

[← Zurück zur Übersichtsseite](#)

Veröffentlichungshinweise zu *Absichern von drahtlosen Netzwerken – eine Microsoft® Windows Server 2003-Zertifikatdienste-Lösung*

WPA-Kompatibilitätstest

Die neue Wi-Fi Protected Access (WPA)-Sicherheitslösung funktioniert mit der vorliegenden Lösung ohne Probleme. Dieses Dokument beschreibt einige Punkte, die Sie berücksichtigen sollten, wenn Sie WPA für Ihre Umgebung in Betracht ziehen.

WEP- und WPA-Übersicht

Wi-Fi gibt es heutzutage in zwei verschiedenen Varianten: Wired Equivalent Privacy (WEP) und Wi-Fi Protected Access (WPA). Beide Verfahren stellen Methoden zur Verfügung, um den Netzwerkverkehr zwischen Client und AP zu verschlüsseln.

WEP bietet eine Möglichkeit den Netzwerkzugriff einzuschränken und den Netzwerkverkehr auf Basis von gemeinsamen Schlüsseln zu verschlüsseln. Nachteile von WEP sind die fehlende dynamische Schlüsselverwaltung und Sicherheitslücken in der Implementierung der Verschlüsselung. Diese Sicherheitslücken machen es Angreifern möglich, die Schlüssel herauszufinden.

WPA wurde von der Wi-Fi-Alliance entwickelt und soll die Sicherheit von drahtlosen Netzwerken verbessern. Es stellt Sicherheitsfeatures zur Verfügung, die allgemein als die momentan besten anerkannt sind und unterstützt eine robuste Verschlüsselung. Ein Angriff auf die Schlüssel ist mit WPA sehr viel schwieriger.

Auswirkungen von WPA auf diese Lösung

WPA kann WEP in dieser Lösung vollständig ersetzen. Die meisten der Lösungskomponenten bleiben hiervon unbeeinflusst.

WPA verwendet 802.1X für die Netzwerkauthentifizierung. Daher bleiben RADIUS (Remote Authentication Dial-In User Service), Microsoft®-Zertifizierungsdienste und die meisten Microsoft Active Directory®-Einstellungen unverändert. Die Bereiche, die Sie berücksichtigen müssen, finden Sie in der folgenden Tabelle.

Tabelle 1.1: Lösungskomponenten für die Änderungen erforderlich werden

Lösungskomponenten	Änderung
Microsoft Windows® XP Hardwärtreiber	Sie sollten bei den Herstellern Ihrer Netzwerkkarten nachfragen, welche Karten sich für WPA aufrüsten lassen und ob Windows XP-Treiber für diese zur Verfügung stehen.
Windows XP-Clientkonfiguration	Es müssen Einstellungen geändert werden. Die Authentifizierungsmethode muss auf WPA gesetzt werden und das Verschlüsselungsprotokoll auf Temporal Key Integrity Protocol (TKIP).

RADIUS- Session-Timeout	TKIP führt bei jedem Paket eine Schlüsselerneuerung durch. Daher ist die Einstellung überflüssig.
Gruppenrichtlinie	Da die Microsoft Windows Server™ 2003-Gruppenrichtlinie vor der Entwicklung von WPA erstellt wurde, können keine WPA-Einstellungen vorgenommen werden. Microsoft wird ein entsprechendes Update zur Verfügung stellen.

Konfiguration der Lösung mit WPA

Über die folgenden Schritte konfigurieren Sie die Lösung für WPA:

1. Aktualisieren Sie die Firmware auf den bestehenden APs für eine WPA-Unterstützung, oder stellen Sie neue APs mit WPA-Unterstützung zur Verfügung.
2. Aktualisieren Sie die Treiber der WLAN-Netzwerkkarten auf eine Version, die WPA unterstützt.
3. Entfernen Sie die WLAN-Computer aus der Gruppe, die für die Anwendung der WLAN-Gruppenrichtlinie verantwortlich ist. Konfigurieren Sie die WPA- und 802.11-Einstellungen manuell.
4. Testen Sie die WLAN-Authentifizierung mit WPA.

Microsoft wird eine aktualisierte Gruppenrichtlinie für Windows Server 2003 zur Verfügung stellen.

Zusätzliche Informationen

- *The Cable Guy* — März 2003, *Wi-Fi Protected Access (WPA) Overview* unter <http://www.microsoft.com/technet/columns/cableguy/cg0303.asp> (englischsprachig).
- Microsoft Knowledge Base-Artikel 815485 *Overview of the WPA Wireless Security Update in Windows XP* unter <http://support.microsoft.com/?kbid=815485> (englischsprachig).
- *Microsoft Press Pass Announcement* zur WPA-Verfügbarkeit unter <http://www.microsoft.com/presspass/press/2003/mar03/03-31WiFiProtectedAccessPR.asp> (englischsprachig).