

DMA Version 4.2 release notes

Viktigt: Innan du installerar DMA 4.x så måste du uppdatera övriga tjänster.

- | | |
|-------------------------|------------------|
| 1. Autoupdater | 4.0 eller senare |
| 2. Autoupdater-Webb | 4.0 eller senare |
| 3. DHCP-Windows-service | 4.0 eller senare |

Säkerhetsuppdateringar

Som alltid är alla säkerhetsuppdateringar för använda programpaket uppdaterade.

Rättning: Hämtning av anpassade fält via REST-api (version 4.1.2)

För att ett anpassat fält skulle kunna exporteras så var det tvunget att vara synligt i enhetslistan, detta är nu rättat (dvs synlighet i enhetslistan är inget krav för export)

Rättning: DHCP-synkronisering av reservationer med BootP

DHCP reservationer för enheter som var konfigurerade med BootP lyckades inte hämtas in i DMA.

Rättning: DNS uppslagning av anpassade fält med IP-adresser (version 4.1.2.3)

Fel hostname kunde hämtas vid DNS-uppslagning, detta är nu rättat.

Utökade möjlighet till datahämtning av sessionsattribut från ISE (version 4.1.2)

När man lägger till anpassat fält så är nu uppnystningen av data förbättrad och det finns nu möjlighet att hämta ut ytterligare information in i DMA från attributet CiscoAVPair.

Exempelvis:

```
other:CiscoAVPair:service-type
other:CiscoAVPair:audit-session-id
other:CiscoAVPair:method
other:CiscoAVPair:client-iif-id
other:CiscoAVPair:vlan-id
other:CiscoAVPair:dc-profile-name
other:CiscoAVPair:dc-device-name
other:CiscoAVPair:dc-device-class-tag
other:CiscoAVPair:dc-certainty-metric
other:CiscoAVPair:dc-protocol-map
other:CiscoAVPair:AuthenticationIdentityStore
```

Anpassade fält med alternativ (version 4.1.2)

För att förenkla (och eventuellt begränsa) editeringen av ett anpassat fält så finns nu möjlighet att ställa in alternativ för fälttyperna "Text" och "Fasta alternativ"

Alternativen anges semi-kolon separerade.

För fält-typen "Text" så är dessa enbart förslag, men för fält-typen "Fasta alternativ" så är dessa alternativ tvingande, dvs de enda alternativ användaren kan använda vid editering av en enhet.

Ändra på anpassat fält

Källa

DMA

* Fältnamn

Testfält

* Rubrik för fält

Test

Beskrivning

Detta är ett test-fält för att beskriva möjligheten att definiera alternativ

Fälttyp

Text

Alternativ

Alternativ 1;Alternativ 2;Alternativ 3

Möjliga alternativ, separera med semikolon ;

Sorteringsordning

16

Ange i vilken ordning som fältet ska presenteras ut mot användare. Anpassat fält med lägst sorteringsindex visas först.

☐ Fältet ska vara obligatoriskt att fylla i

☒ Fältet ska visas i tabellen på sidan "Enheter"

☒ Kan man söka på detta fält

☒ Kan man sortera på detta fält i enhetslistan

☐ Fältet ändras ej via DMA, endast presentation

* Obligatoriskt fält

Spara

Avbryt

Redigera enhet

* MAC-adress

00:00:00:00:00:0A

XEROX CORPORATION

Beskrivning

Testenhet

* Enhetsgrupp

Test

☒ Statisk grupptilldelning

* Placering

Plan 1 huvudbyggnad

Test

Alternativ 1

Alternativ 2

Alternativ 3

* Obligatoriskt fält

Förenklad hantering av konfiguration av anpassade fält

För att förenkla konfigurationen av DMA avseende integration av data hämta från olika källor (Cisco Prime, ISE sessionsattribut, ISE custom-attribute eller Catalyst Center) så finns nu ett enkelt sätt att söka på en enhet och se vilken all data som returneras för denna enhet och därifrån kunna välja vilken data du vill lägga till i DMA.

DMAEnheterGruppuppdatera enheterEnhetsgrupperLoggInställningarSpråkLogga ut

Anpassade fältInloggad som: ADMIN

Här kan du sätta upp och ändra anpassade fält som en enhet ska innehå.

+ Lägg till anpassat fältSök anpassade fält genom datauttag

Anpassat fält	Källa	
Senast aktiv	[DMA (statiskt)] 'LastActiveDateTime'	Redigera↩
Senast autentiserad	[DMA (statiskt)] 'LastAuthenticatedDateTime'	Redigera↩

Med knappen "Sök anpassade fält genom datauttag", så får du upp följande sida.

