SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Hilfe (iOS)

Produktversion: 9.6

Inhalt

1 Barrierefreiheit

Sophos Intercept X for Mobile entspricht den Richtlinien für barrierefreie Webinhalte (WCAG) 2.1, Stufe AA. Weitere Informationen zu diesen Richtlinien finden Sie unter „Verwandte Informationen“.

Wir empfehlen Ihnen Sophos Intercept X for Mobile mit dem VoiceOver-Bildschirmleser und der Zoom-Lupen-Software zu verwenden, die auf iOS-Geräten vorhanden sind. Sie finden Links zur Verwendung von VoiceOver und Zoom unter „Verwandte Informationen“. Wenn Sie weitere Hilfe zu VoiceOver oder Zoom benötigen, können Sie sich an den technischen Support von Apple wenden.

Wenn Sie technische Hilfsmittel mit unserer Software verwenden wollen, empfehlen wir Ihnen, sich mit der Funktionsweise Ihres ausgewählten Produkts und den verfügbaren Tastaturbefehlen vertraut zu machen.

Verwandte Informationen

Richtlinien für barrierefreie Webinhalte

iPhone Benutzerhandbuch: Aktivieren und Einüben von VoiceOver auf dem iPhone

iPhone Benutzerhandbuch: Einzoomen auf dem iPhone-Bildschirm

2 Über Sophos Intercept X for Mobile

Sophos Intercept X for Mobile hilft Ihnen, sicher auf Ihrem iPhone oder iPad zu arbeiten.

Wenn Sie das Sophos-Symbol berühren und gedrückt halten, erhalten Sie ein Menü mit Quick Actions. Auf einem 3D-Touch-Gerät können Sie kurz auf das Symbol drücken, um das Menü anzuzeigen.

3 Die Seite „Übersicht“

Die Übersichtsseite von Sophos Intercept X for Mobile gibt Ihnen einen Überblick über den Gerätestatus.

Funktionen haben je nach Status unterschiedliche Farben:

- Grün: Keine Probleme gefunden
- Rot: Probleme gefunden
- Blau: Funktion ist aktiviert
- Grau: Die Funktion ist ausgeschaltet oder nicht konfiguriert

4 Gerätesicherheit

Unter **Gerätesicherheit** wird der Integritätsstatus des Gerätes angezeigt.

Sophos Intercept X for Mobile zeigt folgende Informationen an:

- Allgemeine Geräteinformationen wie Modellbezeichnung und iOS-Version.
- Update-Empfehlungen, wenn Sie nicht die neueste verfügbare iOS-Version installiert haben.
- Jailbreak-Informationen, wenn Sophos Intercept X for Mobile einen Jailbreak auf dem Gerät erkannt hat.

5 Web Filtering

Ihr Unternehmen kann Web Filtering verwenden um Sie vor Internetseiten mit schädlichem, unerwünschtem oder illegalem Inhalt zu schützen.

Wenn Ihr Unternehmen Ihr Gerät verwaltet, kann es Arten von Websites angeben, vor denen Sie gewarnt werden, bevor Sie sie öffnen oder Websites blockieren. Dies schützt Sie vor Seiten mit schädlichem, unerwünschtem oder illegalem Inhalt.

Auf dem Dashboard ist Web Filterung unter **Netzwerksicherheit** verfügbar.

Hinweis

- Ihr Unternehmen muss diese Funktion aktivieren.

Die Liste **Erlaubt**

Sie können Warnung vor bestimmten schädlichen oder kategorisierten Seiten dauerhaft unterdrücken. Dies ist nützlich, wenn eine der Seiten, die Sie oft besuchen, in eine Kategorie fällt, für die Sie bei Zugriff gewarnt werden. Wischen Sie die **Web request blocked** Benachrichtigung nach unten und tippen Sie auf **Add to allow list**.

Unter **Erlaubt** wird die Anzahl der erlaubten Seiten angezeigt. Tippen Sie auf die Zahl, um alle Seiten anzuzeigen.

