ANTURA

Antura Document Utilities

Antura AB, www.antura.se

2608 (Augusti 2026)

Antura Document Utilities

Antura Document Utilities (ADU) är en valfri Windows-skrivbordsapplikation som förenklar redigering av dokument i Antura filarkiv. Programmet är utvecklat och signerat av Antura.

Detta dokument är uppdelat i tre delar:

1. **Vad ADU används till** — programmets syfte och när det är aktuellt att använda det.
2. **Hur det fungerar** — arkitekturen och flödet från början till slut, på den nivå som kundens IT-avdelning behöver.
3. **Säkerhet** — kontrollerna och designvalen som kundens informationssäkerhetsteam behöver granska innan utrullning.

Två appendix följer: en installationsguide och en FAQ.

1. Vad ADU används till

Syfte

ADU är **inte** nödvändigt för att arbeta med dokument i Antura — all läsning, redigering och uppladdning kan också göras direkt i Anturas webbgränssnitt. ADU finns för att minska antalet klick som behövs för att ladda ner, öppna, spara och ladda upp ett dokument under ett *Redigera och låsa*-flöde.

När ADU är installerat och användaren klickar *Redigera och lås* på ett dokument i Antura:

- Laddas filen ner i bakgrunden.
- Öppnas den i den associerade editorn (Word, Excel, AutoCAD, etc.).
- Övervakas filen medan användaren arbetar.
- Får användaren en fråga om att ladda upp den nya versionen (eller kasta ändringarna, eller fortsätta redigera) när editorn stängs.

Utan ADU innebär samma arbetsflöde manuella steg för att ladda ner, öppna, spara och ladda upp filen igen.

Vem behöver det

ADU installeras **per användardator** — av användaren själv eller av IT — på de datorer där användaren vill ha det förenklade flödet. En och samma installation fungerar mot flera Antura-instanser. Användare som inte har ADU kan fortfarande använda Antura — de tar bara den manuella vägen via webbgränssnittet.

Systemkrav

- **Operativsystem**: Microsoft Windows 11.
- **.NET Framework 4.8** måste vara installerat på klientdatorn (ingår i aktuella Windows-versioner).
- **Testade webbläsare**: Microsoft Edge, Mozilla Firefox eller Google Chrome (senaste version). Andra webbläsare kan fungera men är inte testade.
- macOS / Safari stöds **inte**, eftersom ADU förlitar sig på .NET Framework som endast finns på Windows.

2. Hur det fungerar

Arkitekturöversikt

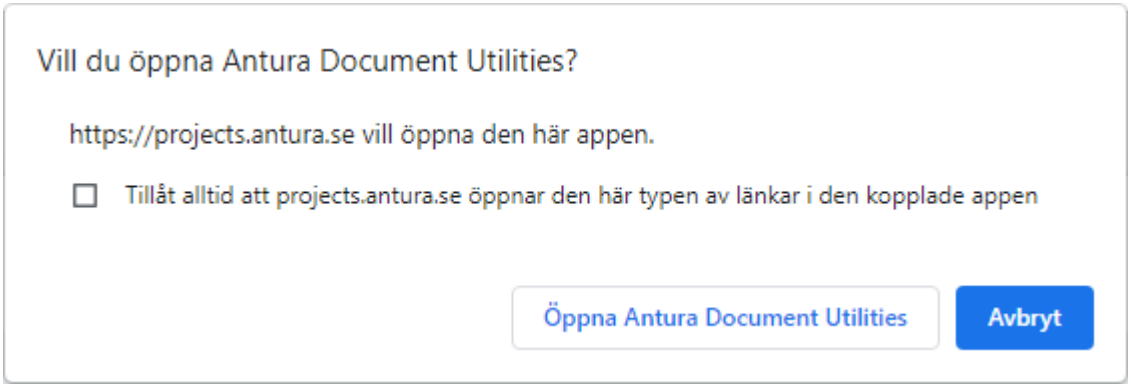
ADU är en Windows-skrivbordsapplikation som körs i användarläge och levereras som ett standardiserat, signerat MSI-installationspaket. Paketet innehåller programfilen och dess tillhörande bibliotek — inget annat. Programmet körs i den inloggade användarens kontext, endast när det startas av en åtgärd användaren utfört inne i Antura.