DMAEnheterGruppuppdatera enheterEnhetsgrupperLoggInställningarSpråkLogga ut

Sök anpassade fältInloggad som: ADMIN

Sök anpassade fält från en källa för att enkelt kunna lägga till i DMA

KällaCisco Prime

* MAC-adress00:00:00:00:00:00

Sök anpassade fält

Fältnamn i Prime	Värde	
@displayName	1715649	+ Lägg till anpassat fält
@id	1715649	+ Lägg till anpassat fält
apIpAddress	0.0.0.0	+ Lägg till anpassat fält
apSlotId	0	+ Lägg till anpassat fält
associationTime	1620024200070	+ Lägg till anpassat fält

Du kan här välja källa och ange en MAC-adress och få utdrag på den data som returneras, och enkelt lägga till resp. fält i DMA.

Utökad säkerhet med TOTP (Time limited One Time Password)

DMA är nu uppdaterad med ytterligare säkerhet, TOTP tvåfaktorsautentisering, denna kan aktiveras på två sätt, dels genom att ändra standard-metoden (Inställningar->Allmänna inställningar->Användarkonton).

DMA Enheter Grupppuppdatera enheter Enhetsgrupper Logg Inställningar Språk Logga ut

Spara

Användarkonton Cisco Catalyst Center Cisco Prime Databas/certifikat DHCP Gränssnitt Intern cachning ISE-synkronisering Loggning Programuppdatering Standardvärde för nya enheter

2FA autentiserings-metod TOTP (Time-based One-Time Password)

Standard 2FA autentiseringsmetod som ska användas i systemet.

TOTP Antal tillåtna överhopp 5

Antal gånger användare tillåts hoppa över aktivering av TOTP

TOTP information

Använd [Google authenticator](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2) eller [Microsoft Authenticator](https://www.microsoft.com/sv-se/security/mobile-authenticator-app) för att scanna QR-koden.

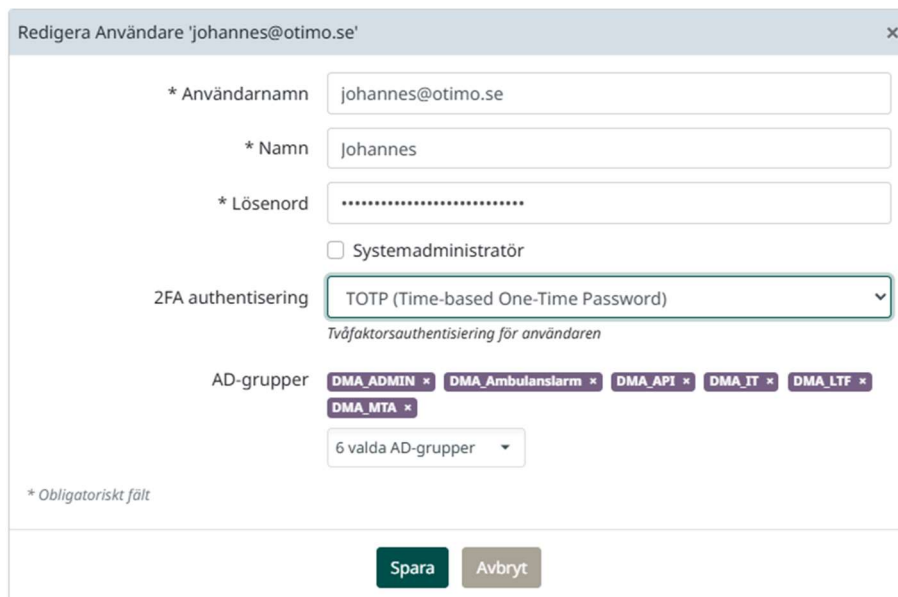
Använd Google authenticator eller Microsoft Authenticator för att scanna QR-koden.

Information till användarna om TOTP inloggningen (html)

Här anger man standardinställningen för 2FA-auktorisering, antal tillåtna gånger en användare kan "hoppa över" att aktivera TOTP auktorisering, samt vilken hjälp-text man vill visa användaren vid aktiveringen av TOTP. (denna text kan anges i html, med länkar för att t.ex. hjälpa användaren till rätt auktoriseringsprogram).

Vid ändring av standard-metod så gäller detta för samtliga användare om det inte på användarnivå är inställt på annat sätt.

För respektive användare kan man definiera om standard-metoden ska gälla, eller om man vill ha specifik inställning för resp. användare.



