9234999
Ausgabe 2 DE

VPN-Client Bedienungsanleitung

9234999

Ausgabe 2

Inhalt

Virtuelles privates Netzwerk

Mit **virtuellem privaten Netzwerk** (VPN) können Sie verschlüsselte Verbindungen zu Informationen, die Sie außerhalb des Büros benötigen, erstellen. Sie haben mit verschlüsseltem Zugriff auf Ihr Unternehmensnetzwerk die Kontrolle über E-Mail, Datenbankanwendungen und Intranet.

Remote-Netzwerkverkehr muss geschützt werden. Ihr Unternehmen verwendet möglicherweise ein VPN, um Netzwerkverkehr zu tunneln und entsprechende Sicherheitsrichtlinien anzuwenden. Ein VPN unterstützt Datenschutz und Integrität von Netzwerktransaktionen und ermöglicht es Benutzern, für den Zugriff auf Netzwerke und Netzwerkdienste authentifiziert und autorisiert zu werden.

Zur Erstellung eines VPN authentifizieren ein Gateway und das Gerät einander und übertragen Verschlüsselungs- und Authentifizierungsalgorithmen, um Datenschutz und Integrität der Informationen, auf die Sie zugreifen, zu gewährleisten.

Verwalten eines virtuellen privaten Netzwerks

Um VPN-Verbindungen zu verwenden, erstellen Sie zuerst VPN-Zugänge. Anschließend wählen Sie VPN-Zugänge aus, wenn Sie Anwendungen verwenden, um eine Verbindung zum Unternehmen herzustellen. Eine VPN-Verbindung zum Unternehmensnetzwerk wird über einen anderen Internetverbindungstyp erstellt. Die Verbindung wird erstellt und entsprechend einer VPN-Richtlinie verschlüsselt, die beim Herstellen einer Verbindung zu einem VPN-Zugang geladen wird.

So verwenden Sie ein virtuelles privates Netzwerk

1. Installieren Sie VPN-Client.
   Weitere Informationen finden Sie unter „Installieren des VPN-Client“ auf Seite 6.
2. Legen Sie eine Verbindung zu einem VPN-Richtlinienserver fest.
   Sie können Einstellungen für einen VPN-Richtlinienserver in *VPN-Verwaltung* festlegen oder die Einstellungen von einer **Symbian Installation System** (SIS)-Datei installieren.
   Weitere Informationen finden Sie unter „Herstellen von Verbindungen zu VPN-Richtlinienservern“ auf Seite 10.

   

   Hinweis: Wenn Sie VPN-Richtlinien von SIS-Dateien installieren, müssen Sie keine Verbindungen zu VPN-Richtlinienservern erstellen.
3. Installieren Sie VPN-Richtlinien vom VPN-Richtlinienserver.
   Weitere Informationen finden Sie unter „Installieren von VPN-Richtlinien von VPN-Richtlinienservern“ auf Seite 7.

4 Erstellen Sie VPN-Zugänge.
VPN-Zugänge legen einen Internetzugang und eine VPN-Richtlinie fest.

Hinweis: VPN-Zugänge kombinieren VPN-Richtlinien mit Internetzugängen. Wenn Sie einen VPN-Richtlinienserver zum ersten Mal synchronisieren, werden übereinstimmende VPN-Zugänge für jede Richtlinie erstellt, die Sie auf dem Gerät installieren.

Weitere Informationen zum Erstellen und Auswählen von VPN-Zugängen finden Sie unter „Verwalten von VPN-Zugängen" auf Seite 14.

5 Wählen Sie einen VPN-Zugang, wenn Sie Anwendungen verwenden, um eine Verbindung zum Unternehmensnetzwerk herzustellen.
Weitere Informationen finden Sie unter „Verwenden von VPN mit Anwendungen" auf Seite 17.
Eine VPN-Verbindung wird im Vordergrund einer Internetzugangsverbindung erstellt.

Installieren des VPN-Client

Sie erhalten VPN-Client als Standard-SIS-Datei. Sie installieren VPN-Client auf dem Gerät genauso wie Sie auch andere Software installieren. Weitere Informationen zur Installation von Software auf dem Gerät finden Sie in der Dokumentation des Geräts.

Sie benötigen die VPN-Client SIS-Datei nach der Installation nicht mehr. Löschen Sie die SIS-Datei, um Speicherplatz freizugeben.

Systemanforderungen

Sie können den VPN-Client auf einer Speicherkarte oder auf dem Gerätespeicher installieren. Die Speicherkarte muss sich im Gerät befinden, damit der VPN-Client funktioniert.

Während der Installation des VPN-Client benötigen Sie mindestens 1,5 MB Speicherplatz im Gerät.

Nach der Installation reserviert VPN-Client 900 KB Speicherplatz auf dem Gerät oder einer Speicherkarte. Jede VPN-Richtlinie erfordert i.d.R. 1-16 KB Speicherplatz auf dem Gerät.

Verwalten von VPN-Richtlinien

VPN-Richtlinien legen die Methode fest, die der VPN-Client und ein VPN-Gateway verwenden, um einander sowie die verwendeten Verschlüsselungsalgorithmen zu authentifizieren, die die Vertraulichkeit der Daten gewährleisten sollen. Administratoren erstellen VPN-Richtlinien und speichern sie auf VPN-Richtlinienservern oder leiten sie als SIS-Dateien an Sie weiter. Sie installieren VPN-Richtlinien von einem VPN-Richtlinienserver in *VPN-Verwaltung*.

