# Serviços da postura no manual de configuração de Cisco ISE

## Índice

# Introdução

Este original descreve serviços da postura, abastecimento do cliente, criação da política da postura, e configuração da política de acesso para o Cisco Identity Services Engine (ISE). Os resultados da avaliação do valor-limite para ambos os clientes prendidos (conectados aos switch Cisco) e clientes Wireless (conectados aos controladores do Cisco Wireless) são discutidos.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Identity Services Engine (ISE)
- Configuração do switch de software do ® do Cisco IOS
- Configuração do controlador de LAN do Cisco Wireless (WLC)

## Componentes Utilizados

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

- Versão 1.1.3 de Cisco ISE
- Versão 15.0(2) SE2 do Cisco Catalyst 3560 Series Switch
- Versão 7.4.100.0 do Cisco 2504 Series WLC

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# Informações de Apoio

## Serviços da postura ISE

Os trabalhos dos serviços da postura são compreendidos de três seções de configuração principal:

- Abastecimento do cliente
- Política da postura
- Política da autorização

## Abastecimento do cliente

A fim executar a avaliação da postura e determinar o estado da conformidade de um valor-limite, é necessário provision o valor-limite com um agente. O agente do Network Admission Control (NAC) pode ser persistente, por meio de que o agente é instalado e carregado automaticamente cada vez um usuário entra. Alternativamente, o agente NAC pode ser temporal, por meio de que um agente com suporte na internet é transferido dinamicamente ao valor-limite para cada sessão nova e removido então depois que o processo da avaliação da postura. Os agentes NAC igualmente facilitam a remediação e fornecem uma política de uso aceitável opcional (AUP) ao utilizador final.

Consequentemente, uma das primeiras etapas nos trabalhos é recuperar os arquivos do agente da site da Cisco na Web e criar as políticas que determinam que agente e arquivos de configuração são transferidos aos valores-limite, com base em atributos tais como a identidade do usuário e o tipo ósmio do cliente.

## Política da postura

A política da postura define o grupo de exigências para que um valor-limite seja complacente julgado baseado na presença do arquivo, a chave de registro, o processo, o aplicativo, o Windows, e (AV) verificações anti-vírus e regras /anti-spyware (COMO). A política da postura é aplicada aos valores-limite baseados em um conjunto de condição definido tal como a identidade do usuário e o tipo ósmio do cliente. O estado da conformidade (postura) de um valor-limite pode ser:

- Desconhecido: Nenhum dados foi recolhido a fim determinar o estado da postura.
- Noncompliant: Uma avaliação da postura foi executada, e umas ou várias exigências falharam.
- Complacente: O valor-limite é complacente com todos os requisitos imperativos.

As exigências da postura são baseadas em um grupo configurável de umas ou várias circunstâncias. As circunstâncias simples incluem uma única verificação da avaliação. As circunstâncias compostas são um grupo lógico de umas ou várias circunstâncias simples. Cada exigência é associada com uma ação da remediação que ajude valores-limite a satisfazer a exigência, tal como a atualização de assinatura AV.

## Política da autorização

A política da autorização define os níveis do acesso de rede e de serviços opcionais a ser entregados a um valor-limite baseado no estado da postura. Os valores-limite que são julgados não complacentes com política da postura podem opcionalmente ser quarantined até que o valor-limite se torne complacente; por exemplo, uma política típica da autorização pode limitar o acesso de rede de um usuário para posture e os recursos da remediação somente. Se a remediação pelo agente ou pelo utilizador final é bem sucedida, a seguir a política da autorização pode conceder acesso de rede privilegiado ao usuário. A política é reforçada frequentemente com listas de controle de acesso carregável (dACLs) ou atribuição do VLAN dinâmico. Neste exemplo de configuração, os dACLs são usados para a aplicação do acesso do valor-limite.

## Trabalhos do exemplo da postura

Nestes arquivos persistentes (agente NAC) e temporais do exemplo de configuração, (da Web do agente) do agente são transferidos ao ISE, e as políticas de abastecimento do cliente são definidas que exigem usuários de domínio transferir o agente e usuários convidado NAC para transferir o agente da Web.

Antes da avaliação da postura as políticas e as exigências são configuradas, a política da autorização é atualizada para aplicar perfis da autorização aos usuários de domínio e aos convidados que são embandeirados como noncompliant. O perfil novo da autorização definido no este limites de configuração alcança para posture e recursos da remediação. O acesso de rede é permitido aos empregados e os usuários convidado embandeirados como complacente regular. Uma vez que os serviços do abastecimento do cliente foram verificados, as exigências da postura estão configuradas a fim verificar para ver se há a instalação anti-vírus, atualizações da definição de vírus, e atualizações críticas de Windows.

> Nota: Verifique todos os artigos nestes valor-limite e listas de verificação ISE antes que você tente configurar a postura.

## Lista de verificação do valor-limite

1. O nome de domínio totalmente qualificado ISE (FQDN) deve ser solucionável pelo dispositivo de ponto final.
2. Verifique que o navegador do valor-limite está configurado como mostrado aqui:

   **Firefox ou Chrome**: De encaixe de Javas deve ser permitido nos navegadores.**Internet explorer**: ActiveX deve ser permitido nas configurações do navegador.**Internet explorer 10**:**Importando o certificado auto-assinado**: Se você está usando um certificado auto-assinado para o ISE, execute o internet explorer 10 no modo de administração a fim instalar estes Certificados.**Modo de compatibilidade**: O modo de compatibilidade deve ser mudado em ajustes do internet explorer 10 a fim permitir a transferência do agente NAC. A fim mudar estes ajuste, direito-clique a barra azul na parte superior da tela do internet explorer 10, e escolher a **barra do comando**. Navegue às **ferramentas >** aos ajustes da **opinião da compatibilidade**, e adicionar o IP ou o FQDN ISE à lista do local.
   **Permitindo o controle activex**: Cisco ISE instala o agente de Cisco NAC e o agente da Web com o controle activex. No internet explorer 10, a opção a alertar para controles activex é desabilitada à revelia. Tome estas etapas a fim permitir esta opção:
   Navegue às **ferramentas > às opções de internet**.Navegue à **ABA de segurança**, e clique o **nível do Internet** e do **costume**.Nos controles activex e nos encaixes secione, permita o **alerta automático para controles activex**.
3. Se um Firewall existe localmente no cliente ou ao longo do caminho de rede ao ISE, você deve abrir estas portas para uma comunicação ISE NAC:

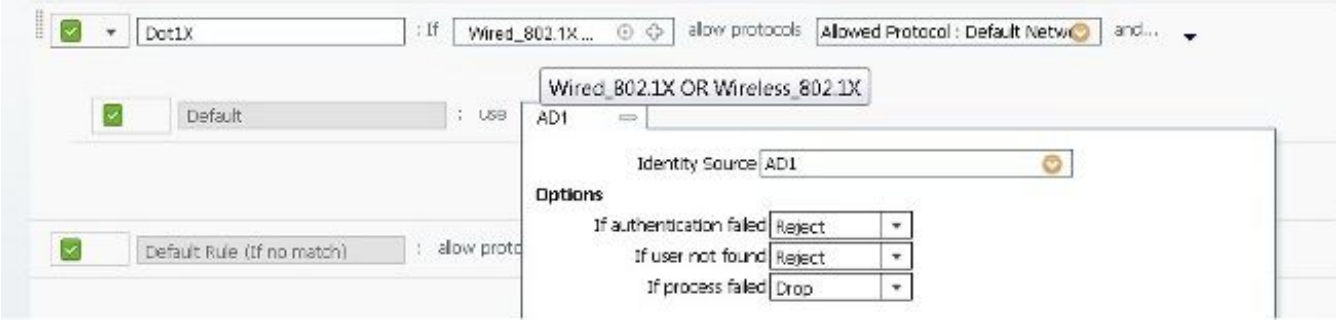
   UDP/TCP 8905: Usado para uma comunicação da postura entre o agente NAC e o ISE (porta suíça).UDP/TCP 8909: Usado para o abastecimento do cliente.TCP 8443: Usado para o convidado e a descoberta da postura.Nota: O ISE já não usa a porta TCP 8906 do legado.
4. Se o cliente tem um servidor proxy configurado, altere os ajustes do proxy a fim excluir o IP address do ISE. A falha fazer quebra assim as comunicações exigidas para a autenticação da Web central (CWA) e o abastecimento do cliente.

## Lista de verificação ISE

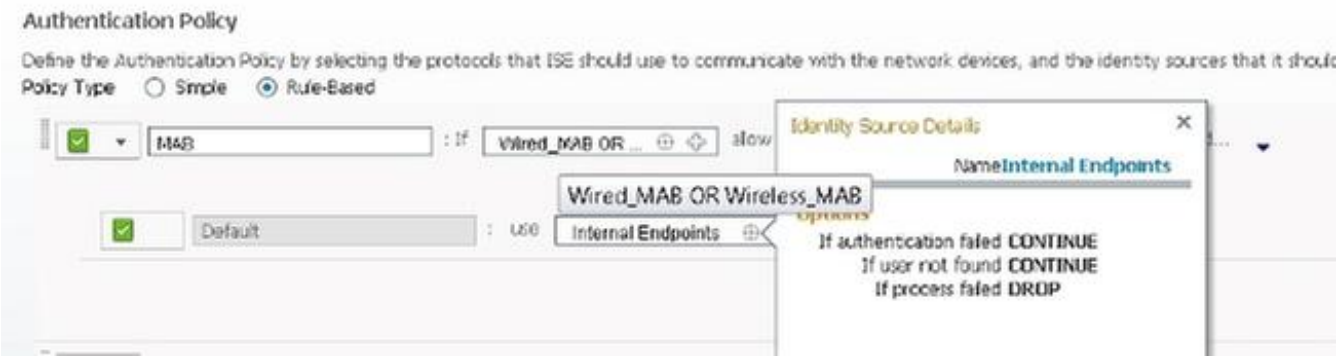
- Navegue à **administração > fontes externos > diretório ativo da identidade**, e verifique que o ISE está juntado ao domínio do diretório ativo (AD).

- Clique a aba dos **grupos**, e verifique que o grupo de usuários de domínio está adicionado à configuração AD.
- Navegue à **administração > aos recursos de rede > aos dispositivos de rede**, e verifique que o interruptor e os WLC estão definidos como os dispositivos do acesso de rede (NAD).
- Sob a **política > a autenticação**, assegure-se de que o dot1x e as regras do desvio da autenticação de MAC (MAB) estejam configurados como descritas aqui:

  As autenticações do dot1x para prendido e clientes Wireless são enviadas à loja da identidade AD.




  As autenticações MAB para prendido e dispositivos Wireless são enviadas aos valores-limite internos; seja certo verificar a opção **se o usuário não encontrado CONTINUA**.




# Configurar o ISE

## Vista geral da configuração ISE

Esta configuração do exemplo ISE é compreendida destas etapas:

1. Configurar e distribua serviços do abastecimento do cliente.
2. Configurar políticas da autorização.
3. Configurar políticas da postura.
4. Configurar a remediação do serviço da atualização de Windows Server (WSUS).

