



## Überblick

---

- Merkmale, auf Seite 1
- Lieferumfang, auf Seite 3
- Positionen von Kensington-Schloss, Konformitätskennzeichnung, „Nicht stapeln“-Kennzeichnung, „Warnung vor heißer Oberfläche“-Kennzeichnung und QR-Code für das digitale Dokumentationsportal, auf Seite 4
- Vorderseite, auf Seite 7
- Management-Port, Konsolen-Ports und USB-Port, auf Seite 7
- Power-Taste und Reset-Taste, auf Seite 8
- Rückseite, auf Seite 9
- LEDs an der Rückseite, auf Seite 10
- Hardwarespezifikationen, auf Seite 12
- Unterstützte Transceiver, auf Seite 13
- Produkt-IDs, auf Seite 15
- Netzkabelspezifikationen, auf Seite 16

## Merkmale

Die Secure Firewall der Cisco 200-Serie ist eine wirtschaftliche, hocheffiziente Ergänzung unserer Firewall-Produktfamilie für das Einstiegssegment. Sie wurde für Unternehmenszweigstellen, Einzelhandelsunternehmen und kleinere Standorte entwickelt und bietet leistungsstarke, erschwingliche Sicherheit mit modernster Threat-Intelligence, Cloud-Security-Funktionen und optimierter Leistung für umfassenden Schutz auf Enterprise-Niveau.

Die Cisco Secure Firewall 220 ist eine kompakte Netzwerksicherheits-Appliance aus der Cisco Secure Firewall-Produktfamilie. Sie wird erstmals in Cisco Secure Firewall Threat Defense Version 10.0 und Cisco Secure ASA Version 9.24.1 unterstützt.

Weitere Informationen finden Sie im [Cisco Secure Firewall Threat Defense-Kompatibilitätsleitfaden](#) und im [Cisco Secure Firewall ASA-Kompatibilitätsleitfaden](#). Diese enthalten Informationen zur Kompatibilität der Cisco Firewall-Software und -Hardware jeder unterstützten Firewall-Version, einschließlich Anforderungen an Betriebssystem und Hosting-Umgebung.

Eine Liste der Produkt-IDs (PIDs) für die Firewall 220 finden Sie unter [Produkt-IDs, auf Seite 15](#).

Die folgende Abbildung zeigt die Cisco Secure Firewall 220.

Abbildung 1: CSF-220



In der folgenden Tabelle sind die Merkmale und Funktionen der Cisco Secure Firewall 220 aufgelistet.

Tabelle 1: Merkmale von CSF-220

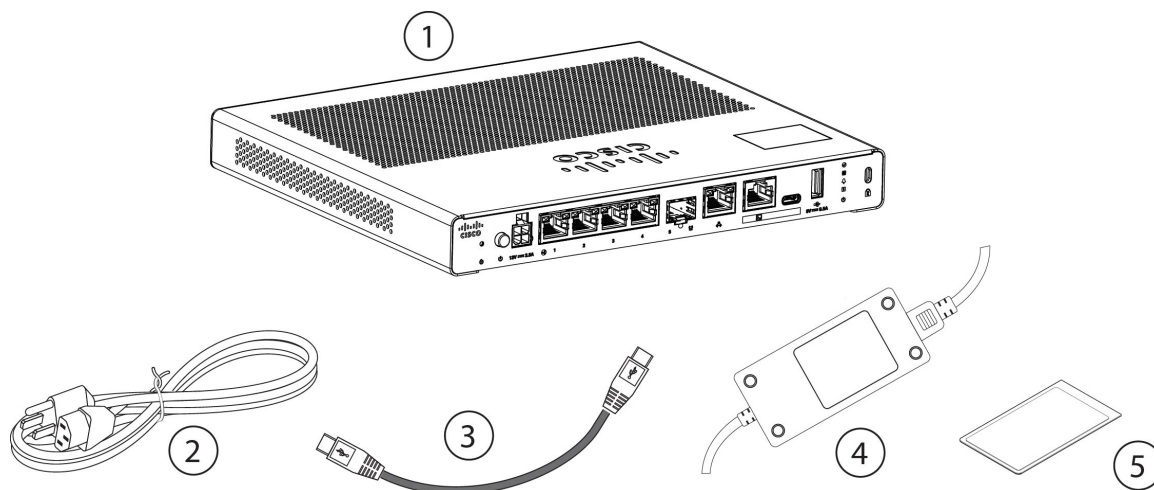
Merkmals	CSF-220
Formfaktor	Kompakt oder 1 HE für Rackmontage-Regal
Montage	<ul style="list-style-type: none"> <li>• Montage auf dem Schreibtisch (Standard)</li> <li>• Wandhalterung (bestellbares Kit)</li> <li>• Rackmontage-Regal (bestellbares Kit)</li> </ul>
Luftstromführung	Kein Lüfter <b>Hinweis</b> Da kein Lüfter vorhanden ist, darf das Chassis nicht gestapelt werden. Es wird erwartet, dass die Aufzeichnungen zur Systemtemperatur höher ausfallen als die in <a href="#">Hardwarespezifikationen, auf Seite 12</a> angegebene Umgebungstemperatur.
Management-Port	Ein Cisco RJ-45 mit 1 Gbit/s Beschränkt auf den Netzwerkverwaltungszugriff; Verbindung mit einem RJ-45-Kabel
Konsolen-Ports	Eine Cisco Seriennummer (RS-232 auf RJ-45) 1 x USB Typ C 2.0 Bietet Verwaltungszugriff über ein externes System
USB-Port	1 x USB Typ A 3.0 Für den Anschluss eines externen Geräts wie Speicher
Netzwerk-Anschlüsse	Vier RJ-45-Gigabit-Ethernet-Ports mit 1 Gbit/s
SFP-Ports (Small Form-Factor Pluggable)	Ein Port mit 1 Gbit/s

Merkmal	CSF-220
Unterstützte SFPs	Eine Liste der unterstützten SFPs mit 1 Gbit/s finden Sie unter <a href="#">Unterstützte Transceiver, auf Seite 13</a> .
PoE+-Ports	Nicht unterstützt
Reset-Taste	<p>Kleine versenkte Taste</p> <p>Drücken und halten Sie sie mit einem Stift 5 Sekunden lang. Dies setzt das Chassis nach dem nächsten Neustart auf den Standardstatus zurück.</p> <p><b>Hinweis</b> Alle Konfigurationsvariablen werden auf die werkseitigen Standardwerte zurückgesetzt. Der Flash-Speicher wird jedoch nicht gelöscht, und es werden keine Dateien entfernt.</p>
Schlitz für Sicherheitsschloss	Kensington T-Verriegelungsmechanismus zur Sicherung des Chassis
Power-Taste	Befindet sich links der E/A-Seite (Rückseite)
Netzkabelsteckdose	<p>IEC320-C14</p> <p>Eine Liste der unterstützten Netzkabel finden Sie unter <a href="#">Netzkabelspezifikationen, auf Seite 16</a>.</p>
Wechselspannungsnetzteil (AC)	Extern +12 V bei 30 W
Speicher	<p>Nur interne Komponente; nicht vor Ort austauschbar.</p> <p>Zum Austausch des Speichers muss das Chassis an Cisco zurückgesendet werden. Weitere Informationen finden Sie im <a href="#">Cisco Returns Portal</a>.</p>
GummifüÙe	Für Stabilität und Kühlung

## Lieferumfang

Die folgende Abbildung zeigt den Lieferumfang für die Cisco Secure Firewall 220. Beachten Sie, dass dieser jedoch variieren und Ihr Paket mehr oder weniger Artikel enthalten kann.

