ANTURA

# Antura Teknisk Dokumentation

Antura AB, www.antura.se

2608 (Augusti 2026)

# Systemkrav för Antura

## Operativssystem

- Microsoft Windows 10
- Microsoft Windows 11
- Mac OS X 11 eller senare version

## Webbläsare

- Edge (senaste versionen)
- Firefox (senaste versionen)
- Chrome (senaste versionen)
- Safari (senaste versionen)

## Rapporter

### PDF-Rapporter

Ett PDF-kompatibelt program krävs för att öppna Antura PDF-rapporter (t.ex. Acrobat Reader).

### Excel-rapporter

Microsoft Excel behövs för att öppna Antura Excel-rapporter.

# Systemkrav för Antura Mobile Web

## Operativsystem

- iOS
- Android

## Webbläsare

- Safari (senaste versionen)
- Google Chrome Mobile (senaste versionen)
- Samsung Internet Browser (senaste versionen)

# Antura Document Utilities

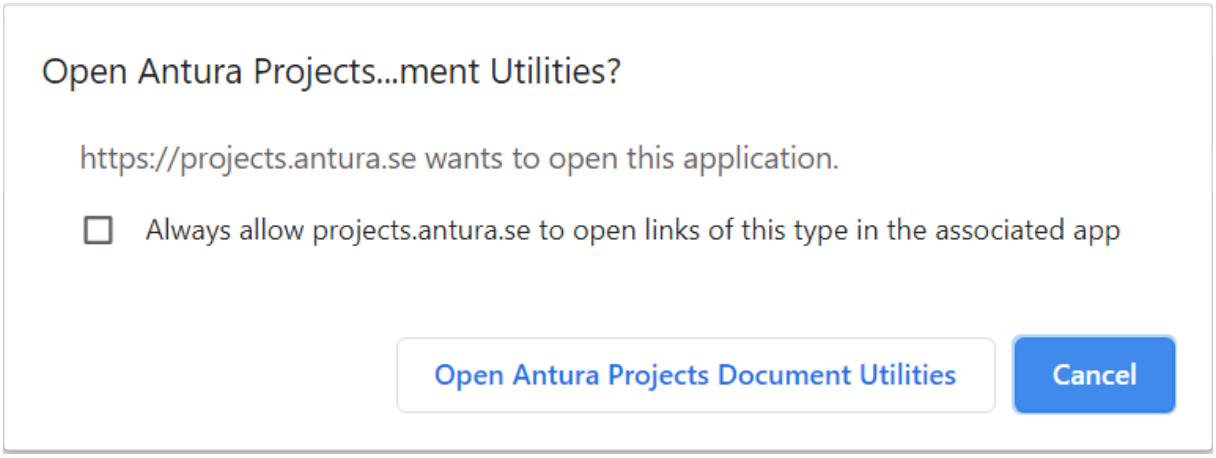
## Introduktion

*Antura Document Utilitites (ADU)* gör det möjligt att enkelt arbeta med dokument i Antura filarkiv. ADU består av applikationen *SaveToServer* som förenklar processen att ladda ner ett dokument, öppna det i ett associerat program och slutligen ladda upp resultatet efter att det associerade programmet har stängts ner.

## Eget URL-protokoll

Antura Document Utilities registrerar ett eget URL-protokoll: "savetoserver:"

Detta berättar för webbläsaren att den kan öppna Antura Document Utilities från filarkivet. Webbläsare kommer inte att öppna länken utan att visa en varning först. Detta exempel är från Google Chrome:




## Windows-installationsprogram (MSI)

Antura Document Utilities levereras som ett Windows-installationsprogram, också känt som en MSI. Det kan installeras tyst så att det kan deployas till en hel organisation centralt.

## Tillgång till Antura Document API

Den lokala applikationen *SaveToServer* använder Antura-instansen via en kryptografiskt säkert 768-bitars tidsbegränsad nyckel som ger tillgång till Antura Document API.

# Begränsad till en temporär katalog

Av säkerhetsskäl så kan bara Antura Document Utilities skriva och läsa till/från en temporär katalog som tas bort efter att programmet är klart.

