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:

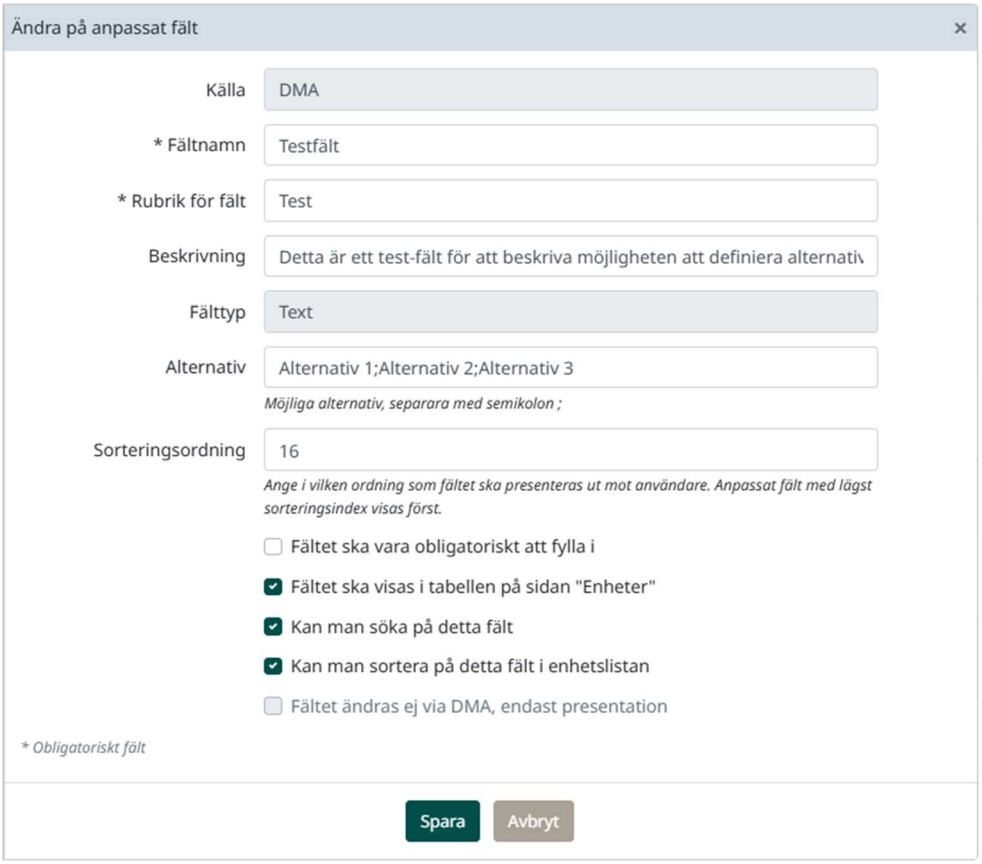
other:CiscoAVPair:service-type
other:CiscoAVPair:audit-session-id
other:CiscoAVPair:method
other:CiscoAVPair:client-iif-id
other:CiscoAVPair:vlan-id
other:CiscoAVPair:dc-profile-name
other:CiscoAVPair:dc-device-name
other:CiscoAVPair:dc-device-class-tag
other:CiscoAVPair:dc-certainty-metric
other:CiscoAVPair:dc-protocol-map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

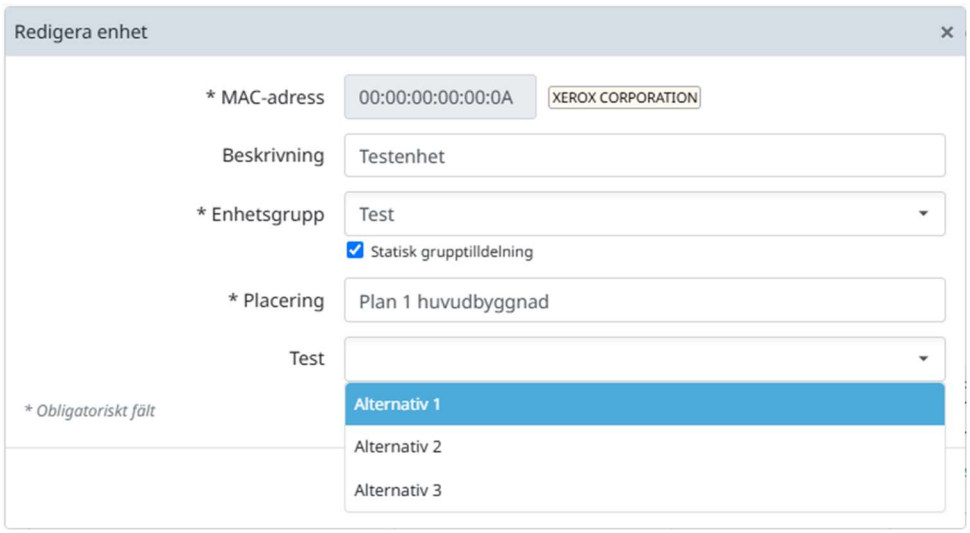
Anpassade fält med alternativ (version 4.1.2)

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.