Abbildung 2: Lieferumfang von CSF-220



<p><b>1</b> Chassis (1 HE)</p>	<p><b>2</b> Netzkabel Eine Liste der zugelassenen Netzkabel finden Sie unter <a href="#">Netzkabelspezifikationen, auf Seite 16</a>.</p>
<p><b>3</b> USB-C-zu-USB-C-Konsolenkabel (~2 m) PID: CAB-CONS-USB-C optional: im Lieferumfang enthalten, sofern bestellt</p>	<p><b>4</b> Netzteil</p>
<p><b>5</b> <i>Cisco Secure Firewall 200</i> Dieses Dokument enthält Links zum Hardware-Installationshandbuch, zum Handbuch zu gesetzlichen Auflagen und Sicherheitshinweisen sowie zu Garantie- und Lizenzierungsinformationen. Es enthält außerdem einen QR-Code und eine URL, die auf das Portal für digitale Dokumentation verweisen. Das Portal enthält Links zur Seite mit Produktinformationen, zum Hardwareinstallationshandbuch, zum Handbuch zu gesetzlichen Vorschriften und Sicherheitsinformationen, zum Leitfaden zu den ersten Schritten sowie zum Leitfaden zur Zero-Touch-Bereitstellung.</p>	<p>—</p>

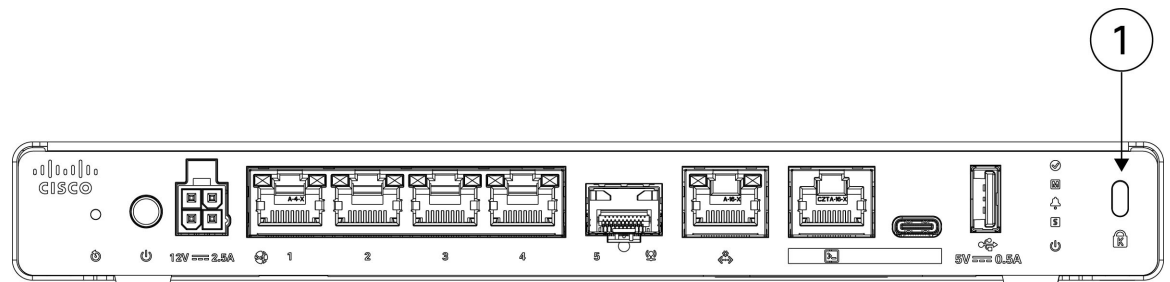
## Positionen von Kensington-Schloss, Konformitätskennzeichnung, „Nicht stapeln“-Kennzeichnung,

# „Warnung vor heißer Oberfläche“-Kennzeichnung und QR-Code für das digitale Dokumentationsportal

Das Chassis verfügt über ein Kensington-Schloss, für das ein standardmäßiger Kensington-T-Verriegelungsmechanismus zur Sicherung des Chassis verwendet werden kann.

Die folgende Abbildung zeigt die Position auf dem CSF-220.

**Abbildung 3: Kensington-Schloss am CSF-220-Chassis**

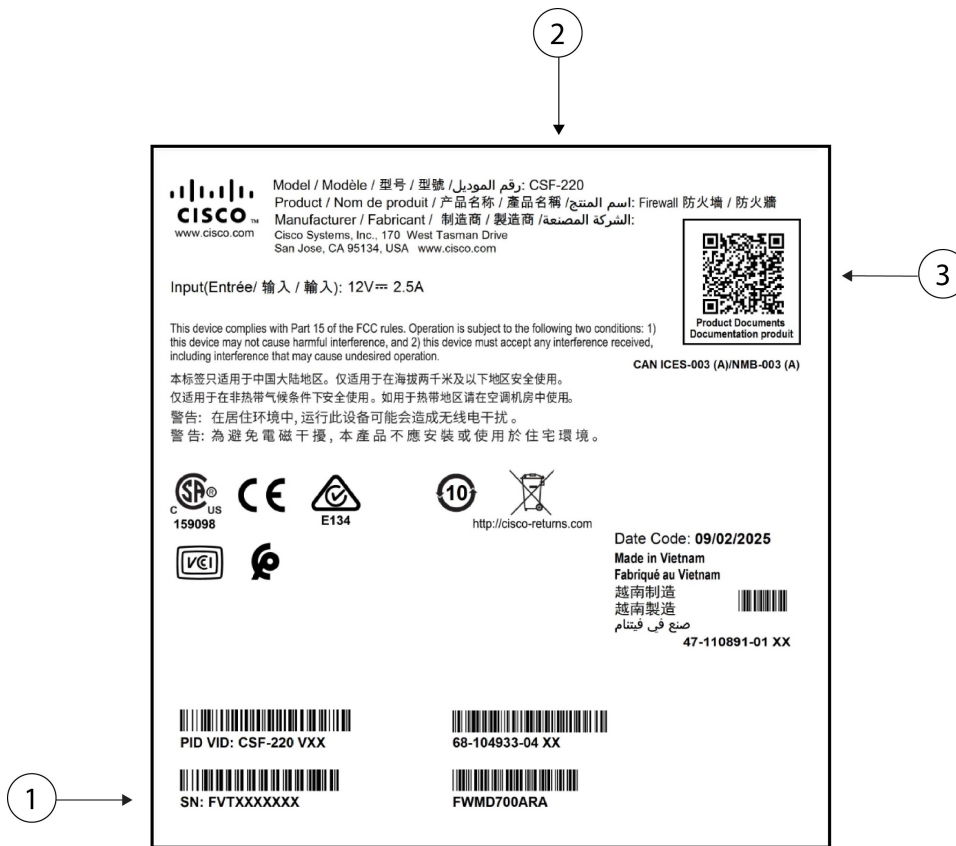


<b>1</b>	Kensington-Schloss oben rechts an der Rückseite (E/A) des Chassis	—
----------	---	---

Das Konformitätsschild an der Unterseite des Chassis enthält die Chassis-Seriennummer, gesetzliche Konformitätskennzeichnungen und den QR-Code des Digital Documentation Portal, der auf den Leitfaden zu den ersten Schritten, den Leitfaden zu rechtlichen Anforderungen und zur Konformität, den Leitfaden zur Zero-Touch-Bereitstellung und den Hardwareinstallationsleitfaden verweist.

Die folgende Abbildung zeigt ein Beispiel für ein Konformitätsschild, das sich an der Unterseite des CSF-220-Chassis befindet.