Von Ihnen hinzugefügte Einträge und von Ihrer Organisation vordefinierte Einträge werden in separaten Abschnitten angezeigt.

Um eine Seite wieder zu filtern, wischen Sie den Eintrag nach links um ihn zu löschen. Sie können dies nur für Einträge tun, die Sie selbst hinzugefügt haben.

Die Liste **Blockiert**

Sie können Webseiten, für die eine Warnung ausgegeben wird, zu einer Liste hinzufügen, damit diese immer gesperrt werden. Wischen Sie die **Web request blocked** Benachrichtigung nach unten und tippen Sie auf **Add to block list**.

Unter **Blockiert** wird die Anzahl der blockierten Seiten angezeigt. Tippen Sie auf die Zahl, um alle Seiten anzuzeigen.

Von Ihnen hinzugefügte Einträge und von Ihrer Organisation vordefinierte Einträge werden in separaten Abschnitten angezeigt.

Um wieder eine Warnung anzuzeigen, wischen Sie den Eintrag nach links um ihn zu löschen. Sie können dies nur für Einträge tun, die Sie selbst hinzugefügt haben.

6 Wi-Fi Security

Mit Wi-Fi Security prüfen Sie Ihre WLAN-Verbindung auf netzwerkbasierte Bedrohungen.

Hinweis
Wenn Sophos Intercept X for Mobile bei Sophos Mobile registriert ist, wird diese Funktion von Ihrem Unternehmen verwaltet.

Auf dem Dashboard ist die Funkion Wi-Fi Security unter **Netzwerksicherheit** verfügbar.

Erkannte Bedrohungen

Sophos Intercept X for Mobile erkennt die folgenden Probleme:

ARP Spoofing	Bei „ARP Spoofing“ sendet ein Angreifer bösartige ARP-Nachrichten (Address Resolution Protocol) an Ihren Computer, um diesen glauben zu lassen, die MAC-Adresse des Angreifers wäre mit der IP-Adresse Ihres Netzwerk-Gateways verknüpft. Dies erlaubt ihm, auf Ihr privates Netzwerk zuzugreifen, vertrauliche Daten zu stehlen, und weitergehende Angriffe durchzuführen (z.B. „Denial Of Service“ oder „Man In The Middle“). ARP Spoofing kann nur auf Geräten bis einschließlich iOS 10.2.1 festgestellt werden.
Captive Portal	Ein „Captive Portal“ wird von öffentlichen WLAN-Netzwerken verwendet, um eine Authentifizierung durchzuführen, bevor der Netzwerkzugriff gewährt wird. Da der gesamte Datenverkehr über das Captive Portal umgeleitet wird, erhalten Sie möglicherweise weitere Warnungen.
Inhaltsmanipulation	Durch Inhaltsmanipulation verändert ein Angreifer den Inhalt einer Webseite so, dass Sie, ohne es zu merken, schädliche Aktionen ausführen. Dies erlaubt ihm zum Beispiel, Authentifizierungen zu umgehen oder Daten zu löschen.
SSL Interception	Bei „SSL Interception“ verwendet ein Angreifer ein falsches Server-Zertifikat, um die gesicherte Verbindung zwischen Ihrem Computer und einer Webseite abzuhören. Der Angreifer kann vertrauliche Daten entschlüsseln, während er Sie in dem Glauben lässt, die Verbindung wäre weiterhin gesichert.
SSL Stripping	Bei „SSL Stripping“ reduziert ein Angreifer das Sicherheitsniveau der Verbindung zu einer Webseite von sicherem HTTPS zu unsicherem HTTP. Der Angreifer kann den gesamten

Datenverkehr zwischen Ihrem Computer und der Webseite über seinen eigenen Proxy-Server umleiten. Dies erlaubt ihm, vertrauliche Daten zu verschlüsseln, während er Sie in dem Glauben lässt, Sie wären weiterhin über HTTPS verbunden.

Prüfungen durchführen

- Tippen Sie auf **WLAN prüfen**, um das WLAN zu überprüfen, mit dem Sie verbunden sind.
- Um Netzwerkprüfungen im Hintergrund durchzuführen, aktivieren Sie **Hintergrundprüfung**. Bei jedem Wechsel der Verbindung wird das neue WLAN automatisch geprüft.