## Configurar e distribua serviços do abastecimento do cliente

1. Verifique a configuração de proxy ISE.

Navegue à **administração > ao sistema > aos ajustes > ao proxy**. Se um proxy é exigido para o acesso ao Internet, termine o server e os detalhes de porta.

2. Transfira verificações PRE-construídas da postura para AV/AS e Microsoft Windows.

   Navegue à **administração > ao sistema > aos ajustes > à postura > às atualizações**. A informação de atualização na placa à direita inferior deve estar vazia desde que nenhuma atualização foi transferida ainda. Configurar estes valores:

   Clique a **atualização agora**, e reconheça o aviso que as atualizações podem tomar algum tempo para terminar.

   Nota: Se o ISE não tem o acesso ao Internet, as atualizações autônomas da postura estão disponíveis para a transferência no cisco.com.

3. (Opcional) configurar ajustes gerais para o comportamento do agente.

   Selecione a **administração > o sistema > os ajustes > a postura > ajustes gerais**, e reveja os valores padrão para o temporizador da remediação, o atraso da transição de rede, e o estado da postura do padrão. Ajuste o temporizador da remediação a 8 minutos.Verifique (permita) a **tela automaticamente próxima do sucesso do início de uma sessão após a** caixa de seleção, e ajuste a hora aos segundos 5 como mostrado aqui:

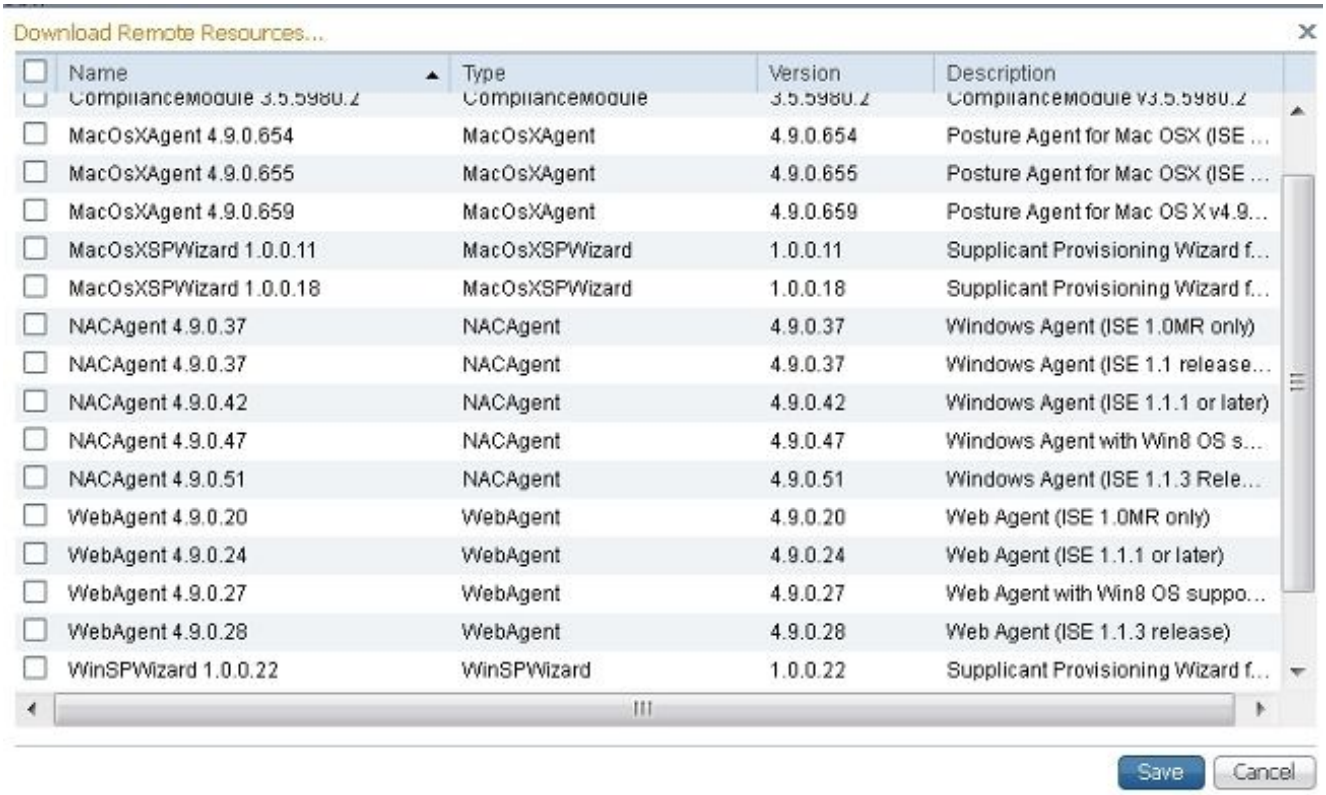
   Click **Save**.
   Nota: Valores atribuídos através da ultrapassagem do perfil do agente estas configurações globais. O estado da postura do padrão define o estado para os clientes que não têm um agente NAC instalado. Se o abastecimento do cliente não está sendo usado, este valor pode ser ajustado a noncompliant.

4. Ajuste o lugar e a política para transferir atualizações do abastecimento do cliente.

   Clique a **administração > o sistema > os ajustes > o abastecimento do cliente do** painel esquerdo, e verifique que estes valores padrão estão ajustados:

5. Transfira os arquivos do agente.

   Navegue à **política > aos elementos > aos resultados da política**, expanda o dobrador do **abastecimento do cliente**, e selecione **recursos**.Da placa à direita, o clique **adiciona > recursos de agente do local de Cisco da** lista de drop-down. Uma janela pop-up indica os recursos remotos:




Pelo menos, selecione o agente atual NAC, o agente da Web, e o módulo da conformidade (módulo do apoio AV/AS) da lista, e da **salvaguarda do** clique. Os tipos de arquivo do abastecimento do cliente são:

**Agente NAC**: Agente persistente da postura para PCes do cliente do Windows.**Agente de Mac OS X**: Agente persistente da postura para PCes do cliente de Mac OS X.**Agente da Web**: Agente temporal da postura para PCes de Windows somente.**Módulo da conformidade**: Módulo OPSWAT que fornece atualizações ao suporte de fornecedor atual AV/AS para o agente NAC e o agente de Mac OS X. Não aplicável ao agente da Web.**Perfis**: Arquivos de configuração do agente para o agente NAC e o agente de Mac OS X. As atualizações localmente instalaram arquivos XML em PCes do cliente. Não aplicável ao agente da Web.Espere até que os arquivos estejam transferidos ao dispositivo ISE.

6. (Opcional) crie um perfil da configuração de agente NAC para seus clientes.

   Da placa à direita, o clique **adiciona**, a seguir seleciona o **perfil do agente da postura ISE da** lista de drop-down. Altere o perfil a fim satisfazer as exigências do desenvolvimento.

   A opção da fusão atualiza o parâmetro atual do perfil do agente somente se nenhum outro valor é definido.A opção do overwrite atualiza o valor de parâmetro se definido explicitamente ou não.Para uma lista completa de parâmetros configuráveis do agente NAC, refira o Guia do Usuário do Cisco Identity Services Engine, a liberação 1.1.x.
7. Defina a política de abastecimento do cliente para usuários de domínio e usuários convidado.

   Navegue à **política > ao abastecimento do cliente**. Adicionar duas regras novas do abastecimento do cliente de acordo com esta tabela. Clique as **AÇÕES** abotoam-se à direita de toda a entrada da regra a fim introduzir ou duplicar regras.

Nota: Se as versões múltiplas do mesmo tipo de arquivo (módulo da conformidade do agente da Web do agente NAC) foram transferidas ao repositório do abastecimento do cliente, selecione a maioria de versão atual disponível quando você configura a regra.**Salvaguarda do** clique quando terminado.

8. Configurar o portal da autenticação da Web a fim transferir o agente da postura como definido pela política de abastecimento do cliente.

   Navegue à **administração > ao Gerenciamento > aos ajustes do portal da web**, expanda o dobrador do **convidado**, **configurações** seletas do Multi-**portal**, e selecione **DefaultGuestPortal**.Sob a aba da **operação**, permita a opção a fim permitir que os usuários convidado transfiram agentes e ao auto registrar-se.

   Defina um perfil do tempo do registro de papel de convidado e de auto do registro do auto como mostrado aqui. O serviço do auto do convidado é uma configuração opcional que deixe usuários criar contas sem a intervenção do patrocinador. Este exemplo permite o serviço do auto a fim simplificar o processo de registro do convidado.


   (Opcional) ajuste o AUP para usuários convidado como mostrado aqui:

   **Salvaguarda do** clique quando terminado.

## Configurar a política da autorização para o abastecimento e a postura do cliente

A política da autorização ajusta os tipos de acesso e de serviços a ser concedidos aos valores-limite baseados em seus atributos tais como a identidade, o método de acesso, e a conformidade com políticas da postura. As políticas da autorização neste exemplo asseguram-se de que os valores-limite que não são postura complacente quarantined; isto é, os valores-limite são concedidos acesso limitado suficiente para provision o agente de software e às exigências falhadas remediate. Somente os valores-limite complacentes da postura são concedidos acesso de rede privilegiado.

1. (Opcional). Defina um dACL que restrinja o acesso de rede para os valores-limite que não são postura complacente.

   Navegue à **política > aos elementos > aos resultados da política**, expanda o dobrador da **autorização**, e selecione **ACL carregável**.O clique **adiciona da** placa à direita sob o Gerenciamento DACL, e incorpora estes valores para o dACL novo.

   Este é um dACL da postura da amostra. Reveja entradas do dACL para a precisão, porque o ISE 1.1.x não apoia atualmente a validação da sintaxe ACL.

O clique **submete-se** quando terminado.

2. Defina um perfil novo da autorização para os usuários do agente 802.1X-authenticated/NAC nomeados **Posture_Remediation**. O perfil leverages o dACL novo para o controle de acesso da porta e a URL reorienta o ACL para a reorientação do tráfego.

   Navegue à **política > aos elementos > aos resultados > à autorização da política**, e selecione **perfis da autorização**.O clique **adiciona da** placa à direita, e incorpora estes valores para o perfil da autorização:

   Estes detalhes resultantes do atributo devem aparecer na parte inferior da página:

   Tipo de acesso = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco: a POSTURA do cisco-av-pair=url-redirect-acl=ACL- REORIENTA
   Cisco: cisco-av-pair=url-redirect = https://
   ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cppO clique **submete-se** a fim aplicar suas mudanças.

   Nota: O ACL-POSTURE-REDIRECT ACL deve ser configurado localmente no interruptor ou no WLC. O ACL é provido por nome na política da autorização ISE. Para o interruptor reoriente o ACL, as entradas da licença determinam que tráfego deve ser reorientado ao ISE visto que, em um WLC, as entradas da licença definem que tráfego não deve ser reorientado.

3. Defina um perfil novo da autorização para os usuários Web-autenticada/da Web agente nomeados **CWA_Posture_Remediation**. O perfil leverages o dACL novo para o controle de acesso da porta e a URL reorienta o ACL para a reorientação do tráfego.

