# Cisco Secure Services Client mit EAP-FAST-Authentifizierung

## Inhalt

Einführung Voraussetzungen Anforderung Verwendete Komponenten Konventionen Designparameter Datenbank Verschlüsselung Einmalige Anmeldung und Anmeldeinformationen des Systems Netzwerkdiagramm Konfigurieren des Zugriffssteuerungsservers (ACS) Access Point als AAA-Client (NAS) in ACS hinzufügen Konfigurieren des ACS zum Abfragen der externen Datenbank EAP-FAST-Unterstützung auf dem ACS aktivieren **Cisco WLAN-Controller** Konfigurieren des Wireless LAN-Controllers Grundlegender Betrieb und Registrierung der LAP zum Controller RADIUS-Authentifizierung über Cisco Secure ACS Konfiguration der WLAN-Parameter Betrieb überprüfen Anhang Sniffer Capture für EAP-FAST Exchange Debuggen am WLAN-Controller Zugehörige Informationen

## **Einführung**

In diesem Dokument wird beschrieben, wie der Cisco Secure Services Client (CSSC) mit den Wireless LAN-Controllern, der Microsoft Windows 2000<sup>®</sup> Software und dem Cisco Secure Access Control Server (ACS) 4.0 über EAP-FAST konfiguriert wird. Dieses Dokument stellt die EAP-FAST-Architektur vor und enthält Bereitstellungs- und Konfigurationsbeispiele. CSSC ist die Client-Softwarekomponente, die die Kommunikation von Benutzeranmeldeinformationen an die Infrastruktur ermöglicht, um einen Benutzer für das Netzwerk zu authentifizieren und einen entsprechenden Zugriff zuzuweisen.

Dies sind einige der Vorteile der CSSC-Lösung, die in diesem Dokument beschrieben werden:

- Authentifizierung jedes Benutzers (oder Geräts) vor der Zugriffsberechtigung für das WLAN/LAN mit Extensible Authentication Protocol (EAP)
- End-to-End-WLAN-Sicherheitslösung mit Server-, Authentifizierungs- und Client-Komponenten
- Gemeinsame Lösung für die Authentifizierung von kabelgebundenen und Wireless-Netzwerken
- Dynamisch, im Authentifizierungsprozess abgeleitete Verschlüsselungsschlüssel pro Benutzer
- Keine Anforderung für Public Key Infrastructure (PKI) oder Zertifikate (Zertifikatsprüfung optional)
- Zuweisung von Zugriffsrichtlinien und/oder NAC-fähiges EAP-Framework

**Hinweis:** Informationen zur Bereitstellung sicherer Wireless-Verbindungen finden Sie im <u>Cisco</u> <u>SAFE Wireless Blueprint</u>.

Das 802.1x-Authentifizierungs-Framework wurde als Teil des 802.11i-Standards (Wireless LAN Security) integriert, um Layer-2-basierte Authentifizierungs-, Autorisierungs- und Abrechnungsfunktionen in einem 802.11-WLAN-Netzwerk zu ermöglichen. Derzeit stehen mehrere EAP-Protokolle zur Verfügung, die sowohl in kabelgebundenen als auch in Wireless-Netzwerken eingesetzt werden können. Zu den häufig eingesetzten EAP-Protokollen gehören LEAP, PEAP und EAP-TLS. Zusätzlich zu diesen Protokollen hat Cisco EAP Flexible Authentication through Secured Tunnel (EAP-FAST) Protocol als standardbasiertes EAP-Protokoll definiert und implementiert, das sowohl in kabelgebundenen als auch in Wireless-LAN-Netzwerken zur Verfügung steht. Die EAP-FAST-Protokollspezifikation ist auf der <u>IETF-Website</u> öffentlich zugänglich.

Wie bei anderen EAP-Protokollen ist EAP-FAST eine Client-Server-Sicherheitsarchitektur, die EAP-Transaktionen innerhalb eines TLS-Tunnels verschlüsselt. Obwohl PEAP oder EAP-TTLS in dieser Hinsicht ähnlich sind, unterscheidet es sich darin, dass die EAP-FAST-Tunneleinrichtung auf starken gemeinsamen geheimen Schlüsseln beruht, die für jeden Benutzer eindeutig sind, im Vergleich zu PEAP/EAP-TTLS (die ein X.509-Serverzertifikat zum Schutz der Authentifizierungssitzung verwenden). Diese gemeinsam genutzten geheimen Schlüssel werden als Protected Access Credentials (PACs) bezeichnet und können automatisch (automatische oder In-Band-Bereitstellung) oder manuell (manuelle oder Out-of-Band-Bereitstellung) auf Client-Geräte verteilt werden. Da Handshakes auf der Grundlage gemeinsam verwendeter Geheimnisse effizienter sind als Handshakes auf Basis einer PKI-Infrastruktur, ist EAP-FAST der schnellste und weniger prozessorintensive EAP-Typ von denjenigen, die geschützte Authentifizierungsaustauschfunktionen bereitstellen. EAP-FAST wurde auch für eine einfachere Bereitstellung entwickelt, da es kein Zertifikat für den Wireless LAN-Client oder die RADIUS-Infrastruktur erfordert, aber einen integrierten Bereitstellungsmechanismus enthält.

Dies sind einige der wichtigsten Funktionen des EAP-FAST-Protokolls:

- Single Sign-On (SSO) mit Windows-Benutzername/Kennwort
- Unterstützung für die Ausführung von Anmeldeskripts
- Wi-Fi Protected Access (WPA)-Unterstützung ohne Drittanbieter-Komponente (nur Windows 2000 und XP)
- Einfache Bereitstellung ohne PKI-Infrastruktur
- Windows Password Aging (d. h. Unterstützung für den Ablauf von serverbasierten Kennworten)
- Integration mit Cisco Trust Agent für Network Admission Control mit entsprechender Client-Software

## Voraussetzungen

### **Anforderung**

Es wird davon ausgegangen, dass das Installationsprogramm über Kenntnisse der grundlegenden Windows 2003-Installation und der Cisco WLC-Installation verfügt, da dieses Dokument nur die spezifischen Konfigurationen behandelt, um die Tests zu erleichtern.

Informationen zur Erstinstallation und Konfiguration der Cisco Controller der Serie 4400 finden Sie in der <u>Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 4400</u>. Informationen zur Erstinstallation und Konfiguration der Cisco Controller der Serie 2000 finden Sie in der <u>Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 2000</u>.

