Instale um certificado de CA da 3ª parte em ISE 2.0

Índice

Introdução

Este documento descreve instalar um certificado assinado de CA da 3ª parte no Cisco Identity Services Engine.

O processo é o mesmo apesar do papel final do certificado (autenticação de EAP, portal, Admin e pxGrid).

Requisitos

Conhecimento básico da infraestrutura de chave pública.

Componentes Utilizados

A informação neste documento é baseada na seguinte versão de hardware e software:

- Liberação 2.0 do Cisco Identity Services Engine (ISE). A mesma configuração aplica-se às liberações 1.3 e 1.4.

Configurar

Gerando a solicitação de assinatura de certificado (CSR):

Para gerar o CSR vá à administração > aos Certificados > às solicitações de assinatura de certificado e seleto gerencia as solicitações de assinatura de certificado (CSR).

- Sob a seção do uso selecione o papel para ser usado para baixo do menu de gota. Se o certificado será usado para papéis múltiplos você pode selecionar o Multi-uso. Uma vez que o certificado é gerado os papéis podem ser mudados caso necessário.
- Selecione o nó para que o certificado será gerado.
- Complete a informação como necessário (unidade organizacional, organização, cidade, estado e país).

Note: Sob o campo do Common Name (CN) o ISE automóvel povoará o nome de domínio totalmente qualificado do nó (FQDN).

Convites:

- Se o objetivo é gerar uma verificação do certificado do convite “permita a caixa dos Certificados do convite”.
- Se o certificado será usado para as autenticações de EAP “*” o símbolo não deve estar no campo sujeito do CN porque os suplicantes de Windows rejeitarão o certificado de servidor.
- Mesmo quando “valide a identidade do server” está desabilitada no suplicante, a saudação de SSL pode falhar quando “*” está no campo do CN.
- Em lugar de, um FQDN genérico pode ser usado no campo do CN, e então o “*.domain.com” pode ser usado no campo de nome de DNS alternativo sujeito do nome (SAN).

Note: Algumas autoridades de certificação (CA) podem adicionar o convite (*) no CN do certificado automaticamente mesmo se ele não presente no CSR. Nesta encenação, um pedido especial precisar-me-á fez para impedir esta ação.

Exemplo do certificado de servidor individual CSR:

Exemplo do convite CSR:

Note: O endereço IP de Um ou Mais Servidores Cisco ICM NT de cada nó do desenvolvimento pode ser adicionado ao campo SAN para evitar um aviso do certificado quando você alcança o server através do endereço IP de Um ou Mais Servidores Cisco ICM NT.

Uma vez que o CSR foi criado, o ISE indicará um PNF acima do indicador com a opção para exportá-la. Uma vez que exportado, este arquivo deve ser enviado a CA para assinar.

Importando o certificate chain novo:

O Certificate Authority retornará o certificado de servidor assinado junto com a corrente de assinatura completa (raiz/intermediário). Uma vez que recebido, siga as etapas abaixo para importar os Certificados em seu server ISE.

1. Importe toda a raiz e (ou) Certificados intermediários fornecidos por CA indo à administração > aos Certificados > aos certificados confiáveis.
2. Importe o certificado de servidor indo à administração >> aos Certificados >> às solicitações de assinatura de certificado.
3. Selecione o CSR criado previamente e clique sobre o certificado do ligamento.
4. Selecione o lugar novo do certificado e o ISE ligará o certificado à chave privada criada e armazenada no base de dados.

Note: Se o papel Admin foi selecionado para este certificado, o ISE reiniciará serviços.

Verificar

Se o papel admin foi selecionado durante a importação do certificado você pode verificar que o certificado novo é no lugar carregando a página de admin no navegador. O navegador deve confiar o certificado novo admin enquanto a corrente esteve construída corretamente e se o certificate chain é confiado pelo navegador.

Para a verificação adicional selecione o símbolo do fechamento no navegador e sob o trajeto do certificado verifique que a corrente completa esta presente e confiou pela máquina. Este não é um indicador direto que a corrente completa esteve passada para baixo corretamente pelo server mas por um indicador do navegador capaz de confiar o certificado de servidor baseado em sua loja local da confiança.

Troubleshooting

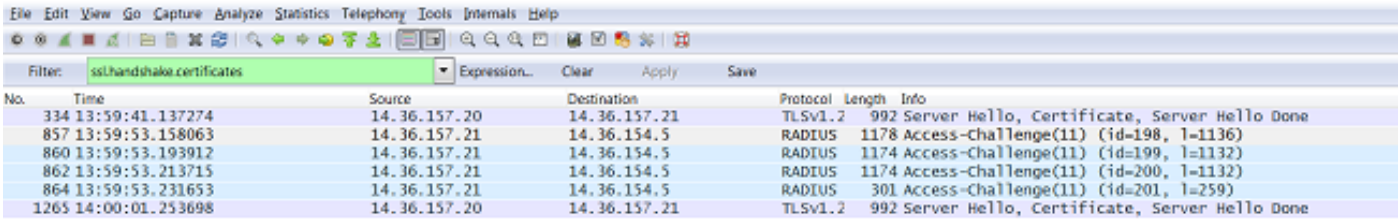
O suplicante não confia o certificado de servidor local ISE durante uma autenticação do dot1x.