Det anpassade URL-protokollet — savetoserver:

ADU registrerar ett anpassat URL-protokoll så att Anturas webbgränssnitt kan starta det via användarens webbläsare:

När användaren klickar *Redigera och lås* i Antura skickas webbläsaren till en URL som börjar med `savetoserver:`. Webbläsaren visar en bekräftelsedialog som frågar om den registrerade hanteraren (Antura Document Utilities) får köras. Efter att användaren accepterar startar Windows den lokala applikationen med URL:en som enda argument.

Exemplet nedan är från Google Chrome:



Windows Installer (MSI)

ADU levereras som ett standardiserat Windows MSI-installationspaket. Det kan installeras interaktivt genom att dubbelklicka på filen, eller tyst som en del av en organisationsövergripande utrullning via SCCM, Intune eller motsvarande verktyg. Detaljerade steg finns i *Appendix A*.

Flödet från början till slut

Användaren klickar på en åtgärd i Antura som kräver att en fil öppnas (till exempel *Redigera och lås*). Följande sekvens körs:

1. **Antura-webbservern bygger en engångs-URL** med `savetoserver:`-schemat plus en autentiseringstoken. Antura-webbtjänstens bas-URL måste vara HTTPS.
2. **Webbläsaren tar emot en redirect till URL:en** och visar användaren en bekräftelsedialog. Den lokala applikationen startas inte utan användarens uttryckliga samtycke.
3. **Windows slår upp protokoll-hanteraren** via registernyckeln `HKLM\Software\Classes\savetoserver` (skrivs endast av MSI:n) och startar den lokala applikationen med URL:en som enda argument.
4. **Den lokala applikationen validerar URL:en** (se *Säkerhet → Defensiva kontroller vid uppstart*).
5. **Applikationen laddar ner filen** från kundens egen Antura-instans och presenterar autentiseringstoken vid varje anrop. Nedladdningen sker i delar; varje del integritetskontrolleras innan den accepteras.
6. **Den nedladdade filen skrivs till en sessionsunik undermapp under användarens `%TEMP%`-katalog** (`%TEMP%\Antura\<unik-tidsstämpel>\`), och en editor startas mot den (se *Filtyper som stöds* nedan).
7. **Applikationen övervakar filen** medan editorn är öppen. När editorn släpper sitt fillås och förändringar har upptäckts får användaren en fråga om att ladda upp som ny version, skriva över, fortsätta redigera, eller kasta ändringarna.
8. **Vid uppladdning** skickas filen i delar tillbaka till kundens Antura-instans med samma autentiseringstoken. Efter uppladdningen jämför server och klient integritetskontrollsummor över de lagrade byten — vid avvikelse görs ett nytt försök eller avbryts uppladdningen.
9. **Städning**: temp-filen tas bort och den sessionsunika undermappen rensas. Eventuellt flyttas en kopia till ett rullande lokalt arkiv under `%USERPROFILE%\Documents\Antura\Archived\` (standard 30 dagar, sedan automatiskt borttaget).

Filtyper som stöds

ADU öppnar endast filer vars filändelse finns på en fast vitlista. För varje tillåten filtyp visar tabellen nedan vad formatet är till för och hur ADU startar en editor mot det.

Filändelse(r)	Vad filen är	Hur ADU öppnar den
`.doc`, `.docx`, `.docm`	Microsoft Word-dokument (inkl. makro-aktiverade `.docm`)	Användarens OS-standardeditor för filändelsen (vanligtvis Microsoft Word)

Filändelse(r)	Vad filen är	Hur ADU öppnar den
`.xls`, `.xlsx`, `.xlsm`	Microsoft Excel-kalkylblad (inkl. makro-aktiverade `.xlsm`)	Den applikation som är registrerad under `HKEY_CLASSES_ROOT` för filändelsen; faller tillbaka på `excel.exe` om ingen registrering hittas
`.ppt`, `.pptx`, `.pp`	Microsoft PowerPoint-presentationer	Användarens OS-standardeditor (vanligtvis Microsoft PowerPoint)
`.vsd`, `.vsdx`, `.vsdm`, `.vdx`, `.vsw`	Microsoft Visio-diagram	Användarens OS-standardeditor (vanligtvis Microsoft Visio)
`.mpp`, `.mpx`, `.msp`	Microsoft Project-planer och utbytesformat	Användarens OS-standardeditor (vanligtvis Microsoft Project)
`.dwg`	AutoCAD-ritning	Användarens OS-standardeditor (vanligtvis AutoCAD)
`.ifc`	Industry Foundation Classes — ett BIM-format för byggnadsinformation	Användarens OS-standardeditor eller -visare för IFC
`.pdf`	Portable Document Format	Användarens OS-standardvisare för PDF
`.txt`	Vanlig text	**Anteckningar** (`notepad.exe`), alltid — den enda filtyp för vilken ADU förbigår OS-fil-associationen
`.xml`	XML-dokument	Användarens OS-standardeditor för XML

För allt utom `.txt` och Excel-formaten startar ADU filens OS-associerade applikation (samma som Windows skulle använda om användaren dubbelklickade på filen i Utforskaren). ADU innehåller inga egna visare eller editorer.