Bevor Sie beginnen, installieren Sie Microsoft Windows Server 2000 mit der neuesten Service Pack-Software. Installieren Sie die Controller und die Lightweight Access Points (LAPs), und stellen Sie sicher, dass die neuesten Software-Updates konfiguriert sind.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Controller der Serie 2006 oder 4400 mit 4.0.155.5
- Cisco 1242 LWAPP AP
- Windows 2000 mit Active Directory
- Cisco Catalyst 3750G-Switch
- Windows XP mit CB21AG Adapterkarte und Cisco Secure Services Client Version 4.05

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

## **Designparameter**

### **Datenbank**

Wenn Sie ein WLAN-Netzwerk bereitstellen und nach einem Authentifizierungsprotokoll suchen, empfiehlt es sich in der Regel, eine aktuelle Datenbank für die Benutzer-

/Computerauthentifizierung zu verwenden. Typische Datenbanken, die verwendet werden können, sind Windows Active Directory, LDAP oder eine One Time Password (OTP)-Datenbank (d. h. RSA oder SecureID). Alle diese Datenbanken sind mit dem EAP-FAST-Protokoll kompatibel. Wenn Sie jedoch eine Bereitstellung planen, müssen einige Kompatibilitätsanforderungen berücksichtigt werden. Die Erstbereitstellung einer PAC-Datei für Clients erfolgt durch anonyme automatische Bereitstellung, authentifizierte Bereitstellung (über das aktuelle X.509-Client-Zertifikat) oder manuelle Bereitstellung. Für die Zwecke dieses Dokuments werden anonyme automatische Bereitstellung und manuelle Bereitstellung in Betracht gezogen.

Bei der automatischen PAC-Bereitstellung wird mithilfe des Authenticated Diffie-Hellman Key

Agreement Protocol (ADHP) ein sicherer Tunnel eingerichtet. Der sichere Tunnel kann entweder anonym oder über einen Serverauthentifizierungsmechanismus eingerichtet werden. Innerhalb der etablierten Tunnelverbindung wird MS-CHAPv2 zur Authentifizierung des Clients und nach erfolgreicher Authentifizierung zur Verteilung der PAC-Datei an den Client verwendet. Nachdem die PAC erfolgreich bereitgestellt wurde, kann die PAC-Datei zum Initiieren einer neuen EAP-FAST-Authentifizierungssitzung verwendet werden, um einen sicheren Netzwerkzugriff zu erhalten.

Die automatische PAC-Bereitstellung ist für die verwendete Datenbank relevant, da der Mechanismus für die automatische Bereitstellung auf MSCHAPv2 basiert, muss die Datenbank zur Benutzerauthentifizierung mit diesem Kennwortformat kompatibel sein. Wenn Sie EAP-FAST mit einer Datenbank verwenden, die das MSCHAPv2-Format nicht unterstützt (z. B. OTP, Novell oder LDAP), ist es erforderlich, einen anderen Mechanismus (d. h. manuelle Bereitstellung oder authentifizierte Bereitstellung) zum Bereitstellen von PAC-Dateien für Benutzer einzusetzen. Dieses Dokument enthält ein Beispiel für die automatische Bereitstellung einer Windows-Benutzerdatenbank.

### **Verschlüsselung**

Für die EAP-FAST-Authentifizierung ist kein bestimmter WLAN-Verschlüsselungstyp erforderlich. Der zu verwendende WLAN-Verschlüsselungstyp wird durch die Funktionen der Client-NIC-Karte bestimmt. Es wird empfohlen, die WPA2- (AES-CCM) oder WPA-(TKIP)-Verschlüsselung zu verwenden, je nach den NIC-Kartenfunktionen in der jeweiligen Bereitstellung. Beachten Sie, dass die Cisco WLAN-Lösung das gleichzeitige Vorhandensein von WPA2- und WPA-Client-Geräten auf einer gemeinsamen SSID ermöglicht.

Wenn die Client-Geräte WPA2 oder WPA nicht unterstützen, ist es möglich, die 802.1X-Authentifizierung mit dynamischen WEP-Schlüsseln bereitzustellen. Aufgrund der bekannten Exploits mit WEP-Schlüsseln wird dieser WLAN-Verschlüsselungsmechanismus jedoch nicht empfohlen. Wenn nur WEP-Clients unterstützt werden sollen, wird empfohlen, ein Sitzungs-Timeout-Intervall zu verwenden. Dazu müssen die Clients in regelmäßigen Abständen einen neuen WEP-Schlüssel ableiten. Das empfohlene Sitzungsintervall für typische WLAN-Datenraten beträgt dreißig Minuten.

### Einmalige Anmeldung und Anmeldeinformationen des Systems

Single Sign-On (Einmalanmeldung) bezeichnet die Möglichkeit, dass ein Benutzer sich anmeldet oder Authentifizierungsdaten eingibt, um auf mehrere Anwendungen oder Geräte zuzugreifen. Für die Zwecke dieses Dokuments bezieht sich die einmalige Anmeldung auf die Verwendung der Anmeldeinformationen, die zur Anmeldung bei einem PC zur Authentifizierung im WLAN verwendet werden.

Mit dem Cisco Secure Services Client können die Anmeldedaten eines Benutzers auch für die Authentifizierung im WLAN-Netzwerk verwendet werden. Wenn ein PC im Netzwerk authentifiziert werden soll, bevor sich der Benutzer beim PC anmeldet, müssen entweder gespeicherte Benutzeranmeldeinformationen oder Anmeldeinformationen verwendet werden, die an ein Computerprofil gebunden sind. Beide Methoden sind nützlich, wenn Sie beim Booten des PCs Anmeldeskripte oder Kartenlaufwerke ausführen möchten, statt sich anzumelden.

## **Netzwerkdiagramm**

Dies ist das in diesem Dokument verwendete Netzwerkdiagramm. In diesem Netzwerk werden vier Subnetze verwendet. Beachten Sie, dass es nicht erforderlich ist, diese Geräte in verschiedene Netzwerke zu segmentieren. Dies bietet jedoch die größte Flexibilität für die Integration in die eigentlichen Netzwerke. Der Catalyst 3750G Integrated Wireless LAN Controller bietet Power over Ethernet (POE)-Switch-Ports, L3-Switching und WLAN-Controller-Funktionen in einem gemeinsamen Chassis.

- 1. Netzwerk 10.1.1.0 ist das Servernetzwerk, in dem sich der ACS befindet.
- 2. Das Netzwerk 10.10.80.0 ist das Verwaltungsnetzwerk, das vom WLAN-Controller verwendet wird.
- 3. Netzwerk 10.10.81.0 ist das Netzwerk, in dem sich die APs befinden.
- 4. Für die WLAN-Clients wird das Netzwerk 10.10.82.0 verwendet.

RADIUS EAP/Datbase Server: CiscoSecure ACS, V4.0(1) Windows 2K Active Directory



## Konfigurieren des Zugriffssteuerungsservers (ACS)

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

**Hinweis:** Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

## Access Point als AAA-Client (NAS) in ACS hinzufügen

In diesem Abschnitt wird beschrieben, wie ACS für EAP-FAST mit In-Band-PAC-Bereitstellung mit Windows Active Directory als externer Datenbank konfiguriert wird.

- 1. Melden Sie sich bei ACS > Network Configuration an, und klicken Sie auf Add Entry (Eintrag hinzufügen).
- 2. Geben Sie den Namen, die IP-Adresse und den geheimen Schlüssel des WLAN-Controllers ein, und wählen Sie unter Authenticate Using (Authentifizieren über) die Option RADIUS (Cisco Air) aus, die auch RADIUS IETF-Attribute enthält.**Hinweis:** Wenn die Netzwerkgerätegruppen (NDG) aktiviert sind, wählen Sie zuerst das entsprechende NDG aus, und fügen Sie den WLAN-Controller hinzu. Weitere Informationen zum NDG finden Sie im ACS-Konfigurationsleitfaden.
- 3. Klicken Sie auf Senden+ Neu starten.