   Navegue à **política > aos elementos > aos resultados > à autorização da política**, e selecione **perfis da autorização**.O clique **adiciona da** placa à direita, e incorpora estes valores para o perfil da autorização:

   Estes detalhes resultantes do atributo devem aparecer na parte inferior da página:

   Tipo de acesso = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco: a POSTURA do cisco-av-pair=url-redirect-acl=ACL- REORIENTA
   Cisco: cisco-av-pair=url-redirect
   =https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cwaO clique **submete-se** a fim aplicar suas mudanças.

   Nota: A diferença entre os dois perfis é a URL reorienta o atributo do Cisco-av-pair. Os usuários que precisam de ser autenticados são reorientados ao portal do convidado para CWA. Uma vez que autenticado, os usuários são reorientados automaticamente ao CPP como necessários. Os usuários autenticados com o 802.1X são reorientados diretamente ao CPP.

4. Atualize a política da autorização a fim apoiar a conformidade da postura.

Navegue à **política > à autorização**. Atualize a política existente da autorização com estes valores. Use o seletor na extremidade de uma entrada da regra a fim introduzir ou duplicar regras:

**Salvaguarda do** clique a fim aplicar suas mudanças.

Nota: Este perfil da autorização é aplicado ao acesso prendido e de usuário Wireless. O WLC não toma na consideração o dACL. A característica do dACL é apoiada somente no Switches. Para o Sem fio, a reorientação ACL é bastante para negar todo o tráfego à exceção do server da remediação e da postura ISE.

## Configurar a política da postura AV

Este exemplo mostra como definir uma política AV com estas condições da postura:

- Posture a política para que os usuários de domínio tenham ClamWin AV instalado e corrente.
- Posture a política para que os usuários convidado instalem ClamWin AV se não anti-vírus é instalado.

1. Defina uma condição da postura AV que valide a instalação de ClamWin AV em um valor-limite. Esta verificação será usada nas exigências da postura aplicadas aos empregados.

   Navegue à **política > aos elementos > às condições da política**, expanda o dobrador da **postura**, e selecione a **condição de composto AV**.O clique **adiciona do** menu à direita da placa. Se nenhum Produtos AV aparece sob o campo do **vendedor**, as atualizações da postura não estiveram transferidas ainda ou a transferência não terminou ainda. Incorpore estes valores:

   O clique **submete-se na** parte inferior da página.
2. Defina uma condição da postura AV que valide a versão da assinatura de ClamWin AV em um valor-limite. Esta verificação será usada nas exigências da postura aplicadas aos empregados.

   Selecione a **condição de composto AV do** painel esquerdo, e o clique **adiciona do** menu à direita da placa. Incorpore estes valores:

   O clique **submete-se na** parte inferior da página.
3. Defina uma condição da postura AV que valide a instalação de todo o AV apoiado em um valor-limite. Esta verificação será usada para as exigências da postura aplicadas aos usuários convidado.

   Selecione a **condição de composto AV do** painel esquerdo, e o clique **adiciona do** menu à direita da placa. Incorpore estes valores:

   O clique **submete-se na** parte inferior da página.
4. Defina uma ação da remediação da postura que instale ClamWin AV em um valor-limite.

Navegue à **política > aos elementos > aos resultados da política**, e expanda o dobrador da **postura**.Expanda os índices de **ações da remediação**.Selecione a **remediação da relação**, e o clique **adiciona do** menu à direita da placa. Incorpore estes valores:

Clique em Submit.

Nota: *O IP DE SERVIDOR REM* representa o IP address de seu server da remediação onde a instalação de ClamWin existe. O arquivo executável neste exemplo PRE-foi posicionado no server da remediação. Para que a remediação trabalhe, assegure-se de que o IP de servidor da atualização de ClamWin esteja incluído no dACL previamente configurado e reoriente-se o ACL.

5. Defina uma ação da remediação da postura essa as atualizações ClamWin AV em um valor-limite.

   Selecione a **remediação AV/AS do** painel esquerdo, e o clique **adiciona do** menu à direita da placa. Incorpore estes valores:

   Clique em Submit.
6. Defina as exigências da postura que serão aplicadas aos empregados e aos usuários convidado.

   Selecione **exigências da política > dos elementos > dos resultados > da postura da política**. Incorpore estas entradas na tabela. Use o seletor na extremidade de uma entrada da regra a fim introduzir ou duplicar regras:

   Clique a **salvaguarda** quando terminado.

   Nota: Se uma condição preconfigured não indica sob a lista de condições, verifique que o ósmio apropriado esteve selecionado para a condição assim como a regra da exigência. Somente circunstâncias que são as mesmas ou são um subconjunto do ósmio selecionado para o indicador da regra na lista da seleção das circunstâncias.
7. Configurar a política da postura a fim assegurar-se de que ClamWin AV esteja instalado e a corrente em computadores do empregado com Windows 7 e que todo o AV apoiado está instalado e corrente em computadores do usuário convidado.

   Navegue à **política > à postura**, e crie regras novas da política com os valores fornecidos nesta tabela. A fim especificar uma exigência da postura como imperativa, opcional, ou a auditoria, clique o ícone à direita do nome da exigência, e escolha uma opção da lista de drop-down.

   **Salvaguarda do** clique a fim aplicar suas mudanças.

## Configurar a remediação WSUS

Este exemplo mostra como assegurar-se de que todos os computadores do empregado com Windows 7 tenham as correções de programa críticas as mais atrasadas instaladas. Os serviços da atualização de Windows Server (WSUS) são controlados internamente.

1. Defina uma ação da remediação da postura que verifique e instale as correções de programa as mais atrasadas de Windows 7.

   Navegue à **política > aos elementos > aos resultados da política**, e expanda o dobrador da **postura**.Expanda os índices de **ações da remediação**.Selecione a **remediação da atualização de Windows Server**, e o clique **adiciona do** menu à direita da placa. Incorpore estes valores, e o clique **submete-se**:

   Nota: Se você quer usar regras de Cisco a fim validar a atualização de Windows, crie suas condições da postura, e defina suas condições em etapa 2.
2. Defina as exigências da postura que serão aplicadas aos empregados.

   Navegue à **política > aos elementos > aos resultados > à postura da política**, e selecione **exigências**. Incorpore estas entradas na tabela. Use o seletor na extremidade de uma entrada da regra a fim introduzir ou duplicar regras:

   Nota: Você pode encontrar que **pr_WSUSRule da** circunstância sob **Cisco definiu a circunstância > condição composta regular**. (Esta é uma regra do manequim escolhida porque Step1 ajustou as atualizações de Windows a ser validadas pelo nível de seriedade.)
3. Configurar a política da postura a fim assegurar-se de que os computadores do empregado com Windows 7 tenham as correções de programa críticas as mais atrasadas de Windows 7.

   Navegue à **política > à postura**, e crie regras novas da política com os valores nesta tabela:

   **Salvaguarda do** clique a fim aplicar suas mudanças.

## Configuração de switch da amostra

Esta seção fornece um trecho da configuração de switch. Pretende-se para a referência somente e não se deve ser copiado ou colado em um switch de produção.

### Configuração global do raio e do dot1x

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
ip radius source-interface Vlan (x)
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-acce ss-req
radius-server attribute 25 access-request include
radius-server host <ISE IP> key <pre shared key>
radius-server vsa send accounting
radius-server vsa send authentication
```

### ACL padrão a ser aplicado na porta

```
ip access-list extended permitany
permit ip any any
```

### Permita a mudança do raio da autorização

```
aaa server radius dynamic-author
client <ISE IP> server-key <pre share d key>
```

### Permita a reorientação e o registro URL

```
Ip device tracking
Epm logging
Ip http server
Ip http secure server
```

### Reorientação ACL

```
ip access-list extended ACL-POSTURE-REDIRECT
deny udp any eq bootpc any eq bootps
deny udp any any eq domain
deny udp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8909
deny udp any host <ISE IP> eq 8909
deny tcp any host <ISE IP> eq 8443
deny ip any host <REM SERVER IP>
deny ip any host 192.230.240.8           (one of the ip of CLAMwin database virus Definitions)
permit ip any any
```

> Nota: O IP address do dispositivo de ponto final deve ser alcançável da interface virtual do interruptor (SVI) para que a reorientação trabalhe.

### Configuração de switchport

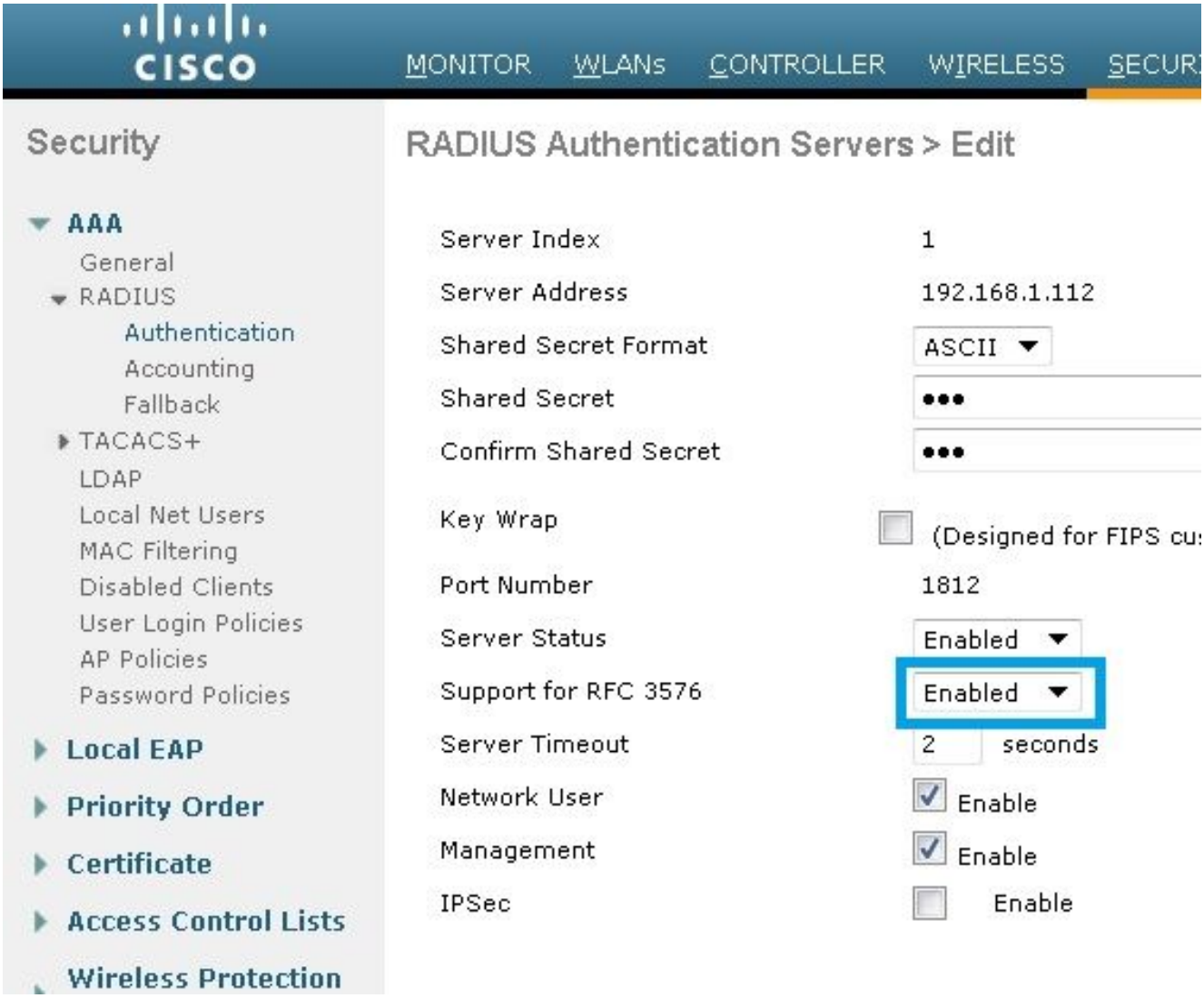
```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier
than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

# Configuração da amostra WLC

## Configuração global

1. Assegure-se de que o servidor Radius tenha o RFC3576 (CoA) permitido; não é permitido à

revelia.



