:

- Um unsignierte Inhalte nur mit den Berechtigungen auszuführen, die die "Sandbox," erlaubt, klicken Sie auf **In geschützter Umgebung (Sandbox) ausführen**. Hierdurch können Sie jede der Berechtigungen einzeln auf **Deaktivieren** oder **Aktivieren** zurücksetzen.
- Um unsignierte Inhalte automatisch ohne Reaktion auf eine Eingabeaufforderung zurückzuweisen, klicken Sie auf **Deaktivieren**. Alle Berechtigungen unter **Zusätzliche nicht signierte Zugriffsrechte** werden auf **Deaktivieren** gesetzt. Sie können keine Berechtigungen einzeln auf **Aktivieren** zurücksetzen.
- Um unsignierte Inhalte automatisch ohne Reaktion auf eine Eingabeaufforderung zu akzeptieren, klicken Sie auf **Aktivieren**. Alle Berechtigungen unter **Zusätzliche nicht signierte Zugriffsrechte** werden auf **Aktivieren** gesetzt. Sie können keine Berechtigungen einzeln auf **Deaktivieren** zurücksetzen.

Signierten Inhalt ausführen

Sie können Berechtigungen einzeln angeben, indem Sie **Signierten Inhalt ausführen** auf **Bestätigung** setzen. Hierdurch werden alle Berechtigungen unter **Zusätzliche signierte Zugriffsrechte** auf **Bestätigung** gesetzt. Anschließend können Sie jede Berechtigung einzeln auf **Deaktivieren** oder **Aktivieren** zurücksetzen. Wenn Sie **Deaktivieren** oder **Aktivieren** angeben, verwenden alle Berechtigungen unter **Zusätzliche signierte Zugriffsrechte** diese Einstellung.

Wählen Sie eine der folgenden Einstellungen für **Signierten Inhalt ausführen**:

- Wenn Sie aufgefordert werden möchten, das Ausführen des Java-Applets mit den angeforderten Berechtigungen zu bestätigen, klicken Sie auf **Bestätigung**. Wenn Sie **Bestätigung** für **Signierten Inhalt ausführen** gewählt haben, werden alle Berechtigungen unter **Zusätzliche signierte Zugriffsrechte** auf **Bestätigung** gesetzt; Sie können jedoch jede der Berechtigungen einzeln auf **Deaktivieren** oder **Aktivieren** zurücksetzen.
- Wenn Sie das Ausführen signierter Inhalte automatisch ohne Reaktion auf eine Eingabeaufforderung zurückweisen möchten, klicken Sie auf **Deaktivieren**. Alle Berechtigungen unter **Zusätzliche signierte Zugriffsrechte** werden auf **Deaktivieren** gesetzt, und Sie können keine Berechtigung einzeln auf **Bestätigung** oder **Aktivieren** zurücksetzen.
- Wenn Sie das Ausführen signierter Inhalte automatisch ohne Reaktion auf eine Eingabeaufforderung akzeptieren möchten, klicken Sie auf **Aktivieren**. Alle Berechtigungen unter **Zusätzliche signierte**

Zugriffsrechte werden auf **Aktivieren** gesetzt, und Sie können keine Berechtigung einzeln auf **Bestätigung** oder **Deaktivieren** zurücksetzen.

Schließen Sie dieses Dialogfeld, und speichern Sie alle vorgenommenen Änderungen.

Klicken Sie hierauf, um alle Java-Berechtigungen zurückzusetzen. Wählen Sie eine der folgenden Optionen aus, und klicken Sie dann auf **Zurücksetzen**.

- **Gespeicherte Zugriffsrechte** Setzt auf die letzten bekannten Berechtigungen zurück. Alle Änderungen, die vorgenommen wurden, nachdem die Berechtigungen zuletzt gespeichert wurden, gehen verloren.
- **Hohe Sicherheit** Setzt auf die Berechtigungen **Hohe Sicherheit** zurück (restriktivste Einstellung, Applets werden im sicheren Modus ausgeführt). Hierdurch werden alle Berechtigungen unter **Signierten Inhalt ausführen** auf **Bestätigung** und unter **Zusätzliche nicht signierte Zugriffsrechte** auf **Deaktivieren** zurückgesetzt.
- **Mittlere Sicherheit** Setzt auf die Berechtigungen **Mittlere Sicherheit** zurück (Applets werden in der Sandbox mit den zwei zusätzlichen Berechtigungen **Scratchbereich** und **Datei-I/O der Benutzer** ausgeführt). Hierdurch werden alle Berechtigungen (mit Ausnahme von **Geschützter Arbeitsbereich** und **Benutzerdefinierter Dateizugriff**) unter **Signierten Inhalt ausführen** auf **Bestätigung** und unter **Zusätzliche nicht signierte Zugriffsrechte** auf **Deaktivieren** zurückgesetzt.
- **Niedrige Sicherheit** Setzt alle Berechtigungen auf **Niedrige Sicherheit** zurück (am wenigsten restriktiv; Applets werden mit allen Berechtigungen ausgeführt). Hierdurch werden alle Berechtigungen unter **Signierten Inhalt ausführen** auf **Aktivieren** und unter **Zusätzliche nicht signierte Zugriffsrechte** auf **Deaktivieren** zurückgesetzt.

