Exemplo de configuração de servidor EAP local de rede sem fio unificada

Contents

Introdução

Este documento descreve a configuração de um servidor local de Extensible Authentication Protocol (EAP) em um Controlador de LAN Wireless (WLC) da Cisco para a autenticação dos usuários sem fio.

O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema de back-end for interrompido ou o servidor de autenticação externo for desativado. Quando você habilita o EAP local, o controlador serve como o servidor de autenticação e o banco de dados de usuário local, removendo assim a dependência de um servidor de autenticação externo. O EAP Local recupera as credenciais do usuário do banco de dados do usuário local ou do banco de dados back-end do Lightweight Diretory Access Protocol (LDAP) para autenticar usuários. O EAP local oferece suporte à autenticação EAP leve (LEAP), Autenticação flexível EAP via encapsulamento seguro (EAP-FAST) e Segurança de camada de transporte EAP (EAP-TLS) entre o controlador e os clientes sem fio.

Observe que o servidor EAP local não estará disponível se houver uma configuração de servidor RADIUS externo global na WLC. Todas as solicitações de autenticação são encaminhadas para o RADIUS externo global até que o servidor EAP local esteja disponível. Se a WLC perder a conectividade com o servidor RADIUS externo, o servidor EAP local se tornará ativo. Se não houver configuração global do servidor RADIUS, o servidor EAP local se tornará imediatamente ativo. O servidor EAP local não pode ser usado para autenticar clientes conectados a outras WLCs. Em outras palavras, uma WLC não pode encaminhar sua solicitação EAP para outra WLC para autenticação. Cada WLC deve ter seu próprio servidor EAP local e banco de dados individual.

Observação: use esses comandos para impedir que a WLC envie solicitações a um servidor radius externo .

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

O servidor EAP local suporta estes protocolos na versão de software 4.1.171.0 e mais recente:

- LEAP
- EAP-FAST (nome de usuário/senha e certificados)
- EAP-TLS

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar WLCs e pontos de acesso lightweight (LAPs) para operação básica
- Conhecimento do Lightweight Access Point Protocol (LWAPP) e dos métodos de segurança sem fio
- Conhecimento básico da autenticação EAP local.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows XP com placa adaptadora CB21AG e Cisco Secure Services Client versão 4.05
- Controladora de LAN sem fio 4400 4.1.171.0 da Cisco

- Autoridade de Certificação Microsoft no servidor Windows 2000

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar o EAP Local no Cisco Wireless LAN Controller

Este documento supõe que a configuração básica da WLC já foi concluída.

Configuração de EAP Local

Conclua estas etapas para configurar o EAP Local:

1. Adicionar um usuário de rede local:

   Na GUI, selecione Security > Local Net Users > New, insira o User Name, Password, Guest User, WLAN ID e Description e clique em Apply.

   Na CLI, você pode usar o comando config netuser add <username> <password> <WLAN id> <description> :

   Observação: esse comando foi reduzido para uma segunda linha devido a razões espaciais.

   ```
   <#root>

   (Cisco Controller) >

   config netuser add eapuser2 cisco123 1 Employee user local database
   ```

2. Especifique a ordem de recuperação de credencial do usuário.

   Na GUI, escolha Security > Local EAP > Authentication Priority. Em seguida, selecione LDAP, clique no botão "<" e clique em Apply. Isso coloca as credenciais do usuário no banco de dados local primeiro.

   Na CLI:

   ```
   <#root>

   (Cisco Controller) >

   config local-auth user-credentials local
   ```

3. Adicionar um perfil EAP:

Para fazer isso na GUI, escolha Security > Local EAP > Profiles e clique em New. Quando a nova janela for exibida, digite o Nome do perfil e clique em Aplicar.

Você também pode fazer isso usando o comando CLI config local-auth eap-profile add <profile-name>. Em nosso exemplo, o nome do perfil é EAP-test.

```
<#root>

(Cisco Controller) >

config local-auth eap-profile add EAP-test
```

4. Adicione um método ao perfil EAP.

   Na GUI, escolha Security > Local EAP > Profiles e clique no nome do perfil ao qual deseja adicionar os métodos de autenticação. Este exemplo usa LEAP, EAP-FAST e EAP-TLS. Clique em Apply para definir os métodos.