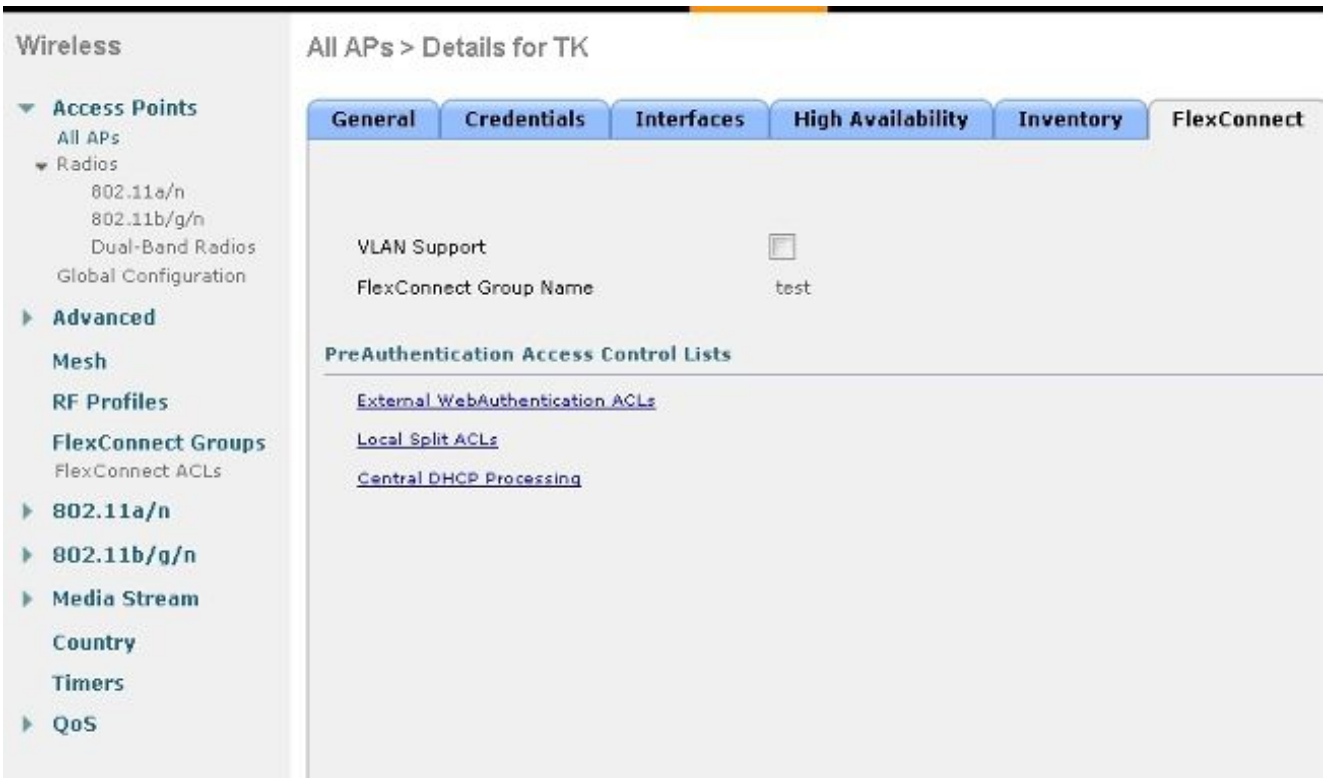

2. Navegue à **Segurança > às listas de controle de acesso**, crie um ACL no WLC e chame-o "ACL-POSTURE-REDIRECT."

15 e 16 são usados neste exemplo para a atualização de ClamWin AV onde 192.230.240.8 contém o arquivo de definição do base de dados.

Para FlexConnect com switching local, você deve criar um FlexConnect ACL, e aplica-o ao WebPolicy ACL. O ACL tem o mesmo nome que o ACL no WLC e tem os mesmos atributos.

1. Clique **FlexConnect ACL**.


2. Clique **WebAuthentication externo ACL**.




3. Adicionar o WebPolicy ACL.


4. Clique em Apply.

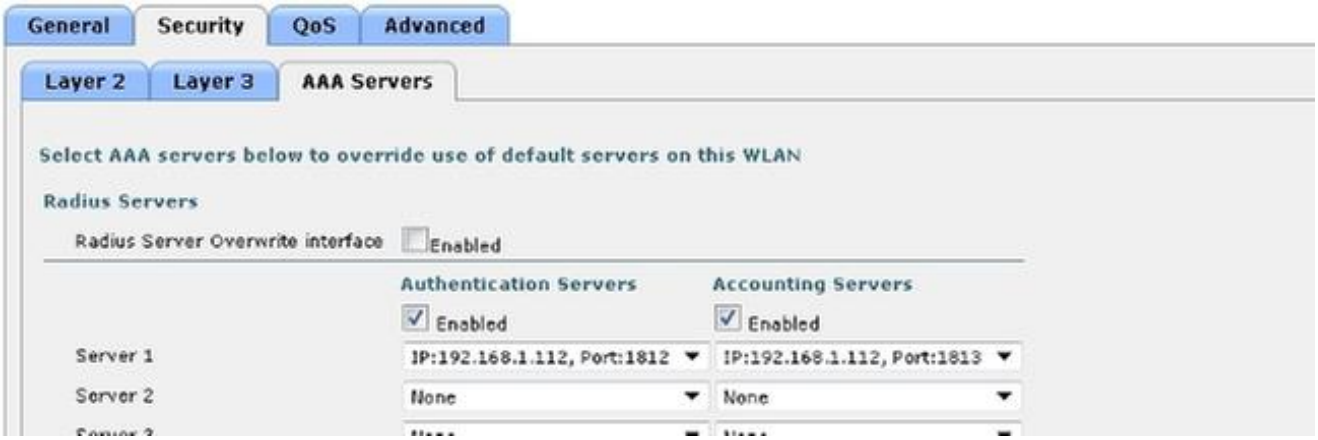
## Configuração do empregado SSID

Crie um Service Set Identifier (SSID) novo do empregado ou altere atual.

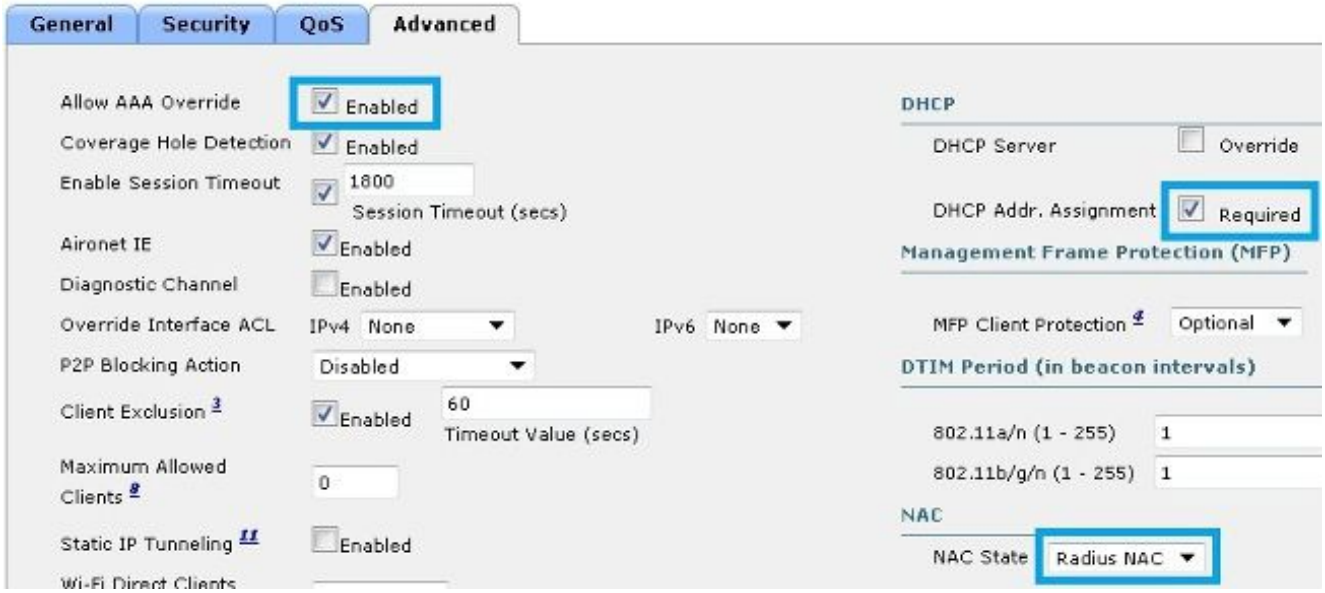
1. Na aba **WLAN**, o clique **cria novo** ou clica um WLAN existente.


2. Clique a **ABA de segurança**, clique a aba da **camada 2**, a seguir ajuste a Segurança apropriada. Está aqui uma configuração do WPA com dot1x.


3. Clique a aba dos **servidores AAA**, e verifique (permita) o ISE como o servidor Radius para ver se há a autenticação e a contabilidade.




4. Clique o **guia avançada**, verifique (permita) a **ultrapassagem reservar AAA** e o **ADDR DHCP.** As caixas de seleção da **atribuição**, e ajustaram o **estado NAC ao** raio NAC.




## Configuração do convidado SSID

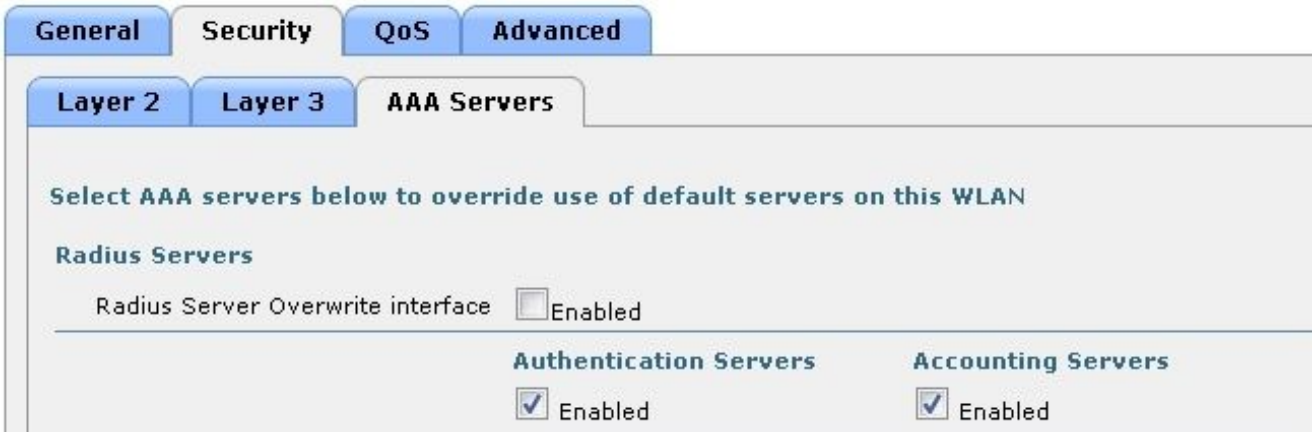
Crie um WLAN novo com o convidado SSID ou altere atual.