Abbildung 4: Konformitätsschild am CSF-220-Chassis



1	Chassis-Seriennummer	2	Chassis-Modellnummer
3	QR-Code des Portals für digitale Dokumentation		—

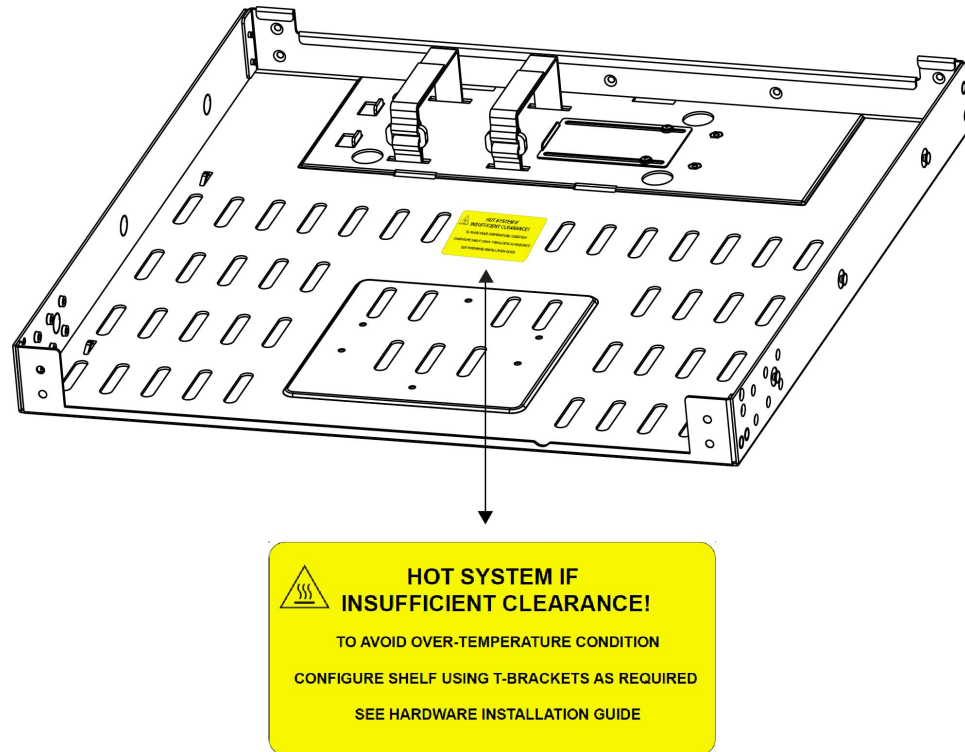
Die „Nicht stapeln“-Kennzeichnung befindet sich oben auf der Chassis-Abdeckung. Die folgende Abbildung zeigt die „Nicht stapeln“-Kennzeichnung.

Abbildung 5: „Nicht stapeln“-Kennzeichnung am Chassis



Die „Warnung vor heißer Oberfläche“-Kennzeichnung befindet sich auf dem Rackmontage-Einschub, wie in der folgenden Abbildung gezeigt.

Abbildung 6: „Warnung vor heißer Oberfläche“-Kennzeichnung am Rackmontage-Einschub



## Vorderseite

Die folgende Abbildung zeigt die Vorderseite der kompakten Appliance Secure Firewall 220. Beachten Sie, dass sich auf der Vorderseite keine Anschlüsse oder LEDs befinden.

Abbildung 7: Vorderseite von CSF-220



## Management-Port, Konsolen-Ports und USB-Port

### Management-Port

Das Chassis der Secure Firewall 220-Serie verfügt über einen Cisco RJ-45-Management-Port mit 1 Gbit/s. Dieser ist auf Zugriff für das Netzwerkmanagement beschränkt – die Verbindung erfolgt über ein RJ-45-Kabel.

### RJ-45-Konsolen-Ports

Die Secure Firewall 220 verfügt über zwei externe Konsolen-Ports, einen seriellen Cisco RJ-45-Port und einen seriellen USB-C-Port. Es kann jeweils nur ein Konsolen-Port aktiv sein. Der RJ-45-Port wird

deaktiviert, wenn ein Kabel an den USB-Konsolen-Port angeschlossen wird. Wird das USB-Kabel hingegen wieder vom USB-Port getrennt, wird der Port RJ-45 aktiviert. Die Konsolen-Ports haben keine Hardware-Flusskontrolle. Sie können mithilfe der CLI das Chassis über einen seriellen Konsolen-Port konfigurieren. Verwenden Sie dazu einen Terminal-Server oder ein Terminalemulationsprogramm über einen Computer.

- RJ-45-Port (8P8C): Unterstützt die RS-232-Signalübertragung an einen internen UART-Controller. Der RJ-45-Konsolen-Port unterstützt keine Remote-Einwahlmodems. Über einen Adapter kann die RJ-45-Verbindung bei Bedarf in eine DB9-Verbindung konvertiert werden.
- USB-Typ-C-Port: Ermöglicht die Verbindung mit einem USB-Port an einem externen Computer. USB-Kabel können mit dem Konsolen-Port verbunden und vom Port getrennt werden, ohne den Betrieb des Windows HyperTerminals zu beeinträchtigen. Abgeschirmte USB-Kabel mit ordnungsgemäßen Enden werden empfohlen. Die Standardeinstellung ist 9.600 Baud. Verwenden Sie diese Option für die Erstverbindung. Die Baudraten für den USB-Konsolen-Port sind 1.200, 2.400, 4.800, 9.600, 19.200, 38.400, 57.600 und 115.200 Bit/s.

### USB 3.0-Port, Typ A

Zur Ausstattung der Secure Firewall 220 gehört ein USB 3.0-Port vom Typ A, über den Sie ein externes Gerät anschließen können. Der USB-Port liefert eine Ausgangsleistung von 5 V und bis zu 0,5 A (2,5 W).

- Externes USB-Laufwerk (optional): An den externen USB-Port (Typ A) kann ein Datenspeichergerät angeschlossen werden. Die Kennung für das externe USB-Laufwerk lautet *disk1*. Beim Einschalten des Chassis wird ein angeschlossenes USB-Laufwerk als *disk1* gemountet und kann anschließend verwendet werden. Darüber hinaus sind die für *disk0* verfügbaren Dateisystembefehle auch für *disk1* verfügbar, einschließlich **copy**, **format**, **delete**, **mkdir**, **pwd**, **cd** usw.
- FAT-32-Dateisystem: Für das externe Laufwerk der Cisco Secure Firewall 220 und werden nur FAT-32-formatierte Dateisysteme unterstützt. Wenn Sie ein externes USB-Laufwerk anschließen, das nicht FAT-32-formatiert ist, kann das Laufwerk vom System nicht gemountet werden, und eine Fehlermeldung wird angezeigt. Sie können den Befehl **format disk1**: eingeben, um die Partition in FAT-32 zu formatieren und erneut als *disk1* zu mounten. Dabei können jedoch möglicherweise Daten verloren gehen.

