



Q-interactive®

Guide för användning av tvåfaktorsautentisering (2FA)

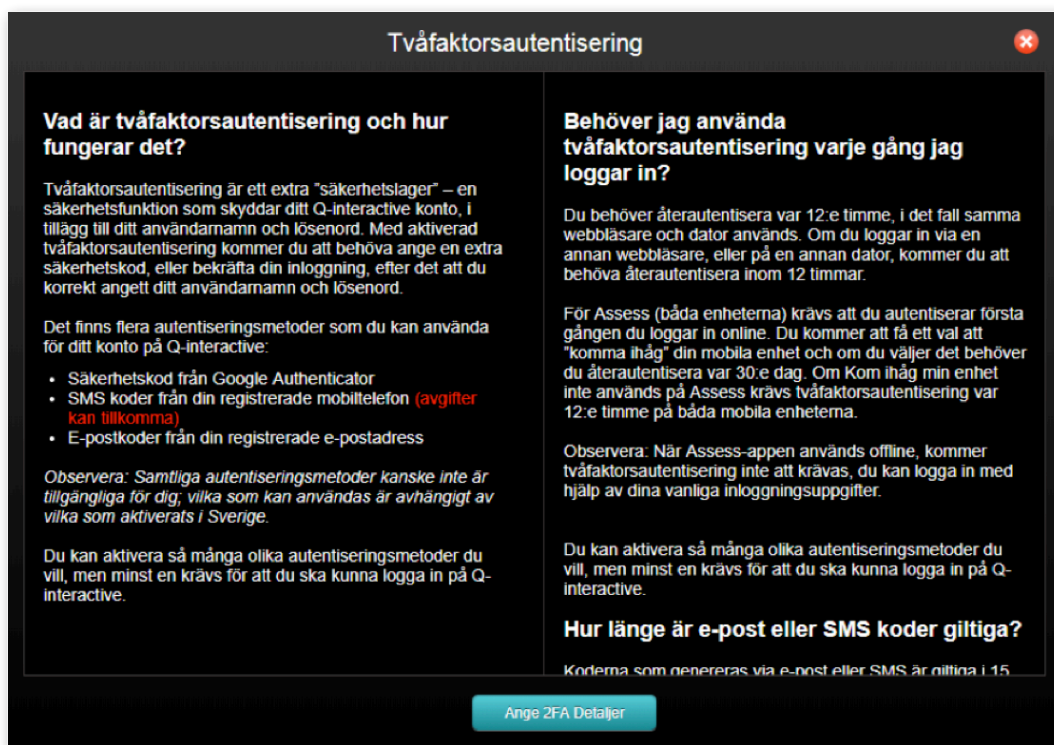
Q-interactive Användarguide

Februari 2018

Tvåfaktorsautentisering, härafter kallat 2FA, är ett komplement till användarnamn och lösenord för att ytterligare öka säkerheten för konton på Q-interactive och Q-global. När du loggar in med 2FA anger du ditt användarnamn och lösenord som vanligt, men också en engångskod som bara du kan komma åt. Detta ger dig en extra säkerhetsnivå mot att obehöriga får åtkomst till din data.

Pearson har infört tvåfaktorsautentisering på Q-interactive och Q-global för att uppfylla kraven i den nya sekretessförordningen GDPR (General Data Protection Regulation).

Första gången du loggar in på Central innan 2FA blivit aktiverat ser du ett fönster som beskriver vad 2FA är:



Du kan inte gå vidare i programmet innan du har konfigurerat minst en autentiseringsmetod. Nedan visas metoden för Q-interactive.