Installieren von VPN-Richtlinien von VPN-Richtlinienservern

In *VPN-Verwaltung* können Sie VPN-Richtlinien von einem VPN-Richtlinienserver installieren.

Tipp! VPN-Richtlinienserver sind Server im Unternehmensnetzwerk, die VPN-Richtlinien enthalten.

So installieren Sie VPN-Richtlinien:

1. Wechseln Sie zu *Optionen* > *Systemsteuerung* > *Verbindungen* > *VPN-Verwaltung*.
2. Drücken Sie *Ja*, wenn *VPN-Verwaltung* Sie auffordert, VPN-Richtlinien zu installieren.
3. Drücken Sie erneut *Ja*, um VPN-Richtlinienserver hinzuzufügen.
4. Legen Sie Einstellungen für das Herstellen einer Verbindung zu einem VPN-Richtlinienserver fest und drücken Sie *Fertig*.
   Weitere Informationen finden Sie unter „Herstellen von Verbindungen zu VPN-Richtlinienservern" auf Seite 10.
5. Drücken Sie *Ja*, um den VPN-Richtlinienserver zu synchronisieren.
6. Erstellen Sie ein Passwort für den Schlüsselspeicher und drücken Sie *OK*.

   Tipp! Ein Passwort für den Schlüsselspeicher schützt private Schlüssel in VPN-Richtlinien und VPN-Richtlinienserver-Verbindungen vor unberechtigter Nutzung.

   Weitere Informationen finden Sie unter „Erstellen oder Ändern eines Passworts für den Schlüsselspeicher" auf Seite 16.
   Das Gerät stellt eine Verbindung zum VPN-Richtlinienserver her.
7. Überprüfen Sie den Identitätscode des VPN-Richtlinienservers und geben Sie die fehlenden Zeichen ein, um Vertrauen zwischen dem Gerät und dem VPN-Richtlinienserver zu herzustellen, und drücken Sie *OK*.
   Sie können diesen Schritt überspringen, wenn Sie die Einstellungen für den VPN-Richtlinienserver von einer SIS-Datei installieren.

   Tipp! Ein VPN-Richtlinien-Identitätscode ist der Fingerabdruck des VPN-Richtlinienserver-Zertifikats, der das Zertifikat identifiziert.

   Weitere Informationen finden Sie unter „Hinzufügen von VPN-Richtlinienservern" auf Seite 11.
8. Geben Sie die Authentifizierungsinformationen ein, um auf den VPN-Richtlinienserver zuzugreifen, und drücken Sie *OK*.
   Administratoren informieren Sie darüber, welche Informationen Sie eingeben müssen.

VPN-Richtlinien sind auf dem Gerät installiert.

Hinweis: Wenn Sie Abbrechen drücken, werden VPN-Richtlinien nicht installiert. Wählen Sie Installieren, um VPN-Richtlinien von einem VPN-Richtlinienserver zu installieren.

Installieren von VPN-Richtlinien von SIS-Dateien

Administratoren können VPN-Richtlinien als SIS-Dateien an Sie weiterleiten. Wenn Sie VPN-Richtlinien von SIS-Dateien installieren, müssen Sie keine Verbindungen zu VPN-Richtlinienservern festlegen. Nach dem Installieren von VPN-Richtlinien können Sie VPN-Zugänge erstellen und sie Anwendungen zuordnen.

Wenn die VPN-Richtlinien private Schlüssel und entsprechende Zertifikate enthalten, legen Administratoren **Passwörter für den Schlüsselimport** fest, um die privaten Schlüssel zu schützen. Administratoren sollten eine sichere Methode verwenden, um das Passwort für den Schlüsselimport an Sie weiterzuleiten.

Tipp! Ein Passwort für den Schlüsselimport schützt die privaten Schlüssel in einer VPN-Richtliniendatei.

Um VPN-Richtlinien von SIS-Dateien zu installieren, geben Sie das Passwort für den Schlüsselimport in *Passwort* ein und drücken Sie *OK*. Geben Sie anschließend das Passwort für den Schlüsselspeicher in *Passwort* ein und drücken Sie *OK*.

Anzeigen von VPN-Richtlinien

In *VPN-Verwaltung* können Sie die VPN-Richtlinien, die Sie auf dem Gerät installieren, anzeigen, aktualisieren und löschen.

Um VPN-Richtliniendetails anzuzeigen, wählen Sie eine VPN-Richtlinie und drücken Sie *Öffnen*, um weitere Informationen anzuzeigen.

Führen Sie einen Bildlauf durch, um die folgenden Informationen zu jeder VPN-Richtlinie anzuzeigen.

- *Beschreibung* zeigt zusätzliche Informationen zur VPN-Richtlinie an. Die Beschreibung wird von der VPN-Richtlinie gelesen. Administratoren legen die Beschreibung fest, wenn sie die VPN-Richtlinie erstellen.
- *Richtlinienstatus* zeigt an, ob die VPN-Richtlinie verwendet werden kann oder bereits verwendet wird.
- *Zertifikatsstatus* zeigt an, ob gültige Benutzerzertifikate im Gerät verfügbar sind.
- *Richtliniename* zeigt den Namen der VPN-Richtlinie an. Administratoren legen den Namen fest, wenn sie die VPN-Richtlinie erstellen.
- *Name des Richtlinienservers* zeigt den Namen des VPN-Richtlinienservers an, von dem Sie die VPN-Richtlinie installiert haben. Sie benennen VPN-Richtlinienserver, wenn Sie Verbindungen zu VPN-Richtlinienservern festlegen. Dieses Feld ist ausgeblendet, wenn Sie die VPN-Richtlinie von einer SIS-Datei installiert haben.
- *Aktualisiert* zeigt das Datum an, an dem die VPN-Richtlinie zuletzt vom VPN-Richtlinienserver aktualisiert wurde. Dieses Feld ist ausgeblendet, wenn Sie die VPN-Richtlinie von einer SIS-Datei installiert haben.

