

# Verificar as limitações de local do CMX e os requisitos de hardware

## Contents

[Introduction](#)

[Componentes Utilizados](#)

[Requisitos de hardware para nó baixo, padrão e high-end](#)

[Especificações de hardware do MSE 3365 e MSE 3375](#)

[Limitações de CMX](#)

[Consequências de recursos insuficientes e quando você excede as limitações](#)

[Mais de 400.000 endereços MAC exclusivos por mês](#)

[Valor máximo excedido de endereços MAC únicos diários](#)

[Número de elementos de mapa excedido](#)

[Número excedente de mensagens NMSP por segundo](#)

[Número de notificações ascendentes por segundo](#)

[Randomização MAC e rastreamento de clientes sonoros](#)

[Randomização MAC](#)

[CMX E Rastreamento De Clientes Probing](#)

[Bugs relevantes](#)

## Introduction

Este documento descreve os requisitos de hardware do Connected Mobile Experience (CMX) Location, suas limitações de software e possíveis consequências quando você os excede.

## Componentes Utilizados

- Controlador de LAN sem fio (WLC) 3504 com versão de imagem 8.8.120
- CMX 10.6.1-47 instalado no dispositivo físico MSE 3375

Todos os comandos, requisitos e limitações descritos neste artigo são aplicáveis ao CMX 10.5 e posterior executado no VMware ESXi (vSphere) ou em um dispositivo físico Mobility Service Engine (MSE) 3365/3375.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Requisitos de hardware para nó baixo, padrão e high-end

Determinado pela quantidade de recursos disponíveis, o nó CMX implantado pode ser Low-end, Standard ou High-end. O CMX executado no MSE 3365 e no 3375 appliance é um high-end por padrão.

A Tabela 1 mostra os requisitos de hardware (processador (CPU) / memória (RAM) / Disco) para todos os três tipos de nó.

Requisitos de hardware	Low-end	Padrão	High-end
núcleos da CPU	8 vCPUs / 4 núcleos físicos	16 vCPUs / 8 núcleos físicos	20 vCPUs / 10 núcleos físicos
Frequência básica mínima da CPU	2,3 GHz	2,3 GHz	2,3 GHz
RAM	24 GB	48 GB	64 GB
Armazenamento	550 GB	550 GB	1 TB
Tipo de armazenamento	SSD ou disco rígido SAS	SSD ou disco rígido SAS	SSD ou disco rígido SAS

Tabela 1. Requisitos de hardware CMX

## Especificações de hardware do MSE 3365 e MSE 3375

Os dispositivos MSE 3365 e 3375 têm recursos suficientes para a implantação do nó CMX sofisticado. Suas especificações de hardware podem ser encontradas na Tabela 2:

Especificações de hardware	MSE 3365	MSE 3375
CPU	Intel E5-2650 v3 de 10 núcleos a 2,4 GHz	Intel Xeon Gold de 12 núcleos a 2,4 GHz
Armazenamento	HDD SAS de 4 x 600 GB	2x SSD SATA de 960 GB
Fator de forma	1U	1U

Tabela 2. especificações de hardware do dispositivo MSE

## Limitações de CMX

A quantidade de dados que o Local CMX pode lidar depende muito do tamanho do nó. Limitações de software de nó de extremidade baixa, padrão e alta podem ser encontradas na Tabela 3:

Limitações	Low-end	Padrão	High-end
Máximo de APs	2,000	5,000	10,000
Máximo de endereços MAC exclusivos rastreados por dia (com ou sem hiperlocal)	25,000	50,000	90,000
Suporte a hiperlocalização	No	No	Yes
Máximo de clientes ativos exclusivos (com hiperlocalização habilitada)	X	X	9,000
Máximo de endereços MAC exclusivos por mês (consulte a observação*)	400,000	400,000	400,000
Zonas máximas	150	600	900
Máximo de elementos do mapa	200	750	1000
Máximo de solicitações de API V3 de local MAC por segundo	1	10	60

Máximo de mensagens NMSP por segundo	750	1300	2500
Máximo de notificações ascendentes por segundo	10	50	300
Número máximo de receptores de notificação ascendentes	5	5	5
Máximo de conexões CMX por segundo	10	10	10

Tabela 3. Limitações de localização do CMX

**Note:** Depois que o número de endereços mac exclusivos excede 400.000 em um mês de duração, o CMX stop é incapaz de diferenciar entre os visitantes novos e os que retornam. Outros serviços continuam a funcionar, a menos que outras limitações sejam excedidas.