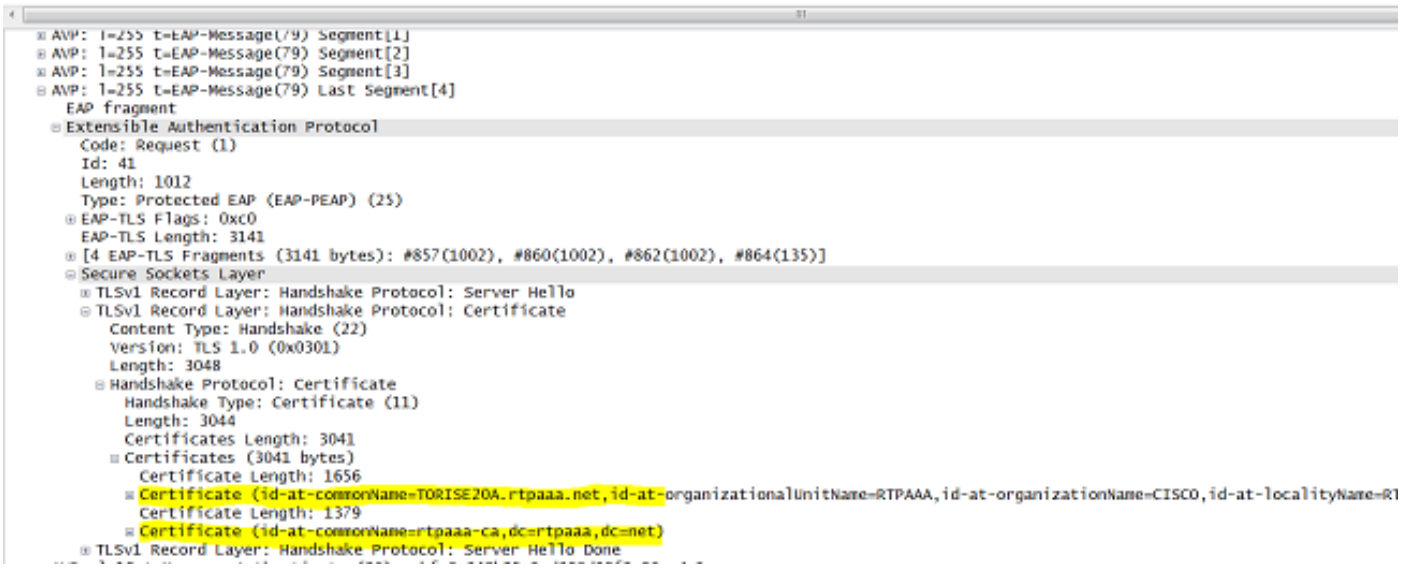
Verifique que o ISE está passando o certificate chain completo durante o processo da saudação de SSL.

Ao usar os métodos de EAP que exigem um certificado de servidor (isto é PEAP) e “valide a identidade do server” é selecionado, o suplicante validará o certificate chain usando os Certificados que tem em sua loja local da confiança como parte do processo de autenticação. Como parte do processo da saudação de SSL o ISE apresentará seu certificado e igualmente toda a raiz e (ou) Certificados intermediários atuais em sua corrente. O suplicante não poderá validar a identidade do server se a corrente está incompleta. Para verificar o certificate chain é passada de volta a seu cliente, você pode executar as seguintes etapas:

1. Tome uma captação de ISE (tcpdump) durante a autenticação. Encontrou sob operações > Diagostic utiliza ferramentas > ferramentas gerais > descarga TCP
2. Transfira/abra a captação e aplique o filtro “ssl.handshake.certificates” em Wireshark e encontre um acesso-desafio.
3. Uma vez que selecionado, expanda o protocolo de raio > os pares de valor de atributo > segmento > protocolo extensible authentication > secure sockets layer > certificado > Certificados do mensagem EAP o últimos

Certificate chain na captação.