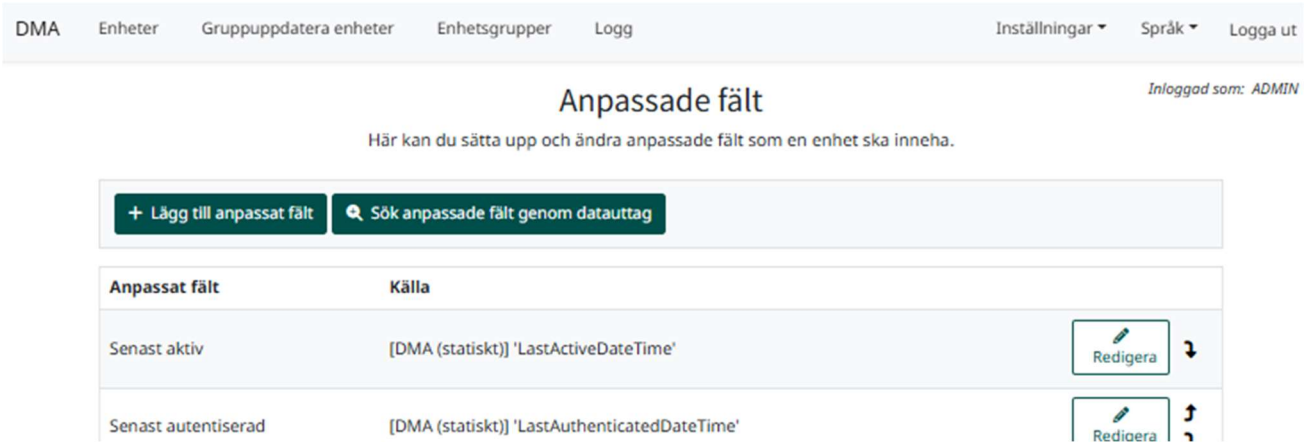
För fält-typen ”**Text**” så är dessa enbart förslag, men för fält-typen ”**Fasta alternativ**” så är dessa alternativ tvingande, dvs de enda alternativ användaren kan använda vid editering av en enhet.