Überprüfen des Richtlinienstatus

Richtlinienstatus kann folgende Werte besitzen:

Aktiv - Sie haben eine Verbindung zu einem VPN-Zugang erstellt, der der VPN-Richtlinie zugeordnet ist. Wenn Sie eine Verbindung erstellen, wird die VPN-Richtlinie aktiviert.

Einem VPN-Zugang zugeordnet - Sie haben die VPN-Richtlinie einem oder mehreren VPN-Zugängen zugeordnet. Sie können einen beliebigen VPN-Zugang auswählen, um die VPN-Richtlinie zu aktivieren.

Keinem VPN-Zugang zugeordnet - Sie müssen die VPN-Richtlinie einem VPN-Zugang zuordnen, um die VPN-Richtlinie zu aktivieren.

Hinweis: Die Ansicht der VPN-Richtliniendetails wird nicht aktualisiert, wenn sich der Richtlinienstatus ändert, während die Ansicht geöffnet ist.

Überprüfen des Zertifikatsstatus

Zertifikatsstatus kann folgende Werte besitzen:

OK - Mindestens ein gültiges Zertifikat ist im Gerät verfügbar oder Sie verwenden keine Zertifikate, um VPN-Gateways zu authentifizieren.

Abgelaufen - Lebensdauer eines oder mehrerer Zertifikate ist abgelaufen. Wenn Sie keine VPN-Verbindung erstellen können, aktualisieren Sie die VPN-Richtlinie, um neue Zertifikate anzumelden.

Nicht vorhanden - Eines oder mehrere der erforderlichen Zertifikate können nicht auf dem Gerät gefunden werden. Wenn Sie keine VPN-Verbindung erstellen können, versuchen Sie, die VPN-Richtlinie zu aktualisieren, um neue Zertifikate anzumelden.

Noch nicht gültig - Eines oder mehrere Zertifikate sind für zukünftige Verwendung bestimmt. Dieser Wert kann auch bedeuten, dass Datum und Uhrzeit auf dem Gerät in der Vergangenheit eingestellt sind, die Zeitzonen nicht richtig festgelegt sind oder die Sommerzeit aktiviert ist.

Um die VPN-Richtlinie zu löschen, drücken Sie *Löschen*.

Um die VPN-Richtliniendetails zu schließen, drücken Sie *Schließen*.

Aktualisieren von VPN-Richtlinien

Wenn Sie eine Verbindung zu einem VPN-Zugang erstellen, überprüft der VPN-Client den Status der VPN-Richtlinie, die dem VPN-Zugang vom VPN-Richtlinienserver zugeordnet ist. Wenn Administratoren eine neue Version der VPN-Richtlinie erstellt haben, wird die neue Version auf dem Gerät installiert. Wenn Administratoren die VPN-Richtlinie vom VPN-Richtlinienserver gelöscht haben, wird die VPN-Richtlinie vom Gerät entfernt.

Änderungen treten in Kraft, wenn Sie das nächste Mal eine Verbindung zu einem VPN-Zugang erstellen, d. h. sie betreffen die aktuelle VPN-Verbindung nicht.

Sie können eine VPN-Richtlinie auch in *VPN-Verwaltung* aktualisieren.

Um eine VPN-Richtlinie zu aktualisieren, wählen Sie eine VPN-Richtlinie und drücken Sie *Aktualisieren*. Der VPN-Client überprüft den Status der VPN-Richtlinie vom VPN-Richtlinienserver.

Löschen von VPN-Richtlinien

VPN-Richtlinien werden automatisch gelöscht, nachdem Administratoren sie vom VPN-Richtlinienserver löschen, wenn Sie eine VPN-Richtlinie aktualisieren oder den VPN-Richtlinienserver synchronisieren.

Wenn Sie eine VPN-Richtlinie in *VPN-Verwaltung* löschen, die noch auf dem VPN-Richtlinienserver vorhanden ist, wird die VPN-Richtlinie erneut installiert, wenn Sie VPN-Richtlinien vom VPN-Richtlinienserver synchronisieren.

Um eine VPN-Richtlinie zu löschen, wählen Sie die VPN-Richtlinie und drücken Sie Strg + *D*.

Sie können keinen VPN-Zugang verwenden, wenn Sie die VPN-Richtlinie löschen, die ihm zugeordnet ist.

Verwalten von VPN-Richtlinienservern

In *Richtlinienserver* können Sie VPN-Richtlinien von VPN-Richtlinienservern installieren. Wenn Sie eine Verbindung zu einem VPN-Zugang erstellen, stellt das Gerät eine Verbindung zum VPN-Richtlinienserver her, um automatisch die VPN-Richtlinie zu aktualisieren, die dem VPN-Zugang zugeordnet ist. Um alle VPN-Richtlinien zu aktualisieren, synchronisieren Sie VPN-Richtlinienserver mit dem Gerät.

