Edição do certificado de servidor do Cisco Unified Mobility Advantage com ASA

Índice

Introdução

Este documento descreve como trocar e vice-versa certificados auto-assinados entre a ferramenta de segurança adaptável (ASA) e o server do Cisco Unified Mobility Advantage (CUMA). Igualmente explica como pesquisar defeitos os problemas comuns que ocorre quando você importar os Certificados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- 5500 Series de Cisco ASA
- Server 7 do Cisco Unified Mobility Advantage

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.

Convenções

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

Cenários de distribuição

Há dois cenários de distribuição para o **proxy TLS** usado pela solução da **vantagem da mobilidade de Cisco**.

Nota: Em ambas as encenações, os clientes conectam do Internet.

1. A ferramenta de segurança adaptável funciona como o Firewall e o proxy TLS.
2. A ferramenta de segurança adaptável funciona como o proxy TLS somente.

Em ambas as encenações, você precisa de exportar o **certificado de servidor** e o **par de chaves de Cisco UMA no** formato **PKCS-12** e de importá-lo à ferramenta de segurança adaptável. O certificado é usado durante o aperto de mão com os clientes de Cisco UMA.

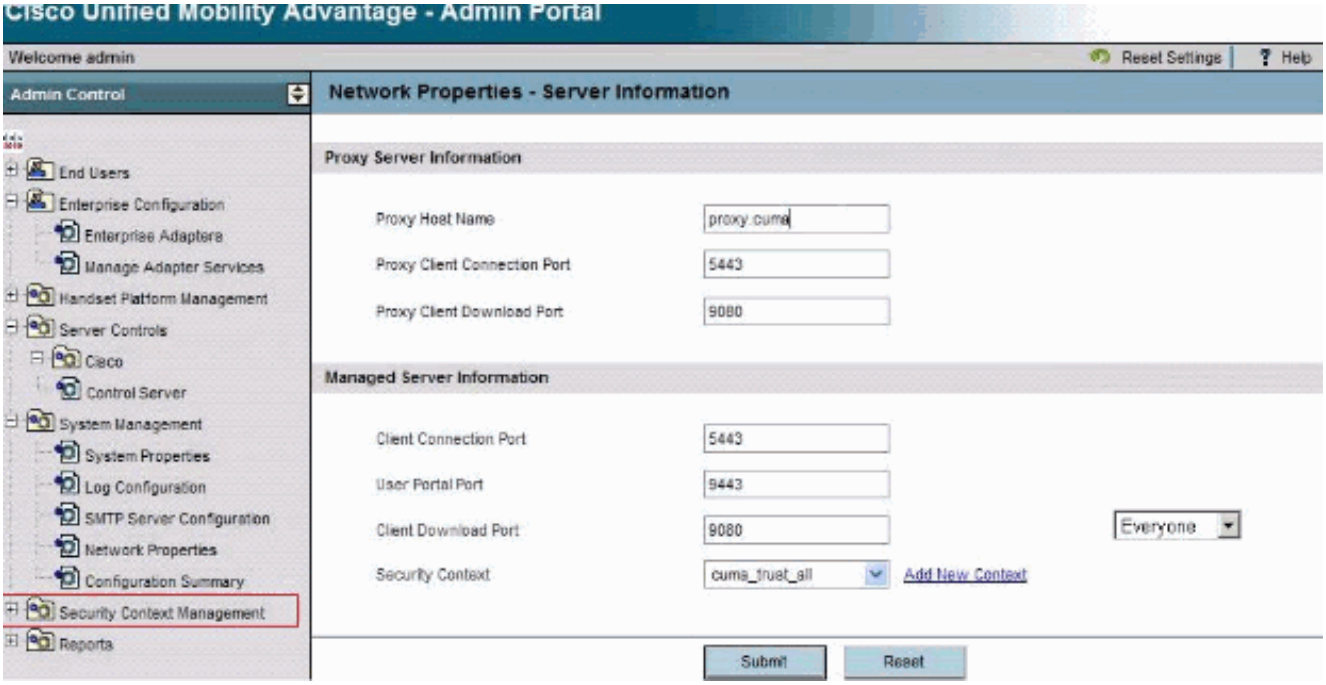
A instalação do certificado auto-assinado do server de Cisco UMA no truststore adaptável da ferramenta de segurança é necessária para que a ferramenta de segurança adaptável autentique o server de Cisco UMA durante o aperto de mão entre o proxy da ferramenta de segurança e o server adaptáveis de Cisco UMA.

Instale o certificado auto-assinado do server de Cisco UMA

Tarefas ser feito no server CUMA

Estas etapas precisam de ser executadas no server CUMA. Com estas etapas, você cria um certificado auto-assinado em CUMA para trocar com o ASA com o CN=portal.aipc.com. Isto precisa de ser instalado na loja da confiança ASA. Conclua estes passos:

1. Crie um CERT auto-assinado no server CUMA.Assine dentro ao portal Admin do Cisco Unified Mobility Advantage.Escolha o **[+]** ao lado do Gerenciamento do contexto de segurança.