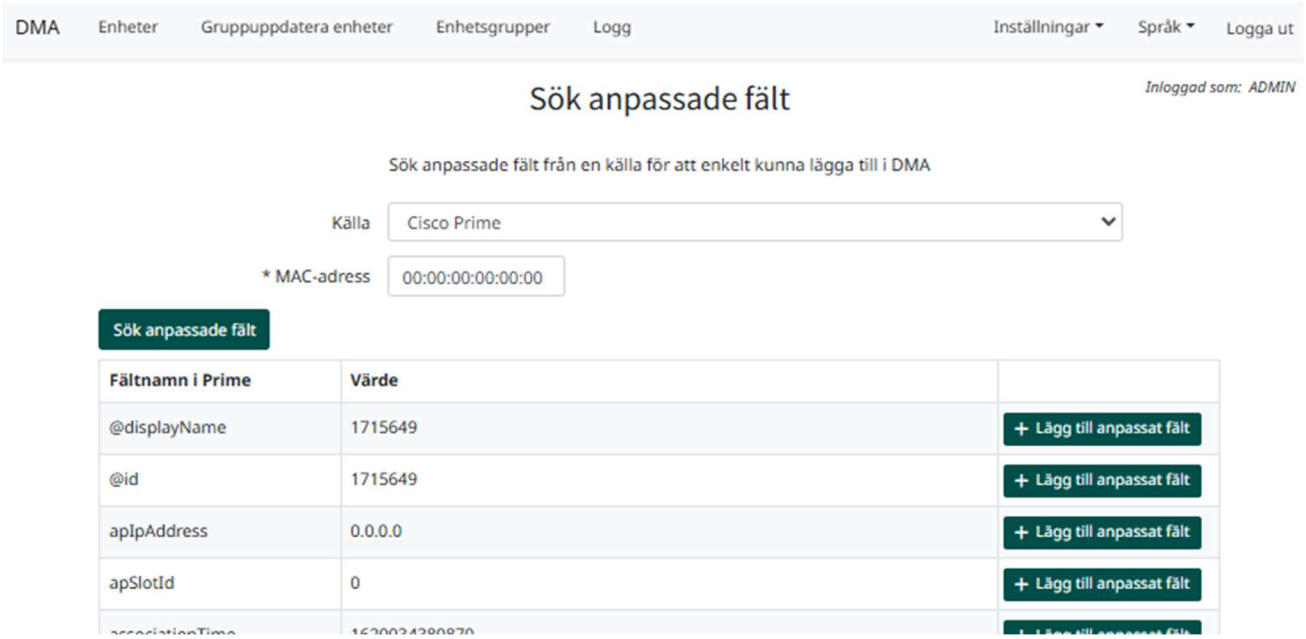


Förenklad hantering av konfiguration av anpassade fält

För att förenkla konfigureringen 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.



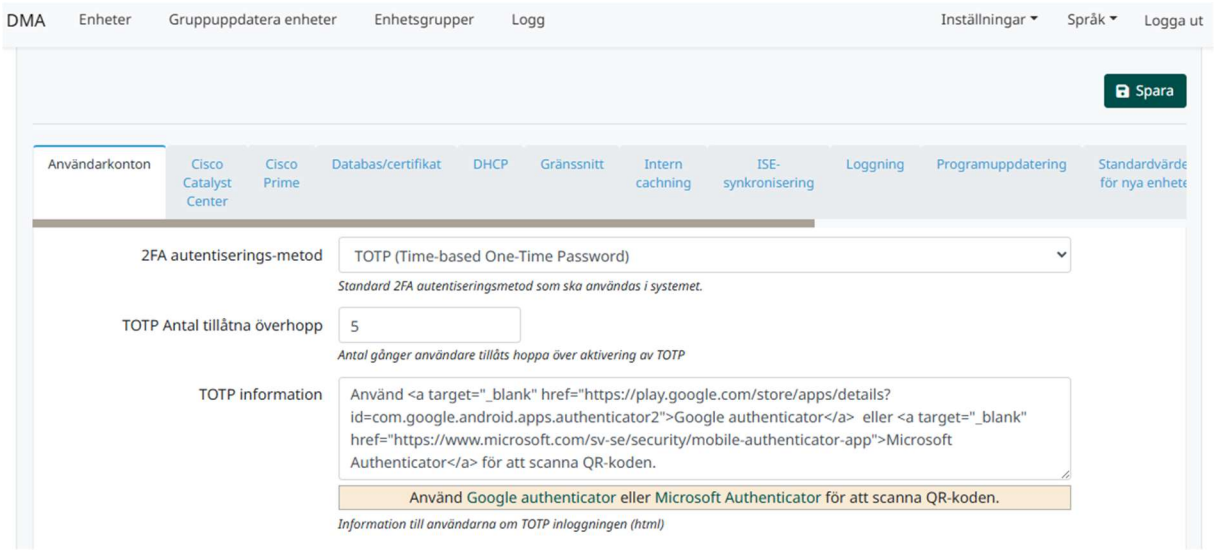
Med knappen "Sök anpassade fält genom datauttag", så får du upp följande sida.



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)

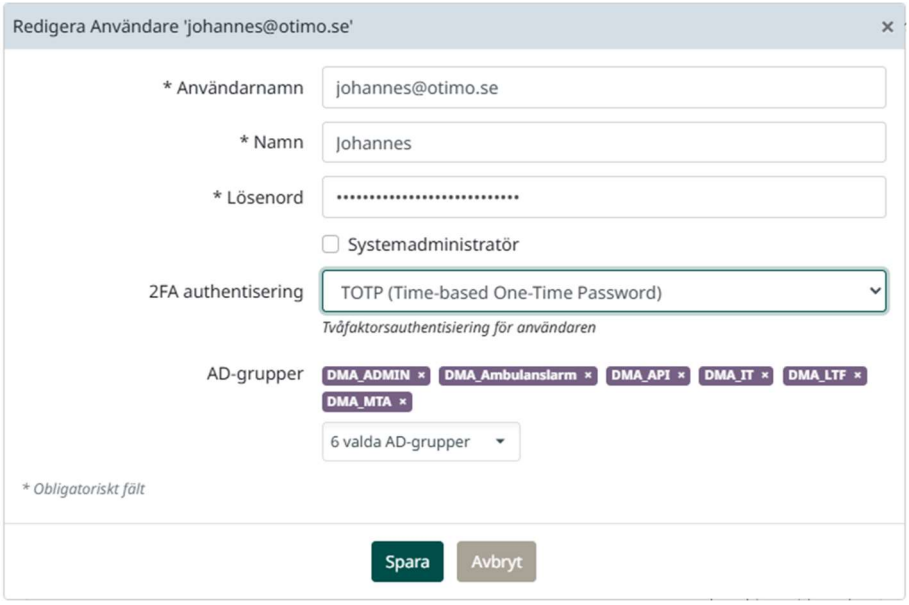
DMA är nu uppdaterad med ytterligare säkerhet, TOTP tvåfaktorsautentisering, denna kan aktiveras på två sätt, dels genom att ändra standard-metoden (Inställningar->Allmänna inställningar->Användarkonton).