3. Säkerhet

Detta avsnitt vänder sig till kundens informationssäkerhetsteam som behöver utvärdera ADU innan utrullning. Det täcker autentiseringstoken, läs/skriv/körrättighets-fotavtrycket, nätverksexponeringen, de defensiva kontrollerna som skyddar användare och kunddata, samt försörjningskedje-kontrollerna som skyddar binären i sig.

Antura kan svara på djupare tekniska frågor skriftligen eller under NDA.

Ingen bakgrundsnärvaro

Efter installation lägger ADU till **ingen** Windows-tjänst, schemalagd uppgift, automatisk uppdaterare, autostart-post, webbläsartillägg, kärndrivrutin eller brandväggsregel. MSI:n installerar endast programfilen och dess tillhörande bibliotek. ADU startas **på begäran** när användaren klickar på en åtgärd i Antura, körs så länge redigeringssessionen pågår och avslutas sedan.

Användarsamtycke vid start

Bekräftelsedialogen som beskrivs i *Hur det fungerar → Det anpassade URL-protokollet* är den första säkerhetskontrollen i startflödet. Första gången en `savetoserver:`-URL påträffas frågar webbläsaren användaren om Antura Document Utilities får hantera länken. Användarens val är per webbläsare och kan när som helst ändras via webbläsarens inställningar för protokollhanterare — ADU startas endast därför att användaren uttryckligen har gett den behörigheten.

Autentiseringstoken

Token är den autentiseringsuppgift som den lokala applikationen presenterar vid varje anrop till kundens Antura-instans. Det är det som auktoriserar läs- och skrivåtkomst till användarens dokument.

Kryptografiska egenskaper

- **Algoritm**: AES-256 i GCM-läge (autenticerad kryptering med associerad data).
- **Nyckel**: 256-bitars symmetrisk nyckel, genererad en gång med en kryptografiskt säker slumptalsgenerator och som endast finns på kundens Antura-webbserver. Nyckeln lämnar aldrig servern.

- **Nonce**: 96-bitars slumpmässig nonce, nygenererad för varje token.
- **Autentiseringstag**: 112-bitars GCM-tag som täcker krypttexten. Varje manipulation av token får tag-verifieringen att misslyckas och anropet avvisas.
- **Opak utanför den utfärdande servern**: överallt där token transporteras eller refereras — URL:er, webbläsarens adressfält, lokal diagnostik — är den AES-256-GCM-krypterad chiffertext. Dess innehåll (användaridentitet, mapp, utgångstid, sessionsidentifierare etc.) kan inte läsas utan den nyckel som endast finns på servern.

Innehåll i den krypterade tokenen

- Den Antura-användaridentitet som anropet ska köras som.
- Mappen/filen redigeringssessionen utfärdades för.
- En utfärdande- och utgångstidsstämpel.
- En unik sessionsidentifierare.
- Användarens språk.

Validering vid varje anrop

Vid varje serveranrop dekrypteras token; om GCM-tag-kontrollen misslyckas avvisas anropet. Om utgångstiden har passerats avvisas anropet. Anropet körs sedan i kontexten av användaridentiteten från token, och **användarens normala Antura-rättigheter kontrolleras för varje åtgärd** — läsrättighet vid nedladdning, skrivrättighet vid uppladdning, lås/upplåsningsrättighet vid utcheckning, och så vidare. ADU kan inte utföra någon operation som användaren inte redan får utföra i Anturas webbgränssnitt.