## Consequências de recursos insuficientes e quando você excede as limitações

Se você exceder as limitações mencionadas na tabela 3, poderá ter consequências fatais no nó CMX. Antes da instalação de um nó CMX, certifique-se de estimar o tamanho da implantação e decidir qual tamanho de implantação atende às suas necessidades.

Se o tamanho da implantação for simplesmente muito grande mesmo para vários nós CMX, considere a mudança para [DNA Spaces](#), a nova plataforma de análise baseada em nuvem da Cisco que está disponível para substituir o CMX. Com o DNA Spaces, todos os cálculos são descarregados na infraestrutura de nuvem, onde os recursos são alocados dinamicamente com base na carga.

Todos os sintomas e as soluções propostas abaixo se baseiam na experiência anterior do Technical Assistance Center (TAC) com implantações que variam de um único nó Básico a vários nós high-end que cobrem centenas de locais.

Para obter informações adicionais sobre como lidar com CMX sobrecarregado, consulte o documento: <https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx-performance.html>

### Mais de 400.000 endereços MAC exclusivos por mês

#### Sintomas:

- O CMX para poder diferenciar entre os visitantes novos e os que retornam. Outros serviços de localização continuam a funcionar, a menos que outras limitações sejam excedidas

#### Soluções:

- Desabilitar o rastreamento de clientes em sondagem
- Se a rede consiste em vários controladores e um nó high-end não é suficiente, considere a divisão da carga de vários controladores para vários nós CMX
- Se um high-end não for suficiente para um único controlador, considere a atualização da

WLC para a versão 8.8 ou posterior e o uso de um recurso especial de [Agrupamento CMX](#) que permite que uma única WLC descarregue partes dos dados em vários nós CMX

- Considere a migração para o DNA Spaces, um serviço de análise baseado em nuvem que substitui o CMX. Toda carga de trabalho é descarregada para a infraestrutura de nuvem dinamicamente escalável

## Valor máximo excedido de endereços MAC únicos diários

### Sintomas:

- Interface da Web muito lenta ou quebrada
- Alto uso de CPU e memória
- Perda de dados analíticos
- Serviços CMX que travam ou não podem iniciar
- Corrupção de dados potencialmente irreversível que exige reinstalação
- Mensagens de erro dentro de **locationserver.log** em um pacote de log techsupport que diz:  
`Cleaning up element counts, unique devices 347684, locally administered macs 0 as part of daily midnight job`

### Soluções:

- Interrompa a trilha de clientes de sondagem pelo menos até que o CMX esteja estável novamente
- Aumente o tamanho do nó CMX (Low-end -> Standard -> High-end) ou implante nós CMX adicionais para redistribuir a carga
- Considere a migração para o DNA Spaces, um serviço de análise baseado em nuvem que substitui o CMX. Toda carga de trabalho é descarregada para a infraestrutura de nuvem dinamicamente escalável
- Se vários controladores forem adicionados a um único CMX, remova-os e tente adicioná-los novamente um por um a cada dia enquanto você monitora a contagem total diária de dispositivos

## Número de elementos de mapa excedido

### Sintomas:

- Interface da Web lenta, especialmente a guia Detectar e localizar
- Serviços CMX que travam
- Perda de dados analíticos

### Soluções:

- Aumente o tamanho do nó CMX (Low-end -> Standard -> High-end) ou implante nós CMX adicionais
- Remover alguns dos elementos do mapa

## Número excedente de mensagens NMSP por segundo

Esse problema geralmente é observado quando uma grande quantidade de controladores com carga elevada é adicionada a um único nó CMX.

## Sintomas:

- Interface da Web lenta
- Perda de dados analíticos
- Alto uso de CPU e memória
- Serviços CMX que travam ou não podem iniciar
- Mensagens de erro dentro do **analyticserver.log** do pacote de log techsupport que diz:  
`Notification queue is full - incoming notifications are being rejected. Please increase more processing capacity`

## Soluções:

- Implantação de nós CMX adicionais para dividir a carga
- Considere a migração para o DNA Spaces, um serviço de análise baseado em nuvem que substitui o CMX. Toda carga de trabalho é descarregada para a infraestrutura de nuvem dinamicamente escalável

## Número de notificações ascendentes por segundo

Esse problema geralmente é observado quando o CMX é configurado para enviar notificações a um grande número de servidores. O CMX 10.6.3 introduziu uma limitação de 5 receptores de notificação ascendentes

## Sintomas:

- Descartes de notificação que resultam em dados imprecisos/incompletos no servidor que recebe notificações

## Soluções:

- Remover alguns dos receptores de notificação configurados
- Aumentar o tamanho do nó CMX (Low-end -> Standard -> High-end) ou a implantação de nós adicionais

## Randomização MAC e rastreamento de clientes sonoros

### Randomização MAC

Antes da associação à rede sem fio, os dispositivos sem fio primeiro precisam enviar uma solicitação de sondagem. O dispositivo pode investigar um SSID específico ao qual ele se associava anteriormente ou pode enviar uma solicitação de sondagem "geral", também conhecida como Curinga.

