Zugriffsgenehmigung erforderlich

Ein Java-Applet hat die im Dialogfeld **Sicherheitshinweis** angezeigten Berechtigungen angefordert. Unter Umständen sind zur Ausführung von Java-Applets Dateizugriffe und andere Ressourcen auf Ihrem Computer erforderlich. Diese Aktionen bedürfen speziellen Berechtigungen. Möglicherweise hat der Netzwerkadministrator bereits die zulässigen Berechtigungen festgelegt. Der Netzwerkadministrator kann zusätzlich angeben, ob Sie benachrichtigt werden, wenn zugelässige Berechtigungen angefordert werden. Andernfalls werden Sie nur benachrichtigt, wenn ein Java-Applet mehr als die automatischen Berechtigungen anfordert.

Entscheiden Sie auf der Grundlage Ihrer Kenntnisse über den Herausgeber der Software und der Berechtigungen, die das Programm anfordert, ob Sie das betreffende Java-Applet installieren und ausführen möchten. Wenn Sie sich nicht sicher sind, klicken Sie im Dialogfeld **Sicherheitshinweis** auf **OK**, und klicken Sie im anschließend angezeigten Dialogfeld **Sicherheitshinweis** auf **Nein**.

Weitere Informationen zu den folgenden Berechtigungen erhalten Sie durch Anklicken eines Listeneintrags.

Clientspeicher

Custom

Datei-I/O

Datei-I/O der Benutzer

Execution

Multimedia

Netzwerk-I/O

Printing

Property

Reflection

Registry

Security

Systemeigenschaften

Thread

Zugriff des BenutzerinterfaceI

Weitere Informationen über das Anzeigen der Berechtigungseinstellungen auf Ihrem Computer finden Sie unter den folgenden Themen.

{button ,AL("A_IDH_SEC_ALERT_VIEW_JAVA_CUSTOM_SETTINGS")} Siehe auch

Zeigt den Zugriffstyp an, den Sie gerade einsehen oder ändern. Sie können auf einen Zugriffstyp klicken und dann die Einstellungen für diesen Zugriffstyp vornehmen.

Geben Sie hier einen Dateinamen ein, um ihn der Liste der Dateien hinzuzufügen, für die Sie den angegebenen Zugriff besitzen. Sie können einzelne Dateinamen eingeben oder Stellvertreterzeichen, wie in ***.exe**, verwenden.

Listet die Dateien auf, für die Sie den angegebenen Zugriff zulassen.

Fügt das Objekt der Liste hinzu, für die diese Berechtigungen gelten sollen.

Entfernt das ausgewählte Objekt aus der Liste.

Geben Sie hier einen Dateinamen ein, der aus der Liste der Dateien ausgenommen werden soll, für die Sie den angegebenen Zugriff zulassen.

Listet die Dateien auf, für die der angegebene Zugriff untersagt werden soll.

Gibt an, ob der Zugriff auf die Datei-URL-Codebasis gewährt werden soll.

Zeigt den Zugriffstyp an, den Sie gerade einsehen oder ändern.

Geben Sie hier einen Registrierungseintrag an, um ihn der Liste der Registrierungseinträge hinzuzufügen, für die Sie den angegebenen Zugriff zulassen.

Listet die Registrierungseinträge auf, für die Sie den angegebenen Zugriff zulassen.

Geben Sie hier einen Registrierungseintrag ein, der aus der Liste der Registrierungseinträge ausgenommen werden soll, für die Sie den angegebenen Zugriff zulassen.

Listet die Registrierungseinträge auf, für die der angegebene Zugriff untersagt wird.

Gibt an, ob die Erzeugung von Dialogfeldern durch Java-Applets zulässig ist.

Gibt an, ob die Erzeugung von Fenstern der obersten Ebene durch Java-Applets zulässig ist.

Gibt an, ob eine Warnung angezeigt wird, wenn ein Java-Applet die Erzeugung eines Fensters der obersten Ebene anfordert.