1. Na aba **WLAN**, o clique **cria novo** ou clica um WLAN existente.

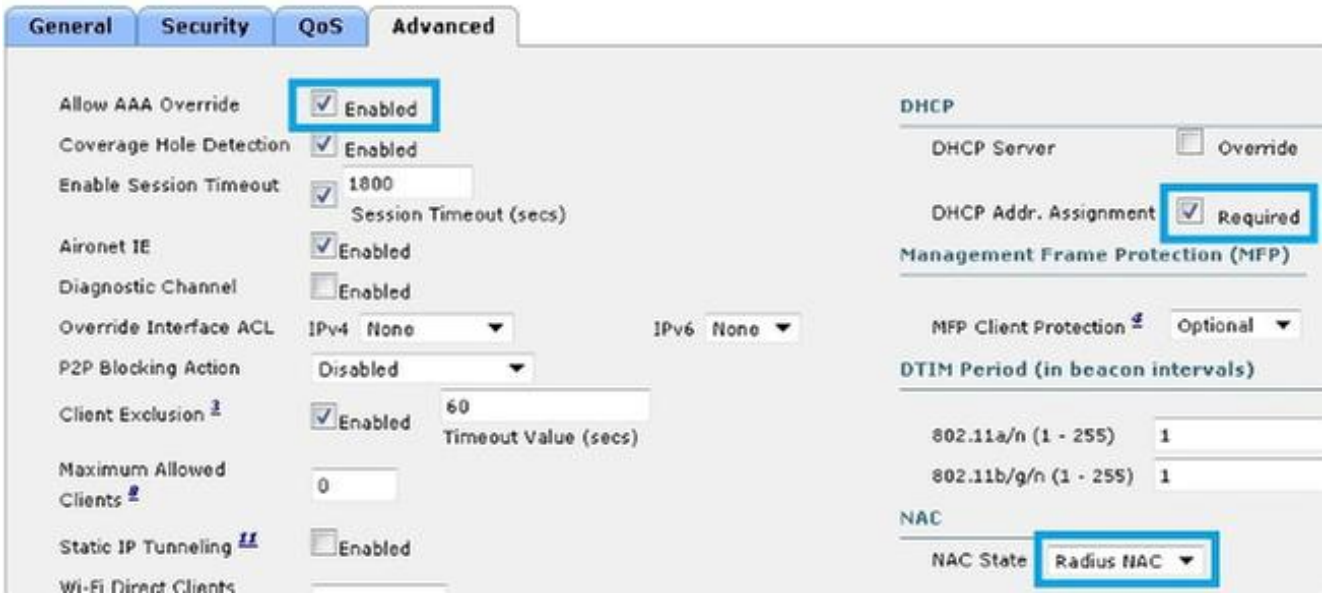

2. Clique a **ABA de segurança**, clique a aba da **camada 2**, a seguir verifique (permita) a caixa de seleção de **filtração MAC**.


3. Clique a aba da **camada 3**, e assegure-se de que todas as opções estejam desabilitadas.


4. Clique a aba dos **servidores AAA**, e verifique (permita) o ISE como um Authentication Server e um servidor de contabilidade.




5. Clique o **guia avançada**, verifique (permita) a **ultrapassagem reservar AAA** e o **ADDR DHCP.** As caixas de seleção da **atribuição**, e ajustaram o **estado NAC ao** raio NAC.

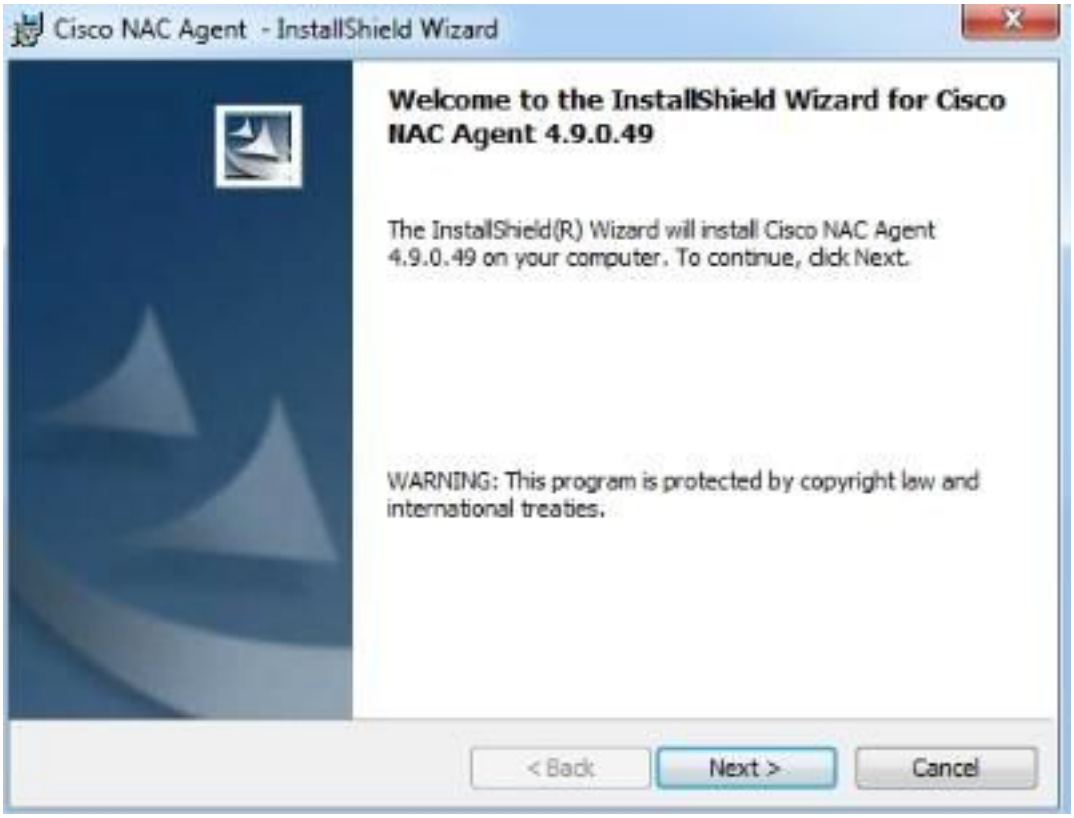



## Postura do dot1x do empregado (agente NAC)

Este é o procedimento da postura próprio de uma perspectiva do cliente, uma vez que o cliente conecta aos WLAN configurados previamente.

1. Configurar seu Sem fio SSID (empregado) ou rede ligada com fio para PEAP MSCHAP V2, e conecte-os com um usuário AD no grupo de usuário de domínio.
2. Abra um navegador, e tente-o navegar a um local. Um alerta da reorientação é indicado.
3. **Clique do** clique **para instalar o agente**.