Herstellen von Verbindungen zu VPN-Richtlinienservern

Wenn Sie VPN-Richtlinien von einem VPN-Richtlinienserver installieren, erstellen Sie eine Vertrauensbeziehung zwischen dem Gerät und dem VPN-Richtlinienserver. Um die Vertrauensbeziehung zu erstellen, müssen Sie den VPN-Richtlinienserver authentifizieren und der VPN-Richtlinienserver muss Sie authentifizieren.

Nachdem der VPN-Richtlinienserver Sie authentifiziert, erstellt der VPN-Client einen privaten Schlüssel und meldet ein entsprechendes Zertifikat für Sie an. Der private Schlüssel und das Zertifikat werden in einem Schlüsselspeicher auf dem Gerät gespeichert. Das Zertifikat authentifiziert Sie für den VPN-Richtlinienserver.

Tipp! Administratoren können eine SIS-Datei mit Einstellungen an Sie weiterleiten, die eine Verbindung zu einem VPN-Richtlinienserver festlegen, oder Sie können den VPN-Richtlinienserver in *VPN-Verwaltung* hinzufügen.

Installieren von Einstellungen von SIS-Dateien

Sie können VPN-Richtlinienserver-Einstellungen auf dem VPN-Richtlinienserver von einer SIS-Datei installieren. Sie installieren die Einstellungen auf dem Gerät genauso wie Sie auch andere Software installieren.

Die Einstellungen bestehen aus der Adresse und dem Serverzertifikat des VPN-Richtlinienservers. Aufgrund des Serverzertifikats vertraut das Gerät dem VPN-Richtlinienserver, so dass Sie nur einen Benutzernamen und ein Passwort eingeben müssen, um Ihre Identität zu beweisen.

Die SIS-Datei enthält keine Einstellungen für den Internetzugang, um eine Verbindung zum VPN-Richtlinienserver herzustellen. Um den Internetzugang festzulegen, bearbeiten Sie die VPN-Richtlinienserver-Einstellungen. Sie können auch den Internetzugang wählen, wenn Sie eine Verbindung zum VPN-Richtlinienserver herstellen.

Wenn Administratoren die SIS-Datei nicht signieren, wird eine Sicherheitswarnung beim Installieren der SIS-Datei angezeigt. Sie können die Warnung ignorieren, wenn Sie sicher sein können, dass Sie die SIS-Datei von den Administratoren erhalten haben.

Sie müssen *VPN-Verwaltung* beenden, bevor Sie die Einstellungen von einer SIS-Datei installieren. Andernfalls schlägt die Installation fehl.

Hinzufügen von VPN-Richtlinienservern

In *Richtlinienserver* können Sie Einstellungen für einen VPN-Richtlinienserver festlegen, wenn Sie die Einstellungen nicht von einer SIS-Datei installieren.

Wenn Sie zum ersten Mal eine Verbindung zur VPN-Richtlinienserver-Adresse herstellen, vertraut das Gerät dem VPN-Richtlinienserver nicht. Aus diesem Grund müssen Sie den VPN-Richtlinienserver authentifizieren. Sie erhalten einen Identitätscode für den VPN-Richtlinienserver von den Administratoren. Sie überprüfen und vervollständigen den Identitätscode für den VPN-Richtlinienserver und der VPN-Client bestätigt ihn.

Nach erfolgreicher Authentifizierung meldet der VPN-Client ein Zertifikat vom VPN-Richtlinienserver für die spätere Authentifizierung beim VPN-Richtlinienserver an.

Um einen VPN-Richtlinienserver hinzuzufügen, drücken Sie *Neu*. Geben Sie die folgenden Einstellungen ein:

- *Name des Richtlinienservers* - Sie können einen beliebigen Namen wählen, aber er muss in *VPN-Richtlinienserver* eindeutig sein.
  Wenn Sie dieses Feld leer lassen, wird in dieses Feld *Adresse für Richtlinienserver* eingefügt.
  Der Name des Richtlinienservers wird in der VPN-Richtlinienserver-Liste und in der Titelleiste des Dialogfelds für die VPN-Richtlinienserver-Einstellungen angezeigt.

- *Adresse für Richtlinienserver* - Der Hostname oder die IP-Adresse des VPN-Richtlinienservers, von dem Sie VPN-Richtlinien installieren. Sie können auch eine Anschlussnummer festlegen, durch einen Doppelpunkt getrennt (:).
  Sie erhalten die Adresse des Richtlinienservers von den Administratoren.
- *Internetzugang* - Internetzugang, der zum Herstellen einer Verbindung zu diesem VPN-Richtlinienserver verwendet wird.
  Administratoren informieren Sie darüber, welchen Zugang Sie auswählen müssen.

Um VPN-Richtlinien vom VPN-Richtlinienserver zu installieren, drücken Sie *Ja*, wenn *VPN-Verwaltung* Sie auffordert, den VPN-Richtlinienserver zu synchronisieren.

Tipp! Synchronisieren bedeutet, dass der VPN-Client eine Verbindung zu einem VPN-Richtlinienserver herstellt, um neue, aktualisierte oder entfernte VPN-Richtlinien zu prüfen, und installiert die VPN-Richtlinien auf dem Gerät.

Wenn Sie zum ersten Mal eine Verbindung zur VPN-Richtlinienserver-Adresse herstellen, vertraut das Gerät dem VPN-Richtlinienserver nicht. Aus diesem Grund müssen Sie den VPN-Richtlinienserver authentifizieren. Sie erhalten einen Identitätscode für den VPN-Richtlinienserver von den Administratoren.