Qualquer dispositivo sem fio que ouça solicitações de sondagem pode "ouvir" uma sonda, anotar a presença do dispositivo e, se possível, gravar a localização dos dispositivos com precisão de até vários metros.

Devido ao crescimento das preocupações com privacidade, com o lançamento do Cisco IOS 8 em 2014, os fabricantes de smartphones começaram a implementar um recurso chamado randomização MAC, onde os dispositivos usariam um novo endereço MAC gerado aleatoriamente cada vez que enviassem uma solicitação de sondagem.

Quando geram um endereço mac aleatório que é usado para enviar solicitações de sondagem, os fabricantes podem usar endereços mac universalmente ou localmente administrados.

Os endereços mac administrados localmente têm o segundo bit menos significativo do primeiro octeto do endereço definido como 1. Esse bit atua como um sinalizador que anuncia que o endereço mac é na verdade um endereço gerado aleatoriamente.

Há quatro formatos possíveis de endereços MAC administrados localmente (x pode ser qualquer valor hexadecimal)

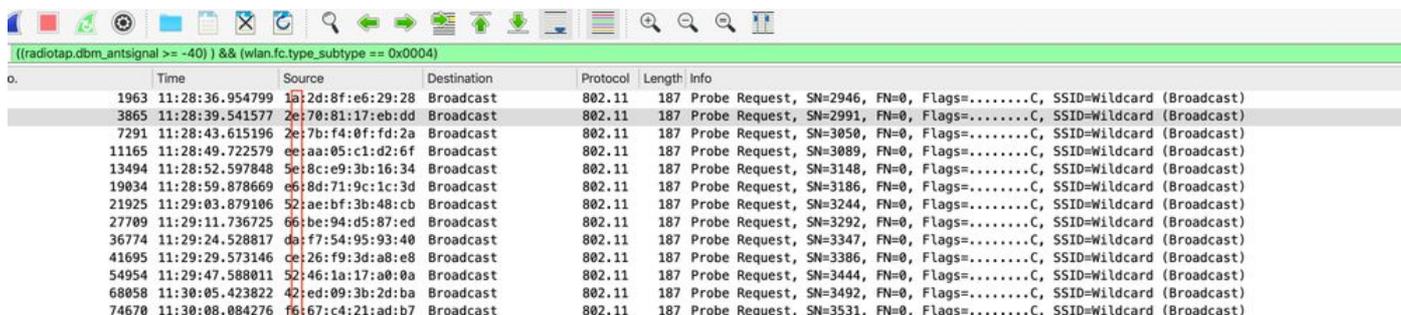
- x2-xx-xx-xx-xx-xx
- x6-xx-xx-xx-xx-xx
- xA-xx-xx-xx-xx-xx
- xE-xx-xx-xx-xx-xx

Todos os outros endereços MAC são considerados universalmente administrados. Os primeiros 3 octetos do endereço MAC universalmente administrado são chamados de Organizationally Unique Identifier (OUI) e são específicos do fabricante.

Cada fabricante atribuiu um determinado número de OUIs exclusivos atribuídos.

Nas capturas por ar de um iPhone que executa o IOS 12.3, que envia solicitações de sondagem, vemos que as solicitações de sondagem são enviadas a cada poucos segundos se a tela do dispositivo estiver ligada e a cada dois minutos se a tela do dispositivo estiver desligada.