## Power-Taste und Reset-Taste

### Power-Taste

Die Power-Taste befindet sich auf der linken Seite der Rückwand. Er regelt die Spannungsversorgung des Systems. Wenn die Wechselstromversorgung zum ersten Mal eingeschaltet wird, müssen Sie die Power-Taste nicht drücken, da das System standardmäßig eingeschaltet wird. Das System ist AUS, wenn die Taste herausragt, und EIN, wenn die Taste eingedrückt wird. Während des Abschaltvorgangs blinkt die Betriebsanzeige-LED grün und zeigt an, dass der Vorgang gestartet wurde. Sobald das Herunterfahren abgeschlossen ist, wird das System ausgeschaltet. Warten Sie, bis die Betriebsanzeige-LEDs erlöschen, bevor Sie die Wechselstromkabel abziehen. Unter [LEDs an der Rückseite, auf Seite 10](#) finden Sie eine detaillierte Beschreibung der Betriebsanzeige-LED.

Bei der ROMMON- oder FX-OS-Eingabeaufforderung:

- Halten Sie die Power-Taste 5 Sekunden lang gedrückt und lassen Sie sie los, um einen Neustart einzuleiten. Die Betriebsanzeige-LED blinkt grün mit einer Frequenz von 2 Hz.

- Halten Sie die Power-Taste 15 Sekunden lang gedrückt und lassen Sie sie los, um ein ordnungsgemäßes Herunterfahren einzuleiten. Die Betriebsanzeige-LED blinkt grün mit einer Frequenz von 10 Hz.



**Hinweis** Threat Defense erfordert ein ordnungsgemäßes Herunterfahren. Einzelheiten zur Vorgehensweise finden Sie im [Leitfaden zu den ersten Schritten](#).



**Vorsicht** Wenn Sie die Netzkabel des Systems abziehen, bevor das ordnungsgemäße Herunterfahren abgeschlossen ist, kann die Festplatte beschädigt werden. Sie können den Netzschalter vor dem Herunterfahren auf „OFF“ (AUS) stellen. Das System ignoriert dies.



**Hinweis** Nachdem Sie das Chassis von der Stromversorgung getrennt haben, warten Sie mindestens 10 Sekunden, bevor Sie die Stromversorgung wieder einschalten. Lassen Sie das System, einschließlich der Standby-Stromversorgung, 10 Sekunden lang ausgeschaltet.

#### Taste zum Zurücksetzen auf die Werkseinstellungen

Das Chassis verfügt über eine versenkte Reset-Taste zum Zurücksetzen des Systems auf die Werkseinstellungen. Sie können sie betätigen, indem Sie sie mit einem Stift 5 Sekunden lang drücken und halten. Beim nächsten Neustart wird das Chassis auf die Standardeinstellungen zurückgesetzt.



**Hinweis** Verwenden Sie die Reset-Taste, wenn die aktuellen Anmeldeinformationen verloren gegangen sind und Sie das System ohne Konsolenzugriff initialisieren möchten.



**Hinweis** Alle Konfigurationsvariablen werden auf die werkseitigen Standardwerte zurückgesetzt. Der Flash-Speicher wird jedoch nicht gelöscht, und es werden keine Dateien entfernt.

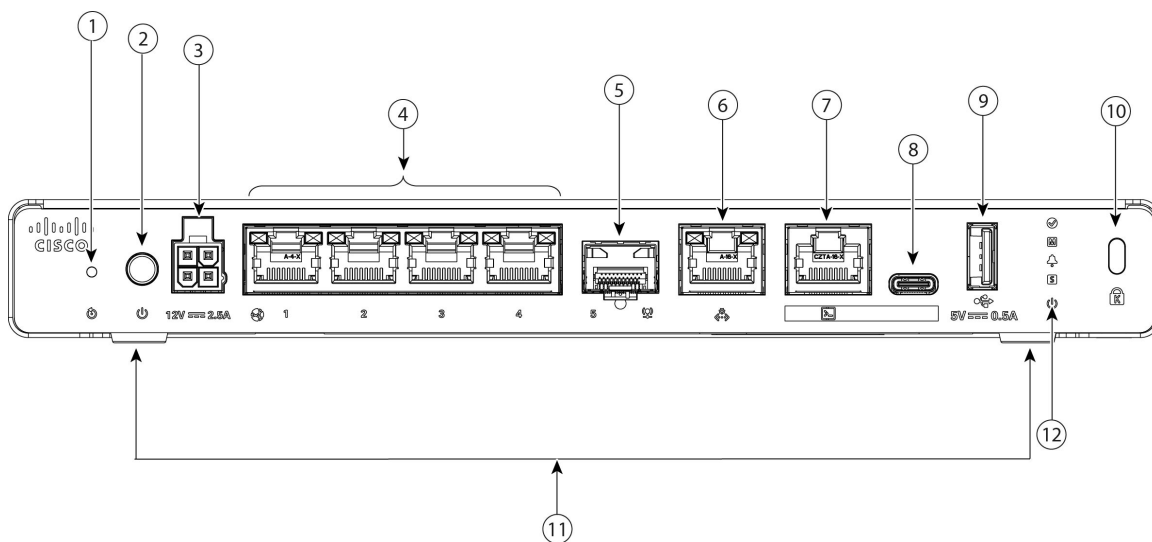


**Hinweis** Wenn die Stromversorgung zwischen dem Drücken der Reset-Taste und dem Abschluss des Zurücksetzvorgangs unterbrochen wird, stoppt der Prozess, und Sie müssen die Taste erneut drücken, sobald das System wieder mit Strom versorgt wird.

## Rückseite

Die folgende Abbildung zeigt die Rückseite der Cisco Secure Firewall 220. Unter [LEDs an der Rückseite](#), auf [Seite 10](#) finden Sie eine Beschreibung der LEDs.

Abbildung 8: Rückseite von CSF-220



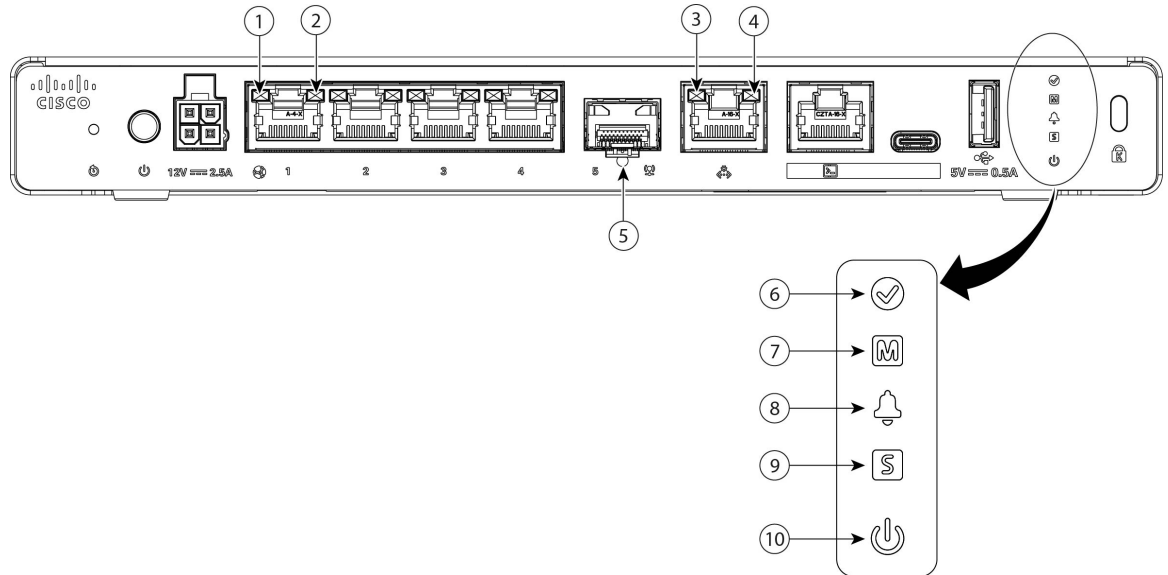
1	Reset-Taste	2	Power-Taste Die Power-Taste ist ein Schalter mit zwei Stellungen. Wenn er herausragt, befindet er sich im Status AUS, wenn er hineingedrückt ist, befindet er sich im Status EIN.
3	Netzkabelsteckdose	4	Ethernet-Ports 1–4 1G/100M/10M Base-T-Schnittstellen mit Auto-Duplex/Auto MDI-X
5	SFP-Port (1 Gbit/s)	6	Management-Port
7	Konsolen-Port RJ-45	8	Serieller Konsolen-Port (USB Typ C)
9	USB-Port (Typ A)	10	Kensington-Schloss
11	GummifüÙe	12	Status-LEDs