Livstid och sessionsomfång

- **Maximal livstid**: 5 dagar. Utgångsstämpeln sätts när token utfärdas och kontrolleras vid varje anrop; utgångna tokens avvisas.
- **Signalering av aktiv redigering**: medan editorn är öppen skickar ADU en enkelriktad puls till servern (se *Nätverksyta*); när pulsen upphör släpper servern redigeringsposten så att dokumentet inte längre visas som “redigeras nu”. 5-dagarsgränsen är den bindande gränsen för själva tokenen.
- **Sessionsidentifierare**: varje token bär en unik sessionsidentifierare så att enskilda utfärdanden kan följas individuellt i serverns granskningslogg.
- **Bunden till en enskild Antura-instans.** Token skickas endast tillbaka till den Antura-instans som utfärdade den, och endast över HTTPS.

Rättigheter och process-fotavtryck

Detta avsnitt besvarar frågan “vilka läs- / skriv- / körrättigheter behöver ADU?”.

Rättigheter vid installation (engångs, av IT)

- **Lokal administratör** krävs för att köra MSI:n, eftersom den skriver under `C:\Program Files\Antura AB\` och skapar protokoll-hanterar-nyckeln under `HKLM\Software\Classes\savetoserver`.
- Tyst utrullning i organisation stöds (`msiexec /qn /i antura-document-utilities.msi`).
- Paketet är ett standardiserat signerat MSI och kan repacketeras eller wrappas av SCCM, Intune eller motsvarande utrullningsverktyg.

Rättigheter vid körning (varje gång en användare redigerar ett dokument)

ADU körs i den inloggade användarens **standardanvändarkontext**. Det begär **inte** elevering, körs **inte** som en tjänst och kräver **inte** lokal administratör vid körning. Det fullständiga fotavtrycket är:

Resurs	Åtkomst	Anmärkning
`%TEMP%\Antura\<unik-tidsstämpel>\`	läs + skriv + ta bort	Det nedladdade dokumentet medan det redigeras. Den unika undermappen tas bort vid städning.
`%USERPROFILE%\Documents\Antura\Archived\`	läs + skriv + ta bort	Valfritt rullande arkiv av redigerade dokument (standard 30 dagar). Se *Lokalt arkiv över redigerade dokument (konfigurerbart)* nedan för hur det stängs av.

Resurs	Åtkomst	Anmärkning
`%LOCALAPPDATA%\Antura\Logs\` (faller tillbaka på `%TEMP%\Antura\Logs\`)	skriv	Lokala rullande loggfiler — en fil per dag (`Log<datum>.txt`), beskärs automatiskt till de senaste **14 dagarna**. Aktiverad som standard; **loggning kan stängas av** genom att sätta Antura-instansens konfigurationsnyckel `Document:LogApdu` till `false` (hanteras av Antura support — det finns ingen admin-UI-toggle för detta).
`HKLM\Software\Classes\savetoserver`	läs vid körning	Används av Windows för att slå upp protokoll-hanteraren. Skrivs endast av MSI:n.
`HKEY_CLASSES_ROOT\<filändelse>\shell\open\command`	läs vid körning	Används för att slå upp operativsystemets registrerade editor för dokumentets filändelse.
OS-registrerad editor (Word, Excel, AutoCAD, etc.)	körrättighet	Startas i användarens kontext med temp-filen som argument.
Nätverk: HTTPS till kundens egen Antura-instans	utgående TLS	Den enda nätverks-destinationen. Ingen telemetri, inga tredjepartsändpunkter.

Utöver detta använder ADU inga andra mappar, registerhive:ar eller nätverks-destinationer.

Lokalt arkiv över redigerade dokument (konfigurerbart)

Som standard behåller ADU efter en redigeringssession en lokal kopia av varje redigerat dokument i ett rullande per-användar-arkiv (standard 30 dagar, sedan automatiskt borttaget). Arkivet är tänkt som ett skyddsnät så att användaren kan återställa en pågående redigering om något skulle gå fel.

För känsliga miljöer kan detta vara oönskat — det innebär att fullständiga, okrypterade kopior av varje redigerat dokument finns kvar på användarens dator i minst 30 dagar. Det finns ingen

schemalagd rensning; gamla filer tas bort först nästa gång ADU körs, så filerna kan ligga kvar längre om ADU inte används. En Antura-administratör kan stänga av arkivet:

- **Var**: *Administration → System → Inställningar*.
- **Inställningens namn**: **"Arkivera 'Spara till Server'-dokument lokalt"** (engelska: *"Archive Save to Server documents locally"*).
- **Standard**: aktiverad.
- **Effekt när avstängd**: den sessionsunika temp-mappen tas fortfarande bort i slutet av sessionen, men ingen kopia flyttas till arkivet — det finns då ingen rullande lokal kopia av redigerade dokument på användarens dator.