Redigera Användare 'johannes@otimo.se'

* Användarnamn johannes@otimo.se

* Namn Johannes

* Lösenord

☐ Systemadministratör

2FA authenticisering TOTP (Time-based One-Time Password)

Tvåfaktorsauthenticisering för användaren

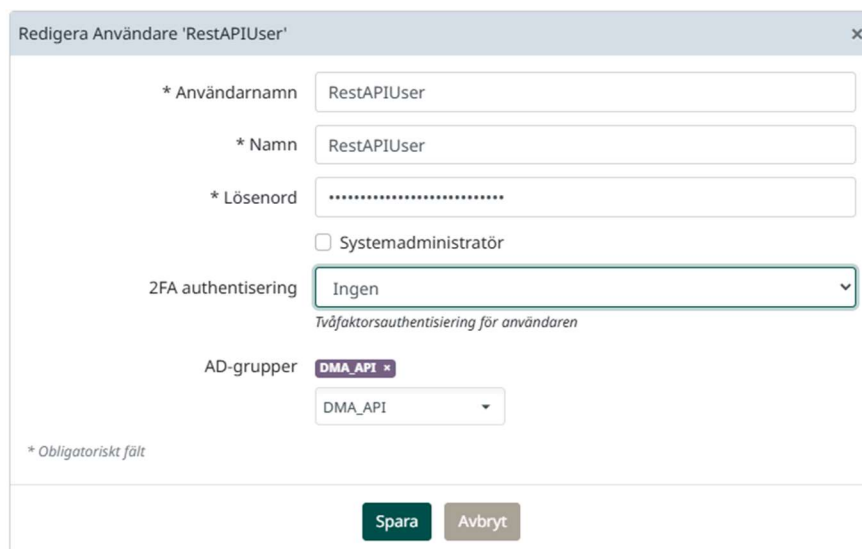
AD-grupper DMA_ADMIN x DMA_Ambulanslarm x DMA_API x DMA_IT x DMA_LTF x DMA_MTA x

6 valda AD-grupper

* Obligatoriskt fält

Spara Avbryt

Att tänka på: om ni har specifika användare som tex gör REST-api anrop så kan ni behövs stänga av 2FA authenticisering för dessa.



Redigera Användare 'RestAPIUser'

* Användarnamn RestAPIUser

* Namn RestAPIUser

* Lösenord

☐ Systemadministratör

2FA authenticisering Ingen

Tvåfaktorsauthenticisering för användaren

AD-grupper DMA_API x

DMA_API

* Obligatoriskt fält

Spara Avbryt

Om TOTP aktiverats för en användare så kommer då användaren efter inloggning att få följande alternativ.

DMA Språk ▾ Logga in

Aktivera tvåfaktorsautentisering

Tvåfaktorsautentisering är inte aktiverad.

Du kan välja att nu aktivera tvåfaktorsautentisering, eller att hoppa över denna gång (5 ggr kvar)

AktiveraHoppa över denna gångAvbryt

Användaren kan välja att hoppa över aktiveringen ett antal gånger (inställning finns för hur många gånger), alternativt att aktivera auktoriseringen, då en QR-kod presenteras för användaren att scanna. (Här presenteras även definierad hjälp-text med eventuella länkar till önskvärda appar.)

DMA

Logga in

Använd Google authenticator eller Microsoft Authenticator för att scanna QR-koden.



Öppna din autentiseringsapp och hämta OTP

OTP måste anges

Avbryt

Vid efterföljande inloggningar så kommer ingen QR-kod att presenteras, endast OTP för godkänd inloggning.

Om användaren skulle förlora sitt scannade konto i appen så finns möjlighet för en administratör att via användarlistan återställa användarens TOTP-konto, då användaren på nytt kommer presenteras med aktiveringsalternativet.

Utökad säkerhet med API-nyckel för REST-API anrop.

Man kan nu ställa in att en API-nyckel krävs angiven vid REST-API anrop. (Inställningar->Allmänna inställningar->Användarkonton)

☒ Kräv genererad API-nyckel för att få tillgång till REST-API

Denna inställning gör att för att ett anrop ska godkännas så måste en även användarunik api-nyckel anges i huvudet på alla anrop.

```
curl -X 'POST' \
      'https://{url}/api/v1/endpoint/search' \
      -H 'accept: application/json' \
      -H 'api-key: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
      -H 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
      -H 'Content-Type: application/json' \
      -d '{
        "searchText": "test"
      }'
```

Denna API-nyckel kan antingen genereras utav en administratör (Användarlistan->Generera API-nyckel), alternativt av användare själv (Inställningar->Generera ny API-nyckel).

API-nyckeln för en användare är aktiv till dess att en ny genereras.

Ta bort användargränssnitt för REST-API

Det går nu att ta bort användargränssnittet för DMA REST-API (Swagger).

Detta görs via konfigurationsfilen för DMA appsettings.kund.json genom att sätta parametern "ShowSwaggerUI" till false.

```
{
  ...
  "ShowSwaggerUI": false,
  ...
}
```