Registerkarte "Zugriffsrechte anzeigen"

Diese Java-Berechtigungen wurden von Ihrem Netzwerkadministrator eingestellt hat.

Damit ein Java-Applet ausgeführt werden kann, benötigt es möglicherweise Dateizugriff und andere Ressourcen auf Ihrem Computer. Jeder dieser Aktionen muss eine bestimmte Berechtigung gewährt werden, bevor sie ausgeführt wird. Ihr Netzwerkadministrator hat möglicherweise die erlaubten Berechtigungen bereits angegeben. Bei erlaubten Berechtigungen kann Ihr Netzwerkadministrator festlegen, ob Sie benachrichtigt werden, wenn diese angefordert werden. Andernfalls werden Sie nur benachrichtigt, wenn ein Java-Applet mehr Berechtigungen anfordert als automatisch erlaubt sind.

Im Folgenden werden drei Berechtigungsmengen unterschieden:

Zugriffsrechte für nicht signierten Inhalt Berechtigungen, die unsignierten, gedownloadeten Inhalten gewährt werden (Applets werden in der Sandbox ausgeführt).

Erlaubte Zugriffsrechte für signierten Inhalt Berechtigungen, die keine Benutzerbestätigung erfordern.

Abgelehnte Zugriffsrechte für signierten Inhalt Berechtigungen, die Benutzerbestätigung erfordern oder absolut verweigert werden.

Sie können auf jeden dieser Berechtigungstitel doppelklicken, um die einzelnen Berechtigungen und angegebenen Einstellungen anzuzeigen.

Die folgenden Berechtigungen können diesen Mengen zugewiesen werden:

Clientspeicher

CustomDatei-I/ODatei-I/O der Benutzer

Execution

Multimedia

Netzwerk-I/O

Printing

Property

Reflection

Registry

Security

Systemeigenschaften

Threads

Zugriff des Benutzerinterface

Eine Berechtigung, die den Lese-, Schreib- und Löschzugriff auf Dateien steuert.

Eine Berechtigung, die die Möglichkeit steuert, Netzwerkoperationen oder eine netzwerkbezogene Aktion durchzuführen.

Eine Berechtigung, die die Möglichkeit steuert, Threads und Threadgruppen erstellen und beeinflussen zu können.

Eine Berechtigung, die die Möglichkeit steuert, auf globale Systemeigenschaften zugreifen oder diese beeinflussen zu können.

Eine Berechtigung, die die Möglichkeit steuert, andere Programme auszuführen.

Eine Berechtigung, die die Möglichkeit steuert, die Reflektions-API für den Zugriff auf Elemente einer bestimmten Klasse verwenden zu können.

Eine Berechtigung, die den Zugriff auf die Druck-APIs steuert.

Eine Berechtigung, die die Möglichkeit steuert, auf die Registrierung zugreifen zu können.

Eine Berechtigung, die den Zugriff auf die JDK-Sicherheitsklassen **java.lang.security** steuert.

Eine Berechtigung für die Zugriffssteuerung der clientseitigen Speicherung, die über die Klasse **ClientStore** zur Verfügung steht.

Eine Berechtigung, die die Möglichkeit steuert, einige der erweiterten Funktionen des AWT zu verwenden.

Eine Berechtigung, die den Zugriff auf Systeminformationen steuert.

Eine Berechtigung, die die Möglichkeit steuert, Dateidialogfelder zum Durchführen von Dateioperationen anzuzeigen. Wenn ein Applet beispielsweise eine Datei öffnen muss, muss es das Standarddialogfeld **Datei öffnen** zur Verfügung stellen und den Benutzer dann auswählen lassen, welche Datei geöffnet werden soll. Das Applet selbst kann keine Dateioperationen durchführen. Daher wird diese Operation als sicherer betrachtet als Code, der direkten Dateizugriff bietet, da der Benutzer unmittelbar eingreifen muss. Diese Berechtigung hat die Stufe **Mittel**.

Eine Berechtigung, die die Verwendung von erweiterten Multimediafunktionen steuert.

Eine Berechtigung, die präzise Steuerungsmöglichkeiten für die Zuweisung von Berechtigungen zu signiertem Inhalt bietet.

Eine Berechtigung, die die Möglichkeit steuert, mit signiertem Code einen Scratchbereich von bis zu 1 MB zu erstellen, in dem temporäre Informationen gespeichert werden können. Ein Java-Applet darf keine anderen Dateien auf der Festplatte des Benutzers lesen oder auf diese schreiben. Ein signiertes Applet kann nur auf seinen eigenen Scratchbereich zugreifen. Diese Berechtigung hat die Stufe **Mittel**.

Eine Berechtigung, die die Möglichkeit steuert, Dialogfelder anzuzeigen.

Eine Umgebung zum Schutz bestimmter Ressourcen (z.B. System-, Festplatte, Netzwerk, lokaler Computer usw.) vor Zugriff von außen, in der ein Java-Applet mit benutzergesteuerten Berechtigungen ausgeführt werden kann.