Vemos que o bit administrado localmente está definido como 1. Com a versão do IOS 14 e do Android 10, o endereço mac aleatório também é usado quando o dispositivo se associa à rede. Os dispositivos geralmente usam um único endereço MAC administrado localmente e aleatorizado por SSID.



o.	Time	Source	Destination	Protocol	Length	Info
1963	11:28:36.954799	1a:2d:8f:e6:29:28	Broadcast	802.11	187	Probe Request, SN=2946, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
3865	11:28:39.541577	2e:70:81:17:eb:dd	Broadcast	802.11	187	Probe Request, SN=2991, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7291	11:28:43.615196	2e:7b:f4:0f:fd:2a	Broadcast	802.11	187	Probe Request, SN=3050, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
11165	11:28:49.722579	0e:aa:05:c1:d2:6f	Broadcast	802.11	187	Probe Request, SN=3089, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
13494	11:28:52.597848	5e:8c:e9:3b:16:34	Broadcast	802.11	187	Probe Request, SN=3148, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
19034	11:28:59.878669	e9:8d:71:9c:1c:3d	Broadcast	802.11	187	Probe Request, SN=3186, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
21925	11:29:03.879186	52:ae:bf:3b:48:cb	Broadcast	802.11	187	Probe Request, SN=3244, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
27709	11:29:11.736725	66:be:94:d5:87:ed	Broadcast	802.11	187	Probe Request, SN=3292, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
36774	11:29:24.528817	da:f7:54:95:93:40	Broadcast	802.11	187	Probe Request, SN=3347, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
41695	11:29:29.573146	ce:26:f9:3d:a8:e8	Broadcast	802.11	187	Probe Request, SN=3386, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
54954	11:29:47.588011	52:46:1a:17:a0:8a	Broadcast	802.11	187	Probe Request, SN=3444, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
68058	11:30:05.423822	42:ed:09:3b:2d:ba	Broadcast	802.11	187	Probe Request, SN=3492, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
74670	11:30:08.084276	f6:67:c4:21:ad:b7	Broadcast	802.11	187	Probe Request, SN=3531, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

## CMX E Rastreamento De Clientes Probing

O CMX tem a capacidade de rastrear clientes que somente testam. Essa opção está habilitada por padrão.

Para excluir os clientes que usam endereços MAC administrados localmente, marque a opção "Habilitar filtragem MAC administrada localmente" em **Sistema > Configurações > Filtragem**.

Esse campo está presente no CMX 10.5.x, mas foi removido da interface da Web 10.6.x e foi ativado por padrão.

## SETTINGS

### Tracking

### Filtering

### Location Setup

### Mail Server

### > Controllers and Maps Setup

### Upgrade

### High Availability

## Filtering Parameters

Duty Cycle Cutoff ( Interferer )

RSSI Cutoff ( Probing Only Client )

Exclude Probing Only clients

Enable Locally Administered MAC Filtering

Enable Location MAC Filtering

Enable Location SSID Filtering

Alguns fabricantes decidem não usar endereços administrados localmente quando testam. O CMX não tem como distinguir entre o endereço MAC aleatório e não administrado localmente do endereço MAC real do dispositivo. Isso significa que um desses dispositivos clientes pode ser gravado como um novo cliente toda vez que envia uma nova solicitação de sondagem. Durante o uso, em um período de 1 minuto, um smartphone em média sonda algumas vezes. No CMX, esse dispositivo é gravado como vários clientes diferentes a cada vez. Isso ignora completamente a análise do CMX e, às vezes, leva a dados de análise quase inutilizáveis.

Quando se associam ao mesmo SSID, os dispositivos sempre usam um único endereço MAC que nunca muda (esse endereço pode ser um MAC aleatório real ou administrado localmente). A quantidade de clientes associados é sempre menor ou igual à quantidade de clientes que enviam apenas sondas.

A trilha de clientes que somente a sonda não é suposta ser usada como um contador de visitantes. No entanto, ele pode ser usado para acompanhar tendências diárias (por exemplo, se quarta-feira é mais movimentada que terça-feira), mas mesmo esses dados podem ser imprecisos devido a variações extremamente altas.

O Cisco TAC geralmente lida com problemas em implantações maiores (aeroportos, shoppings, áreas públicas abertas), onde a trilha de clientes que somente testam introduz um número extremamente grande de endereços MAC exclusivos por dia, que até nós CMX high-end não podem lidar (mais de 90.000 por dia).

Se você rastrear apenas clientes associados, diminuirá o número total de clientes registrados, mas tornará precisos os dados de análise coletados.

**O TAC da Cisco recomenda enfaticamente a ativação da opção "Excluir somente clientes de prospecção".**

## Bugs relevantes

- ID de bug da Cisco [CSCvq25953](#) - Habilitando a filtragem de SSID do local desabilita a exclusão de MACs administrados localmente e vice-versa
- ID de bug Cisco [CSCvo43574](#) - CMX filtra os endereços MAC associados administrados localmente
- ID de bug da Cisco [CSCvs85182](#) - O comando de verificação de Cmxos está errado sobre os requisitos de min de HDD