## LEDs an der Rückseite

Die LEDs befinden sich an Rückseite der Secure Firewall 220.

Die folgende Abbildung zeigt die LEDs an der Rückseite der Secure Firewall 220 und beschreibt deren Status.

Abbildung 9: LEDs an Rückseite der CSF-220



<p><b>1 Netzwerk</b></p> <p>Status der Netzwerk-Ports:</p> <p>Link-Status (L):</p> <ul style="list-style-type: none"> <li>• Aus: Kein Link oder Port wird nicht verwendet.</li> <li>• Grün: Link hergestellt.</li> <li>• Grün blinkend: Link-Aktivität.</li> </ul>	<p><b>2 Netzwerk</b></p> <p>Status der Netzwerk-Ports:</p> <p>Aktivitätsstatus (R):</p> <ul style="list-style-type: none"> <li>• Aus: Keine Netzwerkaktivität.</li> <li>• Grün: Netzwerkaktivität.</li> </ul>
<p><b>3 Management</b></p> <p>Status der Management-Ports:</p> <p>Link-Status (L):</p> <ul style="list-style-type: none"> <li>• Aus: Kein Link oder Port wird nicht verwendet.</li> <li>• Grün: Verbindung wurde hergestellt.</li> <li>• Grün blinkend: Link-Aktivität.</li> </ul>	<p><b>4 Management</b></p> <p>Status der Management-Ports:</p> <p>Aktivitätsstatus (R):</p> <ul style="list-style-type: none"> <li>• Grün blinkend: einmal alle drei Sekunden = 10 Mbit/s.</li> <li>• Grün blinkend: zweimal schnell = 100 Mbit/s.</li> <li>• Grün blinkend: dreimal schnell = 1000 Mbit/s.</li> </ul>

<p><b>5 SFP</b></p> <p>Status des SFP-Ports:</p> <ul style="list-style-type: none"> <li>• Aus: Keine SFP vorhanden.</li> <li>• Gelb: Ein SFP ist vorhanden, aber es wurde keine Verbindung hergestellt.</li> <li>• Grün blinkend: Link hergestellt und Übertragung.</li> </ul>	<p><b>6 Aktiv</b></p> <p>Status des Failover-Paares:</p> <ul style="list-style-type: none"> <li>• Aus: Gerät im Standby-Modus.</li> <li>• Grün: Gerät in aktivem Modus.</li> </ul>
<p><b>7 Verwaltet</b></p> <p>Cloud-Verbindungsstatus für Zero-Touch-Bereitstellung:</p> <ul style="list-style-type: none"> <li>• Grün, langsam blinkend (zweimal in 5 Sekunden): Cloud ist verbunden.</li> <li>• Grün und gelb, blinkend: Cloud-Verbindungsfehler.</li> <li>• Grün: Cloud ist nicht verbunden.</li> </ul>	<p><b>8 Alarm</b></p> <ul style="list-style-type: none"> <li>• Aus: Keine Alarme.</li> <li>• Gelb: Umgebungsfehler.</li> </ul>
<p><b>9 System</b></p> <p>Systembetriebsstatus:</p> <ul style="list-style-type: none"> <li>• Aus: Bootvorgang noch nicht ausgeführt.</li> <li>• Grün, schnell blinkend: Bootvorgang wird ausgeführt.</li> <li>• Grün: Normale Systemfunktion.</li> <li>• Gelb: Kritischer Alarm, der mindestens eines der folgenden Ereignisse anzeigt: <ul style="list-style-type: none"> <li>• Vollständiger Ausfall einer Hardware- oder Software-Komponente.</li> <li>• Übermäßig hohe Temperatur.</li> <li>• Spannung außerhalb des Toleranzbereichs.</li> </ul> </li> </ul>	<p><b>10 Spannung</b></p> <p>Netzteilstatus:</p> <ul style="list-style-type: none"> <li>• Aus: Stromversorgung ausgeschaltet.</li> <li>• Grün: Stromversorgung eingeschaltet.</li> <li>• Grün, blinkend: System wird ordnungsgemäß heruntergefahren.</li> <li>• Gelb: Stromversorgung des Systems funktioniert und IO-MCU wird aktualisiert (nimmt bis zu 3 Minuten in Anspruch), oder es liegt ein Fehler bei der Stromversorgung vor.</li> </ul>

## Hardwarespezifikationen

In der folgenden Tabelle sind die Hardwarespezifikationen für die Cisco Secure Firewall 220 aufgeführt.

Tabelle 2: Hardwarespezifikationen

Spezifikation	CSF-220
Chassis-Abmessungen (H x B x T)	2,9 x 23,4 x 19,8 cm (1,15 x 9,2 x 7,8 Zoll)
Chassis-Gewicht	1,18 kg (2,6 lb)
Abmessungen des Rackmontage-Regals (H x B x T)	1,7 x 17,3 x 15,7 Zoll ( 4,3 x 43,9 x 39,9 cm)
Spannungsversorgung des Systems	Maximale Leistung 19 W
Temperatur	Betrieb: 0 bis 40 °C (32 bis 104 °F)  Die maximale Betriebstemperatur verringert sich um 1,5 °C (2,7 °F) pro 304,8 m (1.000 ft) Anstieg ü. NN. Die maximale Einsatzhöhe beträgt 3.048 m (10.000 ft) ü. NN.  Ruhezustand: -25 bis 70 °C (-13 bis 158 °F)  Ruhezustand: Maximale Höhenlage 4.570 m (15.000 ft)
Luftfeuchtigkeit	Betrieb: 5 bis 85 %, nicht kondensierend  Ruhezustand: 5 bis 95 % (nicht kondensierend)
Höhenlage	Betrieb: 0 bis 3.048 m (10.000 ft)  Ruhezustand: 0 bis 4.570 m (15.000 ft)