CISCO SYSTEMS	Network Configuration
	Edit
User Setup	
Group Setup	AAA Client Setup For
SharedProfile Components	ws-3750
Network Configuration	10.10.80.3
System Configuration	AAA Client IP Address
Configuration	Key cisco123
Administration Control	Authenticate Using RADIUS (Cisco Airespace)
Databases	□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Posture Validation	Log Update/Watchdog Packets from this AAA Client
Network Access	Log RADIUS Tunneling Packets from this AAA Client
Reports and	Replace RADIUS Port info with Username from this AAA Client
Online Documentation	Submit Submit + Apply Delete Delete + Apply Cancel
	💡 Back to Help

### Konfigurieren des ACS zum Abfragen der externen Datenbank

In diesem Abschnitt wird beschrieben, wie Sie den ACS so konfigurieren, dass die externe Datenbank abgefragt wird.

- 1. Klicken Sie auf Externe Benutzerdatenbank > Datenbankkonfiguration > Windows-Datenbank > Konfigurieren.
- Verschieben Sie unter Domänenliste konfigurieren die Domänen von Verfügbaren Domänen in die Domänenliste. Hinweis: Der Server, der den ACS ausführt, muss über diese Domänen verfügen, damit die ACS-Anwendung diese Domänen erkennen und für Authentifizierungszwecke verwenden kann.



- Konfigurieren Sie unter den Windows EAP-Einstellungen die Option, die Kennwortänderung innerhalb der PEAP- oder EAP-FAST-Sitzung zuzulassen. Im <u>Konfigurationsleitfaden für</u> <u>Cisco Secure ACS 4.1</u> finden Sie weitere Informationen zum Älterwerden von EAP-FAST und Windows Password.
- 4. Klicken Sie auf Senden.Hinweis: Sie können auch die Dialin-Berechtigung für EAP-FAST unter der Windows-Benutzerdatenbankkonfiguration aktivieren, um der externen Windows-Datenbank die Steuerung der Zugriffsrechte zu ermöglichen. Die MS-CHAP-Einstellungen für Kennwortänderungen auf der Windows-Datenbankkonfigurationsseite sind nur für die Nicht-EAP MS-CHAP-Authentifizierung anwendbar. Um die Kennwortänderung in Verbindung mit EAP-FAST zu aktivieren, muss die Kennwortänderung unter den Windows EAP-Einstellungen aktiviert werden.



User Setup	Windows EAP Settings 💡
Group	Enable password change inside PEAP or EAP-FAST.
1 Shared Brofile	EAP-TLS Strip Domain Name.
Components	
Network Ma	chine Authentication.
Configuration	Enable PEAP machine authentication.
System Configuration	Enable EAP-TLS machine authentication.
Interface Configuration	EAP-TLS and PEAP machine authentication name host/
Administration	Enable machine access restrictions.
Control	Aging time (hours): 12
External User Databases	Group map for successful user authentication without (No Access)
Posture Validation	User Groups that are exempt from passing machine authentication:
Network Access Profiles	Available User Groups Selected User Groups
Busuchaused	Default Group
otivity	Group 2
nline	Group 3 Group 4
ocumentation	Group 5
	Group 7
	Oroup 8
Th	ese settings can be used to enable or disable specific Windows EAP functionality
	Submit Cancel

- 5. Klicken Sie auf **Externe Benutzerdatenbank > Unbekannte Benutzerrichtlinie** und wählen Sie das Optionsfeld **Folgende externe Benutzerdatenbanken überprüfen aus**.
- 6. Verschieben der Windows-Datenbank aus **externen Datenbanken** in **ausgewählte Datenbanken**.
- 7. Klicken Sie auf Senden. Hinweis: Ab diesem Zeitpunkt überprüft der ACS die Windows-DB. Wenn der Benutzer nicht in der lokalen ACS-Datenbank gefunden wird, wird er in die ACS-Standardgruppe aufgenommen. Weitere Informationen zu Datenbankgruppenzuordnungen finden Sie in der ACS-Dokumentation. Hinweis: Während der ACS die Microsoft Active Directory-Datenbank abfragt, um Benutzeranmeldeinformationen zu überprüfen, müssen unter Windows zusätzliche Einstellungen für Zugriffsrechte konfiguriert werden. Weitere Informationen finden Sie im Installationshandbuch für Cisco Secure ACS für Windows Server.



## EAP-FAST-Unterstützung auf dem ACS aktivieren

In diesem Abschnitt wird beschrieben, wie die EAP-FAST-Unterstützung auf dem ACS aktiviert wird.

- 1. Gehen Sie zu System Configuration > Global Authentication Setup > EAP-FAST Configuration.
- 2. Wählen Sie EAP-FAST zulassen aus.
- Konfigurieren Sie die folgenden Empfehlungen: TTL/TTL-Master-Schlüssel (wiederhergestellt)/ TTL-Master-Schlüssel (wiederhergestellt)/ PAC TTL. Diese Einstellungen werden in Cisco Secure ACS standardmäßig konfiguriert:TTL bei Master-Schlüssel: 1 MonatTTL für die gelöschte Taste: 3 MonatePAC TTL: 1 Woche
- 4. Füllen Sie das Feld **Authority ID Info (Autoritäts-ID-Informationen**) aus. Dieser Text wird auf einigen EAP-FAST-Client-Software angezeigt, bei denen die PAC Authority als Controller ausgewählt wird.**Hinweis:** Der Cisco Secure Services Client verwendet für die PAC-Behörde diesen beschreibenden Text nicht.
- 5. Wählen Sie das Feld Allow In-Band PAC Provisioning (In-Band-PAC-Bereitstellung zulassen) aus. Dieses Feld ermöglicht die automatische PAC-Bereitstellung für korrekt aktivierte EAP-FAST-Clients. In diesem Beispiel wird die automatische Bereitstellung verwendet.
- 6. Wählen Sie **Zulässige innere Methoden**: EAP-GTC und EAP-MSCHAP2. Dies ermöglicht den Betrieb von EAP-FAST v1- und EAP-FAST v1a-Clients. (Cisco Secure Services Client

unterstützt EAP-FAST v1a.) Wenn EAP-FAST v1-Clients nicht unterstützt werden müssen, ist es nur erforderlich, EAP-MSCHAPv2 als interne Methode zu aktivieren.

- 7. Aktivieren Sie das Kontrollkästchen EAP-FAST Master Server, um diesen EAP-FAST-Server als Master zu aktivieren. Dadurch können andere ACS-Server diesen Server als PAC-Hauptbehörde nutzen, um die Bereitstellung eindeutiger Schlüssel für jeden ACS in einem Netzwerk zu vermeiden. Weitere Informationen finden Sie im ACS-Konfigurationsleitfaden.
- 8. Klicken Sie auf **Senden+Neu** starten.



