Apoio do SHA-256 para UCCX

Índice

Introdução

Este documento descreve o apoio do SHA-256 para o Cisco Unified Contact Center Express (UCCX). A criptografia SHA-1 será suplicada logo e todos os navegadores da Web apoiados para UCCX começarão a obstruir página da web dos server que oferecem Certificados com a criptografia SHA-1.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Express (UCCX)
- Gerenciamento certificado

Anúncios de Microsoft e de Mozilla

[Atualização do Deprecation SHA-1](#)

[Continuação pôr em fase para fora - os Certificados SHA-1](#)

Nestas observações, os fabricantes do navegador indicaram que os navegadores mostrarão avisos bypassable para os Certificados SHA-1 encontrados que são emitidos com datas de

ValidFrom depois do 1º de janeiro, 2016.

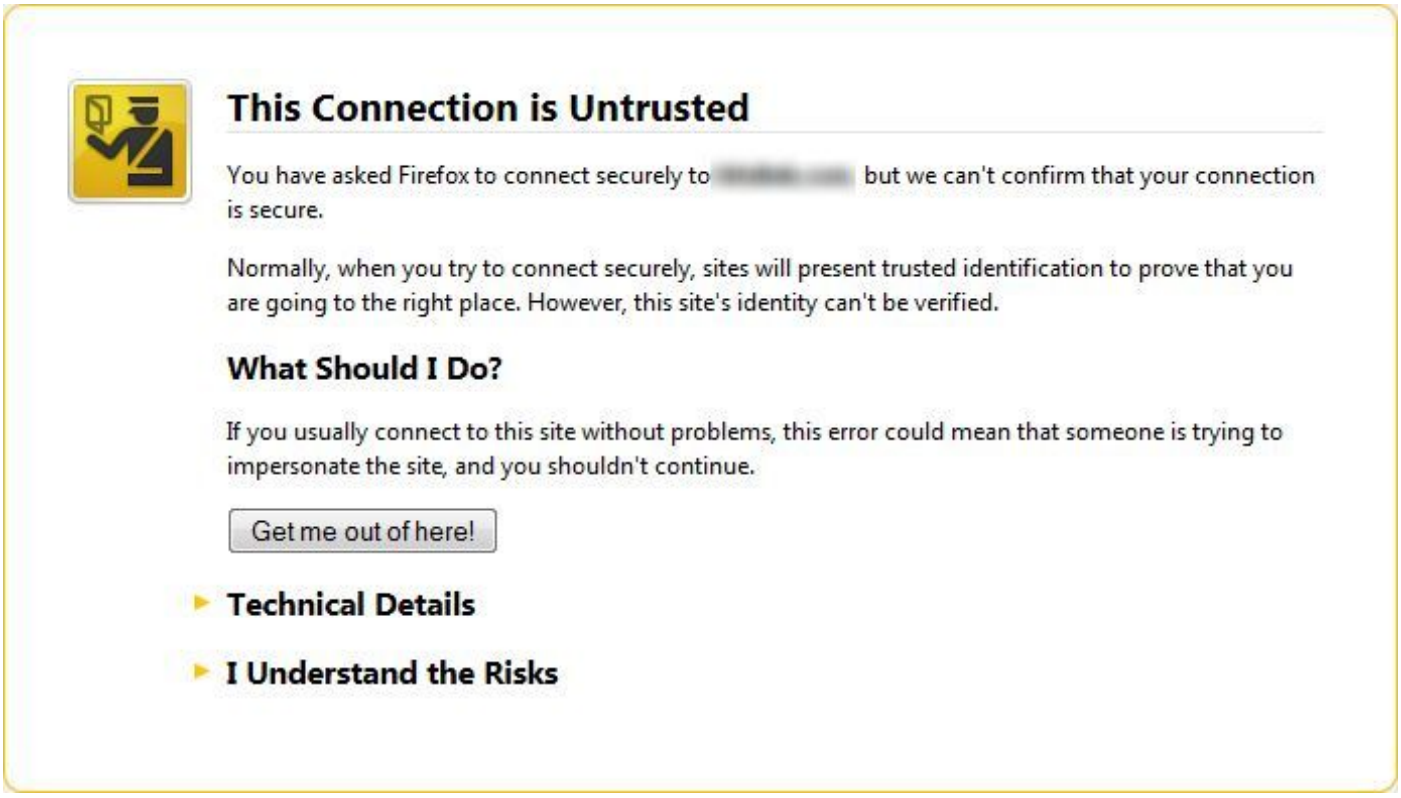
Além, o plano atual do registro é obstruir os Web site que usam os Certificados SHA-1 depois do 1º de janeiro de 2017 apesar da entrada de ValidFrom no certificado. Contudo, com ataques recentes que visam os Certificados SHA-1, estes navegadores puderam mover este período e obstruir os Web site que usam os Certificados SHA-1 depois do 1º de janeiro de 2017 apesar da data de edição do certificado.