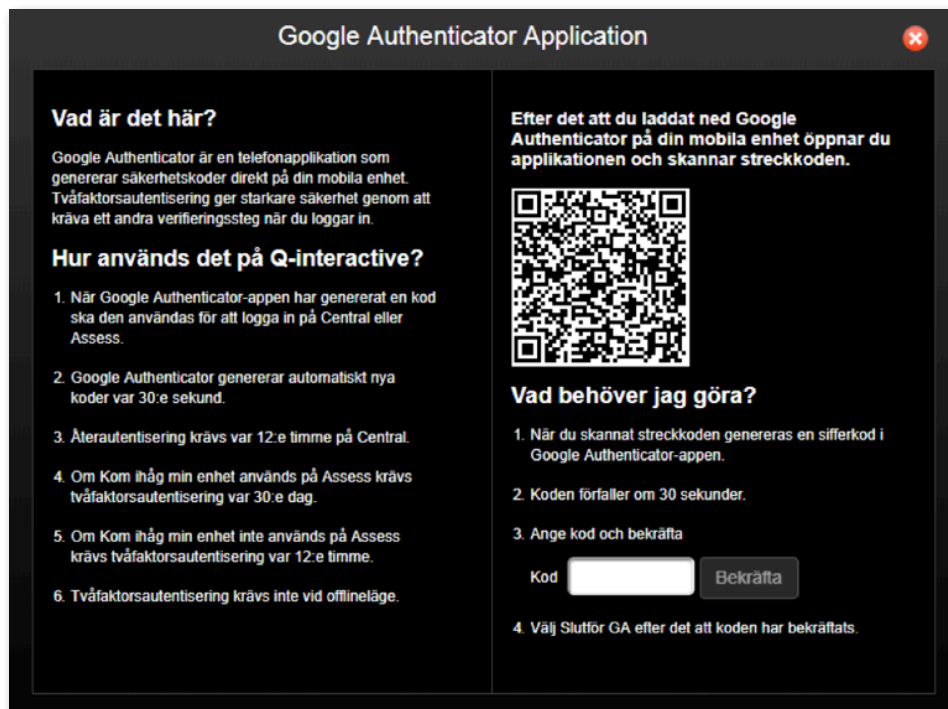
Klicka på **Ange 2FA detaljer** för att fortsätta.

På nästa sida kan du ställa in tre olika metoder för 2FA: Google Authenticator, SMS eller e-post. Den förstnämnda är en app som gratis kan laddas ned till de flesta smartphones. Appen genererar engångskoder som kan användas för att verifiera inloggningen på olika webbplatser och applikationer. Google Authenticator är lätt att använda och fungerar utan internet och nätverksanslutning. Applikationen genererar en ny kod var 30:e sekund, och är därför en mycket säker metod för tvåfaktorsautentisering.

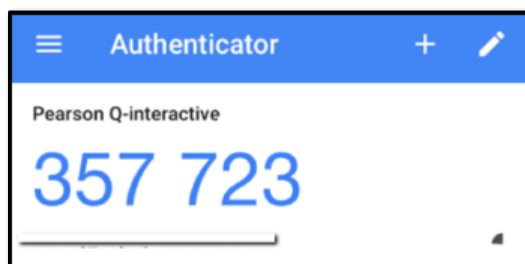
För att *aktivera Google Authenticator* måste du först ladda ned appen. Sök efter "Google Authenticator" i App Store, Google Play, BlackBerry World eller Microsoft Store beroende på om du har iPhone, Android, BlackBerry eller Windowstelefon. När Google Authenticator installerats på din telefon, öppna appen och klicka på plustecknet. Välj "Läs av streckkoden" och godkänn att appen får åtkomst till telefonens kamera.

Klicka sen på **Konfigurera GA** i Central.