User Setup

### System Configuration

### EAP-FAST Configuration

Group   Setup	EAP-F4	NST Settings	?			
Shared Profile	EAP-FAST					
ale   components	Allow EAP-FAST					
Configuration	Active master key TTL	1 months 💌				
System Configuration	Retired master key TTL	3 months 😪				
Interface	Tunnel PAC TTL	1 weeks 💌				
Configuration	Client initial message:	TME				
Control	Authority ID Info:	TME				
External User Databases	Allow anonymous in-band PAC prov	isioning				
and Posture	Allow authenticated in-band PAC p	rovisioning				
Validation	Accept client on authenticated	provisioning				
Network Access	Require client certificate for pro	ovisioning				
	Allow Machine Authentication					
Activity	Machine PAC TTL	1 weeks 💙				
Documentation	Allow Stateless session resume					
	Authorization PAC TTL	1 hours 😪				
	Allowed inner methods					
	EAP-GTC					
	EAP-MSCHAPv2					
	EAP-TLS					
	Select one or more of the following EA	P-TLS comparison methods:				
Certificate SAN comparison						
	Certificate CN comparison					
	Certificate Binary comparison					
	EAP-TLS session timeout (minutes)	120				
	EAP-FAST master server					
	Actual EAP-FAST server status	Master				

### **Cisco WLAN-Controller**

Für die Zwecke dieses Bereitstellungsleitfadens wird ein Cisco WS3750G Integrated Wireless LAN Controller (WLC) mit Cisco AP1240 Lightweight APs (LAP) verwendet, um die WLAN-Infrastruktur für CSSC-Tests bereitzustellen. Die Konfiguration gilt für alle Cisco WLAN-Controller. Die verwendete Softwareversion ist 4.0.155.5.

## Konfigurieren des Wireless LAN-Controllers

### Grundlegender Betrieb und Registrierung der LAP zum Controller

Verwenden Sie den Assistenten für die Startkonfiguration in der Befehlszeilenschnittstelle (CLI), um den WLC für den Basisbetrieb zu konfigurieren. Alternativ können Sie die Benutzeroberfläche verwenden, um den WLC zu konfigurieren. In diesem Dokument wird die Konfiguration auf dem WLC mit dem Startup Configuration Wizard (Start-Konfigurationsassistent) in der CLI erläutert.