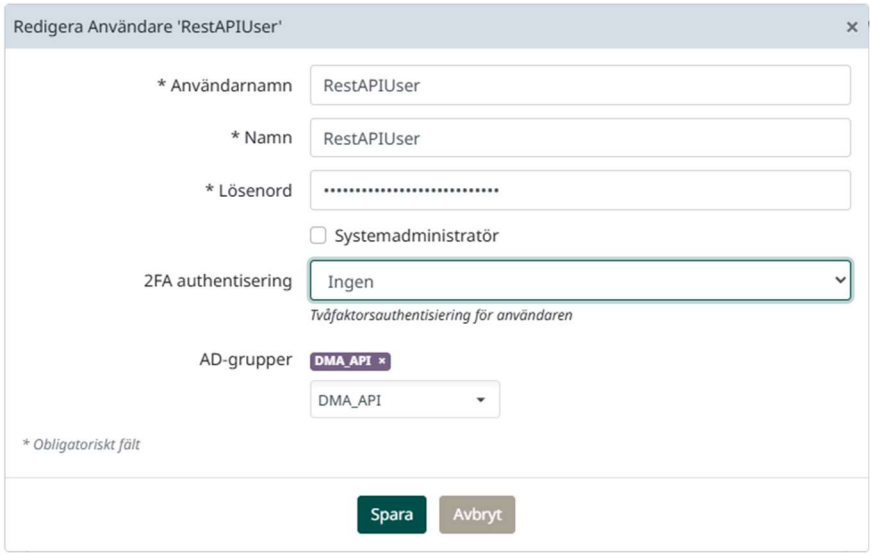
Här anger man standardinställningen för 2FA-auktorisering, antal tillåtna gånger en användare kan ”hoppa över” att aktivera TOTP auktorisering, samt vilken hjälp-text man vill visa användaren vid aktiveringen av TOTP. (denna text kan anges i html, med länkar för att t.ex. hjälpa användaren till rätt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

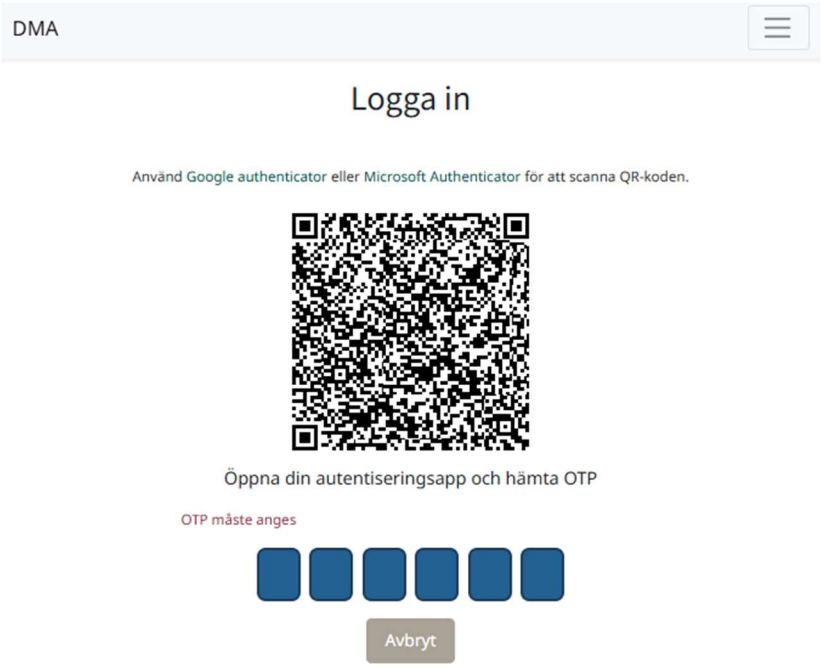


Att tänka på: om ni har specifika användare som tex gör REST-api anrop så kan ni behövs stänga av 2FA authentisieringen för dessa.



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

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.)

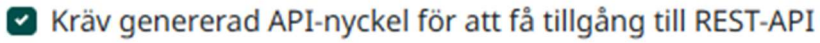


Vid efterföljande inloggningar så kommer ingen QR-kod att presenteras, endast OTP för godkänd inloggning.

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)



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: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
    -H 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
    -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,
    …
}
```