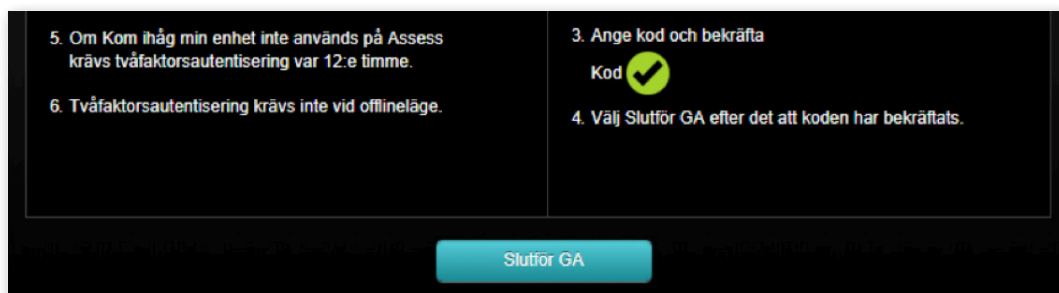
Längst upp till höger finns en QR-kod som kan skannas med mobiltelefonen.



Plocka upp telefonen och rikta kameran mot kodbilden från Central så att kodbilden visas i rutan på telefonen. Ett sexsiffrigt nummer visas på telefonen:



Ange numret (sex siffror, mellanslag behöver inte anges) i punkt 3 på Q-interactive Central och klicka på **Bekräfta**. En grön bock visas för att bekräfta att koden verifierats. Klicka sedan på **Slutför GA**.



VIKTIGT: Se till att autentiseringen är klar. Avsluta med att klicka på **Spara** längst upp till höger.

Tvåfaktorsautentisering ?

Min profil

Ändra lösenord

Tvåfaktorsautentisering

Ditt val för tvåfaktorsautentisering har registrerats.

[Pearson] SE Content QA - ztokay_se

Du kan aktivera så många olika autentiseringsmetoder du vill, men minst en krävs för att du ska kunna logga in på Q-interactive. Aktivera andra valfria metoder, när det är tillämpligt, för att minimera eventuella autentiseringsproblem. Genererade koder kommer att skickas till bekräftad e-postadress eller bekräftat mobilnummer under registreringen, samt vid senare inloggning med tvåfaktorsautentisering.

Du måste ladda ned Google Authenticator-appen innan du kan börja. Med en ny telefon måste du konfigurera Google Authenticator igen.

Konfigurera Google Authenticator ☐ Slutfört ☒

Spara

Google Authenticator är nu aktiverad på ditt konto och du måste ange ett sexsiffrigt nummer från programmet när du loggar in på Central. 2FA är giltigt i 12 timmar på samma dator.

2FA via SMS eller e-post konfigureras på samma sätt.

Tvåfaktorsautentisering ?

Min profil

Ändra lösenord

Tvåfaktorsautentisering

[Pearson] SE Content QA - ztokay_se

Du kan aktivera så många olika autentiseringsmetoder du vill, men minst en krävs för att du ska kunna logga in på Q-interactive. Aktivera andra valfria metoder, när det är tillämpligt, för att minimera eventuella autentiseringsproblem. Genererade koder kommer att skickas till bekräftad e-postadress eller bekräftat mobilnummer under registreringen, samt vid senare inloggning med tvåfaktorsautentisering.

Du måste ladda ned Google Authenticator-appen innan du kan börja. Med en ny telefon måste du konfigurera Google Authenticator igen.