Escolha **contextos de segurança**.Escolha **adicionam o contexto**.Insira esta informação:`Do you want to create/upload a new certificate? create`
`Context Name "cuma"`
`Description "cuma"`
`Trust Policy "Trusted Certificates"`
`Client Authentication Policy "none"`
`Client Password "changeme"`
`Server Name cuma.ciscodom.com`
`Department Name "vsec"`
`Company Name "cisco"`
`City "san jose"`
`State "ca"`
`Country "US"`

2. Transfira os certificados auto-assinados do Cisco Unified Mobility Advantage. Termine estas etapas a fim realizar a tarefa:Escolha o **[+]** ao lado do Gerenciamento do contexto de segurança.Escolha **contextos de segurança**.Escolha **controlam o contexto** ao lado do contexto de segurança que guarda o certificado para transferir.Escolha o **certificado da transferência**.**Nota:** Se o certificado é uma corrente, e associou Certificados da raiz ou do intermediário, simplesmente o primeiro certificado na corrente está transferido. Isto é suficiente para certificados auto-assinados.Salve o arquivo.
3. A próxima etapa é adicionar o certificado auto-assinado do Cisco Unified Mobility Advantage no ASA. Termine estas etapas no ASA:Abra o certificado auto-assinado do Cisco Unified Mobility Advantage em um editor de texto.Importe o certificado na loja adaptável da confiança da ferramenta de segurança de Cisco:`cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert cuma-asa(config-ca-trustpoint)# enrollment terminal cuma-asa(config-ca-trustpoint)# crypto ca authenticate cuma-server-id-cert Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself ----BEGIN CERTIFICATE---- ** paste the contents from wordpad ** ----END CERTIFICATE----`
4. Exporte o certificado auto-assinado ASA no server CUMA. Você precisa de configurar o Cisco Unified Mobility Advantage para exigir um certificado da ferramenta de segurança adaptável de Cisco. Termine estas etapas a fim fornecer o certificado auto-assinado exigido. Estas etapas precisam de ser executadas no ASA.Gerencia um par de chaves novo:`cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024 INFO: The name for the keys will be: asa-id-key Keypair generation process begin. Please wait...`Adicionar um ponto confiável novo:`cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert cuma-asa(config-ca-trustpoint)# keypair asa-id-key cuma-asa(config-ca-trustpoint)# enrollment`

`self` Registre o ponto confiável:`cuma-asa(config-ca-trustpoint)# **crypto ca enroll asa-self-signed-id-cert** % The fully-qualified domain name in the certificate will be: cuma-asa.cisco.com % Include the device serial number in the subject name? [yes/no]: n Generate Self-Signed Certificate? [yes/no]: y`Exporte o certificado para um arquivo de texto.`cuma-asa(config)# **crypto ca export asa-self-signed-id-cert** identity-certificate The PEM encoded identity certificate follows: -----BEGIN CERTIFICATE----- Certificate data omitted -----END CERTIFICATE-----`

5. Copie a saída precedente a um arquivo de texto e adicionar-la à loja da confiança do server CUMA e use-o este procedimento:Escolha o **[+]** ao lado do Gerenciamento do contexto de segurança.Escolha **contextos de segurança**.Escolha **controlam o contexto** ao lado do contexto de segurança em que você importa o certificado assinado.Escolha a **importação na** barra dos certificados confiáveis.Cole o texto do certificado.Nomeie o certificado.Escolha a **importação**.**Nota:** Para a configuração do destino remoto, atendimento no telefone de mesa a fim determinar se o celular soa ao mesmo tempo. Isto confirmaria que o móbil conecta trabalhos e que não há nenhuma edição com a configuração do destino remoto.

Problema que adiciona o pedido do certificado CUMA a outras autoridades de certificação

Problema 1

Muito as instalações do programa demonstrativo/protótipo onde ajuda se os trabalhos da solução CUMC/CUMA com certificados confiáveis auto-são assinados ou obtidos de *outras autoridades de certificação*. Os certificados Verisign são caros e toma um muito tempo obter estes Certificados. É bom se a solução apoia certificados auto-assinados e Certificados de outros CA.

Os Certificados atuais apoiados são GeoTrust e Verisign. Isto é documentado na identificação de bug Cisco CSCta62971 (o clientes registrados somente)

Erro: Incapaz de conectar

Quando você tenta alcançar a página portal do usuário, por exemplo, `https://<host>:8443`, o `incapaz de conectar o` Mensagem de Erro aparece.

Solução

Esta edição é documentada na identificação de bug Cisco CSCsm26730 (clientes registrados somente). A fim alcançar a página portal do usuário, termine esta ação alternativa:

A causa desta edição é o caráter do dólar, assim que escape o caráter do dólar com um outro caráter do dólar no **arquivo server.xml do** server controlado**. Por exemplo**, edite /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

Na linha: **keystorePass= " pa$word”** maxSpareThreads="15"

Substitua o caráter `$` com o `$$`. Olha como o **keystorePass= " pa$$word”** maxSpareThreads="15".

Algumas páginas no portal CUMA Admin não são acessíveis

Estas páginas não podem ser vistas no **portal CUMA Admin**:

- ative/desative o usuário
- busca/manutenção

Se o usuário clica sobre uma das duas páginas acima no menu à esquerda, o navegador parece indicar que está carregando uma página, mas nada acontece (somente a página anterior que estava no navegador é visível).

Solução

A fim resolver esta edição relacionou-se à página de usuário, muda a porta usada para o diretório ativo a **3268** e reinicia o CUMA.

Informações Relacionadas

- Configuração passo a passo do proxy ASA-CUMA
- AI ASR5000 v1 de Introduccion
- Promovendo o Cisco Unified Mobility Advantage
- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Suporte Técnico e Documentação - Cisco Systems