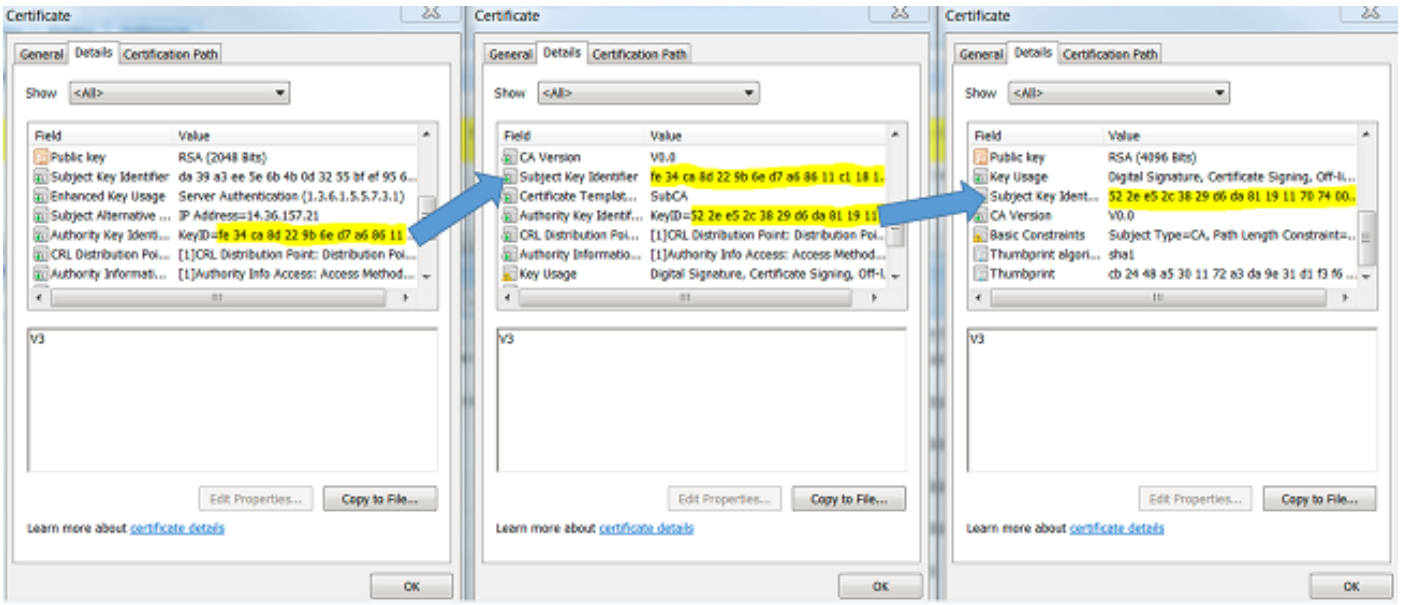




Se a corrente não está completa você deve ir à administração > aos Certificados > aos certificados confiáveis ISE e verificar que a raiz e (ou) os Certificados intermediários estam presente. Se o certificate chain é passado com sucesso, a corrente própria deve ser verificada como válida usando o método esboçado abaixo.

Abra cada certificado (server, intermediário e raiz) e verifique a corrente da confiança combinando o identificador chave sujeito (ESQUI) de cada certificado ao identificador da chave da autoridade (AKI) do certificado seguinte na corrente.

Exemplo do certificate chain.