Konfigurera Google Authenticator ☐ Konfigurera GA

2FA e-postadress Verifiera

E-postkod Bekräfta

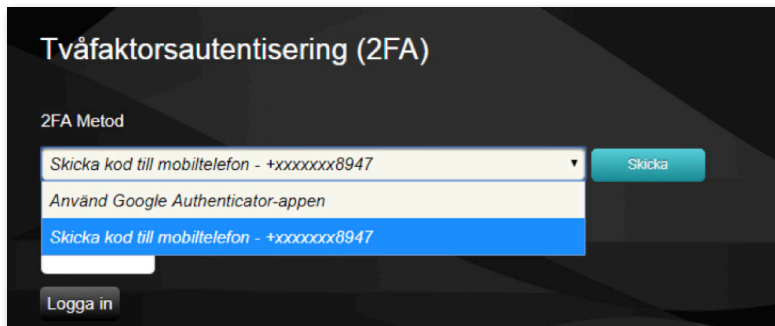
2FA mobiltelefonnummer Verifiera

Mobiltelefonkod ☒ Slutfört

Spara

Ange e-postadress eller mobiltelefonnummer och klicka på **Verifiera**. En engångskod skickas till din e-post eller telefon, beroende på vilken metod du valt. Ange koden i rutan nedanför och klicka på **Bekräfta**. En grön bock verifierar att configurationsprocessen är klar. Kom också här ihåg att klicka på **Spara** längst upp till höger.

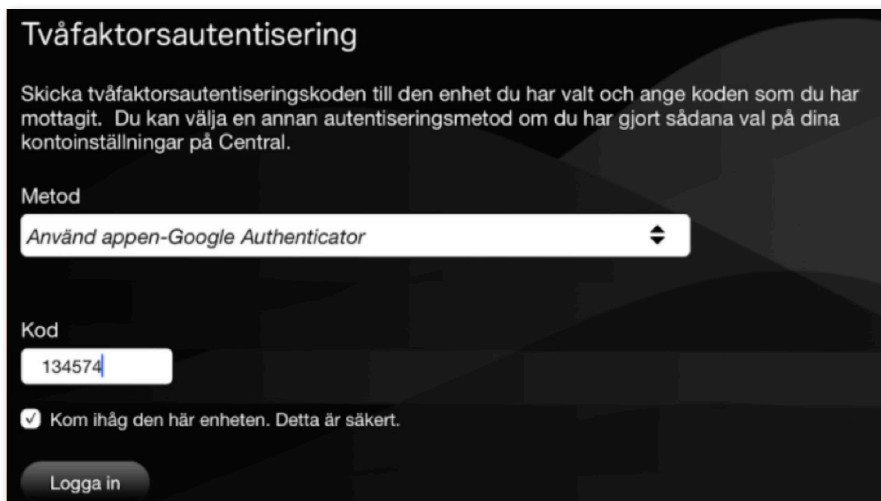
Nästa gång du loggar in kommer du att bli ombedd att ange 2FA-metod. Om du har valt mer än en autentiseringsmetod kan du välja mellan dem. Till exempel välja att få koden via e-post eller använda Google Authenticator.



The screenshot shows a dark-themed interface titled "Tvåfaktorsautentisering (2FA)". Under the heading "2FA Metod", there is a dropdown menu with three options: "Skicka kod till mobiltelefon - +xxxxxxx8947", "Använd Google Authenticator-appen", and "Skicka kod till mobiltelefon - +xxxxxxx8947". The first and third options are highlighted in blue. To the right of the dropdown is a teal "Skicka" button. At the bottom left is a grey "Logga in" button.

Ange koden från Google Authenticator, eller den du får via SMS eller e-post. Klicka på **Logga in**.

När du loggar in på Assess på testledarens eller testpersonens iPad måste du även ange en engångskod så länge dessa iPads är anslutna till internet. Ange ditt användarnamn och lösenord som vanligt. Välj sedan autentiseringsmetod och ange engångskoden på samma sätt som när du loggar in på Central.



The screenshot shows a dark-themed interface titled "Tvåfaktorsautentisering". It contains a paragraph of instructions: "Skicka tvåfaktorsautentiseringskoden till den enhet du har valt och ange koden som du har mottagit. Du kan välja en annan autentiseringsmetod om du har gjort sådana val på dina kontoinställningar på Central." Below this is a "Metod" dropdown menu with the selected option "Använd appen-Google Authenticator". Underneath is a "Kod" input field containing the text "134574". Below the input field is a checked checkbox with the text "Kom ihåg den här enheten. Detta är säkert." At the bottom is a grey "Logga in" button.

Om du väljer SMS eller e-post, klicka på **Skicka** och ange koden du får.

Klicka sedan på **Logga in**.