   Você também pode usar o comando CLI config local-auth eap-profile method add <method-name> <profile-name> . Em nosso exemplo de configuração, adicionamos três métodos ao perfil EAP-teste. Os métodos são LEAP, EAP-FAST e EAP-TLS cujos nomes de método são leap, fast e tls, respectivamente. Esta saída mostra os comandos de configuração da CLI:

```
<#root>

(Cisco Controller) >

config local-auth eap-profile method add leap EAP-test

(Cisco Controller) >

config local-auth eap-profile method add fast EAP-test

(Cisco Controller) >

config local-auth eap-profile method add tls EAP-test
```

5. Configure os parâmetros do método EAP. Usado somente para EAP-FAST. Os parâmetros a serem configurados são:

   - Chave do servidor (chave do servidor) — Chave do servidor para criptografar/descriptografar as PACs (Protected Access Credentials) (em hexadecimal).
   - Time to Live para PAC (pac-ttl) — Define o Time to Live para a PAC.
   - ID da autoridade (authority-id) — Define o identificador da autoridade.

- Provisão anônima (não comprovada) — Configura se a provisão anônima é permitida. Iss está habilitado por padrão.

Para a configuração por meio da GUI, escolha Security > Local EAP > EAP-FAST Parameters e insira a chave do servidor, Time to live para a PAC, o ID da autoridade (em hexadecimal) e os valores de Authority ID Information.

Estes são os comandos de configuração de CLI a serem usados para definir estes parâmetros para EAP-FAST:

```
<#root>

(Cisco Controller) >

config local-auth method fast server-key 12345678

(Cisco Controller) >

config local-auth method fast authority-id 43697369f1 CiscoA-ID

(Cisco Controller) >

config local-auth method fast pac-ttl 10
```

6. Habilitar autenticação local por WLAN:

   Na GUI, escolha WLANs no menu superior e selecione a WLAN para a qual você deseja configurar a autenticação local. Uma nova janela é exibida. Clique nas guias Security > AAA. Verifique a autenticação EAP local e selecione o nome do perfil EAP correto no menu suspenso, como mostra este exemplo:

   Você também pode executar o comando de configuração CLI config wlan local-auth enable <profile-name> <wlan-id> , como mostrado aqui:

```
<#root>

(Cisco Controller) >

config wlan local-auth enable EAP-test 1
```

7. Defina os parâmetros de segurança da camada 2.

   Na interface GUI, na janela WLAN Edit, vá para as guias Security > Layer 2 e escolha WPA+WPA2 no menu suspenso Layer 2 Security. Na seção Parâmetros WPA+WPA2, defina a Criptografia WPA como TKIP e a Criptografia WPA2 AES. Em seguida, clique em Apply.

   Na CLI, use estes comandos:

<#root>

```
(Cisco Controller) >
config wlan security wpa enable 1

(Cisco Controller) >
config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >
config wlan security wpa wpa2 ciphers aes enable 1
```

8. Verificar a configuração:

<#root>

```
(Cisco Controller) >
show local-auth config

User credentials database search order:
    Primary .....................................
Local DB

Timer:
    Active timeout ............................. Undefined
Configured EAP profiles:

 Name ..................................... EAP-test

      Certificate issuer ....................... cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No

Enabled methods ........................... leap fast tls


Configured on WLANs ....................... 1

EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key ................................ <hidden>
```

```
      TTL for the PAC ............................ 10
      Anonymous provision allowed ................ Yes
      Authority ID ............................... 43697369f10000000000000000000000
      Authority Information ...................... CiscoA-ID
```

Você pode ver parâmetros específicos da wlan 1 com o comando show wlan <wlan id> :