# Filtyper som kan öppnas

När en associerad applikation startas för att redigera ett dokument så öppnas filen av operativsystemet. Av säkerhetsskäl öppnar SaveToServer bara följande filtyper:

doc, docm, docx, dwg, ifc, pdf, ppt, pptx, txt, vdx, vsd, vsdm, vsdx, vsw, xls, xlsm, xlsx.

# Säkerhet

Koden för Antura Document Utilities har utvecklats av Antura med samma säkra rutiner som används för att fram Antura web-applikation och följer vår ISO27001-certifierade process. Processen inkluderar kodgranskning, säkerhetsanalys och penetrationstestning.

# Autentisering

Det finns flera sätt att autentisera mot Antura som passar olika typer av IT-miljöer. För mer detaljer se separat dokument *Antura – Autentisering och provisionering*.

## Formulärsinloggning

Användare presenteras med en inloggningsruta där de skriver in sina användarnamn med tillhörande lösenord och blir då insläppta i systemet.

### Hantering av lösenord

Inga lösenord lagras i klartext i databasen av säkerhetsskäl. Uppslag använder ett saltat hash.

## Active Directory

Om den inbyggda kopplingen mot *Active Directory* (AD nedan) används, loggas behöriga användare automatiskt in i systemet utan att behöva använda en inloggningsruta. Slutanvändarna kommer alltså att ha tillgång till Antura utan att behöva ange sitt användarnamn och lösenord. AD ger också möjlighet att styra användarnas behörigheter i systemet. Detta kan sedan kombineras med behörighetsadministrationen som finns i Antura.

*Inga lösenord lagras i Antura när autentiseringen sker med Microsoft Active Directory.*

## Tjänstautentisering

Tjänstautentisering kan användas i de fall där det finns en egen, anpassad autentiseringstjänst på företaget. Antura kan kopplas mot den anpassade tjänsten och på så sätt använda den *Single Sign On*-lösning (SSO) som redan finns på företaget.

*Inga lösenord lagras i Antura när autentiseringen sker med kundens egna system.*

# Mixed Mode

Med mixed mode-autentisering kan ovan metoder kombineras. Exempelvis kan systemet konfigureras så att interna användare automatiskt loggas in via AD medan externa användare presenteras med en inloggningsruta.

# Integrationer

Se separat dokument *Antura – Integrera med Antura*.

# Applikationssäkerhet

## Loggning

Antura har flera olika loggar för att spara och följa upp olika typer av fel, intrångsförsök, förändringar och andra typer av viktiga händelser som sker i systemet. Det finns även fler typer av loggar som inte är en del av Antura, såsom t ex Windows Server Event Logs, IIS Site Logs och HAProxy Logs.

Att läsa loggarna Audit log, Exception Log och Access Log kräver att man har åtkomst till databasen. För loggar som sparas till fil krävs att man har åtkomst till servern. Anturas Supportpersonal kan för de kunder som Antura har driftansvaret för, hjälpa till med felsökning i loggarna om man tex misstänker intrångsförsök.

Nedan följer en genomgång av Antura loggar och syftet med respektive logg.

### Audit Log

Antura Audit Log sparas i databasen. Audit Log kan inte förändras från applikationen, utan endast utökas med mer information.

Det primära syftet med Audit Log är att hitta vilken användare som skapat/tagit bort/förändrat något i systemet. Ett exempel är när en användare fått behörighet i systemet och någon i efterhand vill ta fram vem som gett behörigheten och när det skedde.

Audit Log sparar följande information:

- **VEM** som utfört handlingen
- Vad det är för **TYP** av handling
- Vad handlingen **PÅVERKAR** (t ex vilket projekt, användare, fil, grupp, ärende)
- **RELATERAD INFORMATION** (t ex IP-nummer)
- **TIDPUNKT** för handlingen (datum + tid)

Hur länge informationen ska sparas är konfigurerbart, som standard sparas informationen i 2 år.

# Access Log

Antura Access Log sparas i databasen. Access Log kan inte heller förändras från applikationen, utan endast utökas med mer information.