Um die Identität des VPN-Richtlinienservers zu überprüfen, vergleichen Sie sorgfältig den Identitätscode für den VPN-Richtlinienserver im Dialogfeld *Identitätscode für VPN-Richtlinienserver* mit dem Code, den Sie von den Administratoren erhalten, geben Sie die fehlenden Zeichen in *Fehlende Zeichen* ein und drücken Sie *OK*.

Hinweis: Wenn Sie VPN-Richtlinienserver-Einstellungen von einer SIS-Datei installieren, müssen Sie die Identität des VPN-Servers nicht überprüfen und diese Ansicht wird nie angezeigt.

Um den VPN-Richtlinienserver zu authentifizieren, geben Sie Ihren Benutzernamen in *Benutzername für Richlinienserver* ein und Ihr Passwort in *Passwort für Richtlinienserver* ein, und drücken Sie *OK* im Dialogfeld *Authentifizierung des VPN-Richtlinienservers*.

Administratoren informieren Sie darüber, welchen Benutzernamen und welches Passwort Sie eingeben müssen.

Tipp! Ein Benutzername und ein Passwort für den Richtlinienserver schützen den VPN-Richtlinienserver vor unberechtigtem Zugriff.

VPN-Client meldet ein Zertifikat für die spätere Authentifizierung beim VPN-Richtlinienserver an und installiert VPN-Richtlinien auf dem Gerät.

Tipp! Anmeldung eines Zertifikats bedeutet, dass eine Zertifizierungsanfrage an eine Zertifizierungsbehörde gesendet und ein Zertifikat empfangen wird.

Sie können jetzt VPN-Zugänge erstellen und sie Anwendungen zuordnen.

Bearbeiten von VPN-Richtlinienservern

In *Richtlinienserver* können Sie VPN-Richtlinienserver anzeigen, bearbeiten, synchronisieren und löschen.

Um die Einstellungen für einen VPN-Richtlinienserver anzuzeigen oder zu ändern, wählen Sie den VPN-Richtlinienserver aus und drücken Sie *Bearbeiten*:

- *Name des Richtlinienservers* - Name für den Richtlinienserver. *Richtlinienserver* zeigt den neuen Namen an.
- *Internetzugang* - Internetzugang, der zum Herstellen einer Verbindung zu diesem VPN-Richtlinienserver verwendet wird.
  Wenn Sie den Zugang löschen, der dem VPN-Richtlinienserver zugeordnet ist, zeigt *Internetzugang* den Text *(nicht ausgewählt)* an. Wenn Sie alle Zugänge löschen, kann *VPN-Verwaltung* die Einstellungen nicht speichern.

Sie können die *Adresse für Richtlinienserver* nicht ändern, nachdem Sie VPN-Richtlinien vom VPN-Richtlinienserver installiert haben, weil der VPN-Richtlinienserver während der ersten Verbindung die Adresse an *VPN-Verwaltung* sendet.

Um die VPN-Richtlinie zu löschen, drücken Sie *Löschen*.

Um die Einstellungen zu speichern, drücken Sie *Fertig*.

Tipp! Um das Fenster zu schließen, ohne Ihre Änderungen zu speichern, drücken Sie Esc.

Synchronisieren von VPN-Richtlinienservern

Um Richtlinien von einem VPN-Richtlinienserver zu installieren und zu aktualisieren, wählen Sie einen VPN-Richtlinienserver und drücken Sie *Synchronisieren*. Der VPN-Client stellt eine Verbindung zum VPN-Richtlinienserver her, um zu überprüfen, ob Administratoren hinzugefügt bzw. aktualisiert oder VPN-Richtlinien gelöscht wurden.

Wenn der VPN-Richtlinienserver neue VPN-Richtlinien oder neue Versionen von VPN-Richtlinien enthält, werden die VPN-Richtlinien auf dem Gerät installiert. Wenn Administratoren VPN-Richtlinien vom VPN-Richtlinienserver gelöscht haben, werden die VPN-Richtlinien vom Gerät entfernt.

Hinweis: Wenn Sie einen VPN-Richtlinienserver zum ersten Mal synchronisieren, werden übereinstimmende VPN-Zugänge für jede Richtlinie erstellt, die Sie auf dem Gerät installieren. VPN-Zugänge kombinieren VPN-Richtlinien mit Internetzugängen.

Wenn Sie eine Verbindung zu einem VPN-Richtlinienserver installieren oder VPN-Richtlinien aktualisieren, müssen Sie möglicherweise VPN-Zertifikate vom VPN-Richtlinienserver anmelden.

Anmelden von VPN-Zertifikaten

Der VPN-Client erstellt eine Zertifizierunganfrage für jedes erforderliche Zertifikat und sendet die Anfrage an den VPN-Richtlinienserver. Der VPN-Richtlinienserver meldet jedes angefragte Zertifikat von einer **Zertifizierungsbehörde** an und gibt es an den VPN-Client zurück.

Die Zertifizierungsanfrage und das entsprechende Zertifikat enthalten die Identität des Benutzers. Je nach VPN-Richtlinienserverkonfiguration kann die VPN-Richtlinienserver-Identität als Benutzeridentität in VPN-Zertifikaten verwendet werden. Wenn dies nicht möglich ist, fragt Sie *VPN-Verwaltung* nach der Benutzeridentität für eine bestimmte Domäne. Administratoren stellen Ihnen die einzugebenden Informationen zur Verfügung.