4. Clique em Next.

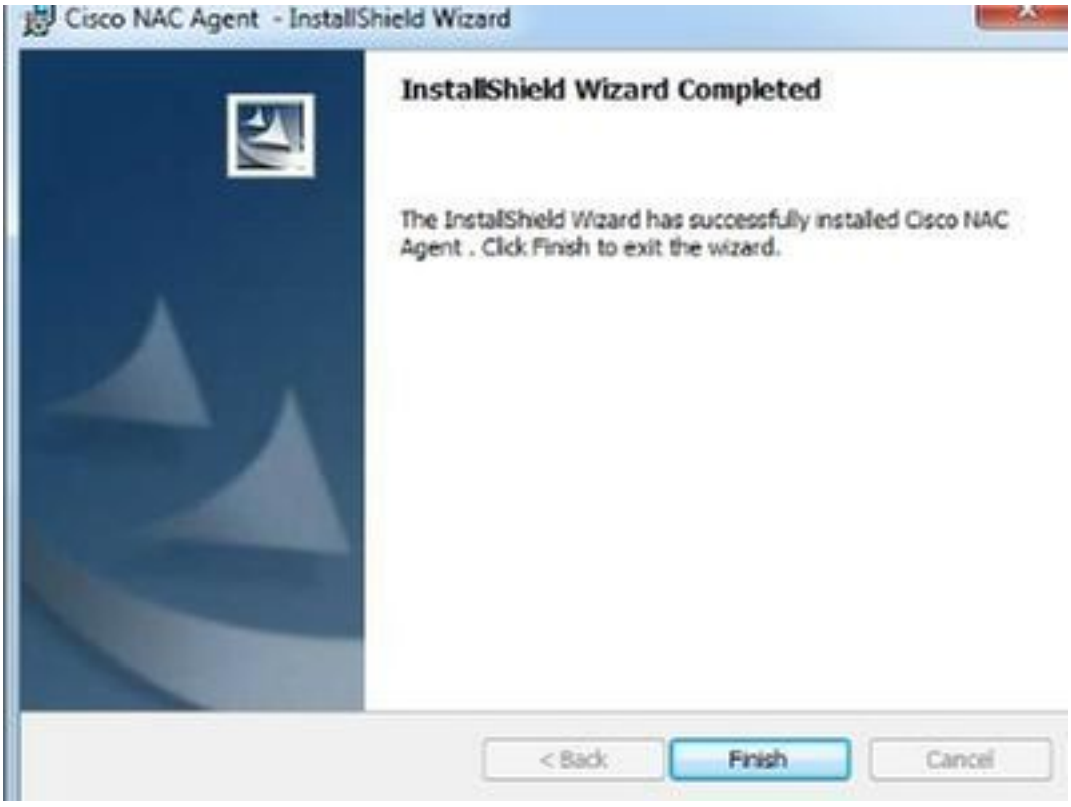



5. Clique **eu aceito os termos do contrato de licença**, e clico-os **em seguida**.

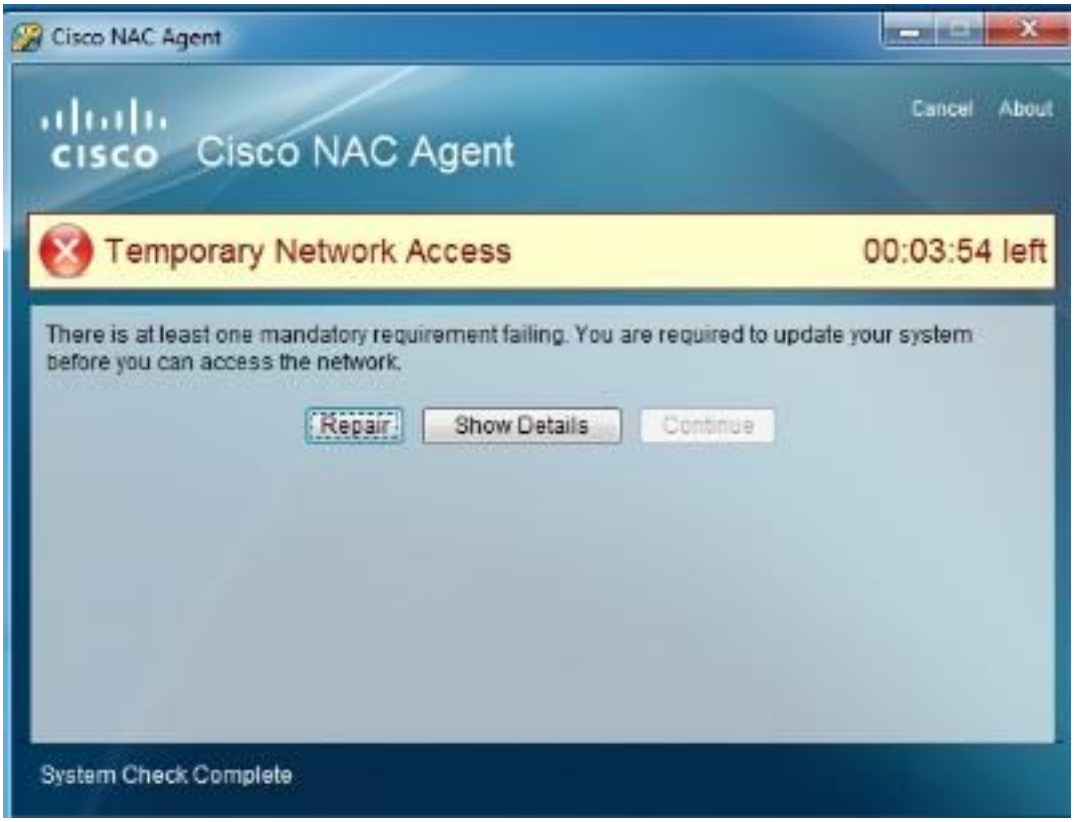

6. Clique **completo**, e clique **em seguida**.


7. O clique **instala**.

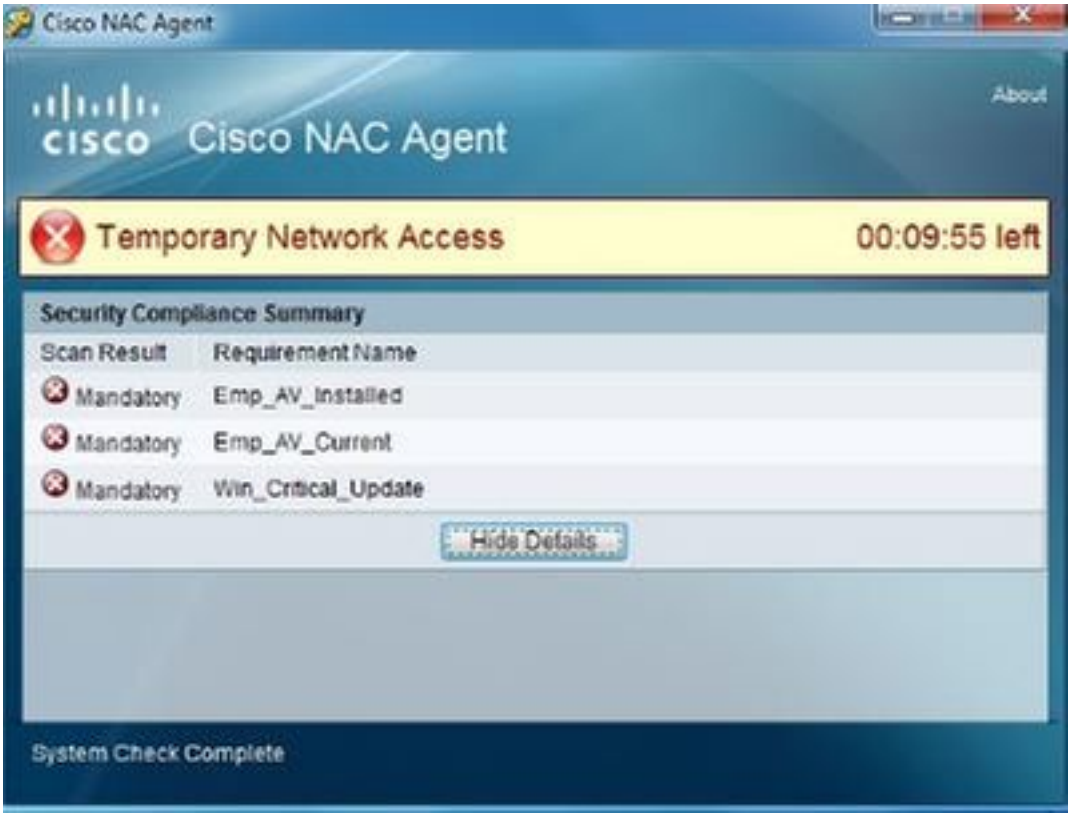

8. Selecione o **revestimento**.




9. Uma vez que a instalação está completa, o agente NAC estala acima. **Detalhes da mostra do** clique.



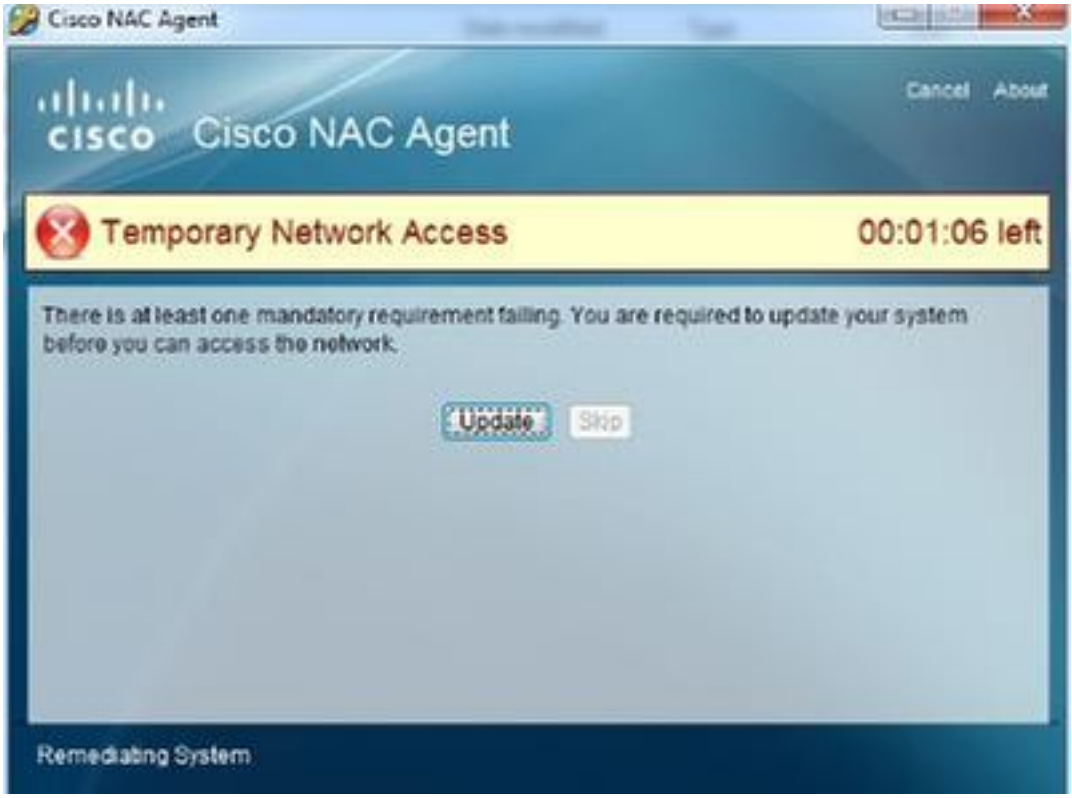

A saída mostra que ClamWin não está instalado e não é atualizada. Algumas atualizações críticas de Windows não são instaladas.