Det primära syftet med Access Log är att registrera otillåtna försök att logga in eller hämta/förändra data som användaren inte har behörighet att göra. Exempelvis loggas misslyckade inloggningsförsök eller om en användare försöker navigera till en sida/ett objekt som den inte har behörighet till.

Access Log sparar följande information:

- **VEM** som utfört försöket (både användar-ID samt IP-adress)
- **VARFÖR** försöket nekades (t ex felaktigt användarnamn/lösenord, behörighet saknas)
- Vad som försökte **PÅVERKAS** (t ex vilket projekt, användare, fil, grupp, ärende)
- **RELATERAD INFORMATION** (t ex IP-nummer)
- **TIDPUNKT** för försöket (datum + tid)
- **VAR** i applikationen försöket gjordes

Hur länge informationen ska sparas är konfigurerbart, som standard sparas informationen i 2 år.

# Exception Log

Antura loggar även alla oväntade fel som uppstår. Felen loggas automatiskt i databasen, även om de sker i bakgrunden av t ex automatiska jobb.

I det fallet att felet påverkar användaren så har denne möjlighet att skicka in ett meddelande till Anturas support med hjälp av en inbyggd funktion i produkten.

Antura samlar in alla registrerade fel och använder det som underlag för felkorrigeringar och förbättringar av applikationen. Loggen kan också hämtas från databasen per miljö om så behövs.

Exception Log sparar följande information:

- **VEM** som fått felet
- **VAR** i applikationen felet uppstod
- Eventuell **BESKRIVNING** från användaren
- **RELATERAD INFORMATION** (t ex typ av fel, meddelande, stack trace, applikationsversion)
- **TIDPUNKT** för felet (datum + tid)

## Application Log

Antura Application Log är applikationens huvudlogg. Huvudsyftet är att kunna spåra flödet i applikationen genom att logga händelser och aktiviteter. Informationen sparas till fil på servern under sökvägen *<serverPathToSite>\Logs*. Hur länge informationen ska sparas är konfigurerbart, som standard sparas informationen i 14 dagar.

Antura stödjer följande logg-destinationer via SeriLog:

- Console
- File
- GrayLog

## Integration Log

Antura Integration Log är separata loggfiler som produceras av eventuella integrationer som är installerade på siten. Informationen sparas till fil på servern på samma katalog som Application Log.

# Statistik

Alla Antura-installationer samlar generell och aggregerad information om miljön. Informationen innehåller ingen känslig information eller data skapad av kunden. Statistiken innefattar t ex hur många användare som är registrerade, hur många projekt som skapats, webbadress och databasstorlek. Statistiken skickas regelbundet till Antura och används för att följa upp användningen och arbeta proaktivt med t ex utökning av serverkapacitet, förvaltning och felhantering.

# Lösenord till externa system

Ibland kräver Antura åtkomst till externa system som kräver autentisering med hjälp av användarnamn och lösenord. För att kunna upprätta kontakt med externa system när som helst måste dessa lösenord lagras säkert i Antura databas. Hårda krav ställs på säkerheten då dessa lösenord måste både kunna krypteras och avkrypteras vid behov. Lösenorden ska dessutom endast kunna avkrypteras av den instans av Antura som krypterade dem.

För denna typ av lagring använder sig Antura av en erkänd lösning från Microsoft i form av Data Protection API (DPAPI), vilket är en del av Windows. DPAPI använder AES-256 för kryptering och SHA-512 för hashning.

Lagring av krypterade lösenord används idag i följande delar av Antura:

- Lösenord till användarprofiler till SharePoint Online när tilläggsprodukten “Antura for SharePoint” är installerad.
- Lösenord till Active Directory-konto som används för att synkronisera användare mot ett lokalt AD när AD-integrationen är aktiverad. Lösenord sparas per grupp under Administration – Grupper.

# Säkerhetspolicy

Informationssäkerhet i Antura efterföljs enligt bifogad säkerhetspolicy.

Se separata dokument *Antura – Informationssäkerhetspolicy* och *Informationssäkerhet på Antura*.