Nachdem der WLC zum ersten Mal gestartet wurde, wird er in den Startup Configuration Wizard (Startup-Konfigurationsassistent) eingegeben. Konfigurieren Sie mithilfe des Konfigurationsassistenten die Grundeinstellungen. Sie können über die CLI oder die GUI auf den Assistenten zugreifen. Diese Ausgabe zeigt ein Beispiel für den Startup Configuration Wizard (Start-Konfigurationsassistent) in der CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
```

Configuration saved! Resetting system with new configuration.

Diese Parameter richten den WLC für den Basisbetrieb ein. In dieser Beispielkonfiguration verwendet der WLC als IP-Adresse der Verwaltungsschnittstelle **10.10.80.3** und **10.10.80.4** als IP-Adresse der AP-Manager-Schnittstelle.

Bevor andere Funktionen auf den WLCs konfiguriert werden können, müssen sich die LAPs beim WLC registrieren. In diesem Dokument wird davon ausgegangen, dass die LAP beim WLC registriert ist. Weitere Informationen zur Registrierung der Access Points beim WLC finden Sie im Abschnitt <u>Registrieren des Lightweight Access Points zum WLCs</u>-Abschnitt <u>WLAN Controller Failover for Lightweight Access Points (WLAN-Controller-Failover für Lightweight-Access Points)</u> im Konfigurationsbeispiel. Als Referenz für dieses Konfigurationsbeispiel werden die AP1240-Router in einem separaten Subnetz (10.10.81.0/24) vom WLAN-Controller (10.10.80.0/24)

bereitgestellt, und die DHCP-Option 43 wird für die Controller-Erkennung verwendet.

### RADIUS-Authentifizierung über Cisco Secure ACS

Der WLC muss so konfiguriert werden, dass die Benutzeranmeldeinformationen an den Cisco Secure ACS-Server weitergeleitet werden. Der ACS-Server validiert dann die Benutzeranmeldeinformationen (über die konfigurierte Windows-Datenbank) und ermöglicht den Zugriff auf die Wireless-Clients.

Gehen Sie wie folgt vor, um den WLC für die Kommunikation mit dem ACS-Server zu konfigurieren:

 Klicken Sie in der Benutzeroberfläche des Controllers auf Sicherheit und RADIUS-Authentifizierung, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen. Klicken Sie anschließend auf Neu, um den ACS-Server zu definieren

dennieren.		
Core Seren		Save Configuration   Ring   Lagout   Refresh
A.A.	MONITOR MLAYE CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANCE HELP	
Security	RADIUS Authentication Servers	Apply New
ARA General	Call Station ID Type IP Address 👒	
RADJUS Authenticetion RADJUS Accounting Local Net Users	Credentials Caching	
MAC Fibering Disabled Clients User Login Polisies	Use AES Key Wrap	
AP Policies Access Control Lists	Network Nanagement Server Index Server Address Port IPSec Admin Status	
IPSec Certificates CA Certificate ID Certificate		

2. Definieren Sie die ACS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu). Zu diesen Parametern gehören die ACS-IP-Adresse, der Shared Secret, die Portnummer und der Serverstatus. Hinweis: Die Portnummern 1645 oder 1812 sind für die RADIUS-Authentifizierung mit dem ACS kompatibel. Die Kontrollkästchen für Netzwerkbenutzer und -verwaltung legen fest, ob die RADIUS-basierte Authentifizierung für Netzwerkbenutzer (z. B. WLAN-Clients) und die Verwaltung (d. h. administrative Benutzer) gilt. In der Beispielkonfiguration wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 10.1.1.12 verwendet:

Com Surren							Logout Refre
de A.	MONITOR WILANS CONTR	OLLER WIRELESS SECURI	TY NANAGEMENT	COMMANDS HEU			550050505
Security	RADIUS Authentication Ser	rvers > New				< Back	Apply
AAA General	Server Index (Priority)	1 M					
RADIUS Authentication RADIUS Accounting Local Net Deers	Server IPAddress	10.1.1.12					
NAC Filtwing Disabled Clients	Shared Secret Format	ASCII M					
AP Policies	Shared Secret	*******					
Access Control Lists IPSec Certificates CA Certificate	Confirm Shared Secret						
RADIUS Authentication RADIUS Accounting Local Net Users	Berver IPAddress	10.1.1.12					
MAC Filturing Disabled Clients User Locis Relicies	Shared Secret Format	ASCH V					
AP Polities	Shared Secret						
Access Control Lists	Confirm Shered						
IPSec Certificates CA Certificate	Becret						
ID Certificate	Key Wrap						
Wireless Protection Policies	Port Number	1812					
Trusted AP Palicies Rogae Policies	Berver Status	Enabled 💌					
Standard Signatures Custom Signatures Signature Events	Support for RFC 3576	finabled w					
Client Exclusion Policies AP Authentication / MPP	Retransmit Timeout	z seconds					
Nanagement Prame Protection	Network User	C Enable					
Web Lagin Page CIDS	Management	🗆 Enable					
Sensors Shanned Clients	IPSec	Enable					

### Konfiguration der WLAN-Parameter

In diesem Abschnitt wird die Konfiguration des Cisco Secure Services Client beschrieben. In diesem Beispiel wird CSSC v4.0.5.4783 mit einem Cisco CB21AG-Client-Adapter verwendet. Stellen Sie vor der Installation der CSSC-Software sicher, dass nur die Treiber für die CB21AG installiert sind, nicht das Aironet Desktop Utility (ADU).

Sobald die Software installiert ist und als Service ausgeführt wird, sucht sie nach verfügbaren Netzwerken und zeigt diese an.

Hinweis: CSSC deaktiviert die konfigurationsfreie Windows-Funktion.

Hinweis: Nur die SSID, die für Broadcast aktiviert sind, sind sichtbar.



Hinweis: Der WLAN-Controller sendet standardmäßig die SSID, sodass sie in der Liste der gescannten SSIDs "Netzwerke erstellen" angezeigt wird. Um ein Netzwerkprofil zu erstellen, können Sie einfach auf die SSID in der Liste (Enterprise) und das Optionsfeld Create Network (Netzwerk erstellen) klicken.

Wenn die WLAN-Infrastruktur so konfiguriert ist, dass die Broadcast-SSID deaktiviert ist, müssen Sie die SSID manuell hinzufügen. Klicken Sie auf das Optionsfeld **Hinzufügen** unter Access Devices (Zugriffsgeräte), und geben Sie manuell die entsprechende **SSID ein** (z. B. Enterprise). Konfigurieren des aktiven Verhaltens des Clients, d. h., wenn der Client aktiv nach seiner konfigurierten SSID sucht Geben Sie **Aktiv nach diesem Zugriffsgerät suchen** an, nachdem Sie im Fenster Zugriffsgerät hinzufügen die SSID eingegeben haben.

**Hinweis:** Die Porteinstellungen lassen keine Enterprise-Modi (802.1X) zu, wenn die EAP-Authentifizierungseinstellungen nicht zuerst für das Profil konfiguriert wurden.

Das Optionsfeld **Create Network (Netzwerk erstellen**) öffnet das Fenster Network Profile (Netzwerkprofil), in dem Sie die ausgewählte (oder konfigurierte) SSID einem

Authentifizierungsmechanismus zuordnen können. Weisen Sie dem Profil einen beschreibenden Namen zu.

**Hinweis:** Mehrere WLAN-Sicherheitstypen und/oder SSIDs können diesem Authentifizierungsprofil zugeordnet werden.

Damit der Client automatisch eine Verbindung zum Netzwerk herstellen kann, wenn er sich im Funkfrequenzbereich befindet, wählen Sie **Benutzerverbindung automatisch herstellen aus**. Deaktivieren Sie **Verfügbar für alle Benutzer**, wenn dieses Profil nicht mit anderen Benutzerkonten auf dem Computer verwendet werden soll. Wenn **Automatisch herstellen** nicht ausgewählt ist, muss der Benutzer das CSSC-Fenster öffnen und die WLAN-Verbindung mit dem Optionsfeld **Verbinden** manuell initiieren.

Wenn die WLAN-Verbindung vor der Anmeldung des Benutzers initiiert werden soll, wählen Sie **Before user account (Benutzerkonto einrichten)** aus. Dies ermöglicht die einmalige Anmeldung mit gespeicherten Benutzeranmeldeinformationen (Kennwort oder Zertifikat/Smartcard bei Verwendung von TLS in EAP-FAST).

🐵 Network Profile 🛛 🛃