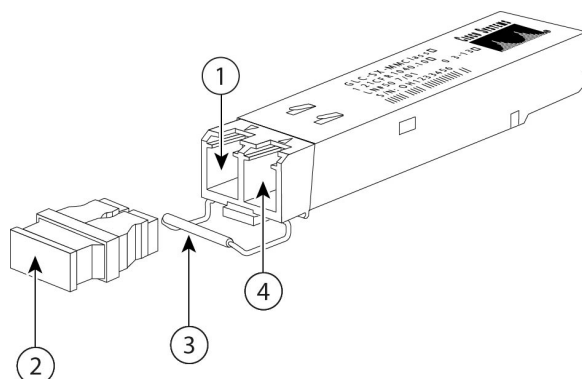
## Unterstützte Transceiver

Der SFP-Transceiver ist ein bidirektionales Gerät, bei dem sich Sender und Empfänger im selben Gehäuse befinden. Es handelt sich um eine Hot-Swap-fähige, optische oder elektrische (Kupfer-)Schnittstelle, die an die SFP-Ports an den fest konfigurierten Ports angeschlossen wird und Ethernet-Verbindungen ermöglicht.

Weitere Informationen finden Sie im [Datenblatt zu Cisco SFP-Modulen für Gigabit-Ethernet-Anwendungen](#).

Die folgende Abbildung zeigt die Komponenten eines Transceivers.

Abbildung 10: SFP-Transceiver



1	Optischer Anschluss (Empfangen)	2	Staubschutzkappe
3	Verschluss	4	Optischer Anschluss (Senden)

### Sicherheitswarnungen

Beachten Sie die folgenden Warnhinweise:



#### Warnung Anweisung 1055 – Laser der Klasse 1/1M

Unsichtbare Laserstrahlung ist vorhanden. Setzen Sie BenutzerInnen von Teleskopoptiken keinem Risiko aus. Dies gilt für Laserprodukte der Klasse 1/1M.



#### Warnung Anweisung 1056 – Nicht abgeschlossenes Glasfaserkabel

Von nicht abgeschlossenen Faserkabeln oder Anschlüssen kann unsichtbare Laserstrahlung ausgehen. Blicken Sie nicht direkt mit optischen Instrumenten darauf. Das Betrachten des Laserausgangs mit bestimmten optischen Geräten (Lupen, Vergrößerungsgläser, Mikroskop usw.) in einem Abstand von 100 mm kann zu Augenschäden führen.



#### Warnung Anweisung 1057 – Freisetzung gefährlicher Strahlung

Die Verwendung von Kontrollen, Anpassungen oder die Durchführung von Verfahren, die sich von den hier angegebenen unterscheiden, kann/können zur Freisetzung gefährlicher Strahlung führen.

**Warnung**

Wenden Sie beim Einlegen des Transceivers geeignete Schutzmaßnahmen gegen elektrostatische Entladungen (ESD) an. Vermeiden Sie es, die Kontakte auf der Rückseite zu berühren, und halten Sie die Kontakte und Ports frei von Staub und Schmutz. Bewahren Sie ungenutzte Transceiver zum Schutz vor elektrostatischer Entladung in der Verpackung auf, in der sie versendet wurden.

**Vorsicht**

SFP anderer Hersteller sind zwar zulässig, aber wir empfehlen deren Verwendung nicht, da sie nicht von Cisco getestet und validiert wurden. Cisco TAC kann den Support für jegliche Interoperabilitätsprobleme verweigern, die aus der Verwendung eines ungetesteten Dritt-SFP-Transceivers hervorgehen.

In der folgenden Tabelle sind die SFPs aufgeführt, die an den festen Ports der Secure Firewall 220 unterstützt werden.

**Tabelle 3: Feste Ports von CSF-220**

Port-Typ	Transceiver-PID	Erste unterstützte Version
Feste SFP-Ports	<ul style="list-style-type: none"> <li>• GLC-TE=</li> <li>• GLC-SX-MMD=</li> <li>• GLC-LH-SMD=</li> <li>• GLC-EX-SMD=</li> <li>• GLC-GE-100FX=</li> <li>• GLC-FE-100FX-RGD=</li> </ul>	Threat Defense 10.0/ASA 9.24

## Produkt-IDs

In der folgenden Tabelle sind die PIDs der vor Ort austauschbaren Komponenten für die kompakte Appliance Secure Firewall 220 aufgeführt. Diese Ersatzkomponenten können Sie unabhängig von der Appliance bestellen. Wenn interne Komponenten ausfallen, müssen Sie eine Retouren genehmigung (Return Material Authorization, RMA) für das gesamte Chassis einholen. Weitere Informationen finden Sie im [Cisco Returns Portal](#).

**Hinweis**

Einzelheiten zum Befehl **show inventory** finden Sie in der [Befehlsreferenz zu Cisco Secure Firewall Threat Defense](#) oder der [Befehlsreferenz zur Cisco Secure Firewall ASA-Serie](#). Darin können Sie nachlesen, wie Sie mit diesem Befehl die PIDs für Ihre Secure Firewall 220 anzeigen können.

**Tabelle 4: PIDs für CSF-220**

PID	Beschreibung
CSF220-ASA-K9	Kompakte Desktop-Appliance Secure Firewall 220, ASA

PID	Beschreibung
CSF220-TD-K9	Kompakte Desktop-Appliance Secure Firewall 220, NGFW
CSF220-PWR-AC	Netzteil für Secure Firewall 220, 30 W Wechselstrom (12 V)
CSF220-PWR-AC=	Netzteil für Secure Firewall 220, 30 W Wechselstrom (12 V) (Ersatzteil)
CSF200-WALL-MNT=	Wandmontage-Kit der Secure Firewall 200-Serie (Ersatzteil)
CSF200-RCKMNT-FX=	Rackmontage-Kit mit festen Halterungen der Secure Firewall 200-Serie (Ersatzteil)
CSF200-RCKMNT-SR=	Rackmontage-Kit mit Gleitschienen der Secure Firewall 200-Serie (Ersatzteil)
CSF200-CBL-MGMT=	Kabelführungsklammer-Kit der Secure Firewall 200-Serie (Ersatzteil)

## Netzkabelspezifikationen

Standardnetzkabel oder Jumper-Kabel sind für die Verbindung mit der Sicherheits-Appliance verfügbar. Die Jumper-Kabel für den Einsatz in Racks sind als Alternative zu den Standard-Netzkabeln erhältlich.