Um Zertifizierungsanfragen zu stellen, geben Sie in das Dialogfeld *VPN-Benutzeridentität* Ihre Zertifikatsbenutzeridentität für die festgelegte Domäne in *Benutzeridentität* ein und drücken Sie *OK*.

Löschen von VPN-Richtlinienservern

Um einen VPN-Richtlinienserver zu löschen, wählen Sie den VPN-Richtlinienserver und drücken Sie Strg + *D*.

VPN-Verwaltung fordert Sie zum Löschen der VPN-Richtlinien auf, die Sie vom VPN-Richtlinienserver installiert haben.

Verwalten von VPN-Zugängen

Ein VPN-Zugang ist ein virtueller Zugang, der eine VPN-Richtlinie und einen Internetzugang kombiniert. Wählen Sie aus der Liste der Internetzugänge einen VPN-Zugang aus, um eine VPN-Verbindung zu erstellen.

In *VPN-Zugänge* können Sie einen VPN-Zugang auf dem Gerät anzeigen, erstellen und löschen. Wechseln Sie zu *Optionen* > *Systemsteuerung* > *Verbindungen* > *VPN-Zugänge*. Ein Symbol zeigt den Internetverbindungstyp an, über den die VPN-Verbindung erstellt wird.

Um VPN-Zugänge zu erstellen, drücken Sie *Neu*. Geben Sie in *Allgemeine Einstellungen* die folgenden Einstellungen ein:

- *Name des VPN-Zugangs* - bestimmt den VPN-Zugang in Internetzugangslisten.
- *Internetzugang* - Name der Internetverbindung, über die die VPN-Verbindung erstellt wird.
- *VPN-Richtlinie* - Name der VPN-Richtlinie, die dem VPN-Zugang zugeordnet ist.
- *Netzwerk* - bestimmt das VPN-Netzwerk. Sie müssen ein anderes Netzwerk als das Netzwerk für den Internetzugang auswählen.

Hinweis: Wenn Sie VPN-Verbindungen zu mehreren VPN-Gateways erstellen, erstellen Sie einzelne Netzwerke für die Verbindung zu jedem VPN-Gateway.

Um ein Netzwerk auszuwählen, wechseln Sie zu *Netzwerk* und drücken Sie *Ändern*:

- Wählen Sie ein Netzwerk aus und drücken Sie *OK*.
- **Um ein Netzwerk hinzuzufügen,** drücken Sie *Netzwerk hinzufügen*, geben Sie einen Namen für das Netzwerk in *Netzwerkname* ein und drücken Sie *OK*.
- **Um ein Netzwerk umzubennen,** drücken Sie *Netzwerk umbenennen*, ändern Sie den Netzwerknamen in *Netzwerkname* und drücken Sie *OK*.

Um Einstellungen für einen Proxy-Server im Unternehmensnetzwerk festzulegen, wechseln Sie zu *Proxy-Einstellungen* und geben Sie die folgenden Einstellungen ein:

Hinweis: Ein Proxy-Server ist ein Zwischenserver, der als Sicherheitsbarriere zwischen einem Intranet und dem Internet fungiert. Administratoren informieren Sie über die entsprechenden Einstellungen.

- *Proxy-Protokoll* - Protokoll, das der Proxy-Server verwendet.
- *Proxy-Server verw.* - Wählen Sie *Ja*, um Einstellungen für einen Proxy-Server im Unternehmensnetzwerk festzulegen.
- *Proxy-Server* - Adresse eines Proxy-Servers im Unternehmensnetzwerk.
- *Portnummer* - Portnummer für die Verbindung zum Proxy-Server.
- *Kein Proxy für* - Internetadressen, um den Proxy-Server für bestimmte Internetseiten zu umgehen.

Um VPN-Zugangseinstellungen anzuzeigen und zu bearbeiten, wählen Sie einen VPN-Zugang aus und drücken Sie *Bearbeiten*.

Um einen VPN-Zugang zu löschen, wählen Sie einen VPN-Zugang und drücken Sie Strg + *D*.

Um die Einstellungen zu speichern, drücken Sie *Fertig*.

Tipp! Um das Fenster zu schließen, ohne Ihre Änderungen zu speichern, drücken Sie Esc.

Anzeigen des VPN-Protokolls

Das VPN-Protokoll enthält Protokollmitteilungen, die aufgezeichnet werden, wenn Sie VPN-Richtlinien aktualisieren bzw. synchronisieren und VPN-Zugänge verwenden, um VPN-Verbindungen zu VPN-Gateways zu erstellen.

In *Protokoll* können Sie Protokollnachrichten anzeigen und löschen. Sie können den Mitteilungstyp, die Aufzeichnungszeit jeder Mitteilung und den Anfang der Protokollmitteilung anzeigen lassen.

gibt Fehler, Warnung und Information an.

Um die gesamte Protokollmitteilung anzuzeigen, drücken Sie *Öffnen*.

Protokoll sortiert Protokollmitteilungen nach Aufzeichnungszeit und -datum, beginnend mit den jüngsten Mitteilungen. Sie können Mitteilungen anzeigen, bis Sie *Protokoll* geöffnet haben.

Um die neuesten Protokollmitteilungen anzuzeigen, drücken Sie *Aktualisieren*.

Protokollmitteilungen können Fehler, Status und Ursachencodes enthalten. Melden Sie den Administratoren die Codes, wenn Sie Fehler melden.

Um alle Protokollmitteilungen aus dem Protokoll zu löschen, drücken Sie *Protokoll zurücksetzen*.