Network         Name:       Enterprise Network         Image: Available to all users (public profile)         Image: Automatically establish Machine connection         Image: Automatically establish User connection         Image: Before user account (supports smartcard/password only)
Network Configuration Summary:
Authentication: FAST;
Credentials: Request when needed and remember forever.
Modify
Access Devices
Access / SSID Mode Notes
Enterprise WPA2 Enterprise
Add Modify Configuration Remove
Help OK Cancel

**Hinweis:** Für den WPA/TKIP-Betrieb mit dem Cisco Aironet Client Adapter der Serie 350 muss die WPA-Handshake-Validierung deaktiviert werden, da derzeit eine Inkompatibilität zwischen dem CSSC-Client und 350 Treibern in Bezug auf die WPA-Handshake-Hash-Validierung besteht. Diese Option ist unter **Client > Advanced Settings > WPA/WPA2 Handshake Validation** deaktiviert. Die deaktivierte Handshake-Validierung lässt weiterhin die WPA-inhärenten Sicherheitsfunktionen (TKIP-Paketverknüpfung und Message Integrity Check) zu, deaktiviert jedoch die ursprüngliche WPA-Schlüsselauthentifizierung.

400	cess 🔺	Data Security 🔥
211 211	bigmonkey (2 accesses detected) employee-local	PA2
1	Enterprise (4 accesses detected) 00141b5a2bd0 High Signal 00141b5a2bdf High Signal 00141b5a33d0 High Signal 00141b5a33df High Signal	WPA2 WPA2 WPA2 WPA2 WPA2 WPA2
211 211 <	guest guest-central	▲ Open ▲ Open
	ess Device: ess (SSID): Enterprise Actively search for this access device	
En	ode: WPA2 Enterprise	AES 💌
M		
M		

Klicken Sie unter "Übersicht über die Netzwerkkonfiguration" auf Ändern, um die EAP-/Anmeldeinformationseinstellungen zu konfigurieren. Geben Sie Authentifizierung einschalten, FAST unter Protokoll auswählen und wählen Sie "Anonymous" als Identität aus (um bei der ursprünglichen EAP-Anforderung keinen Benutzernamen zu verwenden). Es ist möglich, den Benutzernamen als Identitäten als äußere EAP-Identität zu verwenden, aber viele Kunden möchten die Benutzer-IDs nicht in der ursprünglichen unverschlüsselten EAP-Anforderung verfügbar machen. Geben Sie Single Sign on Credentials (Single-Sign-on-Anmeldeinformationen verwenden, um Anmeldeinformationen für die Netzwerkauthentifizierung zu verwenden. Klicken Sie auf Konfigurieren, um EAP-FAST-Parameter einzurichten.

Network Authentication				
Network: Enterprise Network Authentication Methods:	-User Credentials:			
<ul> <li>Turn Off</li> <li>Turn On</li> <li>Use Username as Identity</li> <li>Use 'Anonymous' as Identity</li> <li>Protocol</li> <li>EAP-MD5</li> <li>EAP-MSCHAPv2</li> <li>EAP-TLS</li> <li>FAST</li> <li>GTC</li> <li>Configure</li> </ul>	<ul> <li>Use Machine Credentials</li> <li>Use Single Sign on Credentials</li> <li>Request when needed</li> <li>Remember forever</li> <li>Remember for this session</li> <li>Remember for 5 minutes</li> </ul>			
Help	OK Cancel			

Unter FAST-Einstellungen kann das **Zertifikat "Validate Server" (Validate Server Certificate)** angegeben werden, das es dem Client ermöglicht, das Zertifikat des EAP-FAST-Servers (ACS) vor der Einrichtung einer EAP-FAST-Sitzung zu validieren. Dadurch werden die Client-Geräte vor der Verbindung mit einem unbekannten oder nicht autorisierten EAP-FAST-Server geschützt und die Authentifizierungsdaten versehentlich an eine nicht vertrauenswürdige Quelle gesendet. Dies erfordert, dass auf dem ACS-Server ein Zertifikat installiert ist und auf dem Client auch das entsprechende Zertifikat der Root Certificate Authority installiert ist. In diesem Beispiel ist die Validierung von Serverzertifikaten nicht aktiviert.

Unter den FAST-Einstellungen kann die Option **Fast Session Resumption zulassen** angegeben werden, die die Wiederaufnahme einer EAP-FAST-Sitzung auf Basis der Tunnelinformationen (TLS-Sitzung) ermöglicht, anstatt eine vollständige EAP-FAST-Reauthentifizierung vorzunehmen. Wenn der EAP-FAST-Server und -Client über allgemeine Kenntnisse der im ersten EAP-FAST-Authentifizierungsaustausch ausgehandelten TLS-Sitzungsinformationen verfügen, kann es zu einer Wiederaufnahme der Sitzung kommen.

**Hinweis:** Sowohl der EAP-FAST-Server als auch der Client müssen für die EAP-FAST-Sitzungswiederaufnahme konfiguriert werden.

Geben Sie unter Getunnelte Methoden > EAP-TLS-Einstellungen **Any Method** an, um die automatische PAC-Bereitstellung von EAP-MSCHAPv2 und die EAP-GTC-Authentifizierung

zuzulassen. Wenn Sie eine Datenbank im Microsoft-Format verwenden, z. B. Active Directory, und wenn keine EAP-FAST v1-Clients im Netzwerk unterstützt werden, können Sie auch die Verwendung von **MSCHAPv2** als Tunneled Method angeben.

**Hinweis:** Validieren Sie das Serverzertifikat standardmäßig unter den EAP-TLS-Einstellungen in diesem Fenster. Da im Beispiel EAP-TLS nicht als interne Authentifizierungsmethode verwendet wird, ist dieses Feld nicht anwendbar. Wenn dieses Feld aktiviert ist, kann der Client das Serverzertifikat zusätzlich zur Servervalidierung des Clientzertifikats in EAP-TLS validieren.

👁 Configure EAP Method 🛛 🛛
FAST settings:         Use Client Certificate         Use Smartcard-based Client Certificates Only         Validate Server Certificate         Allow Fast Session Resumption
Tunneled Method
Any Method
EAP-TLS Settings:
Use Smartcard-based Client Certificates Only
✓ Validate Server Certificate
Help OK Cancel

Klicken Sie auf **OK**, um die EAP-FAST-Einstellungen zu speichern. Da der Client für die "automatische Einrichtung" unter Profil konfiguriert ist, initiiert er automatisch die Zuordnung/Authentifizierung zum Netzwerk. Auf der Registerkarte Netzwerke verwalten geben die Felder Netzwerk, Status und Datensicherheit den Verbindungsstatus des Clients an. Aus diesem Beispiel geht hervor, dass das Profile Enterprise Network verwendet wird und das Network Access Device (Netzwerkzugriffsgerät) die SSID Enterprise (SSID-Enterprise) ist, die Connected:Authenticated (Verbunden) anzeigt und Autoconnect verwendet. Das Feld Datensicherheit gibt den verwendeten 802.11-Verschlüsselungstyp an, der in diesem Beispiel WPA2 ist.

Cisco Secure Services Client			
Client Administration Help			
Create Networks Manage Networks			
Network 🔺	Status	Data Security	
Enterprise Network	Connected: Authenticated		
1 Enterprise	Connected: Authenticated (AutoConnect)	🗃 WPA2	
			Details
Connect	Configure Remove Stat	us	
			.:

Nachdem der Client sich authentifiziert hat, wählen Sie auf der Registerkarte "Netzwerke verwalten" unter **SSID** aus, und klicken Sie auf **Status**, um Verbindungsdetails abzufragen. Das Fenster Verbindungsdetails enthält Informationen zum Client-Gerät, zum Verbindungsstatus, zu Statistiken und zur Authentifizierungsmethode. Die Registerkarte WiFi Details enthält Details zum Verbindungsstatus für 802.11, einschließlich RSSI, 802.11-Kanal sowie Authentifizierung/Verschlüsselung.

Connection Status

Connection Details WiFi [	Details
Status:	Connected: Authenticated
Duration:	00:00:47
Network Profile:	Enterprise Network
Network Adapter:	Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A0-36-2F
Access Device:	Enterprise
Access Device MAC Addr	ess: 00-14-1B-5A-33-D0
Transmitted packets:	121
Received packets:	6
Speed:	54.0 Mbps
Authentication Method:	FAST / GTC
Authentication Server:	TME (not verified)
IP Address:	10.10.82.11
Help	Close

X

@ Connec	tion Statu	S			
Connectio	n Details	WiFi Details			
Connectio Access Channe Signal 3 Associa Encryp	n Details Device MA el: Strength: ation Method	WiFi Details C Address (BSS	SID]:	00-14-1B-5A- Ver, WPA2 Ent	-33-D0 1 y High erprise AES
Help					Close