Probleme ausblenden

Sie können WLAN-Probleme für bestimmte Netzwerke ausblenden. Ausgeblendete Probleme werden bei der Bestimmung des Integritätsstatus des Gerätes nicht berücksichtigt.

Um alle Probleme wieder anzuzeigen, wählen Sie **Alle WLAN-Probleme anzeigen** in den App-Einstellungen.

7 Authenticator

Mit Authenticator erstellen Sie Einmal-Kennwörter (Prüfcodes), mit denen Sie sich an Ihren Konten mit Mehrfaktor-Authentifizierung anmelden können.

Informieren Sie sich bei Ihrem Kontoanbieter, ob dieser eine Mehrfaktor-Authentifizierung unterstützt und wie dies für Ihr Konto aktiviert wird.

Authenticator unterstützt **zeitbasierte** und **zählerbasierte** Einmal-Kennwörter. Siehe Über Einmal-Kennwörter (Seite 8).

Um Authenticator zu starten, berühren und Sie das Sophos-Symbol und halten sie es gedrückt. Tippen Sie dann auf **Authenticator**.

Funktionen:

- Bei **zeitbasierten** Kennwörtern zeigt der Authenticator das aktuell gültige Einmal-Kennwort an, sowie ein animiertes Symbol, das anzeigt, wann der Code ungültig wird und ein neuer Code berechnet wird.
- Bei **zählerbasierten** Kennwörtern tippen Sie auf **Für Code tippen**, um den ersten Code zu erzeugen, bzw. auf **Weiter**, um den nächsten Code zu erzeugen. Damit Sie nicht versehentlich mehrere Codes hintereinander erzeugen können, wird die Schaltfläche nach jeder Codeerzeugung für einige Sekunden deaktiviert.
- Tippen Sie auf ein Einmal-Kennwort, um es in die Zwischenablage zu kopieren.
- Um die Kontodetails zu bearbeiten, tippen Sie auf **Bearbeiten**, wählen Sie das Konto aus und tippen Sie anschließend auf **Ändern**. Aus Sicherheitsgründen können Sie den Shared-Secret-Schlüssel eines bestehenden Kontos weder anzeigen noch ändern.
- Um ein Konto zu löschen, tippen Sie auf **Bearbeiten**, wählen Sie das Konto aus und tippen Sie anschließend auf das Symbol **Löschen** 🗑.

Warnung
Wenn Sie einen Authenticator-Eintrag löschen, verlieren Sie die Möglichkeit, Einmal-Kennwörter für dieses Konto zu erzeugen. Dadurch wird die Mehrfaktor-Authentifizierung nicht deaktiviert. Wenn Sie den Authenticator-Eintrag löschen, können Sie sich möglicherweise nicht mehr an diesem Konto anmelden.

Stellen Sie daher sicher, dass Sie eine alternative Möglichkeit haben, Einmal-Kennwörter zu erzeugen, bzw. eine alternative Möglichkeit, sich ohne Mehrfaktor-Authentifizierung an Ihrem Konto anzumelden.

7.1 Über Einmal-Kennwörter

Einmal-Kennwörter (auch Prüfcodes genannt) bestehen aus einer Ziffernfolge. Sie werden aus diesen Größen berechnet:

- Einem Shared-Secret-Schlüssel, den nur Ihr Kontoanbieter und Sie kennen.
- Spezifischen Berechnungsparametern Ihres Kontoanbieters.
- Einem fortlaufenden Zähler.

Wenn Sie ein Einmal-Kennwort verwenden, um sich zu authentisieren, erwartet Ihr Kontoanbieter ein Kennwort, das aus einem bestimmten Wert dieses Zählers berechnet wurde. Da Authenticator

den aktuellen Zählerwert nach denselben Regeln ermittelt wie Ihr Kontoanbieter, wird er Ihr Einmal-Kennwort akzeptieren.