Arkivets plats, när det är aktiverat, är `%USERPROFILE%\Documents\Antura\Archived\`. Platsen kan inte konfigureras i admin-gränssnittet — den är fast och bestäms av servern när start-URL:en byggs. Lagringstiden på 30 dagar är också fast; dokument äldre än så tas bort automatiskt av ADU vid nästa körning.

Vitlista för filändelser

Den fullständiga listan över stödda filändelser och vilka editorer som används för att öppna dem finns i *Hur det fungerar → Filtyper som stöds*. Ur säkerhetsperspektiv tillämpas samma vitlista **både på klient och server**:

- Servern vägrar bygga en start-URL för en fil vars filändelse inte finns på listan.
- Klienten vägrar starta någon editor för en fil vars filändelse inte finns på listan, även om den på något sätt skulle ha tagit emot en sådan URL.

Filändelser utanför vitlistan får applikationen att avbryta utan att starta någon editor.

Defensiva kontroller vid uppstart

Varje gång ADU startas, innan något dokument berörs, kontrolleras:

- **Endast HTTPS** — server-URL:er som inte är HTTPS får applikationen att visa ett felmeddelande och avslutas.
- **Ingen system-proxy** — en systemövergripande HTTP-proxy-konfiguration får applikationen att visa ett felmeddelande och avslutas. Proxy stöds uttryckligen inte, för att förhindra att fil-innehåll i tysthet omdirigeras.
- **Editor-livstid bunden till sessionen** — server-side-redigeringssessionen hålls vid liv endast medan editorn körs. Långvarig kontaktförlust med servern får applikationen att be användaren spara manuellt och avslutas.

Dataintegritet

Integriteten på kunddata säkerställs i tre lager, i ordning av styrka:

- **Token-integritet (kryptografisk).** AES-256-GCM-autentiseringstaggen på token avvisar varje ändring av credentialen — anropet avvisas innan någon dokumentoperation körs.
- **Transport-integritet (kryptografisk).** HTTPS ger kryptografisk integritet för varje byte som utbyts med Antura-instansen, i båda riktningar, inklusive själva fil-innehållet.
- **Applikationsnivå-kontrollsumma.** Som ett skyddsnät utöver TLS jämför ADU och servern en kontrollsumma över varje nedladdad och uppladdad fil. Detta fångar oavsiktlig korruption från sammanslagning av filsegment eller lagringsrundtur som TLS inte ser (eftersom det sker utanför TLS-sessionen). Vid avvikelse görs ett nytt försök eller avbryts.

Nätverksyta

- All nätverkstrafik är utgående och initieras av den användarstartade ADU-processen.
- Den enda destinationen är **kundens egen Antura-instans** — given till ADU av servern när start-URL:en byggs.
- Transporten är endast HTTPS.
- ADU kontaktar inte **`antura.se`** eller någon Antura-värdad tjänst direkt. Strängen **`savetoserver:antura.se`** i start-URL:en är ett fast schema-prefix; ingen DNS-uppslagning görs mot **`antura.se`**.
- Medan editorn är öppen skickar ADU ett periodiskt liveness-anrop (var 60:e sekund) till kundens Antura-instans. Anropet är enkelriktat och har ingen kryptografisk funktion: det **förlänger inte** autentiseringstokens livstid (den maximala 5-dagars-gränsen är fast) och ADU agerar inte på svaret. Enda syftet är att signalera till servern att redigeringssessionen är aktiv så att andra användares webbvyer kan visa dokumentet som “redigeras nu” och uppdatera mappvyn när ändringar sparas.
- Ingen telemetri, analytics, krasch-rapportering eller tredjepartsändpunkter.

Försörjningskedjans integritet

MSI:n är **Authenticode-signerad** av Antura AB. Kunder kan verifiera signaturen innan utrullning med:

```
signtool verify /pa antura-document-utilities.msi
```

eller via filens *Digitala signaturer*-flik i Utforskaren.