<#root>

```
(Cisco Controller) >

show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All

Local EAP Authentication........................ Enabled (Profile 'EAP-test')

Security


   802.11 Authentication:........................ Open System
   Static WEP Keys.............................. Disabled
   802.1X....................................... Disabled


Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Enabled

         AES Cipher.............................. Disabled


   WPA2 (RSN IE)............................... Enabled

         TKIP Cipher............................. Disabled


  AES Cipher............................... Enabled
```

```
                                                                  Auth Key Management
        802.1x.............................. Enabled
        PSK................................. Disabled
        CCKM................................ Disabled
   CKIP ..................................... Disabled
   IP Security............................... Disabled
   IP Security Passthru...................... Disabled
   Web Based Authentication.................. Disabled
--More-- or (q)uit
   Web-Passthrough........................... Disabled
   Conditional Web Redirect.................. Disabled
   Auto Anchor............................... Disabled
   Cranite Passthru.......................... Disabled
   Fortress Passthru......................... Disabled
   H-REAP Local Switching.................... Disabled
   Infrastructure MFP protection............. Enabled
                                          (Global Infrastructure MFP Disabled)
   Client MFP................................ Optional
   Tkip MIC Countermeasure Hold-down Timer..... 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Há outros parâmetros de autenticação local que podem ser configurados, em particular o temporizador de timeout ativo. Esse temporizador configura o período durante o qual o EAP local é usado após a falha de todos os servidores RADIUS.

Na GUI, escolha Security > Local EAP > General e defina o valor de hora. Em seguida, clique em Apply.

Na CLI, emita estes comandos:

<#root>

```
(Cisco Controller) >
```

config local-auth active-timeout ?

```
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >
```

config local-auth active-timeout 60

Você pode verificar o valor para o qual esse temporizador está configurado ao executar o comando show local-auth config.

<#root>

```
(Cisco Controller) >
```

show local-auth config

```
User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 60

Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. Se precisar gerar e carregar a PAC manual, você pode usar a GUI ou a CLI.

   Na GUI, selecione COMMANDS no menu superior e escolha Upload File na lista no lado direito. Selecione PAC (Protected Access Credential) no menu suspenso File Type. Insira todos os parâmetros e clique em Upload.

   Na CLI, digite estes comandos:

   <#root>

```
(Cisco Controller) >
transfer upload datatype pac

(Cisco Controller) >
transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >
transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >
transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >
transfer upload pac test1 60 cisco123

(Cisco Controller) >
transfer upload serverip 10.1.1.1

(Cisco Controller) >
transfer upload filename manual.pac
```

```
(Cisco Controller) >

transfer upload start


Mode..................................... TFTP
TFTP Server IP........................... 10.1.1.1
TFTP Path................................ /
TFTP Filename............................ manual.pac
Data Type................................ PAC
PAC User................................. test1
PAC Validity............................. 60 days
PAC Password............................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Autoridade de Certificação da Microsoft

Para usar a autenticação EAP-FAST versão 2 e EAP-TLS, a WLC e todos os dispositivos clientes devem ter um certificado válido e também devem conhecer o certificado público da Autoridade de Certificação.

Instalação

Se o Windows 2000 Server ainda não tiver os serviços de autoridade de certificação instalados, você precisará instalá-los.

Conclua estes passos para ativar a Microsoft Certification Authority em um Windows 2000 Server:

1. No Painel de controle, selecione Adicionar ou remover programas. :
2. Selecione Add/Remove Windows Components no lado esquerdo.
3. Verifique os serviços de certificado.

   Revise este aviso antes de continuar:
4. Selecione o tipo de Autoridade de Certificação que deseja instalar. Para criar uma autoridade independente simples, selecione CA raiz independente.
5. Insira as informações necessárias sobre a Autoridade de Certificação. Essas informações criam um certificado autoassinado para sua autoridade de certificação. Lembre-se do nome da CA que você usa.

   A Autoridade de Certificação armazena os certificados em um banco de dados. Este exemplo usa a configuração padrão proposta pela Microsoft:
6. Os serviços da Autoridade de Certificação Microsoft usam o Microsoft Web Server do IIS

para criar e gerenciar certificados de cliente e servidor. É necessário reiniciar o serviço IIS para:

O Microsoft Windows 2000 Server agora instala o novo serviço. Você precisa ter o CD de instalação do Windows 2000 Server para instalar novos componentes do Windows.

A Autoridade de Certificação agora está instalada.

Instale o certificado no Cisco Wireless LAN Controller

Para usar EAP-FAST versão 2 e EAP-TLS no servidor EAP local de um Cisco Wireless LAN Controller, siga estas três etapas:

1. Instale o certificado do dispositivo no Controller de LAN Wireless.
2. Baixe um certificado CA do fornecedor para o controlador de LAN sem fio.
3. Configure a controladora Wireless LAN para usar EAP-TLS.

Observe que, no exemplo mostrado neste documento, o Access Control Server (ACS) está instalado no mesmo host que o Microsoft Ative Diretory e a Microsoft Certification Authority, mas a configuração deverá ser a mesma se o servidor ACS estiver em um servidor diferente.

Instale o certificado do dispositivo na controladora Wireless LAN

Conclua estes passos:

1. . Conclua estes passos para gerar o certificado a ser importado para o WLC:
    a. Vá para http://<serverIpAddr>/certsrv.
    b. Selecione Request a Certificate e clique em Next.
    c. Escolha Solicitação avançada e clique em Avançar.
    d. Escolha Enviar uma solicitação de certificado a esta autoridade de certificação usando um formulário e clique em Avançar.
    e. Escolha Servidor Web para Modelo de Certificado e insira as informações relevantes. Em seguida, marque as chaves como exportáveis.
    f. Agora você recebe um certificado que precisa instalar no computador.
2. Conclua estas etapas para recuperar o certificado do PC:
    a. Abra um navegador Internet Explorer e escolha Ferramentas > Opções da Internet > Conteúdo.
    b. Clique em Certificados.

c. Selecione o certificado recém-instalado no menu suspenso.

d. Clique em Exportar.

e. Clique em Next duas vezes e escolha Yes export the private key. Esse formato é o PKCS#12 (formato .PFX).

f. Selecione Enable strong protection.

g. Digite uma senha.

h. Salve-o em um arquivo <time2.pfx>.

3. Copie o certificado no formato PKCS#12 para qualquer computador no qual você tenha o Openssl instalado para convertê-lo no formato PEM.

```
openssl pkcs12 -in tme2.pfx -out tme2.pem

!--- The command to be given, -in

          .

Enter Import Password:

!--- Enter the password given previously, from step 2g.

MAC verified OK
Enter PEM pass phrase:

!--- Enter a phrase.

Verifying - Enter PEM pass phrase:
```

4. Faça o download do certificado do dispositivo em formato PEM convertido no WLC.

<#root>

```
(Cisco Controller) >

transfer download datatype eapdevcert

(Cisco Controller) >

transfer download certpassword password
```

```
!--- From step 3.

Setting password to <cisco123>

(Cisco Controller) >

transfer download filename tme2.pem


(Cisco Controller) >

transfer download start


Mode..................................................... TFTP
Data Type................................................ Vendor Dev Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

5. Depois de reinicializado, verifique o certificado.

```
<#root>

(Cisco Controller) >

show local-auth certificates


Certificates available for Local EAP authentication:

Certificate issuer ..............................vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
  Device certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

Baixar um Certificado de CA do Fornecedor para o Controlador de LAN Sem Fio

Conclua estes passos:

1. Conclua estas etapas para recuperar o Certificado de CA do Fornecedor:

    a. Vá para http://<serverIpAddr>/certsrv.

    b. Escolha Recuperar o Certificado de Autoridade de Certificação e clique em Avançar.

    c. Escolha o Certificado CA.

    d. Clique em DER encoded.

    e. Clique em Download CA certificate e salve o certificado como rootca.cer.

2. Converta a CA do fornecedor do formato DER no formato PEM com o comando openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM.

   O arquivo de saída é rootca.pem no formato PEM.

3. Faça o download do certificado da CA do fornecedor:

```
<#root>
(Cisco Controller) >
transfer download datatype eapcacert

(Cisco Controller) >
transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.
(Cisco Controller) >
transfer download filename rootca.pem

(Cisco Controller) >
transfer download start ?