Protokollmitteilungen werden in einem Ringpuffer aufgezeichnet. Wenn die Protokollgröße 20 KB erreicht hat, werden neue Protokollmitteilungen über die ältesten Protokollmitteilungen geschrieben.

Passwörter für den Schlüsselspeicher

In *Passwort* können Sie ein Passwort für den Schlüsselspeicher erstellen oder ändern. Ein Passwort für den Schlüsselspeicher schützt private Schlüssel im Gerät und VPN-Richtlinienserver-Verbindungen vor unberechtigter Nutzung.

Erstellen oder Ändern eines Passworts für den Schlüsselspeicher

Sie erstellen ein Passwort für den Schlüsselspeicher, wenn Sie die erste VPN-Richtlinie installieren. Erstellen Sie Passwörter für den Schlüsselspeicher, die lang und schwierig genug sind, um die Informationen im Gerät zu schützen. Wenn das Passwort für den Schlüsselspeicher geknackt wird, kann das Unternehmensnetzwerk unberechtigtem Zugriff ausgesetzt sein.

Tipp! Ein Passwort für den Schlüsselspeicher muss mindestens sechs Zeichen lang sein und kann Buchstaben, Zahlen und Sonderzeichen enthalten.

Um das Passwort für den Schlüsselspeicher zu ändern, drücken Sie *Passwort ändern*.

Geben Sie in *Passwort* ein Passwort ein, an das Sie sich einfach erinnern können, aber das für andere schwierig zu erraten ist. Um Tippfehler zu vermeiden, geben Sie das Passwort erneut in *Bestätigen* ein und drücken Sie *OK*.

Eingeben von Passwörtern für den Schlüsselspeicher

Sie müssen das Passwort für den Schlüsselspeicher eingeben, wenn Sie

- neue oder aktualisierte VPN-Richtlinien von VPN-Richtlinienservern installieren.
- Anwendungen verwenden, um Verbindungen zu VPN-Zugängen herzustellen, die eine Zertifikat-Authentifizierung erfordern.

Verwenden von VPN mit Anwendungen

Wenn Sie eine Anwendung verwenden, um eine Verbindung zu einem VPN-Zugang herzustellen, führt das Gerät Folgendes aus:

- Es stellt eine Verbindung zum Internetzugang her, der dem VPN-Zugang zugeordnet ist.
- Es lädt die VPN-Richtlinie, die dem VPN-Zugang zugeordnet ist.
- Es stellt eine Verbindung zu einem VPN-Gateway her, um eine VPN-Verbindung zu erstellen.

Authentifizierung für VPN-Gateways

Sie müssen Ihre Identität beweisen, wenn Sie sich beim Unternehmens-VPN anmelden. Die VPN-Richtlinie legt die zu verwendende Authentifizierungsmethode fest:

- Zertifikatsbasierte Authentifizierung – Sie müssen ein Zertifikat besitzen, das eine vertrauenswürdige Zertifizierungsbehörde signiert. Sie verwenden eine Online-Zertifikatsanmeldung, um das Zertifikat zu erhalten, oder Sie installieren Zertifikate, wenn Sie die VPN-Richtlinie von einer SIS-Datei installieren.
- Legacy-Authentifizierung – Sie verwenden Benutzernamen und Passwörter oder Passcodes zur Authentifizierung. Administratoren erstellen die Benutzernamen und Passwörter oder stellen Ihnen SecurID-Zeichenfolgen zur Verfügung, um die Passcodes zu erstellen.

Wenn Sie Zertifikate für die Authentifizierung verwenden, geben Sie das Passwort für den Schlüsselspeicher ein.

Wenn Sie Legacy-Authentifizierung verwenden, geben Sie die VPN-Authentifizierungsinformationen ein, wenn Sie Anwendungen zum Herstellen von Verbindungen zu VPN-Zugängen verwenden und das Gerät verschlüsselte Verbindungen mit dem VPN-Gateway verhandelt.

Um Benutzernamen und Passwörter für die Authentifizierung für einen VPN-Gateway zu verwenden, geben Sie Ihren VPN-Benutzernamen in *VPN Benutzername* und das VPN-Passwort in *VPN-Passwort* ein. Drücken Sie *OK*.

Um Benutzernamen und Passcodes für die Authentifizierung für einen VPN-Gateway zu verwenden, geben Sie Ihren VPN-Benutzernamen in *VPN-Benutzername* ein. Erstellen Sie einen SecurID-Passcode und geben Sie ihn in *VPN-Passcode* ein. Drücken Sie *OK*.

Wenn die SecurID-Zeichenfolge nicht mehr synchron mit der Zeituhr des ACE / Servers läuft, werden Sie dazu aufgefordert, den nächsten Passcode einzugeben, den der ACE / Server als neue Referenz für die Zeitbasis der Zeichenfolge verwendet. Geben Sie Ihren VPN-Benutzernamen in *VPN-Benutzername* ein. Erstellen Sie einen neuen Passcode, geben Sie ihn in *Nächster Passcode* ein und drücken Sie *OK*. Falls dies nicht gelingt, wenden Sie sich an die Administratoren.

Fehlerbehebung

Dieser Abschnitt listet Fehlermeldungen in alphabetischer Reihenfolge auf, beschreibt die möglichen Fehlerursachen und schlägt Aktionen zur Fehlerbehebung vor.

Authentifizierung fehlgeschlagen.