Cisco recomenda clientes ler em detalhe os anúncios e ficar atualizados em uns anúncios mais adicionais de Microsoft e em um Mozilla neste assunto.

Algumas versões de UCCX gerenciem os Certificados SHA-1. Se você alcança os página da web UCCX protegidos pelos Certificados SHA-1, puderam gerar um aviso ou ser obstruídos de acordo com as datas e as regras notáveis previamente.

Experiência do usuário

Quando um certificado SHA-1 é detectado, dependente da data de ValidFrom e das regras previamente listadas, o usuário pôde ver uma mensagem similar a esta:



O dependente em cima das decisões feitas, um usuário pôde ou não pôde poder contornear este aviso.

Considerações UCCX

Estas tabelas descrevem estratégias do impacto e da mitigação do certificado SHA-1 para cada versão de UCCX atualmente sob a manutenção de software.

Notações usadas neste documento

Notação	Descrição
✓	Já apoiado. Nenhuma ação mais adicional exigida.
⚠	O apoio está disponível, mas a regeneração dos Certificados é precisada.
−	O apoio não está disponível.

UCCX 11.5

	A administração UCCX	A administração CUIC Dados vivos #	Desktop da administração da fineza #	Email e bate-papo do agente com SocialMiner*	Etapas do script do RESTO UCCX	Gravação d MediaSens 11.5
Fresco instale	✓	✓	✓	✓	✓	✓
Elevação da versão anterior	⚠ Os Certificados UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	⚠ Os Certificados unificados Cisco do centro da inteligência UCCX (CUIC) retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	⚠ Os Certificados da fineza UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	⚠ Os Certificados de SocialMiner e UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	⚠ UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação representacional de transferência do estado (RESTO). As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	⚠ Os Certifica de MediaSens UCCX retê algoritmo umas liberaçõe mais velha Se gerado uma chav SHA-11 e umas liberaçõe mais velha os certifica auto-assina são SHA- baseado precisam ser regenerad

Note: os certificados *O regenerados de MediaSense e de SocialMiner devem ser reimported em UCCX.

Note: as ações separadas do #No sãas para a fineza e o CUIC. Os Certificados regenerados somente uma vez na página de administração da plataforma UCCX.

UCCX 11.0(1)

	A administração UCCX	Dados vivos da administração	Desktop da administração da fineza #	Email e bate-papo do agente com	Etapas do script do RESTO	Gravação com MediaSense

	CUIC #			SocialMiner **	UCCX	** 11.0* e 10.5*
Fresco instale	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.
Elevação da versão anterior	Os Certificados UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	Os Certificados UCCX CUIC retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	Os Certificados da fineza UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	Os Certificados de SocialMiner **e** UCCX retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.

Note: O *An que projeta o Special (ES) será liberado a fim permitir que MediaSense 10.5 e 11.0 gerencia e aceite Certificados do SHA-256.

Note: ** Os certificados regenerados de MediaSense e de SocialMiner devem ser reimported em UCCX.

Note: as ações separadas do #No sãas para a fineza e o CUIC. Os Certificados regenerados somente uma vez na página de administração da plataforma UCCX.