Källkod, anpassning och granskning

- ADU utvecklas av Antura under samma ISO 27001-certifierade säkra utvecklingsprocess (SDLC) som Anturas webbapplikation, inklusive kodgranskning, statisk analys och penetrationstestning.
- Antura-plattformen — inklusive ADU — omfattas av **externa penetrationstester som genomförs årligen** av en oberoende specialist. Resultaten återförs till samma SDLC, och kunder tillhandahålls en sammanfattad version av varje rapport.
- Källkoden distribueras inte till kunder. En kunds säkerhetsteam får granska protokoll-kontraktet, de kryptografiska valen (AES-256-GCM), filändelse-vitlistan och körnings-fotavtrycket som beskrivs ovan.
- ADU är **inte** kund-anpassningsbar i fält — det finns ingen scripting, ingen plug-in-yta och ingen konfigurationsfil som ändrar dess säkerhetsbeteende. Allt beteende styrs antingen av användarens egna Antura-rättigheter eller av den fasta vitlistan och de defensiva kontrollerna ovan.
- Versionshantering: MSI-versionen är samordnad med Antura-instansens version. Verktyget behöver dock inte uppdateras vid varje Antura-version — Antura annonserar när en ny version av ADU krävs. Uppgraderingar sker genom att köra det nya MSI:t.

Sammanfattning av säkerhetsrelevanta designval

Risk	Skydd
Otillåten åtkomst till dokument	AES-256-GCM-token bunden till en specifik användare med max 5 dagars utgång; användarens normala Antura-rättigheter kontrolleras server-side vid varje anrop.
Token-manipulation	112-bitars GCM-autentiseringstag avvisar varje ändring av token.
Token-stöld	Token transporteras endast över HTTPS; applikationen vägrar icke-HTTPS-URL:er och vägrar all system-proxy-konfiguration.
Tyst start	ADU startas endast efter att användaren uttryckligen har gett `savetoserver:`-protokollet behörighet i sin webbläsare.

Risk	Skydd
Godtycklig kod-körning via filtyp	Fast filändelse-vitlista tillämpad både på klient och server. ADU startar endast en editor — aldrig ett godtyckligt kommando.
Bestående fotavtryck på disk	Sessionsunik temp-mapp som tas bort vid städning. Det valfria arkivet rensas automatiskt efter den konfigurerade lagringstiden.
Privilege escalation	Körs som inloggad användare; ingen tjänst, ingen schemalagd uppgift, inga administratörsrättigheter krävs vid körning.
Försörjningskedjans integritet	MSI är Authenticode-signerad av Antura AB; signaturen kan verifieras med `signtool` eller via Windows.
Nätverksexponering	Enda HTTPS-ändpunkt — kundens egen Antura-instans.