10. O clique **vai à relação** a fim instalar o anti-vírus do server da remediação.

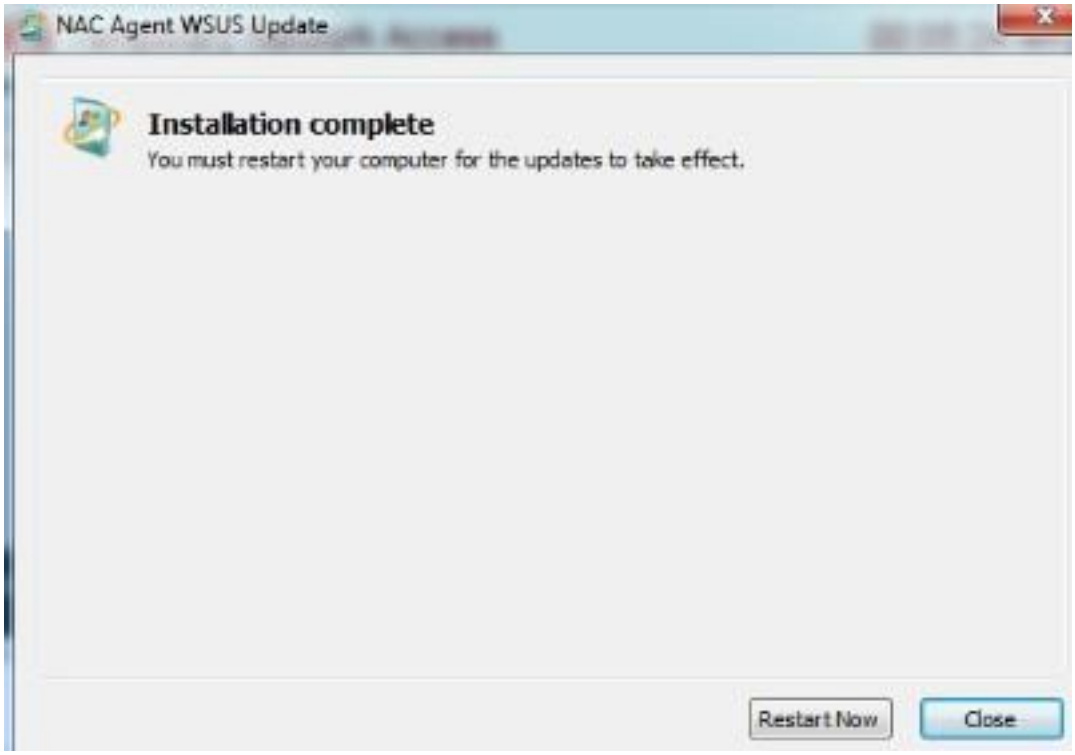

11. Clique a **corrida**, e continue com a instalação de ClamWin AV.

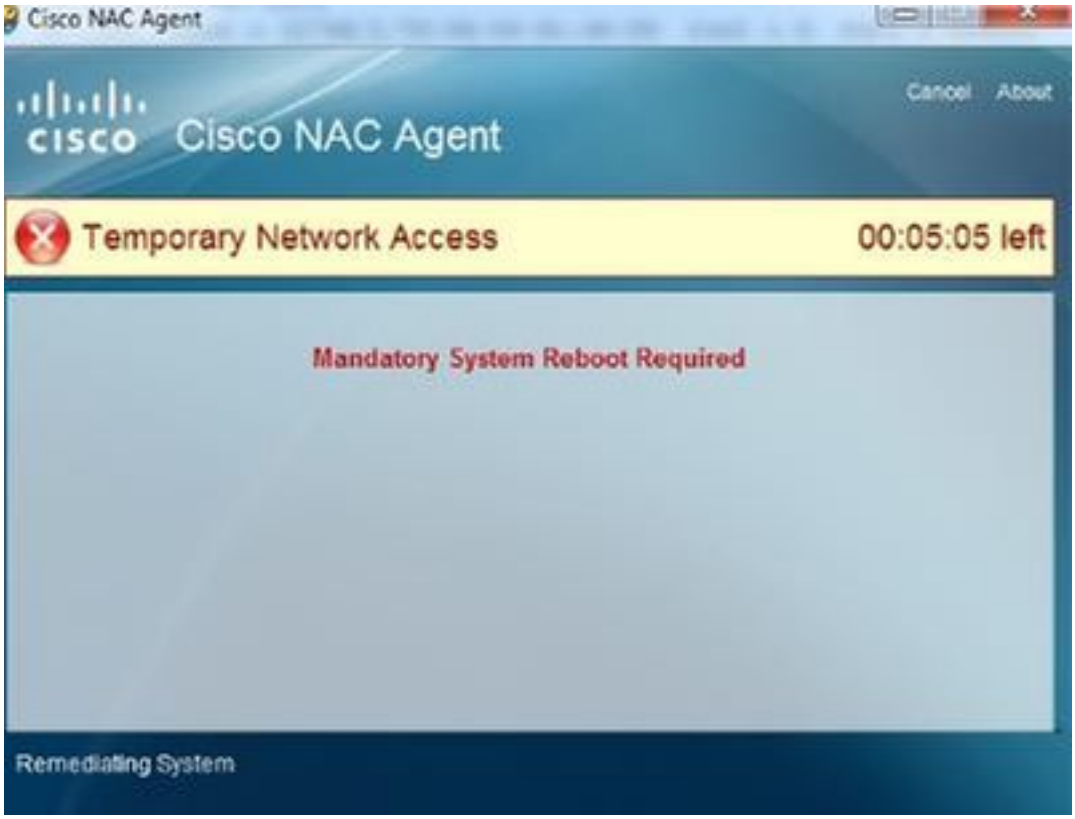

12. Depois que o anti-vírus é instalado, o agente NAC alerta para atualizações. **Atualização do** clique a fim obter o arquivo de definição de vírus o mais atrasado. Quando a mesma tela é apresentada uma segunda vez, clique a **atualização** outra vez a fim instalar as atualizações de Windows.



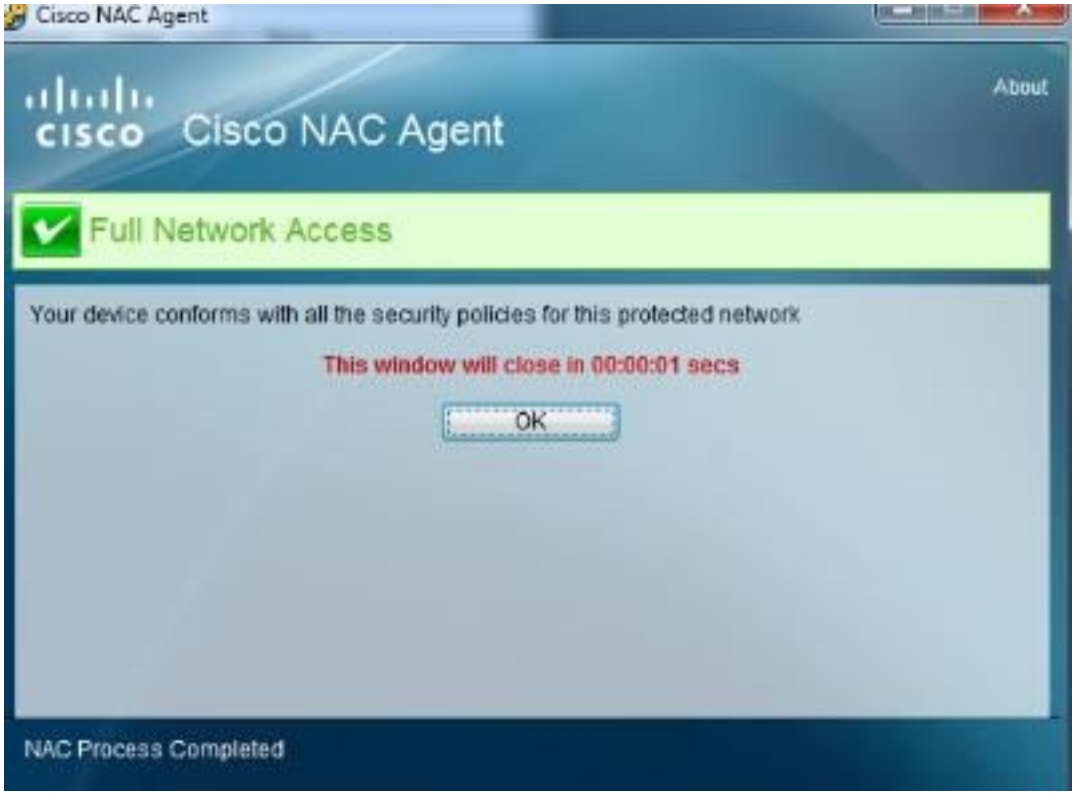

O agente NAC contacta seu WSUS a fim verificar e instalar as atualizações críticas as mais atrasadas.


13. **Reinício do** clique **agora** a fim terminar a atualização.



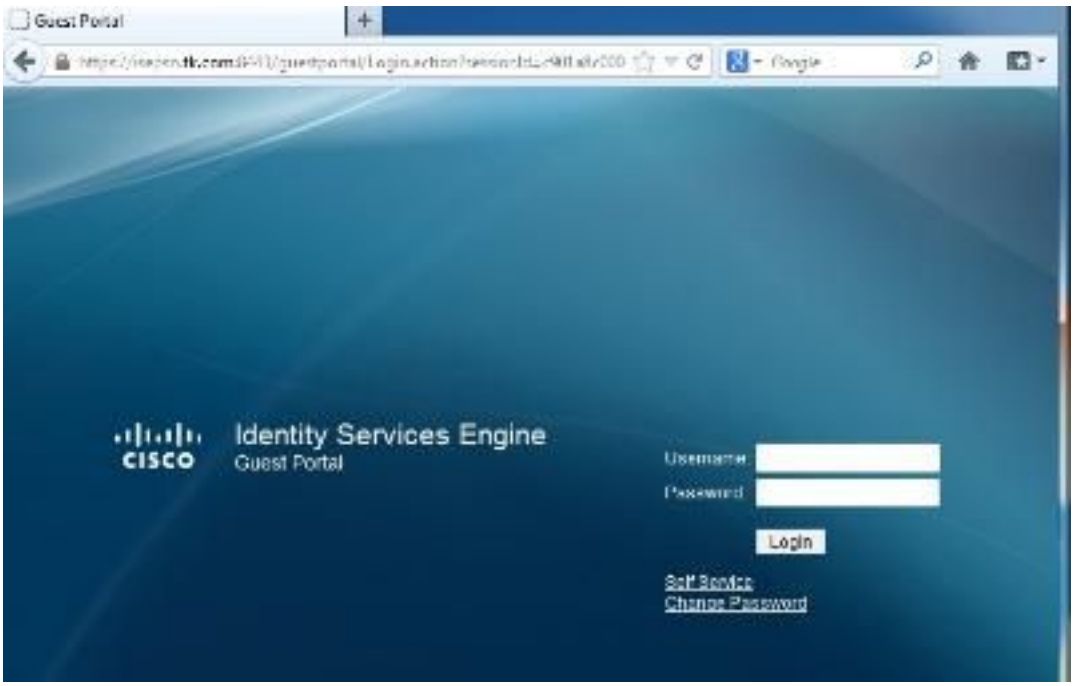

14. Depois que o reinício, o sistema é complacente.



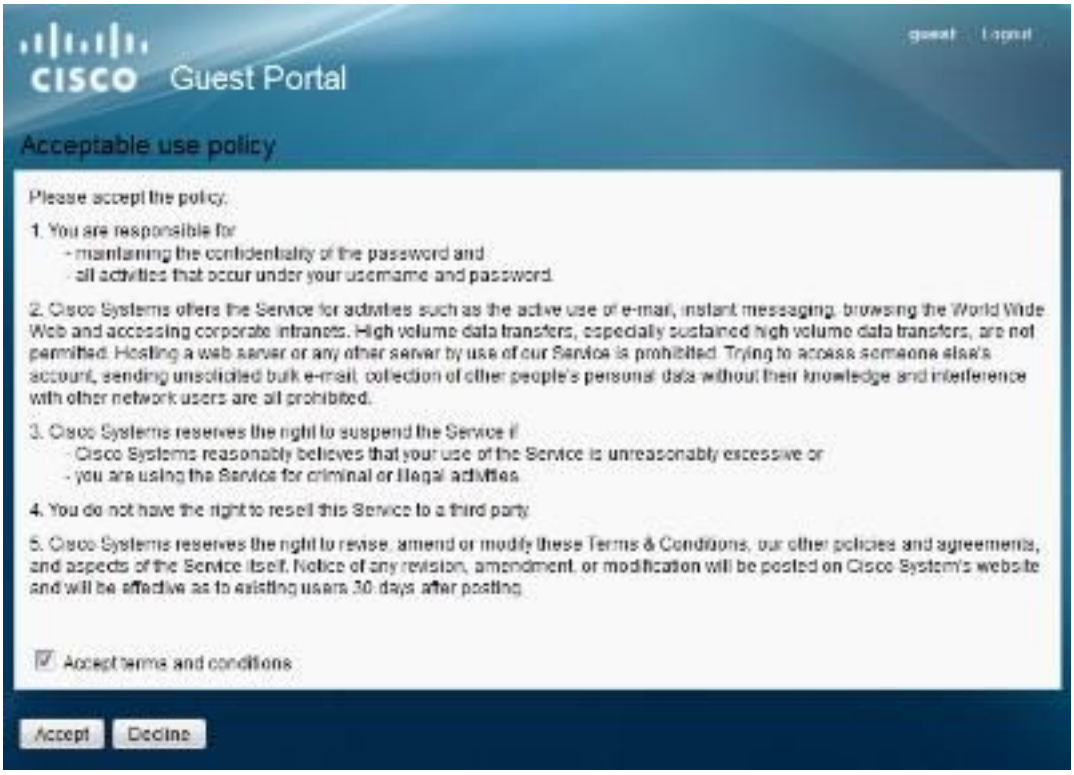

## Postura do convidado CWA (agente da Web NAC)

Este é o procedimento que os usuários executam, uma vez que conectam ao convidado SSID com a postura permitida.

1. Conecte a seu convidado SSID, ou não configurar o dot1x em sua rede ligada com fio.
2. Abra um navegador, e tente-o navegar a um local.
3. O navegador é reorientado ao portal do convidado.
4. Clique o **registro do auto**, e continue com autenticação.