Der Authenticator unterstützt **zeitbasierte** und **zählerbasierte** Einmal-Kennwörter. Diese Typen unterscheiden sich darin, wie der aktuelle Zählerwert bestimmt wird:

- **Zeitbasierte Einmal-Kennwörter** (TOTP, gemäß RFC 6238): Der Zählerwert wird ständig auf Basis der aktuellen Uhrzeit erhöht. Der nächste Prüfcode wird berechnet, wenn eine bestimmte Zeit verstrichen ist.
- **Zählerbasierte Einmal-Kennwörter** (HOTP, gemäß RFC 4226): Der Zählerwert wird bei Bedarf erhöht. Der nächste Prüfcode wird berechnet, wenn Sie dies anfordern.

7.2 Konto mit QR-Code hinzufügen

Verwenden Sie diese Methode, wenn Sie für Ihr Konto die Mehrfaktor-Authentifizierung aktiviert haben und Ihr Kontoanbieter Ihnen einen QR-Code mit den Konfigurationsdetails zur Verfügung gestellt hat.

1. Wählen Sie **Erzeugen > QR-Code scannen** aus.
2. Scannen Sie den QR-Code mit Ihrem Gerät.

Nachdem die App die Konfigurationsdetails aus dem QR-Code gelesen hat, wird ein neues Authenticator-Konto eingerichtet.

7.3 Konto manuell hinzufügen

Verwenden Sie diese Methode, wenn Sie für Ihr Konto die Mehrfaktor-Authentifizierung aktiviert haben und Ihr Kontoanbieter Ihnen eine Liste mit Konfigurationseinstellungen zur Verfügung gestellt hat.

1. Wählen Sie **Erzeugen > Manuell hinzufügen** aus.
2. Geben Sie im Feld **Name** einen Namen für das neue Authenticator-Konto ein.
3. Tippen Sie im Feld **Schlüssel** den Shared-Secret-Schlüssel ein, den Ihr Kontoanbieter angegeben hat. Dieser Schlüssel ist nur für Ihr Konto gültig und liefert die Berechnungsgrundlage für die Einmal-Kennwörter.
4. Wählen Sie im Feld **Typ** die Berechnungsmethode aus, die Ihr Kontoanbieter angegeben hat.
5. Falls Ihr Kontoanbieter weitere Einstellungen angegeben hat, geben Sie diese in den nachfolgenden Feldern ein.

   Achtung
   Füllen Sie nur die Felder aus, die Ihr Kontoanbieter angegeben hat.

   - Geben Sie im Feld **Zeitspanne** die Gültigkeitsdauer in Sekunden ein. Dieses Feld ist nur für zeitbasierte Einmal-Kennwörter verfügbar.
   - Wählen Sie im Feld **Code-Länge** die Ziffernanzahl des Einmal-Kennworts aus.
   - Wählen Sie im Feld **Hash-Algorithmus** aus, welcher Hash-Algorithmus für die Berechnung der Einmal-Kennwörter verwendet wird.
6. Optional: Wählen Sie im Feld **Hintergrundfarbe** eine Farbe für den Kontoeintrag aus, um diesen in der Kontenliste leichter identifizieren zu können.
7. Wenn Sie fertig sind, tippen Sie auf **Speichern** .

Ein neues Authenticator-Konto wird eingerichtet.

8 Password Safe

Mit Password Safe speichern Sie die Daten für alle Ihre Konten an einem gemeinsamen Ort, der durch ein Master-Kennwort geschützt ist.

Um Password Safe zu starten, berühren und halten Sie das Sophos-Symbol, und tippen Sie dann auf **Password Safe**.

Sie haben folgende Möglichkeiten:

- Eine neue Password-Safe-Datei erstellen.
- Eine vorhandene KeePass-KDBX-Datei importieren. Wenn Sie Kennwort-Einträge bearbeiten, wird nur die lokale Kopie geändert.
- Eine vorhandene KeePass-KDBX-Datei öffnen. Wenn Sie Kennwort-Einträge bearbeiten, wird die Originaldatei geändert.