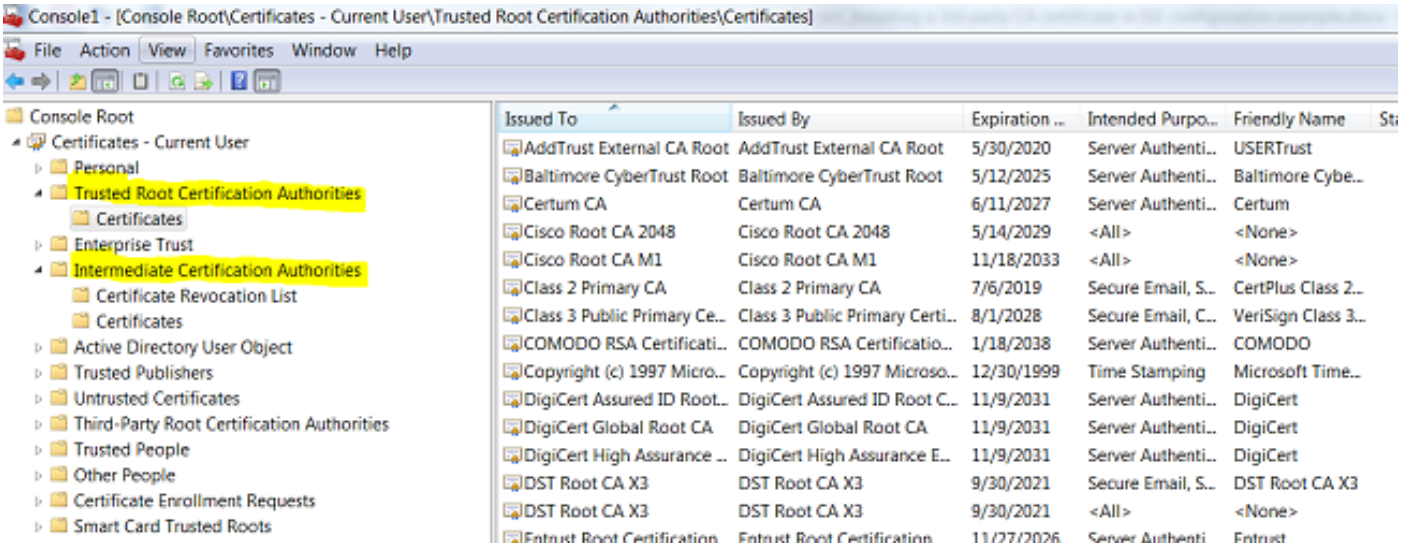


O certificate chain ISE é certificado de servidor correto mas do valor-limite das rejeições ISE durante a autenticação.

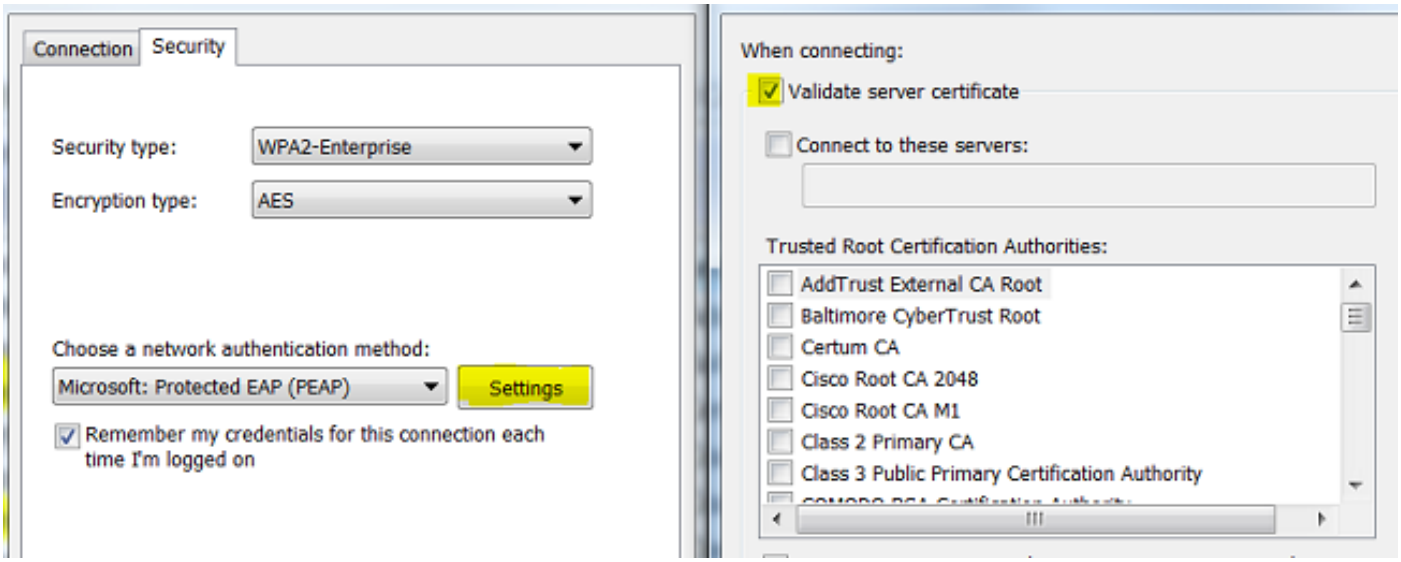
Se o ISE está apresentando seu certificate chain completo durante a saudação de SSL e o suplicante ainda está rejeitando o certificate chain; a próxima etapa é verificar que os Certificados intermediários do and(or) da raiz estão na loja local da confiança do cliente.

Para verificar isto de um arquivo aberto do dispositivo mmc.exe de Windows > Adicionar-remova Pressão-> do > Add seleto dos Certificados da coluna pressão-INS disponível > selecionam “minha conta de usuário” ou do “conta computador” segundo o tipo do autenticação no uso (usuário ou máquina). > APROVADO

Sob Autoridades de certificação de raiz confiável seletas" da opinião do console as "e "as autoridades de certificação intermediárias" para verificar a presença de certificado da raiz e do intermediário na loja local da confiança.



Uma maneira fácil verificar que esta é uma edição da verificação da identidade do server, desmarca "valida o certificado de servidor" sob a configuração de perfil do suplicante e testa-o outra vez.



Note: O ISE atualmente não apoia o processamento de Certificados usando RSASSA-PSS como o algoritmo da assinatura. Isto inclui o certificado de servidor, a raiz, o intermediário ou o certificado de cliente (isto é EAP-TLS, PEAP (TLS), etc.). Consulte para introduzir erros de funcionamento CSCug22137.

Referências

- Guia do administrador do Cisco Identity Services Engine, liberação 2.0