Gibt an, ob Java-Applets die Zwischenablage Ihres Computers zum Ausschneiden, Kopieren und Einfügen von Informationen verwenden dürfen.

Erteilt Java-Applets unbeschränkten Zugriff auf Systemeigenschaften.

Erteilt Zugriff auf die von Ihnen angegebenen Systemeigenschaften und Suffixe, unterbindet den Zugriff auf die von Ihnen ausgenommenen Systemeigenschaften.

Geben Sie hier Suffixe an, auf die Java-Applets zugreifen dürfen.

Geben Sie hier die Systemeigenschaften an, auf die Java-Applets zugreifen dürfen.

Geben Sie hier die Systemeigenschaften an, auf die Java-Applets nicht zugreifen dürfen.

Gibt an, ob ein Ladertyp zulässig ist, der mit diesem öffentlichen Berechtigungsobjekt verknüpft wurde.

Gibt an, ob ein Ladertyp zulässig ist, der auf andere Lader als den mit diesem öffentlichen Berechtigungsobjekt verknüpften verweist.

Gibt an, ob ein Ladertyp zulässig ist, der auf öffentliche Systemklassen verweist.

Gibt an, ob ein Ladertyp zulässig ist, der mit diesem Berechtigungsobjekt verknüpft wurde.

Gibt an, ob ein Ladertyp zulässig ist, der auf andere Lader als den mit diesem Berechtigungsobjekt verknüpften verweist.

Gibt an, ob ein Ladertyp zulässig ist, der auf deklarierte Systemklassen verweist.

Gibt an, ob Java-Applets Dateien lesen dürfen, sofern der Benutzer es gestattet.

Gibt an, ob Java-Applets Dateien schreiben dürfen, sofern der Benutzer es gestattet.

Gibt an, wieviel Speicherplatz auf dem Computer des Benutzers durch Java-Applets belegt werden darf.

Gibt an, ob Java-Applets Speicherplatzlimits überschreiten dürfen, die vom Benutzer für alle Internetdateien festgesetzt wurden.

Gibt an, ob auf dem Server Dateien erstellt werden können. Auf Servern gespeicherte Dateien werden im Profil des Benutzers erstellt und sind auf jedem Computer verfügbar, an dem der Benutzer angemeldet ist.

Gibt an, ob die in **Ausführung erlauben** angegebenen Anwendungen ausgeführt werden können.

Gibt an, welche Programme ausgeführt werden dürfen.

Gibt an, welche Programme nicht ausgeführt werden dürfen.

Gibt an, ob unbeschränkter Thread-Zugang zulässig ist.

Gibt an, ob unbeschränkter Zugang zu Thread-Gruppen zulässig ist.

Gibt an, ob das Berechtigungsobjekt das Setzen des Datenstroms System.in zulässt.

Gibt an, ob das Berechtigungsobjekt das Setzen des Datenstroms System.out zulässt.

Gibt an, ob das Berechtigungsobjekt das Setzen des Datenstroms System.err zulässt.

Gibt an, ob die Klassen, die über die Druckberechtigung verfügen, die Druckdienste nutzen können.

Gibt an, ob der Zugriff auf erweiterte Funktionen der Microsoft DirectX-APIs zulässig ist.

Gibt an, ob der Zugriff auf die JDK-Sicherheitsklassen **java.lang.security** zulässig ist.

Zeigt den Kommunikationstyp an, den Sie gerade einsehen oder ändern. In der folgenden Tabelle werden die Kommunikationstypen und die für sie verfügbaren Einstellungen aufgeführt:

Um die Einstellungen für Folgendes vorzunehmen	***Klicken Sie hierauf***
Allgemeine Kommunikation mit bestimmten Hosts	**Connect Addresses**
Verbindungen über bestimmte Schnittstellen und Anschlüsse	**Bind Addresses**
Beitritt zu bestimmten Multicast-Gruppen	**Multicast Addresses**
Einstellungen, die Vorrang vor speziellen Anschlussregeln haben	**Global Ports**

Geben Sie hier einen Host und einen Anschluss an, die der Liste der Hosts und Anschlüsse hinzugefügt werden sollen, für die Sie die angegebene Kommunikation zulassen.