Automatisches Ausfüllen von Passwörtern aktivieren

In iOS 12 und neuer können Sie Password Safe verwenden, um Passwörter automatisch auszufüllen.

Um **Automatisch ausfüllen** für Password Safe zu aktivieren:

1. Gehen Sie zur App **Einstellungen** und scrollen Sie nach unten zu **Passwörter & Accounts**.
2. Tippen Sie auf **Automatisch ausfüllen** und aktivieren Sie **Automatisch ausfüllen**.
3. Wählen Sie **Intercept X** unter **Ausfüllen erlauben von:**.

Sie können jetzt auf Password Safe zugreifen, indem Sie einfach auf **Passwörter** in der QuickType Leiste über der Tastatur tippen, wenn Sie zur Eingabe von Anmeldeinformationen aufgefordert werden.

8.1 Password-Safe-Eintrag erstellen

So erstellen Sie in einer Password-Safe-Datei einen Eintrag oder eine Eintragsgruppe:

1. Tippen Sie in Password Safe auf **Plus** ⊕.
2. Wählen Sie die Art des Eintrags, den Sie erstellen wollen:
   - **Konto hinzufügen** erstellt einen Eintrag mit vordefinierten Feldern, die für ein Internet-Konto oder ähnliches geeignet sind.
   - **Kreditkarte hinzufügen** erstellt einen Eintrag mit vordefinierten Feldern, die für Kreditkarteninformationen oder ähnliches geeignet sind.
   - **Notizen** erstellt einen Eintrag für eine sichere Notiz.
   - **Gruppe hinzufügen** erstellt einen Ordner innerhalb von Password Safe, um Einträge zu organisieren.
3. Geben Sie Ihre Daten in die Felder des Eintrags ein.
4. Optional: Tippen Sie auf **Plus** ⊕ und anschließend auf **Feld hinzufügen**, um ein benutzerdefiniertes Feld zu dem Eintrag hinzuzufügen.

Wenn Sie **Geschützt** für ein benutzerdefiniertes Feld aktivieren, müssen Sie auf die Augenschaltfläche neben dem Feld tippen, um den Wert anzuzeigen. Außerdem werden geschützte Felder nicht in Suchergebnissen angezeigt.

Mit **Plus** ⊕ können Sie auch eine Datei oder ein Bild zu dem Eintrag hinzufügen.

5. Tippen Sie auf **Fertig**, um den Eintrag zu speichern.

Sie können die Kennwortinformationen auf einfache Art verwenden, um sich an einer Internetseite oder einer App anzumelden. Siehe Kennwortdaten zum Anmelden verwenden (Seite 11).

Hinweis
Möglicherweise stellen Sie Performance-Probleme fest, wenn Sie große Dateien oder eine große Anzahl an Dateien zu einem Eintrag hinzufügen. Wir empfehlen Ihnen, solche Dateien mit der App Sophos Secure Workspace zu verschlüsseln, um sie sicher zu speichern.

8.2 Kennwörter erzeugen

1. Öffnen Sie den Password-Safe-Eintrag, für den Sie ein Kennwort erzeugen wollen.
2. Tippen Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.
3. Tippen Sie auf das Symbol **Zahnrad** ⚙, um den Kennwortgenerator zu öffnen.
4. Definieren Sie die Länge des Kennworts und die Zeichenarten, die in dem Kennwort enthalten sein müssen.
5. Tippen Sie auf **Aktualisieren** ↻, um ein Kennwort auf Basis Ihrer Angaben zu erzeugen.
6. Wenn Sie mit dem erzeugten Kennwort zufrieden sind, schließen Sie den Kennwortgenerator. Das Kennwort wird mit dem erzeugten Wert aktualisiert.
7. Speichern Sie den Eintrag.

8.3 Kennwortdaten zum Anmelden verwenden

- Um einen Wert in die Zwischenablage zu kopieren, tippen Sie auf das gewünschte Feld.
- Um den Wert eines geschützten Feldes anzuzeigen, tippen Sie auf das Symbol **Auge** 👁 neben dem geschützten Feld.
- Um eine URL in Safari zu öffnen, tippen Sie auf das Symbol **Weltkugel** 🌐 neben dem Feld **URL**.