Als Systemadministrator haben Sie Anspruch auf das Diagnosedienstprogramm Cisco Secure Services Client System Report, das mit der standardmäßigen CSSC-Distribution verfügbar ist. Dieses Dienstprogramm ist im Startmenü oder im CSSC-Verzeichnis verfügbar. Um Daten abzurufen, klicken Sie auf **Daten sammeln > In Zwischenablage kopieren > Berichtsdatei suchen**. Dadurch wird ein Fenster von Microsoft File Explorer in das Verzeichnis mit der gezippten Berichtsdatei geleitet. In der Zip-Datei befinden sich die nützlichsten Daten unter log (log\_current).

Das Dienstprogramm gibt den aktuellen Status von CSSC, die Schnittstelle und die Treiberdetails zusammen mit den WLAN-Informationen (SSID erkannt, Zuordnungsstatus usw.) an. Dies kann besonders nützlich sein, um Verbindungsprobleme zwischen dem CSSC und dem WLAN-Adapter zu diagnostizieren.

## Betrieb überprüfen

Nach der Konfiguration des Cisco Secure ACS-Servers, des WLAN-Controllers, des CSSC-Clients und der vermutlich korrekten Konfiguration und Datenbankauffüllung wird das WLAN-Netzwerk für die EAP-FAST-Authentifizierung und die sichere Client-Kommunikation konfiguriert. Es gibt eine Vielzahl von Punkten, die überwacht werden können, um den Fortschritt/Fehler einer sicheren Sitzung zu überprüfen.

Um die Konfiguration zu testen, versuchen Sie, einen Wireless-Client mit dem WLAN-Controller der EAP-FAST-Authentifizierung zu verknüpfen.

 Wenn CSSC f
ür die automatische Verbindung konfiguriert ist, versucht der Client diese Verbindung automatisch. Wenn die WLAN-Verbindung nicht f
ür die automatische Verbindung und die einmalige Anmeldung konfiguriert ist, muss der Benutzer die WLAN-Verbindung 
über das Optionsfeld Verbinden initiieren. Dadurch wird der 802.11-Zuordnungsprozess initiiert, über den die EAP-Authentifizierung erfolgt.Dies ist ein Beispiel:

Cisco Secure Services Client		
Client Administration Help		
Create Networks Manage Networks		
Network 🔺	Status	Data Security
Enterprise Network	Disconnected	
Enterprise (hidden)	Not Available (Manual)	PA2
		>
		Details
Connect Configure	Remove Status	
		.::

 Anschließend wird der Benutzer aufgefordert, den Benutzernamen und das Kennwort f
ür die EAP-FAST-Authentifizierung (von der EAP-FAST PAC Authority oder ACS) einzugeben.Dies ist ein

	Enter Your Credentials	
	Please enter your credentials for network Enterprise, access akita_pkc Username: tmeuser3	
Beispiel:	Send Cancel	
Enter	Your Credentials	
	Please enter your credentials for network Enterprise, access akita_pkc	
	Username: tmeuser3	
	Welcome to the Richfield TME PAC Auth	
Dialog	expires in 10 second(s) Send Cancel	

3. Der CSSC-Client übergibt die Benutzeranmeldeinformationen über den WLC an den RADIUS-Server (Cisco Secure ACS), um die Anmeldeinformationen zu validieren. ACS überprüft die Benutzeranmeldeinformationen durch einen Vergleich der Daten mit der konfigurierten Datenbank (in der Beispielkonfiguration ist die externe Datenbank Windows Active Directory) und ermöglicht den Zugriff auf den Wireless-Client, wenn die Benutzeranmeldeinformationen gültig sind. Der Bericht über die erfolgreich bestandenen Authentifizierungen auf dem ACS-Server zeigt, dass der Client die RADIUS/EAP-Authentifizierung bestanden hat.Dies ist ein Beispiel:

Croca Secrear	Reports and Activity															I
يظله خلله	Select	Salect														
Elerr Strap Strap Barrel Frohe Barrel Frohe	Reports	Persond Aut Regular Exp Apply Fit Filtering is	thenticat ression ter C	lons active Dear Filter d.	]	Balbaah St.	ort Date	6: Tim yy,hh:	e mm:ss	End Dati mm/dd/	e & Time yyyy,hh:	Pa nem:ss 5	ava per Par D	2a		
Configuration	KAULUS Accounting     YolP Accounting     Passed Authentications     Ealed Attempts	Date 🗣	lime	Message- Type	User- Norma	Group- Nome	Caller-	NAS- Earl	NAS-IP- Address	Access Profile Name	Shered RAC	Downloadable ACL	System: Posture: Token	Application Posture: Taken	Reason	EA
Configuration	Disabled Accounts	08/22/2006	16:25:37	Authen OK	test	Default Group	00-40- 96-A0- 36-2F	29	10.10.00.3	(Default)						43
G Constant	Database Replication	08/22/2006	16:09:51	Authen OK	test	Default Group	00-40- 96-A6- 06-F6	29	10.10.80.3	(Default)						42
Rental Parties	User Password Changes	08/22/2006	16:06:55	Authen OK	test	Default Group	00-40- 96-A6- D6-F6	29	10.10.80.3	(Default)						43
Structure .	V ACS Service Monitoring	08/22/2006	16:06:39	Authen OK	test	Default Group	00-40- 96-A6- D6-F6	29	10.10.80.3	(Default)						43
Collection and	Stuck to Helip	08/22/2006	16:06:29	Authen OK	test	Default Group	00-40- 96-A6- D6-F6	29	10.10.80.3	(Default)						43

4. Nach erfolgreicher RADIUS/EAP-Authentifizierung wird der Wireless-Client (in diesem Beispiel 00:40:96:ab:36:2f) mit dem AP/WLAN-Controller authentifiziert.

Enco Serres									Save Carlig	retab	1 Ping	Logost   Refred
.A. A.	MONITOR WLAPA	CONTROLLER	WIRELESS SECURITY	MANAGEMENT DO	MMANDS HELF	P	0.000					
Wireless	Clients								Zero	\$ 1	to 4	of 4
Access Points ALAFE	Search by MAC ad	dress	Search									
802.338 Hados 802.338/g Rados	Client MAC Addy	AP Name	WLAN	Туре	Statue	Auth	Port					
Mesh	88:01:55:45:54:30	AP0854.6948.0594	Usknov	vn 882.5	1b Probing	No	29	<b>Detail LiskText Disable</b>	Remove 882.11aTSH	902.1	15/STSN	
Reques	88 x 89 x 96 x 80 x 36 x 21	AP0054.6940.8594	Enterp	rice 882.1	1g Associated	Yes	29	<b>Detail LiskTect Disable</b>	Remove \$52,11aTSM	902.1	15/STSM	
Roque APs	88140796186184169	AP0054.6948.8480	Uniunov	vii: 882.3	15 Probing	No	29	Detail LinkTest Disable	Receive \$52,11aTSH	802.1	15-STSP	
Knowe Regue APs Roque Clients	88140/96186rd6rf6	AP0054.6948.8480	Enterp	rise 882.3	1g Associated	Ne	29	Detail LiekTest Disable	Remark BE2.114TSH	802.1	10-Statisti	
Adhoc Rogues												
Clients												

## Anhang

Zusätzlich zu den Diagnose- und Statusinformationen, die über den Cisco Secure ACS und den Cisco WLAN Controller verfügbar sind, gibt es weitere Punkte, die zur Diagnose der EAP-FAST-Authentifizierung verwendet werden können. Obwohl die meisten Authentifizierungsprobleme ohne WLAN-Sniffer oder ohne Debugging-EAP-Austausch beim WLAN-Controller diagnostiziert werden können, ist dieses Referenzmaterial zur Unterstützung der Fehlerbehebung enthalten.

### Sniffer Capture für EAP-FAST Exchange

Diese 802.11-Sniffer-Erfassung zeigt den Authentifizierungsaustausch.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=R,SN=2867,FN= 0,Status
00:14:1B:5A:33:D0	+	11	70*	24.0	101	00.036453	802.11 Assoc Rsp	FC=R,SN=2867,FN= 0,Status
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F,SN=2868,FN= 0
Aironet: A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC-T,SN- 3,FN- 0
00:14:18:5A:33:D0	1	11	71%	1.0	14	00.123517	802.11 Ack	FC=
00:14:1B:5A:33:D0		11	674	54.0	65	00.165611	802.1x	FC=.F,SN=2870,FN= 0
Aiconet: A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T,SN= 4,FN= 0
00:14:18:5A:33:D0	8	11	70%	1.0	14	00.174228	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F,SN=2871,FN= 0
Aiconet: A0:36:2F		11	58*	1.0	282	00.200632	EAP Response	FC=T,SN= 5,FN= 0
Aiconet:A0:36:2F		11	584	1.0	282	00.203340	EAP Response	FC=TR,SN= 5,FN= 0
00:14:1B:5A:33:D0	+	11	71%	1.0	14	00.203639	802.11 Ack	FC
00:14:18:5A:33:D0		11	70%	54.0	166	00.207634	802.1x	FC=.F,5N=2872,FN= 0
Aironet:A0:36:2F		11	554	1.0	105	00.216295	EAP Response	FC=T,SN= 6,FN= 0
Aironet: A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC-TR,SN= 6,FN= 0
00:14:18:5A:33:D0	1	11	70%	1.0	14	00.217754	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F,SN=2874,FN= 0
Aiconet: A0:36:2F		11	55>	1.0	152	00.254189	EAP Response	FC=T,SN= 7,FN= 0
00:14:18:5A:33:D0	8	11	684	1.0	14	00.254499	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R,SN=2875,FN= 0