UCCX 10.5 e 10.6

	A administração UCCX	Dados vivos da administração CUIC #	Desktop da administração da fineza #	Email e bate-papo do agente com SocialMiner*	Etapas do script do RESTO UCCX	Gravação com *** 10.0**/10.5** de MediaSense
Fresco instale	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	Àrevelia todos os frescos auto-assinados instalam Certificados são os Certificados SHA-1 e precisam de ser regenerados.	O apoio do SHA-256 para o email do agente e o bate-papo estão disponíveis somente em SocialMiner (S) v11 e S v11 não são compatíveis com UCCX v10.x.	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.
Elevação da versão anterior	Os Certificados retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	Os Certificados retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	Os Certificados retêm o algoritmo de umas liberações mais velhas. Se gerado com uma chave SHA-11 em umas liberações mais velhas, os certificados auto-assinados são SHA-1 baseado e precisam de ser regenerados.	O apoio do SHA-256 para o email do agente e o bate-papo estão disponíveis somente em S v11 e em S v11 não são compatíveis com UCCX v10.x.	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.

Note: O *An que projeta o Special será liberado a fim permitir que SocialMiner 10.6 gerencia

e aceite Certificados do SHA-256.

Note: ** Um Special da engenharia (ES) será liberado a fim permitir que MediaSense 10.0 e 10.5 gerencia e aceite Certificados do SHA-256.

Note: O *** os certificados regenerados de MediaSense e de SocialMiner deve ser reimported em UCCX.

Note: as ações separadas do #No sãas para a fineza e o CUIC. Os Certificados regenerados somente uma vez na página de administração da plataforma UCCX.

UCCX 10.0

	A administração UCCX **	Dados vivos da administração CUIC #	Desktop da administração da fineza #	Bate-papo do agente com SocialMiner*	Etapas do script do RESTO UCCX	Gravação com *** 10.0** de MediaSense
Fresco instale	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O apoio do SHA-256 para o agente que o bate-papo está disponível somente em S v11 e em S v11 não é compatível com UCCX v10.x.	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO trabalharão depois que os Certificados são regenerados no UCCX.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.
Elevação da versão anterior	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.	O apoio do SHA-256 para o agente que o bate-papo está disponível somente em S v11 e em S v11 não é compatível com UCCX	UCCX não rejeitará um servidor de Web remoto que use os Certificados SHA-1 como parte da comunicação do RESTO. As etapas do RESTO	O certificado auto-assinado do padrão é SHA-1. O certificado da regeneração não fornece uma opção para o SHA-256.

v10.x.	trabalharão depois que os Certificados são regenerados no UCCX.

Note: O *An que projeta o Special será liberado a fim permitir que SocialMiner 10.6 gerencia e aceite Certificados do SHA-256.

Note: ** Um Special da engenharia (ES) será liberado a fim permitir que MediaSense 10.0 gerencia e aceite Certificados do SHA-256.

Note: O *** os certificados regenerados de MediaSense e de SocialMiner deve ser reimported em UCCX.

Note: as ações separadas do #No sãas para a fineza e o CUIC. Os Certificados regenerados somente uma vez na página de administração da plataforma UCCX.