(Cisco Controller) >
transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor CA Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ rootca.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.
```

```
Certificate installed.
  Reboot the switch to use new certificate.
```

Configurar o controlador de LAN sem fio para usar EAP-TLS

Conclua estes passos:

Na GUI, escolha Security > Local EAP > Profiles, escolha o perfil e verifique as seguintes configurações:

- Certificado local necessário está habilitado.
- O Certificado de Cliente Necessário está habilitado.
- O Emissor do Certificado é o Fornecedor.
- Verificar se os certificados da autoridade de certificação estão habilitados.

Instalar o Certificado da Autoridade de Certificação no Dispositivo Cliente

Baixar e Instalar um Certificado CA Raiz para o Cliente

O cliente deve obter um Certificado CA raiz de um servidor de Autoridade de Certificação. Há vários métodos que você pode usar para obter um certificado de cliente e instalá-lo na máquina com o Windows XP. Para adquirir um certificado válido, o usuário do Windows XP deve estar conectado usando sua ID de usuário e deve ter uma conexão de rede.

Um navegador da Web no cliente Windows XP e uma conexão com fio à rede foram usados para obter um certificado de cliente do servidor de autoridade de certificação raiz privada. Este procedimento é usado para obter o certificado de cliente de um servidor de Autoridade de Certificação Microsoft:

1. Use um navegador da Web no cliente e aponte o navegador para o servidor da Autoridade de Certificação. Para fazer isso, digite http://IP-address-of-Root-CA/certsrv.
2. Faça login usando Domain_Name\user_name. Você deve fazer login usando o nome de usuário do indivíduo que deve usar o cliente XP.
3. Na janela Welcome (Bem-vindo), escolha Retrieve a CA certificate (Recuperar um certificado CA) e clique em Next.
4. Selecione Codificação Base64 e Fazer download do certificado CA.
5. Na janela Certificado emitido, clique em Instalar este certificado e clique em Avançar.

6. Escolha Automatically select the certificate store e clique em Next, para mensagem de Importação bem-sucedida.

7. Conecte-se à Autoridade de Certificação para recuperar o certificado da Autoridade de Certificação:

8. Clique em Baixar certificado de CA.

9. Para verificar se o certificado da Autoridade de Certificação está instalado corretamente, abra o Internet Explorer e escolha Ferramentas > Opções da Internet > Conteúdo > Certificados.

   Em Autoridade de Certificação Raiz Confiável, você deve ver sua Autoridade de Certificação recém-instalada:

Gerar um certificado de cliente para um dispositivo cliente

O cliente deve obter um certificado de um servidor de Autoridade de Certificação para que a WLC autentique um cliente WLAN EAP-TLS. Há vários métodos que você pode usar para obter um certificado de cliente e instalá-lo na máquina com o Windows XP. Para adquirir um certificado válido, o usuário do Windows XP deve estar conectado usando sua ID de usuário e deve ter uma conexão de rede (uma conexão com fio ou uma conexão WLAN com segurança 802.1x desabilitada).

Um navegador da Web no cliente Windows XP e uma conexão com fio à rede são usados para obter um certificado de cliente do servidor de autoridade de certificação raiz privada. Este procedimento é usado para obter o certificado de cliente de um servidor de Autoridade de Certificação Microsoft:

1. Use um navegador da Web no cliente e aponte o navegador para o servidor da Autoridade de Certificação. Para fazer isso, digite http://IP-address-of-Root-CA/certsrv.

2. Faça login usando Domain_Name\user_name. Você deve fazer login usando o nome de usuário do indivíduo que usa o cliente XP. (O nome de usuário é incorporado no certificado do cliente.)

3. Na janela Welcome (Bem-vindo), escolha Request a certificate (Solicitar um certificado) e clique em Next.

4. Escolha Solicitação avançada e clique em Avançar.

5. Escolha Enviar uma solicitação de certificado a esta autoridade de certificação usando um formulário e clique em Avançar.