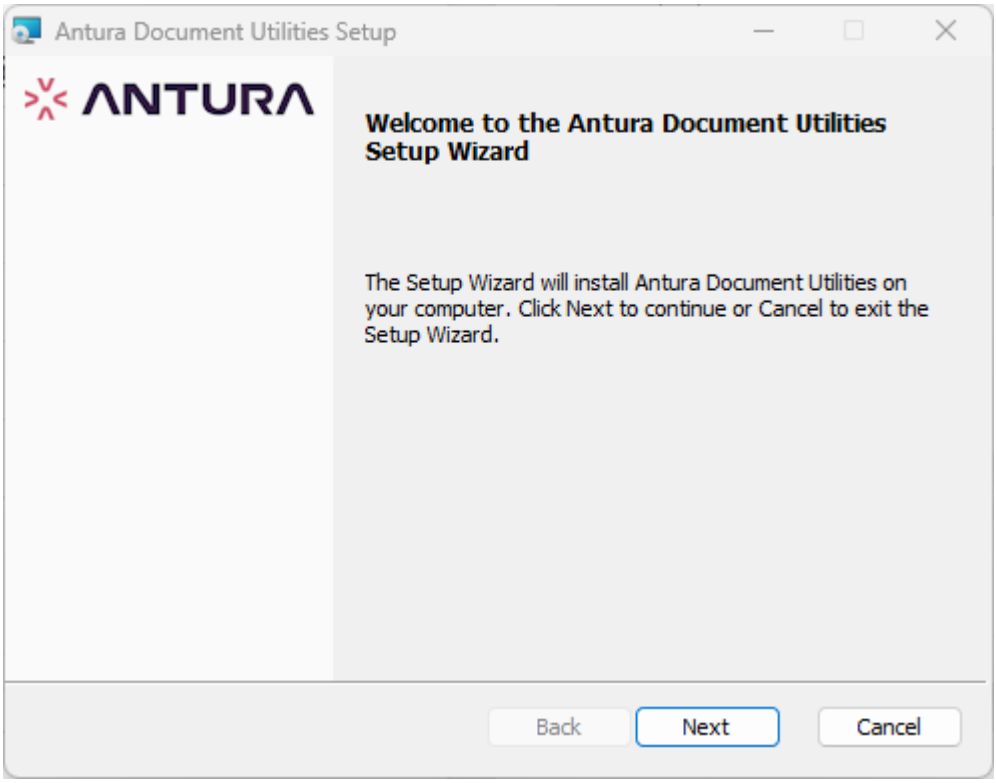
Appendix A: Installationguide

1. För att få tag på MSI-paket som installerar ADU går det att ladda ner i Antura ifrån Min plats - Inställningar med följande knapp.

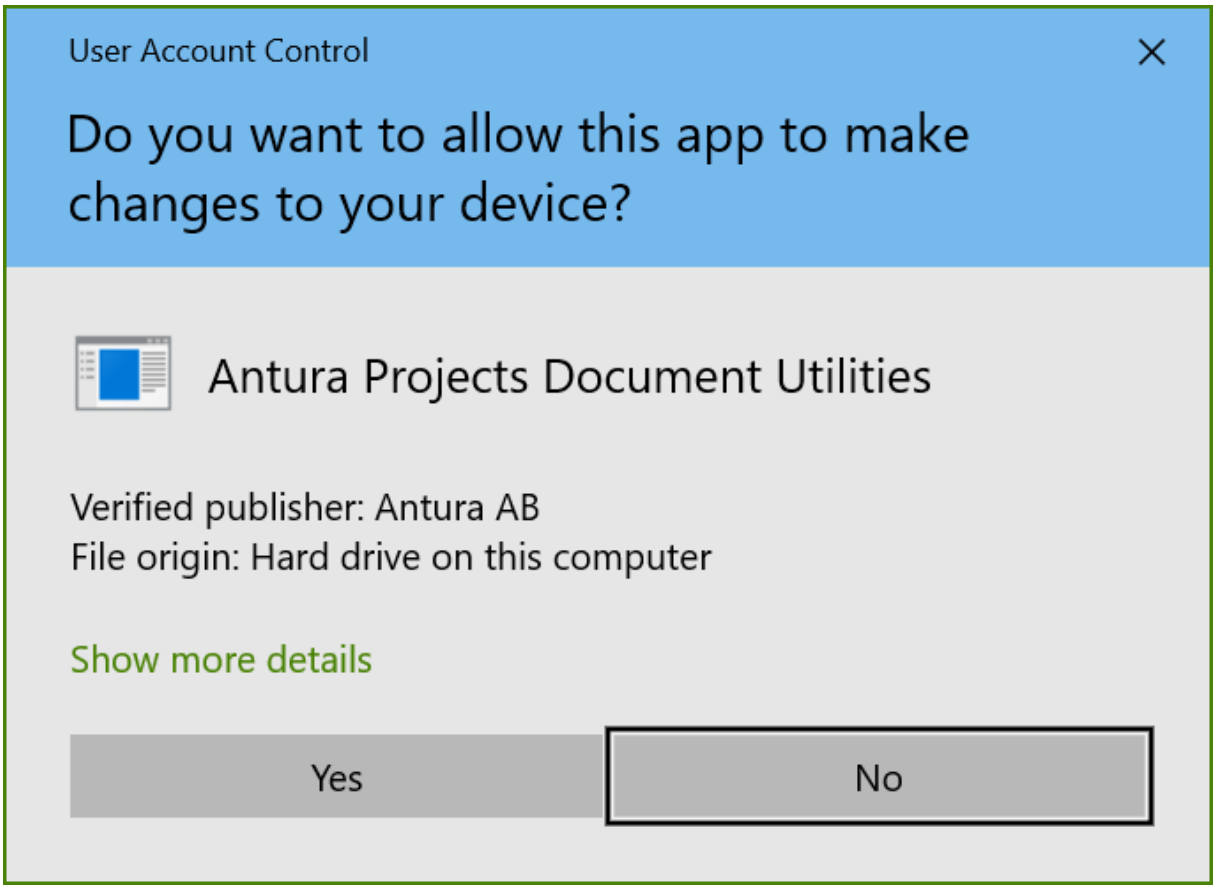
   

   MSI-paketet finns även tillgängligt för nedladdning på Antura publika sida: https://projects.antura.se/Views/ProjectPlace/Public.aspx?Site=565118