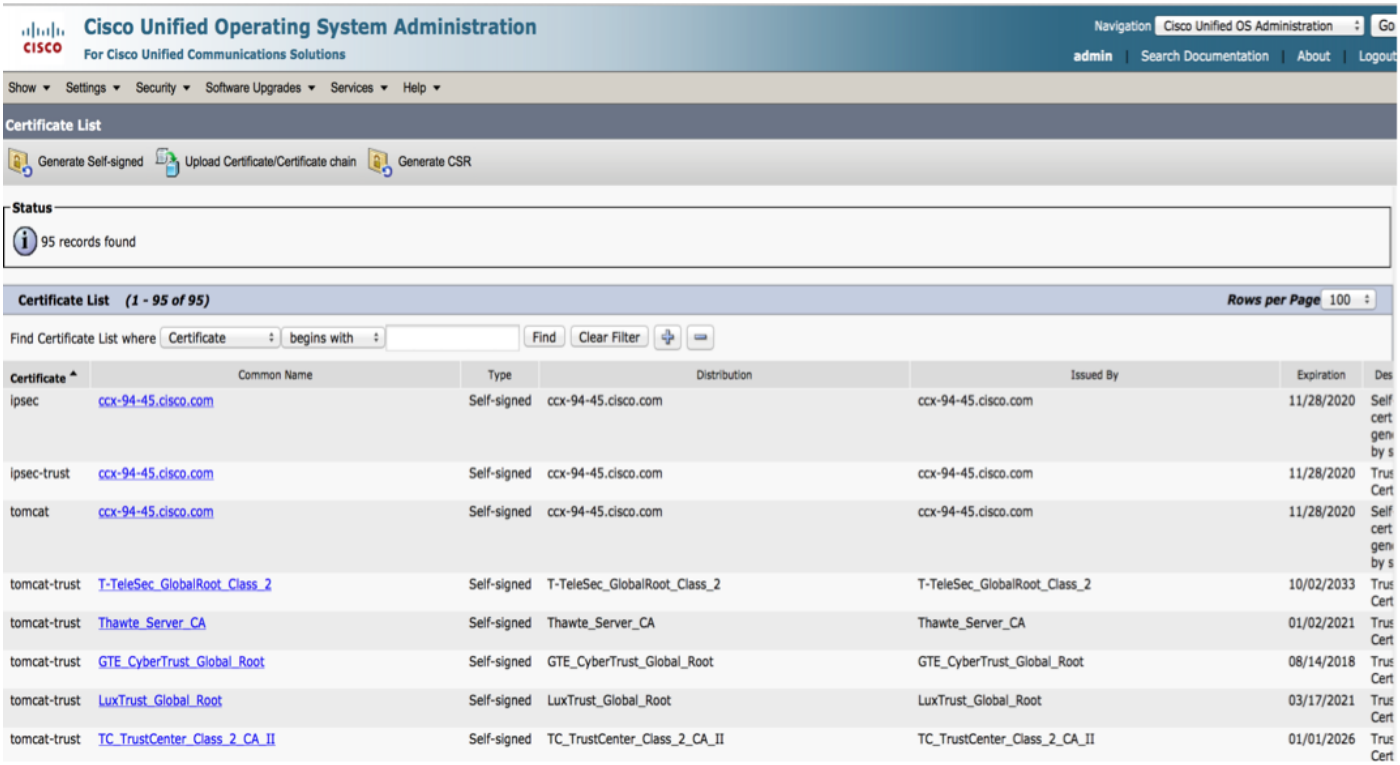
Instruções do gerenciamento certificado

Há três tipos de Certificados que precisam de ser verificados e regenerado potencialmente:

- Certificados assinados do auto
- Certificados do root confiável
- Certificados assinados da terceira parte

Certificados auto-assinados

Navegue à página de administração do OS. Escolha a **Segurança > navegam ao gerenciamento certificado**. Clique em Procurar.



Observe as quatro categorias do certificado:

- IPsec
- IPsec-confiança
- TomCat
- Tomcat-confiança

Os Certificados sob a categoria **TomCat** e o tipo Auto-**assinado** são esses que exigem a regeneração. Na imagem anterior, o terceiro certificado é esse que exige a regeneração.

Termine estas etapas a fim regenerar Certificados:

Etapa 1. Clique o Common Name do certificado.

Etapa 2. Da janela pop-up, **regenerado do** clique.