Aiconet: A0:36:2F		11	553	1.0	232	00.318087	EAP Response	FC=T,SN= 8,FN= 0
00:14:1B:5A:33:D0	¥	11	70%	1.0	14	00.318383	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F,SN=2877,FN= 0
00:14:18:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R, 5N=2877, FN= 0
00:14:1B:5A:33:D0		11	674	48.0	44	00.326922	802.1x	FC=.F.R,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	678	54.0	157	00.326964	802.1x	FC=.F,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAPOL-Key	FC=T,SN= 9,FN= 0
00:14:1B:5A:33:D0	+	11	70%	1.0	14	00.334019	802.11 Ack	FC
00:14:1B:5A:33:D0		11	653	54.0	207	00.340467	802.1x	FC=.F,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	674	54.0	207	00.341130	802.1x	FC=.F.R,SN=2879,FN= 0
Aironet: A0:36:2F		11	57%	1.0	135	00.342542	EAPOL-Key	FC-T,SN- 10,FN- 0

Dieses Paket zeigt die erste EAP-FAST EAP-Antwort an.

**Hinweis:** Wie beim CSSC-Client konfiguriert, wird anonymous in der ersten EAP-Antwort als äußere EAP-Identität verwendet.

Pasket	12 [x] 🖙 📑	
D D-1	Frame Control Flags:	\$0000001 [1]
	-9	0
	-9	.0WFF Hot Emabled
	-9	Ho More Data
	-9	Fower Management - active mode
	-9	0 This is not a Re-Transmission
	-9	
	-9	0. Not an Exit from the Distribution System
	-9	1 To the Distribution System
-6	Buration:	314 Microseconds (2-3)
	BSSID:	00:14:1B:5A:33:D0 [4-9]
	Source:	00:40:96:A0:36:27 Aircost: A0: 36:2F [10-15]
	Bestination:	00:14:1B:5A:33:D0 [16-21]
-6	Seq. Number:	3 [22-23 Hash 0x7770]
-6	Erag. Number:	0 [22 Mask 0x07]
P-7 5	02.2 Logical Link Conts	rol (LLC) Keader
-6	Best. SAP:	ORAA SMAP (24)
-9	Source SAP:	ORAA SWAF [25]
-9	Cornand:	0x03 Uzzumbered Information [26]
-9	Vendor ID:	0x00000 [27-29]
-9	Protocol Type:	0x898# \$02.ix Authentication [30-31]
P- <b>T</b>	02.1x Authentication	
-9	Protocol Version:	1 [32]
-9	Packet Type:	0 EAP - Facket [33]
-9	Body Length:	14 [34-35]
B-1	Extensible Authentica	tion Protocol
	- Q Code:	2 Response [36]
	g identifier:	4 1371
	- g Length:	14 [38-33]
	- (p Type:	1 Zdentzty 1401
	of Type-Bata:	anonymous [41-49]

### Debuggen am WLAN-Controller

Diese Debug-Befehle können am WLAN-Controller verwendet werden, um den Fortschritt des Authentifizierungsaustauschs zu überwachen:

- debug aaa events enable
- debuggen aaa detail enable

- debug dot1x-Ereignisse aktivieren
- debug dot1x status enable

Dies ist ein Beispiel für den Beginn einer Authentifizierungstransaktion zwischen dem CSSC-Client und dem ACS, die vom WLAN-Controller mit den Debuggen überwacht wird:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
  moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
  Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
  Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
  00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
  Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:
                           Callback.....0x10372764
                              protocolType...0x00040001
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:proxyState....00:40:96:A0:36:2F-11:00Thu Aug 24 18:20:54 2006:Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
  Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
  RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006: structureSize..147
                              resultCode....255
protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:
                           proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:
                                Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
  for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
  (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
  AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
  mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

#### Dies ist der erfolgreiche Abschluss des EAP-Austausches vom Controller-Debug (mit WPA2-Authentifizierung):

Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Accept for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA override for station 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station

00:40:96:a0:36:2f source: 4, valid bits: 0x0 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1' Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry for station 00:40:96:a0:36:2f (RSN 2) Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID 00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: New PMKID: (16) Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success to mobile 00:40:96:a0:36:2f (EAP Id 0) Thu Aug 24 18:20:54 2006: Including PMKID in M1 (16) Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0 Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Success state (id=0) for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success while in Authenticating state for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x moving mobile 00:40:96:a0:36:2f into Authenticated state Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-Key from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in PKT\_START state (message 2) from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission timer for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messal Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-Key from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: AccountingMessage Accounting Interim: 0x138dd764 Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs: Thu Aug 24 18:20:54 2006: AVP[01] User-Name.....enterprise (10 bytes) Thu Aug 24 18:20:54 2006: AVP[02] Nas-Port.....0x0000001d (29) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[03] Nas-Ip-Address......0x0a0a5003 (168448003) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[04] Class.....CACS:0/28b5/a0a5003/29 (22 bytes) Thu Aug 24 18:20:54 2006: AVP[05] NAS-Identifier.....ws-3750 (7 bytes) Thu Aug 24 18:20:54 2006: AVP[06] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[07] 96:a0:36:2f/14 (29 bytes) Thu Aug 24 18:20:54 2006: AVP[08] Thu Aug 24 18:20:54 2006: AVP[09] Thu Aug 24 18:20:54 2006: AVP[10]

Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[11] Tunnel-Group-Id.....0x3832 (14386) (2 bytes) Thu Aug 24 18:20:54 2006: AVP[12] Acct-Status-Type.....0x00000003 (3) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[13] Acct-Input-Octets......0x000b99a6 (760230) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[14] Acct-Output-Octets......0x00043a27 (277031) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[15] Acct-Input-Packets......0x0000444b (17483) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[16] Acct-Output-Packets......0x0000099b (2459) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[17] Thu Aug 24 18:20:54 2006: AVP[18] Acct-Delay-Time......0x00000000 (0) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[19] Calling-Station-Id......10.10.82.11 (11 bytes) Thu Aug 24 18:20:54 2006: AVP[20] Called-Station-Id.....10.10.80.3 (10 bytes) Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission timer for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:57 2006: User admin authenticated

## Zugehörige Informationen

- Installationsanleitung für Cisco Secure ACS für Windows Server
- Konfigurationsleitfaden für Cisco Secure ACS 4.1
- Einschränken des WLAN-Zugriffs auf der Basis der SSID mit WLC und Cisco Secure ACS -Konfigurationsbeispiel
- EAP-TLS unter Unified Wireless Network mit ACS 4.0 und Windows 2003
- Konfigurationsbeispiel für dynamische VLAN-Zuweisung mit RADIUS-Server und Wireless
   LAN-Controller
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>