Listet die Hosts und Anschlüsse auf, für die Sie die angegebene Kommunikation zulassen.

Geben Sie hier einen Host und Anschluss an, die aus der Liste der Hosts und Anschlüsse ausgenommen werden sollen, für die Sie die angegebene Kommunikation zulassen.

Listet die Hosts und Anschlüsse auf, für die Sie die angegebene Kommunikation untersagen.

Gibt an, ob Sie eine Verbindung mit einem Datei-URL herstellen möchten.

Gibt an, ob Sie eine Verbindung mit einem nicht für eine Datei stehenden URL herstellen möchten.

Geben Sie hier den Namen und die Daten für Berechtigungen ein, die Sie der Liste der benutzerdefinierten Berechtigungseinstellungen hinzufügen möchten.

Listet den Namen und die Daten für die hinzugefügten benutzerdefinierten Berechtigungseinstellungen auf.

Klicken Sie hierauf, um die Sicherheitsstufe auf **Hoch (am sichersten)** zu setzen.

Klicken Sie hierauf, um die Sicherheitsstufe auf **Mittel (sicherer)** zu setzen.

So zeigen Sie Einstellungen an

Die Berechtigungen werden vom Netzwerkadministrator über das Internet Explorer Administration Kit eingestellt. Sie können diese Einstellungen normalerweise zwar nicht ändern, aber anzeigen. Führen Sie hierzu die folgenden Schritte durch:

1 Klicken Sie mit der rechten Maustaste auf das Symbol **Internet** auf dem Desktop und dann auf **Eigenschaften**.

2 Klicken Sie auf die Registerkarte **Sicherheit** und dann auf **Angepasst (nur für erfahrene Benutzer)**. Klicken Sie dann auf **Einstellungen**.

3 Klicken Sie in der Einstellungsliste unter **Java** auf **Benutzerdefiniert**.

4 Klicken Sie auf die Schaltfläche **Java-Einstellungen** unten in dem Dialogfeld.

Anmerkungen

- Falls unten in dem Dialogfeld für die Java-Einstellungen eine Schaltfläche **Bearbeiten** angezeigt wird, können Sie die Einstellungen ändern.
- Falls keine Schaltfläche **Bearbeiten** angezeigt wird und Sie die Einstellungen ändern müssen, wenden Sie sich an den Netzwerkadministrator.

{button ,AL("A_IDH_SEC_ALERT_MORE_INFO")} Siehe auch

Schließt dieses Dialogfeld und speichert alle Änderungen.

Schließt dieses Dialogfeld, ohne Ihre Änderungen zu speichern.

Dialogfeld "Zone Editor"

Innerhalb dieser Zone können Sie Berechtigungen den Kategorien **Unsigned**, **Allowed**, oder **Query/Deny** zuweisen. Jeder Berechtigung, der weder **Unsigned** noch **Allowed** zugewiesen ist, wird **Query/Deny** zugewiesen.

Innerhalb der **Query/Deny** zugewiesenen Berechtigungen können Sie bestimmten Berechtigungen **Query** zuweisen, während die verbleibenden Berechtigungen **Deny** zugewiesen bekommen. Alternativ könne Sie **Deny** bestimmte Berechtigungen zuweisen, während die verbleibenden Berechtigungen **Query** zugewiesen werden.

Möchten Sie automatisch sämtliche Berechtigungen zulassen, ohne das entsprechende Dialogfeld zu öffnen und alle Berechtigungen zu aktivieren, können Sie **Allow full set of permissions** wählen.