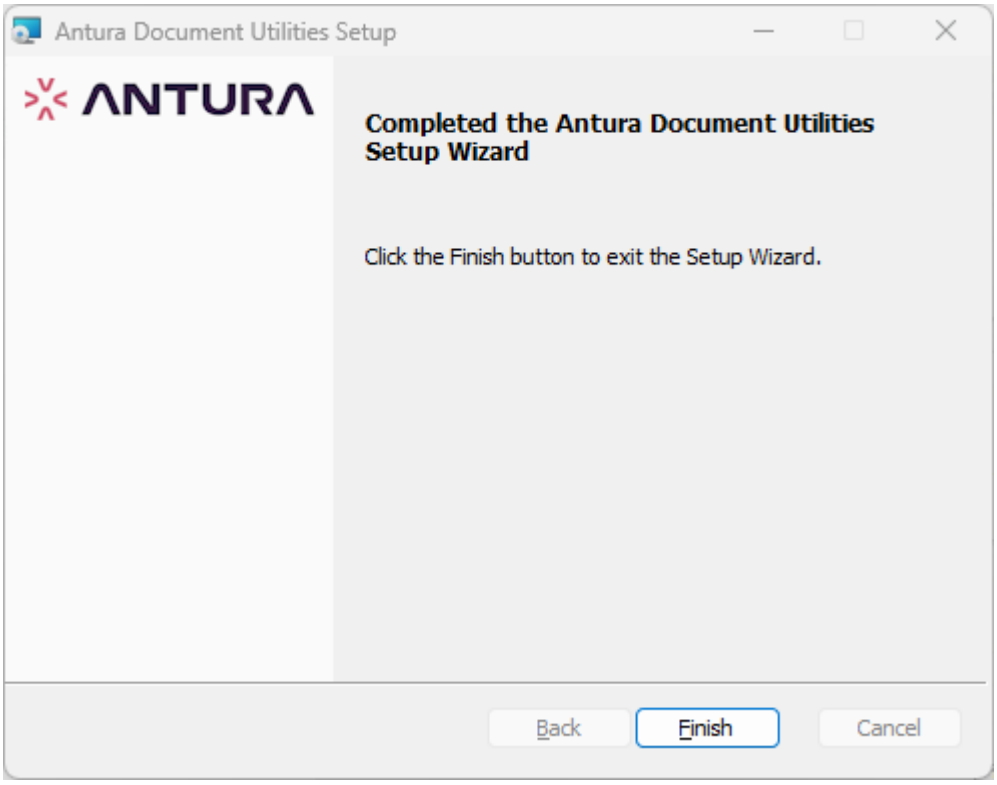
2. Kör MSI-paketet “antura-projects-document-utilities.msi”.
3. Klicka på Next för att genomföra installationen.



1. Under installation kan det, beroende på om User Account Control är aktiverat, dyka upp en prompt om ändringar på datorn.



1. Efter installationen genomförts klicka på Finish för att avsluta installationen.



6.. För att förenkla installationen av MSI-paketet kan er interna IT-avdelning installera paketet genom at distribuera en installation av ADU efter de rutiner som bäst passar er organisation. Det går att köra en “tyst” installation av paket med följande parametrar:

msiexec /qn /i antura-projects-document-utilities.msi

Uppgradera version

För att uppgradera ADU behöver en ladda ner det nya MSI-paketet och installera det för alla klienter som ska uppgraderas.

Versionen på det nerladdade MSI-paket kommer alltid vara kompatibelt med samma version av Antura.

Om en ny version av Antura släpps kan en behöva uppgradera version av ADU.

Appendix B: Vanliga frågor

Måste alla klienter (användare) ha ADU installerat på sin dator?

Nej, men de som vill dra nytta av fördelarna med ADU behöver ha det installerat.

Kan vi installera MSI-paketet i god tid innan en Antura-administratör aktiverar ADU i vår miljö?

Ja.

Kostar ADU något extra?

Nej, ADU är en del av Antura och kostar inget extra.

Om jag uppgraderar version av Antura, behöver jag uppdatera version av ADU?

Nej. Om vi inte uttryckligen meddelar att en uppgradering krävs är äldre ADU-versioner kompatibla med nyare Antura-instanser.

Hur installerar jag ADU om jag inte är administratör på min dator?

Du behöver vända dig till din lokala IT-support som kan installera detta på din dator.