5. O clique **aceita** a fim aceitar o AUP.

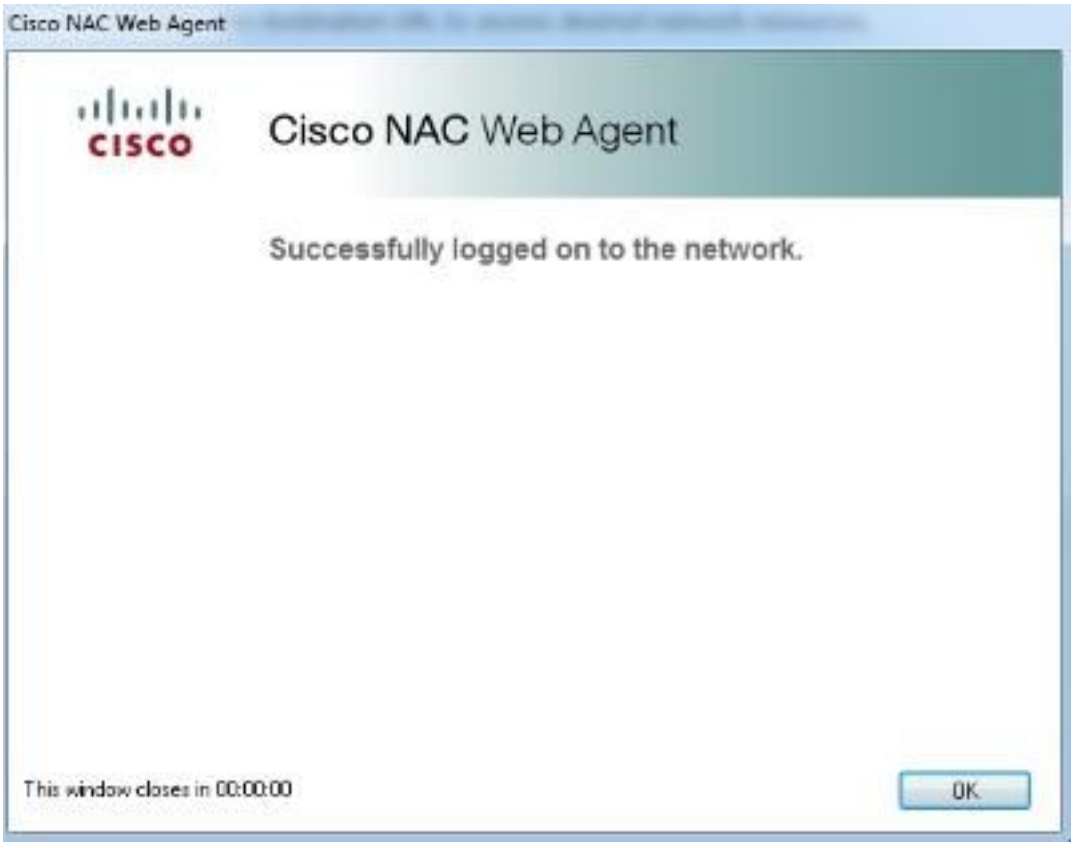



6. Selecione o **clique para instalar o agente**.

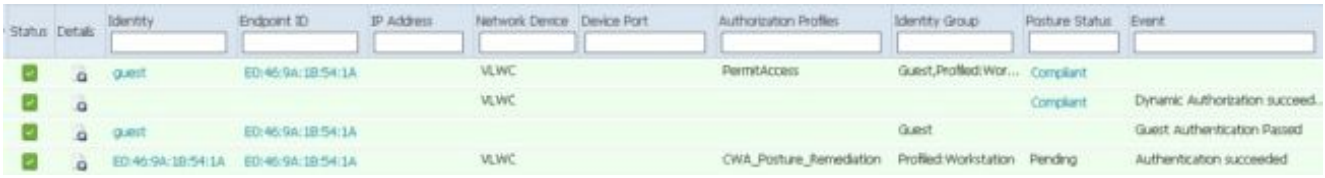

7. Clique **clicam aqui ao remediate**.


8. Clique a **corrida**, e continue com a instalação anti-vírus.


O PC é encontrado agora para ser complacente.




9. Verifique a autenticação ISE entra a ordem para verificar que a autorização dinâmica sucedeu e que você está combinando o perfil da autorização se relacionou ao estado complacente.



| Status | Details | Identity | Endpoint ID | IP Address | Network Device | Device Port | Authorization Profiles | Identity Group | Posture Status | Event |
|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | | guest | E0:46:9A:1B:54:1A | | VLWC | | PermitAccess | Guest,Profiled:Wor... | Compliant | |
| ✓ | | | | | VLWC | | | | Compliant | Dynamic Authorization succeed... |
| ✓ | | guest | E0:46:9A:1B:54:1A | | | | | Guest | | Guest Authentication Passed |
| ✓ | | E0:46:9A:1B:54:1A | E0:46:9A:1B:54:1A | | VLWC | | CWA_Posture_Remediation | Profiled:Workstation | Pending | Authentication succeeded |

# Perguntas mais freqüentes

## Opções de distribuição diferentes do abastecimento do cliente

Refira o Guia do Usuário do Cisco Identity Services Engine, libere 1.1x: Máquinas cliente do abastecimento com o instalador do agente MSI de Cisco NAC.

## Host da descoberta para o agente NAC

O agente NAC alcança o ponto de decisão de política direito ISE (PDP) em maneiras diferentes, segundo se o host da descoberta está definido:

1. Se nenhum host da descoberta é definido: O agente NAC envia o pedido do HTTP na porta 80 ao gateway; este tráfego deve ser reorientado à relação da descoberta da postura (CPP) para que a descoberta trabalhe corretamente.
2. Se um host da descoberta é definido: O agente NAC envia o pedido do HTTP na porta 80 ao host; este tráfego deve ser reorientado à relação da descoberta da postura (CPP) para que a descoberta trabalhe corretamente. Se há um problema com reorientação, as tentativas do agente NAC para contactar diretamente o host da descoberta definiram na porta 8905; a validação da postura não é garantida, porque a informação de sessão não pode estar disponível naquela PDP a menos que os grupos do nó forem definidos, e o PDP está dentro do mesmo grupo.
3. Se o host da descoberta não pode ser alcançado de todo, o agente NAC cai de volta ao método 1, tenta assim contactar com o gateway padrão.

Escolhendo o host da descoberta, um deve tomar na consideração, que o tráfego inicial do agente NAC para o host da descoberta deve ser visível ao PDP. Assim, as boas escolhas podiam ser: Endereço próprio PDP, host inexistente na mesma sub-rede como Nós PDP.

## Os navegadores do empregado são configurados com proxy

1. Se você não está usando o abastecimento do cliente e os PCes do empregado são configurados com proxy, não há nenhuma necessidade para mudanças desde que os pacotes de descoberta da postura são enviados na porta 80 e contorneiam os ajustes do proxy.
2. Se você está usando o serviço do abastecimento do cliente, faça estas mudanças à configuração de switch e ao WLC a fim interceptar o tráfego de HTTP na porta definida do proxy (aqui 8080 neste exemplo) se o proxy não está na porta 80.

    - Configuração de proxy na porta 8080 no interruptor:

```
switchport access Vlan xx
switchport voice Vlan yy
```

```
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

- Configuração de proxy WLC. À revelia, o WLC intercepta pedidos do HTTP com porta 80 do TCP destino somente. Este comando deve ser configurado através do comando line interface(cli) se você quer interceptar o outro tráfego de HTTP na porta 8080:

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

Nota: O Switches permite a reorientação em uma porta. Consequentemente, se você especifica uma outra porta para a reorientação do interruptor, a descoberta da postura falha, e o tráfego da postura é enviado ao host da descoberta definido no NACAgentCFG.xml (o perfil do agente NAC).

## dACL e reorientação ACL

A reorientação ACL é imperativa para o abastecimento do cliente, a autenticação da Web central, e a descoberta da postura. Contudo, o dACL é usado a fim limitar o acesso de rede e aplicado somente ao tráfego NON-reorientado.

A fim resolver esta situação, você pode:

1. Defina somente uma reorientação ACL, e reoriente todo o tráfego que você quer ser deixado

cair (como feito no exemplo).
2. Defina uma reorientação ACL que seja menos restritiva, e aplique um dACL que filtre o tráfego que não é reorientado.
3. Defina uma reorientação ACL, e aplique um VLAN que restrinja o acesso de rede. Esta é a melhor aproximação porque o tráfego de VLAN pode ser filtrado por um Firewall aplicativo-ciente.

## O agente NAC não estala acima

1. Verifique a autenticação viva ISE, e verifique que a autenticação combina seu perfil da autorização da postura.
2. Do PC cliente, abra o cmd. Datilografe o **nslookup**, e verifique-o que você pode resolver o hostname ISE PDP.
3. De seu navegador cliente, datilografe o ISE-*hostname de* **https://: 8905/auth/discovery**, e certificam-se de você receber o FQDN ISE como a resposta.

Se todas estas etapas são bem sucedidas e se seu interruptor ou a configuração WLC seguem com este original, suas próximas etapas devem ser:

- Use Wireshark a fim começar uma captação no PC.
- Reinicie o serviço do agente NAC.
- Recolha o embalador do log de Cisco.
- Encontre NACAgentCFG.xml no diretório de agente NAC.

Contacte o tac Cisco uma vez que você recolheu a captura de pacote de informação, os logs do agente NAC, o arquivo de configuração de NACAgentCFG, e os logs do visualizador de eventos de Windows.

## Incapaz de alcançar WSUS para a remediação

Se você está usando o 3.0 SP2 WSUS e o agente NAC é incapaz de alcançar atualizações WSUS Windows, verifique que você tem a correção de programa a mais atrasada de WSUS instalada. Esta correção de programa é imperativa para clientes do Windows a fim consultar atualizações de WSUS.

Verifique que você pode alcançar este arquivo: *wsus* **/selfupdate/iuident.cab** *IP de* **http://**.

Refira o guia passo a passo do 3.0 SP2 dos serviços da atualização de Windows Server para a informação adicional.

## Não tenha um WSUS controlado interno

Você pode ainda usar server de Windows Update quando você configurar sua regra da remediação da postura.

O cliente deve ser permitido alcançar estes locais, assim que estas URL não devem ser reorientadas:

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com

- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com
- http://stats.microsoft.com
- https://stats.microsoft.com

### Nenhuma autenticação falha vista em logs vivos ISE

Você pôde ser tentado criar uma regra da política da autorização essa disparadores na condição de um cliente noncompliant a fim restringir o acesso. Contudo, você não verá que a tentativa de autenticação falha até que o temporizador da remediação expire, especialmente quando você está usando o agente da Web. De fato, o agente observa o descumprimento e começa o temporizador da remediação.

O ISE está notificado que a postura era uma falha somente quando o temporizador da remediação expira ou o **cancelamento dos** cliques do usuário. Consequentemente, é uma boa prática dar um acesso do padrão a todos os clientes que permita a remediação mas obstrui todo o outro formulário do acesso.

## Verificar

Alguns procedimentos de verificação são incluídos nas seções precedente.

## Troubleshooting

Alguns procedimentos de Troubleshooting são incluídos nas seções precedente.