Dialogfeld "Custom Permissions"

Dieses Dialogfeld zeigt die vom Netzwerkadministrator vergebenen Java-Berechtigungen an.

Zur Ausführung von Java-Applets sind unter Umständen Dateizugriffe und andere Ressourcen auf Ihrem Computer erforderlich. Diesen Aktionen müssen bestimmte Berechtigungen erteilt werden, damit sie ausgeführt werden können. Möglicherweise hat der Netzwerkadministrator bereits die zulässigen Zugriffe festgelegt. Für zulässige Zugriffe kann der Netzwerkadministrator zusätzlich angeben, ob Sie bei jeder Anforderung dieser Zugriffe benachrichtigt werden. Andernfalls werden Sie nur dann benachrichtigt, wenn ein Java-Applet Zugriffe anfordert, die über die automatisch erteilten hinausgehen.

Die folgenden Registerkarten repräsentieren die drei Arten von Berechtigungssätzen:

Registerkarte	***Berechtigungen***
Unsigned	Berechtigungen, die unsignierten übertragenen Inhalten erteilt werden
Allowed	Berechtigungen, die keiner Benutzerbestätigung bedürfen
Query/Deny	Berechtigungen, die vom Benutzer bestätigt werden müssen oder vollkommen verboten sind

Diesen Registerkarten können die folgenden Berechtigungen zugewiesen werden:

Clientspeicher

Custom

Drucken

Execution

FileIO

Multimedia

NetIO

Property

Reflection

Registry

Security

System Streams

Thread

UI

User Directed File IO

Registerkarte "File IO"

Auf dieser Registerkarte können Sie Dateien und Dateitypen angeben, die Sie in diesem Berechtigungssatz für diese Zone zulassen. Standardmäßig werden alle Dateien ausgeschlossen, so dass Sie auszuschließende Dateien nur dann angeben müssen, wenn es sich um eine Untermenge der Dateien handelt, die Sie einschließen. Wenn Sie beispielsweise einen Multimedia-Dateityp (***.avi**) einschließen, können Sie eine bestimmte Datei dieses Typs ausschließen (MyFile.avi). Sie können verschiedene Berechtigungen für verschiedene Zugriffstypen angeben: **Read**, **Write** und **Delete**.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Registerkarte "Registry"

Auf dieser Registerkarte können Sie Registrierungseinträge angeben, die Sie in diesem Berechtigungssatz für diese Zone zulassen. Standardmäßig werden alle Registrierungseinträge ausgeschlossen, so dass Sie auszuschließende Registrierungseinträge nur dann angeben müssen, wenn es sich um eine Untermenge der eingeschlossenen Registrierungseinträge handelt. Wenn Sie beispielsweise **HKEY_CURRENT_USER** einschließen, können Sie eine bestimmte Registrierungskategorie unterhalb dieses Eintrags ausschließen (**HKEY_CURRENT_USER\NETWORK**). Sie können verschiedene Berechtigungen für verschiedene Zugriffstypen angeben: **Read**, **Write**, **Delete**, **Open** und **Create**.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Registerkarte "UI"

Auf dieser Registerkarte können Sie Berechtigungen für einige der sichtbaren Aktionen angeben, die Java-Applets auf dem Computer des Benutzers anfordern, wie das Erstellen eines Fensters oder Dialogfelds, der Zugriff auf Systemeigenschaften (beispielsweise **.ini**-Dateien) oder das Prüfen von Informationen auf deren Struktur, damit sie von dem Applet abgefragt werden können. Diese Berechtigungen werden unter Umständen in den Java-Einstellungen des Benutzers aufgeführt oder in einem Dialogfeld **Security Warning**, das angezeigt wird, wenn ein Java-Applet Berechtigungen anfordert, die über die automatisch erteilten hinausgehen.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Registerkarte "Misc"