8.4 Password-Safe-Einträge verwalten

1. Tippen und halten Sie einen Eintrag, um in den Auswahlmodus zu wechseln.
2. Optional: Wählen Sie weitere Einträge aus, für welche Sie dieselbe Aktion durchführen wollen.
3. Tippen Sie auf ein Symbol, um die entsprechende Aktion durchzuführen:
   - **Bearbeiten** ✎: Den Inhalt des Eintrags bearbeiten. Nur verfügbar, wenn ein einzelner Eintrag ausgewählt ist.
   - **Ausschneiden** ⧉: Die ausgewählten Einträge in eine andere Gruppe in der Password-Safe-Datei verschieben.

- **Kopieren**: Die ausgewählten Einträge in eine andere Gruppe in der Password-Safe-Datei kopieren.
- **Löschen**: Die ausgewählten Einträge in die spezielle Gruppe **Papierkorb** verschieben. Um Einträge endgültig zu löschen, verwenden Sie **Löschen** für Einträge in der Gruppe **Papierkorb**.
- Um einen Eintrag, den Sie ausgeschnitten haben, an eine andere Stelle zu verschieben oder zu kopieren, navigieren Sie zu dem gewünschten Zielort und tippen Sie anschließend auf **Zwischenablage**.

8.5 Password-Safe-Einträge durchsuchen

Sie können in Password Safe nach Namen von Einträgen und Gruppen sowie nach Werten innerhalb von Einträgen suchen.

Hinweis
Kennwortfelder und Felder, die Sie als **Geschützt** konfiguriert haben, sind von der Suche ausgeschlossen.

Tipp
Wenn Sie nicht die gesamte Password-Safe-Datei durchsuchen wollen, navigieren Sie zu einer Gruppe oder Untergruppe. Alle Einträge unterhalb dieser Gruppe werden rekursiv durchsucht.

1. Wischen Sie in Password Safe nach unten, um in den Suchmodus zu wechseln.
2. Geben Sie einen Suchbegriff ein. Die Ergebnisliste wird ständig aktualisiert, während Sie tippen.

8.6 Password Safe sichern

Es ist wichtig, dass Sie Ihre Password-Safe-Datei regelmäßig sichern. Falls Sie die Password-Safe-Datei verlieren, zum Beispiel weil Sie diese unbeabsichtigt gelöscht haben oder weil Sie Ihr Gerät verloren haben, können Sie nicht mehr auf Ihre Kennwortdaten zugreifen, es sei denn, Sie haben eine aktuelle Sicherungskopie.

1. Tippen Sie auf der Übersichtsseite der App in der Password-Safe-Kachel auf **Info** ⓘ.
2. Tippen Sie auf **Password-Safe-Datei sichern**.
3. Wählen Sie den Ort aus, an dem die Sicherungskopie erstellt wird.

Hinweis
Wir empfehlen Ihnen, außerdem ein Notfallblatt auszudrucken, das Ihnen hilft, auf Ihre Passwortdaten zuzugreifen, zum Beispiel, falls Sie Ihr Master-Kennwort vergessen oder Ihre Schlüsseldatei verlieren. Siehe Password-Safe-Notfalldatenblatt drucken (Seite 13).

8.7 Password-Safe-Notfalldatenblatt drucken

Falls Sie das Master-Kennwort für Password Safe vergessen oder die Schlüsseldatei verlieren, können Sie nicht auf die in Password Safe gespeicherten Daten zugreifen. Um dies zu verhindern, können Sie ein Notfallblatt mit den erforderlichen Informationen ausdrucken.

Warnung
Es ist wichtig, dass Sie Ihre Password-Safe-Datei regelmäßig sichern. Falls Sie die Password-Safe-Datei verlieren, zum Beispiel weil Sie diese unbeabsichtigt gelöscht haben oder weil Sie Ihr Gerät verloren haben, reicht das Notfallblatt alleine nicht aus, die Kennwort-Daten zurückzuerhalten. Siehe Password Safe sichern (Seite 12).