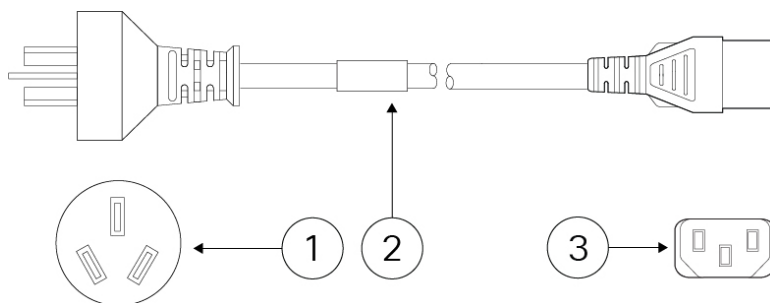
Wenn Sie das optionale Netzkabel nicht zusammen mit dem System bestellen, übernehmen Sie die Verantwortung für die Auswahl des richtigen Netzkabels für das Produkt. Die Verwendung eines nicht kompatiblen Netzkabels mit diesem Produkt kann zu elektrischen Sicherheitsrisiken führen. Bei Bestellungen, die nach Argentinien, Brasilien und Japan ausgeliefert werden, muss das jeweilige Netzkabel zusammen mit dem System bestellt werden.



**Hinweis** Es werden nur die genehmigten Netzkabel oder Jumper-Netzkabel unterstützt, die mit dem Chassis mitgeliefert werden.

Folgende Netzkabel werden unterstützt.

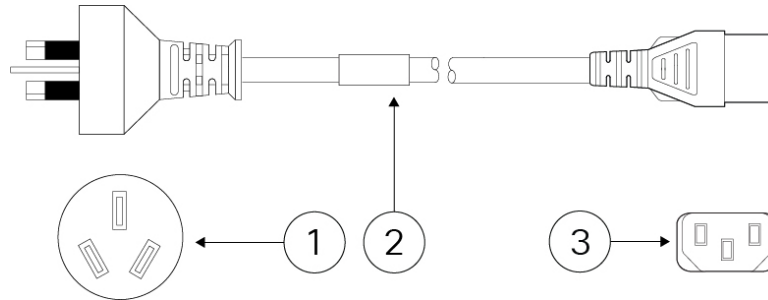
**Abbildung 11: Argentinien (CAB-250V-10A-AR)**



<b>1</b>	Stecker: VA2073	<b>2</b>	Kabelnennwerte: 10 A, 250 V
----------	-----------------	----------	-----------------------------

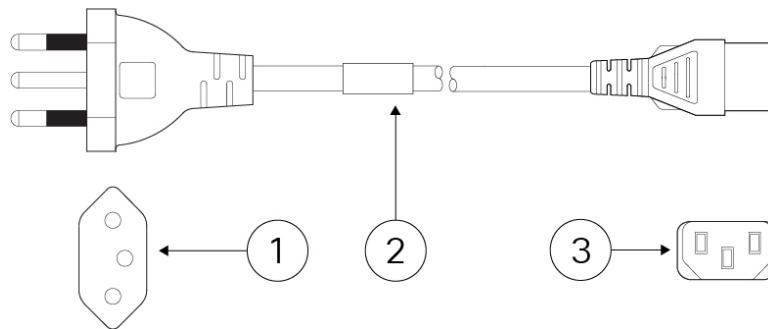
<b>3</b>	Steckverbinder: V1625	—
----------	-----------------------	---

**Abbildung 12: Australien/Neuseeland (CAB-ACA)**



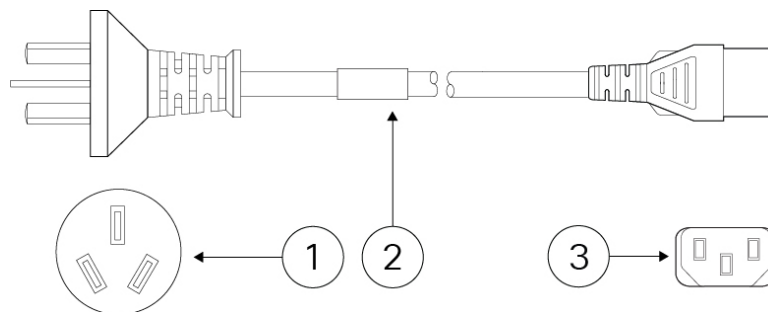
<b>1</b>	Stecker: AU10LS3	<b>2</b> Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625	—

**Abbildung 13: Brasilien (CAB-C13-ACB)**



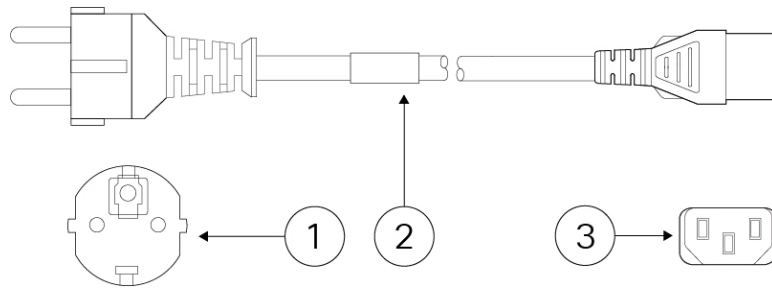
<b>1</b>	Stecker: NBR 14136	<b>2</b> Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: EL 701B (EN 60320/C13)	—

**Abbildung 14: China (CAB-ACC)**



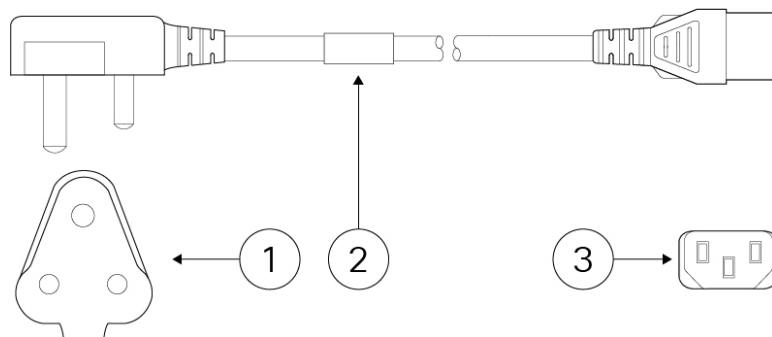
<b>1</b>	Stecker: V3203C	<b>2</b> Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625	—

Abbildung 15: Europa (CAB-ACE)



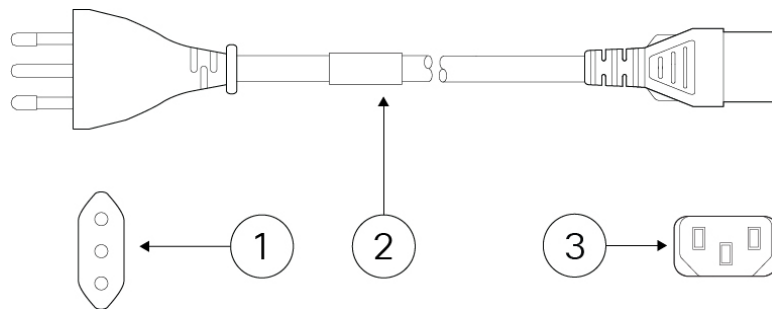
1	Stecker: M2511	2	Kabelnennwerte: 16 A, 250 V
3	Steckverbinder: V1625		—

Abbildung 16: Indien (CAB-IND-10A)