- Sie geben einen falschen Benutzernamen oder ein falsches Passwort für einen VPN-Richtlinienserver ein, wenn Sie eine Authentifizierung für einen VPN-Richtlinienserver durchführen oder sich bei einem VPN anmelden.
- Sie geben den falschen Passcode ein, wenn Sie zur Eingabe des nächsten Passcodes aufgefordert werden.

Versuchen Sie Folgendes:

- Überprüfen Sie Benutzernamen und Passwort und versuchen Sie es erneut.
- Erstellen Sie einen Passcode und geben Sie ihn ein.

Automatische Richtlinienserveranmeldung fehlgeschlagen. Geben Sie Benutzernamen und Passwort des Richtlinienservers ein, um weiterzufahren.

Das Zertifikat, das Sie für den VPN-Richtlinienserver authentifiziert, läuft ab oder die Administratoren erklären das Zertifikat für ungültig.

Melden Sie diesen Fehler den Administratoren, die Ihnen ein einmaliges Passwort für die Anmeldung zur Verfügung stellen. Geben Sie den Benutzernamen und das einmalige Passwort ein, um die Authentifizierung für den VPN-Richtlinienserver durchzuführen. Der VPN-Client meldet ein neues Zertifikat für Sie an.

Automatische Richtlinienserveranmeldung fehlgeschlagen. Details finden Sie im VPN-Protokoll.

Die Gültigkeitsdauer des Zertifikats, das Sie für den VPN-Richtlinienserver authentifiziert, hat noch nicht begonnen.

Überprüfen Sie die Einstellungen für Datum und Uhrzeit oder warten Sie, bis die Gültigkeitsdauer des Zertifikats beginnt.

Kryptografiebibliothek ist zu schwach.

Wenn die auf dem Gerät installierte Kryptografiebibliothek zu schwach ist, können Sie keine VPN-Verbindungen verwenden.

Wenden Sie sich an die Administratoren.

Falsches Passwort.

Sie geben ein falsches Passwort für den Schlüsselspeicher oder für den Schlüsselimport ein.

Überprüfen Sie das Passwort und versuchen Sie es erneut.

Sie erhalten das Passwort für den Schlüsselimport von den Administratoren. Sie erstellen selbst das Passwort für den Schlüsselspeicher.

Richtlinienserver wird derzeit verwendet. Löschen nicht möglich.

Sie können einen VPN-Richtlinienserver nicht löschen, während Sie VPN-Richtlinien vom Server aktualisieren. Wenn Sie eine Anwendung verwenden, die eine Verbindung zu einem VPN-Zugang erstellt, werden VPN-Richtlinien automatisch aktualisiert.

Warten Sie, bis die VPN-Richtlinien-Aktualisierung beendet ist, und versuchen Sie es erneut.

Richtlinienserveranmeldung fehlgeschlagen. Löschen Sie und erstellen Sie die Serverdefinition neu.

Das Serverzertifikat des VPN-Richtlinienservers läuft ab.

Um den VPN-Richtlinienserver zu löschen, wählen Sie den VPN-Richtlinienserver in *Richtlinienserver* und drücken Sie Strg + *D*.

Um den VPN-Richtlinienserver erneut hinzuzufügen, drücken Sie *Neu* oder wenden Sie sich an den Administrator wegen einer SIS-Datei, die neue Einstellungen für den VPN-Richtlinienserver enthält.

Richtlinienaktualisierung fehlgeschlagen. Details finden Sie im VPN-Protokoll.

Richtliniensynchronisation fehlgeschlagen. Details finden Sie im VPN-Protokoll.

Ein Fehler ist aufgetreten, während VPN-Richtlinien vom VPN-Richtlinienserver heruntergeladen oder auf dem Gerät installiert werden.

Um eine VPN-Richtlinie zu aktualisieren, wählen Sie eine VPN-Richtlinie in *Richtlinien* und drücken Sie *Aktualisieren*.

Um Richtlinien vom VPN-Richtlinienserver zu installieren, wählen Sie einen VPN-Richtlinienserver in *Richtlinienserver* und drücken Sie *Synchronisieren*.

Serveridentitätscode ist falsch.

Sie geben eine falsche Zeichenfolge ein, wenn Sie zur Eingabe des VPN-Richtlinien-Identitätscodes aufgefordert werden.

Vergleichen Sie den VPN-Richtlinien-Identitätscode sorgfältig mit dem Code, den Sie von den Administratoren erhalten haben, und geben Sie die fehlenden Zeichen erneut ein.

Aktivierung der VPN-Verbindung fehlgeschlagen. Details finden Sie im VPN-Protokoll.

Die Legacy-Authentifizierung ist fehlgeschlagen oder das Zertifikat, das Sie zur Authentifizierung für den VPN-Gateway verwenden, fehlt, ist abgelaufen, oder seine Gültigkeitsdauer hat noch nicht begonnen.

Überprüfen Sie die Einstellungen für Datum und Uhrzeit auf dem Gerät.

Um eine VPN-Richtlinie zu aktualisieren, wählen Sie eine VPN-Richtlinie in *Richtlinien* und drücken Sie *Aktualisieren*.

Verwendete VPN-Richtlinie wurde gelöscht. Versuchen Sie eine erneute Konfiguration des Internetzugangs.

Die VPN-Richtlinie, die dem VPN-Zugang zugeordnet wurde, ist veraltet und wurde automatisch gelöscht.

Um dem VPN-Zugang eine andere VPN-Richtlinie zuzuordnen, wählen Sie in *VPN-Zugänge* den VPN-Zugang aus und drücken Sie *Bearbeiten*.

Index