1. Tippen Sie auf der Übersichtsseite der App in der Password-Safe-Kachel auf **Info** ⓘ.
2. Tippen Sie auf **Notfallblatt drucken**.
3. Wählen Sie den Drucker und die Anzahl der Kopien aus und tippen Sie anschließend auf **Drucken**.
4. Tragen Sie im Ausdruck folgende Informationen ein:
   - Master-Kennwort
   - Speicherort Ihrer Password-Safe-Datei
   - Speicherort Ihrer Sicherungskopie
5. Verwahren Sie das Notfallblatt an einem sicheren Ort auf.

   Jeder, der Zugriff auf das Notfallblatt und auf Ihre Password-Safe-Datei hat, kann Ihre Kennwort-Daten lesen.

Wenn Sie die Password-Safe-Datei mit einer Schlüsseldatei gesichert haben, enthält das Notfallblatt einen elektronischen Fingerabdruck der Schlüsseldatei in Form eines QR-Codes. Sie können zum Öffnen der Password-Safe-Datei diesen QR-Code verwenden anstatt der eigentlichen Schlüsseldatei.

9 QR Code Scanner

Mit QR Code Scanner scannen Sie QR-Codes und verarbeiten die enthaltenen Informationen.

Um QR Code Scanner zu starten, berühren und halten Sie das Sophos-Symbol, und tippen Sie dann auf **QR Code Scanner**.

Web-Adressen

Wenn Sie den QR-Code scannen, wird die enthaltene URL basierend auf den Einstufungen von SophosLabs auf bösartige oder unangemessene Inhalte geprüft.

- Wenn die URL als sicher eingestuft wird, tippen Sie auf **Fortfahren**, um sie in Safari zu öffnen.

Kontakte

Scannen Sie den QR-Code und tippen Sie anschließend auf **Hinzufügen**, um mit den enthaltenen Visitenkartendaten einen neuen Kontakt zu erstellen.

Additional information
Sophos Intercept X for Mobile kann Visitenkartendaten in den Formaten vCard 2.1 und 3.0 lesen.

WLAN-Konfigurationen

Scannen Sie den QR-Code und tippen Sie anschließend auf **Kopieren**, um das Kennwort in die Zwischenablage zu kopieren. Navigieren Sie in der App **Einstellungen** zu **WLAN**, wählen Sie das Netzwerk aus und fügen Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Hinweis
Sie werden gewarnt, falls Sie sich mit einem unsicheren Netzwerk verbinden wollen. Unsichere Netzwerke sind solche, die nicht mit WPA oder WPA2 gesichert sind.

10 Message Filtering

Ihre Unternehmen kann Web Filtering verwenden, um eingehende SMS/MMS-Nachrichten auf Phishing-URLs zu prüfen.

Verdächtige Nachrichten werden in einer neuen Tab **SMS-Werbung** gefiltert.

Wenn in den App-Einstellungen **Message Filtering aktivieren** angezeigt wird, müssen Sie die Nachrichtenfilterung in der App **Einstellungen** entsprechend den Anforderungen Ihres Unternehmens aktivieren.

Message Filtering aktivieren

Gehen Sie in Ihrer iOS-App **Einstellungen** zu **Nachrichten**, tippen Sie auf **Unbekannt & Spam** und aktivieren Sie **Intercept X** unter **SMS-Filterung**.

Tab SMS-Werbung in der App Nachrichten

Wenn eine Nachricht von einem unbekannten Absender als Spam eingestuft wird, wird die Nachricht in der App **Nachrichten** auf den Tab **SMS-Werbung** verschoben. Bestehende und weitere Nachrichten desselben Absenders werden ebenfalls nach **SMS-Werbung** verschoben.

Hinweis

- Nachrichten eines bekannten Kontakts werden nie als Spam klassifiziert.
- Message Filtering funktioniert nicht für iMessages.

11 Sophos-Verwaltung

In einer Unternehmensumgebung kann Sophos Intercept X for Mobile von Sophos Mobile verwaltet werden. So kann Ihr Unternehmen den Compliance-Status Ihres Gerätes überwachen.