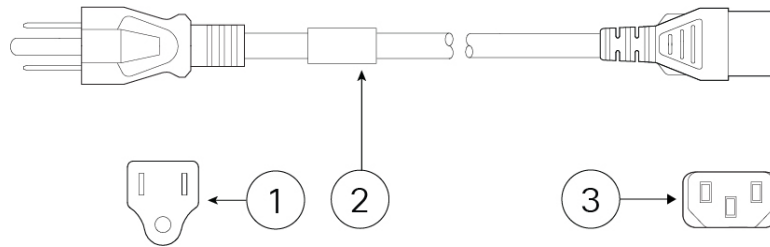
1	Stecker: IA16A3-C	2	Kabelnennwerte: 16 A, 250 V
3	Steckverbinder: V1625BS-E		—

Abbildung 17: Italien (CAB-ACI)



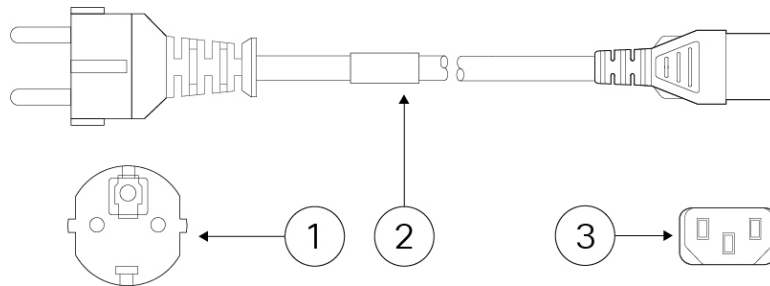
1	Stecker: IT10S3	2	Kabelnennwerte: 10 A, 250 V
3	Steckverbinder: V1625		—

**Abbildung 18: Japan (CAB-JPN-3PIN)**



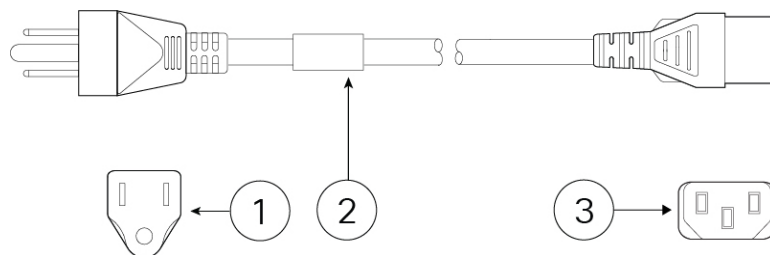
<b>1</b>	Stecker: M744	<b>2</b>	Kabelnennwerte: 12 A, 125 V
<b>3</b>	Steckverbinder: V1625		—

**Abbildung 19: Korea (CAB-AC-C13-KOR)**



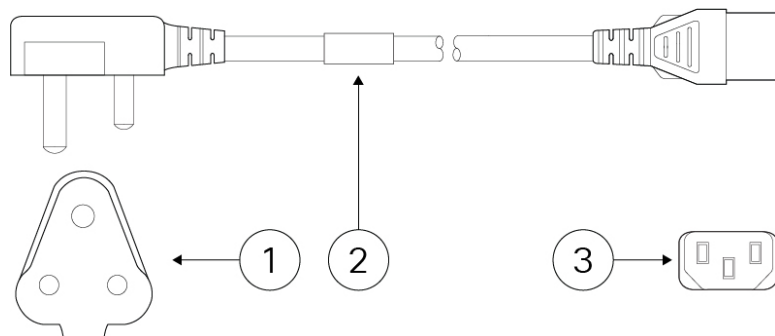
<b>1</b>	Stecker: M2511	<b>2</b>	Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625		—

**Abbildung 20: Nordamerika (CAB-AC)**



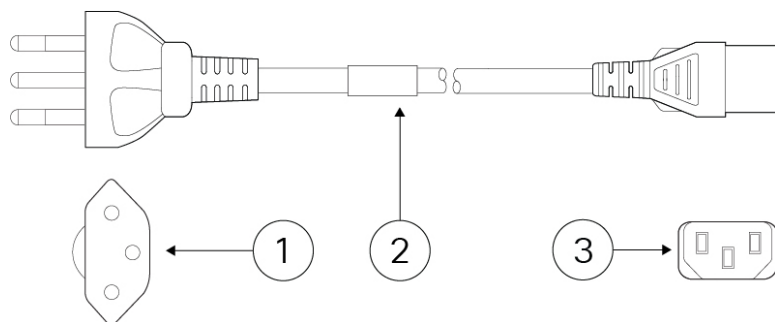
<b>1</b>	Stecker: PS204	<b>2</b>	Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625		—

**Abbildung 21: Südafrika (AIR-PWR-CORD-SA)**



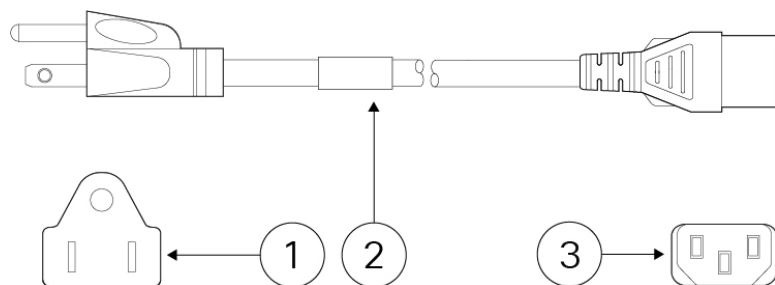
<b>1</b>	Stecker: SA16A	<b>2</b>	Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625		—

**Abbildung 22: Schweiz (CAB-ACS)**



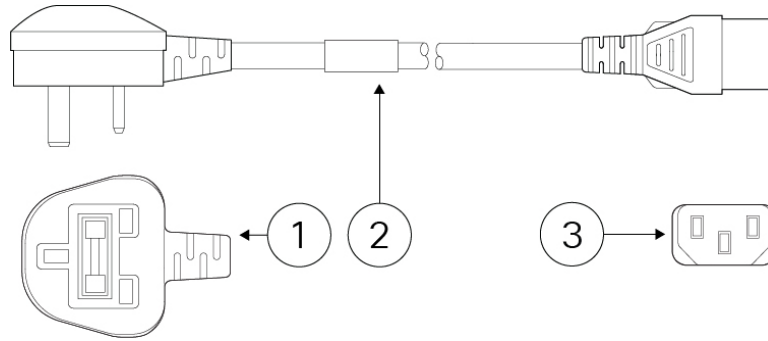
<b>1</b>	Stecker: SW10ZS3	<b>2</b>	Kabelnennwerte: 10 A, 250 V
<b>3</b>	Steckverbinder: V1625		—

**Abbildung 23: Taiwan (CAB-ACTW)**



<b>1</b>	Stecker: EI 302 (CNS10917)	<b>2</b>	Kabelnennwerte: 10 A, 125 V
<b>3</b>	Steckverbinder: EL 701 (EN 60320/C13)		—

Abbildung 24: Vereinigtes Königreich (CAB-ACU)



1	Stecker: 3P BS 1363	2	Kabelnennwerte: 10 A, 250 V
3	Steckverbinder: IEC 60320/C13		—



Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.