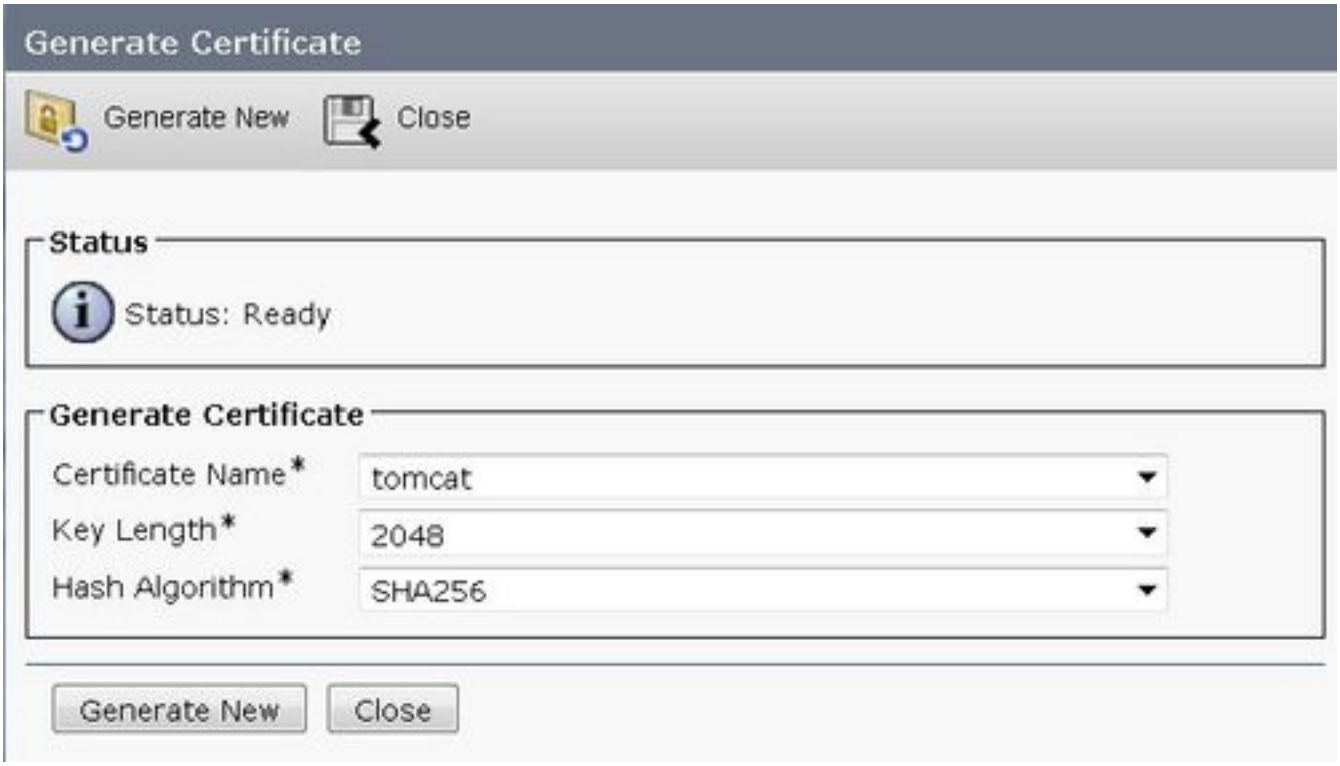
Etapa 3. Escolha o algoritmo de criptografia do SHA-256.

Para a versão 10.6 UCCX, termine estas etapas a fim regenerar Certificados:

Etapa 1. Clique **gerenciem** sobre **novo**.

Etapa 2. Selecione o *nome do certificado* como **TomCat**, o *comprimento chave* como **2048** e o *algoritmo de hash* como **SHA256.**

Etapa 3. O clique **gerencie novo.**



Certificados do root confiável

Estes são os Certificados que são fornecidos pela plataforma. As assinaturas baseadas SHA-1 para estes Certificados não são um problema porque estes Certificados são confiados pelos clientes do Transport Layer Security (TLS) baseados em sua identidade, um pouco do que a assinatura de sua mistura.

Certificados assinados da terceira parte

Os Certificados assinados por um Certificate Authority da terceira parte com o algoritmo SHA-1 precisam de ser reimported com certificados assinados do SHA-256. Todos os Certificados em um certificate chain devem ser renunciados com SHA-256.

Notas adicionais

Os serviços especiais de engenharia os mais atrasados são afixados em cisco.com quando disponíveis. Verifique as páginas de produto correspondentes regularmente para ver se há as transferências do Special da engenharia.

- Para todo o auxílio na regeneração do certificado ou em edições associadas, abra um caso tac Cisco.
- Os clientes que são executado em versões 8.x ou 9.x UCCX devem planejar promover às liberações suportadas as mais atrasadas a fim manter Cisco e o suporte de navegador.