6. No form Solicitação Avançada de Certificado, escolha o Modelo de Certificado como Usuário, especifique o Tamanho da Chave como 1024 e clique em Enviar.

7. Na janela Certificado emitido, clique em Instalar este certificado. Isso resulta na instalação bem-sucedida de um certificado de cliente no cliente Windows XP.

8. Selecione Client Authentication Certificate.

   O certificado do cliente foi criado.

9. Para verificar se o certificado está instalado, vá para o Internet Explorer e escolha Ferramentas > Opções da Internet > Conteúdo > Certificados. Na guia Pessoal, você deverá ver o certificado.

EAP-TLS com Cisco Secure Services Client no dispositivo cliente

Conclua estes passos:

1. A WLC, por padrão, envia o SSID por broadcast, para que ele seja mostrado na lista Create Networks de SSIDs verificados. Para criar um perfil de rede, você pode clicar no SSID na lista (Empresa) e clicar em Criar rede.

   Se a infraestrutura da WLAN estiver configurada com o SSID de broadcast desabilitado, você deverá adicionar o SSID manualmente. Para fazer isso, clique em Add em Access Devices e insira manualmente o SSID apropriado (por exemplo, Enterprise). Configure o comportamento de sondagem ativo para o cliente. Isto é, onde o cliente investiga ativamente o SSID configurado. Especifique Atively search for this access device depois de inserir o SSID na janela Add Access Device.

   Nota:As configurações de porta não permitirão modos corporativos (802.1X) se as configurações de autenticação EAP não forem primeiro configuradas para o perfil.

2. Clique em Create Network para iniciar a janela Network Profile, que permite associar o SSID escolhido (ou configurado) a um mecanismo de autenticação. Atribua um nome descritivo ao perfil.

   Nota:Vários tipos de segurança de WLAN e/ou SSIDs podem ser associados neste perfil de autenticação.

3. Ative a autenticação e verifique o método EAP-TLS. Em seguida, clique em Configure para configurar as propriedades EAP-TLS.

4. Em Resumo da configuração de rede, clique em Modificar para configurar as configurações de EAP/credenciais.

5. Especifique Turn On Authentication, escolha EAP-TLS em Protocol e escolha Username como a Identity.

6. Especifique Usar Credenciais de Logon Único para usar credenciais de logon para autenticação de rede. Clique em Configurar para configurar parâmetros EAP-TLS.

7. Para ter uma configuração EAP-TLS segura, você precisa verificar o certificado do servidor RADIUS. Para fazer isso, marque Validar certificado do servidor.

8. Para validar o certificado do servidor RADIUS, você precisa fornecer informações do Cisco

Secure Services Client para aceitar apenas o certificado correto. Escolha Client > Trusted Servers > Manage Current User Trusted Servers.

9. Dê um nome para a regra e verifique o nome do certificado do servidor.

   A configuração EAP-TLS foi concluída.

10. Conecte-se ao perfil de rede sem fio. O Cisco Secure Services Client solicita o login do usuário:

    O Cisco Secure Services Client recebe o certificado do servidor e o verifica (com a regra configurada e a Autoridade de certificação instalada). Em seguida, ele solicita que o certificado seja usado para o usuário.

11. Depois que o cliente se autenticar, escolha SSID no Perfil na guia Gerenciar redes e clique em Status para consultar os detalhes da conexão.

    A janela Detalhes da conexão fornece informações sobre o dispositivo cliente, status e estatísticas da conexão e método de autenticação. A guia Detalhes de WiFi fornece detalhes sobre o status da conexão 802.11, que inclui o RSSI, o canal 802.11 e a autenticação/criptografia.

Comandos debug

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Esses comandos debug podem ser empregados na WLC para monitorar o progresso da troca de autenticação:

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable
- debug aaa local-auth eap events enable

  OU

- debug aaa all enable

Informações Relacionadas

- Guia de configuração do Cisco Wireless LAN Controller, versão 4.1
- Suporte à tecnologia WLAN
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.