Auf dieser Registerkarte können Sie Berechtigungen zum Lesen, Schreiben und Speichern von Dateien, zum Ausführen von Programmen, zum Threading sowie andere Berechtigungen angeben. Diese Berechtigungen werden unter Umständen in den Java-Einstellungen des Benutzers aufgeführt oder in einem Dialogfeld **Security Warning**, das angezeigt wird, wenn ein Java-Applet Berechtigungen anfordert, die über die automatisch erteilten hinausgehen.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Registerkarte "Net IO"

Auf dieser Registerkarte können Sie den Typ sowie die Ziel-Hosts und -anschlüsse der Verbindungen angeben, die Sie zulassen. Standardmäßig werden sämtliche Hosts und Anschlüsse ausgenommen, so dass Sie auszuschließende Hosts und Anschlüsse nur dann angeben müssen, wenn es sich um eine Untermenge der Hosts und Anschlüsse handelt, die Sie einschließen möchten. Sie können verschiedene Berechtigungen für verschiedene Verbindungstypen angeben: **Connect Addresses**, **Bind Addresses**, **Multicast Addresses** und **Global Ports**.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Registerkarte "Custom"

Auf dieser Registerkarte können Sie benutzerdefinierte Berechtigungseinstellungen pro Name oder Datentyp festlegen.

Anmerkung

Für jede Einstellung in diesem Dialogfeld ist Hilfe verfügbar. Markieren Sie die fragliche Einstellung, oder klicken Sie auf die betreffende Schaltfläche, und drücken Sie dann F1.

Eine Anforderung oder Berechtigung zum Zugriff oder zum Steuern des Zugriffs auf Dateien.

Eine Anforderung oder Berechtigung zum Ausführen von Netzwerkoperationen oder einer das Netzwerk betreffenden Aktion.

Eine Berechtigung, die die Möglichkeit zum Erstellen und Ändern von Threads und Thread-Gruppen steuert.

Eine Anforderung bzw. Berechtigung zum Zugriff auf globale Systemeigenschaften oder deren Änderung.

Eine Anforderung bzw. Berechtigung zum Steuern oder Ausführen anderer Programme.

Eine Anforderung bzw. Berechtigung zum Ausführen von Reflection-Operationen oder zum Einsatz von Reflection-APIs, um Zugriff auf Mitglieder einer bestimmten Klasse zu erhalten.

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

Eine Berechtigung, die die Möglichkeit zum Zugriff auf die Registrierung steuert, oder eine Anforderung zum Zugriff auf einen Registrierungsschlüssel.

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

Eine Berechtigung, die die Möglichkeit steuert, mit signiertem Code einen Scratchbereich von bis zu 1 MB durch ClientStoragePermission 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 Anforderung zum Einsatz einer erweiterten Funktion der Benutzeroberflächen-APIs. Auch eine Berechtigung, die die Möglichkeit zur Verwendung einiger erweiterter Funktionen von Application Windowing Toolkit (AWT) steuert.

Eine Berechtigung, die die Möglichkeit zum Ändern der Werte der Systemdatenströme **java.lang.System.in**, **java.lang.System.out** und **java.lang.System.err** steuert.

Eine Berechtigung zur Steuerung der Anzeige von Dateidialogfeldern zur Ausführung von Dateioperationen. Muss ein Applet z.B. eine Datei öffnen, muss es das Standarddialogfeld **Datei öffnen** anzeigen und dann den Benutzer die Datei auswählen lassen. Daher kann das Applet Dateioperationen nicht selbst durchführen. Daher ist diese Operation sicherer als Code direkten Dateizugriff zu gewähren, da der Benutzer in den Vorgang miteingebunden wird. Die Sicherheitsstufe ist **Mittel**.

Eine Berechtigung, um den Einsatz erweiterter Multimediafunktionen zuzulassen.

Eine Berechtigung, die spezifische Steuerung darüber bietet, welche Art von Berechtigungen signiertem Inhalt zugewiesen werden kann.