Um Sophos Intercept X for Mobile bei Sophos Mobile zu registrieren, befolgen Sie die Anweisungen, die Sie von Ihrem Unternehmen erhalten haben.

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, werden Sie folgende Unterschiede feststellen:

- App-Einstellungen werden zentral von Ihrem Unternehmen festgelegt.
- Falls Ihr Gerät nicht mehr den Unternehmensrichtlinien entspricht (d.h. nicht mehr „compliant“ ist), sind der Netzwerkzugriff und andere Funktionen möglicherweise eingeschränkt. Der Compliance-Status wird auf der Übersichtsseite der App angezeigt. Siehe Compliance-Verstöße beheben (Seite 16).

11.1 Compliance-Verstöße beheben

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, wird auf der Übersichtsseite der Compliance-Status gemäß Ihrer Unternehmensrichtlinie angezeigt.

So zeigen Sie Compliance-Verstöße an und beheben diese:

1. Tippen Sie im Dashboard auf **Sophos-Verwaltung**.
   Bei Compliance-Verstößen ist die Kachel mit einem roten Symbol versehen.
2. Tippen Sie auf den Compliance-Verstoß, und befolgen Sie die Anweisungen, um ihn zu beheben.

Hinweis
Wenn Ihr Gerät nicht den Unternehmensrichtlinien entspricht, sind der Netzwerkzugriff und andere Funktionen möglicherweise eingeschränkt.

11.2 Unterstützung erhalten

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, können Sie Kontaktdetails für Ihre IT und weitere von Ihrem Unternehmen bereitgestellte Informationen anzeigen.

Tippen Sie im Dashboard auf **Sophos-Verwaltung**.

Unter **IT-Kontakt** und **Weitere Informationen** werden die Kontaktdaten angezeigt.

12 Einstellungen

Einstellung	Beschreibung
Message Filtering aktivieren	Überprüft eingehende SMS/MMS auf Phishing-URLs. Ihr Unternehmen muss diese Funktion aktivieren. Siehe Message Filtering (Seite 15).
Web Filtering aktivieren	Blockiert Verbindungen zu bösartigen oder kategorisierten Webseiten. Ihr Unternehmen muss diese Funktion aktivieren. Siehe Web Filtering (Seite 5).
Alle WLAN-Probleme anzeigen	Zeigt alle WLAN-Probleme an, auch jene, die Sie zuvor ausgeblendet haben.
Protokolliergrad	Wenn Sie vom Sophos-Support dazu aufgefordert werden, wählen Sie den Umfang der im Protokoll enthaltenen Informationen aus.
Protokolldateien senden	Tippen Sie auf den Eintrag, um eine E-Mail mit der Protokolldatei zu versenden. Die E-Mail-Adresse des Sophos-Support-Teams wird automatisch eingefügt.
Datenerfassung	Erlauben Sie Sophos, anonyme Nutzungsdaten zu sammeln, um die App zu verbessern.

13 Sichern/Wiederherstellen

Sie können Ihre Authenticator-Konten sichern, um sie auf einem neuen iOS- oder Android-Gerät zu verwenden.

Konten sichern

1. Wählen Sie im Menü die Option **Sichern und Wiederherstellen** aus.
2. Tippen Sie auf **Sichern**.
3. Geben Sie einen Namen für die Sicherungsdatei ein.
4. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
5. Wählen Sie den Ort aus, an dem die Sicherungskopie erstellt wird.

   Tipp
   Speichern Sie die Sicherung in Ihrem Cloudspeicher, damit Sie sie auf anderen Geräten verwenden können.

6. Tippen Sie auf **Hinzufügen**.

Konten wiederherstellen

1. Tippen Sie auf der Seite **Sichern/Wiederherstellen** auf **Wiederherstellen** auf.
2. Gehen Sie zum Speicherort der Datei und tippen Sie auf die Sicherungskopie.
3. Geben Sie das Kennwort für die Sicherungskopie ein und tippen Sie auf **OK**.

14 Rechtliche Hinweise