

pGina manual



<http://pgina.xpasystems.com>

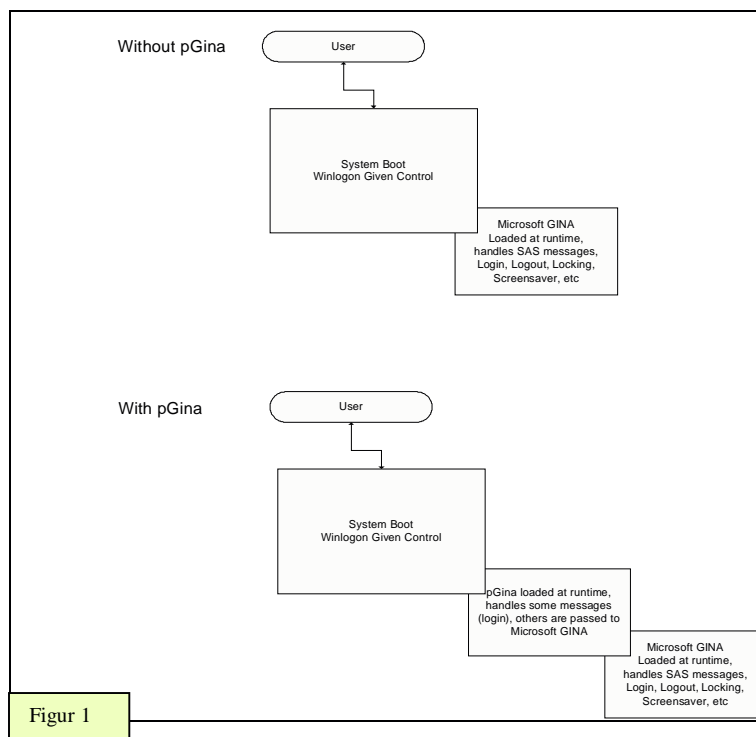


<http://www.xpasystems.com>

Introduktion

pGina er, kort fortalt, en erstatning for domæne autentifikationen i et Windows miljø. Ved hjælp af plug-in teknologi tilbyder pGina en administrator at vælge mellem et antal forskellige autentifikationskilder og metoder. Skulle en administrator have lyst til at implementere en speciel autentifikations metode eller udvide en eksisterende metode har vedkommende også muligheden for at lave egne plug-ins vha. den medfølgende kildekode og pGinas plug-in API.

pGina virker ved at indsætte sig selv i Windows operativ systemet som et GINA (Graphical Identification and Authentication) modul, deraf navnet. Når et Windows system, uden pGina, begynder at boote starter en proces kaldet Winlogon en Microsoft GINA, denne er ansvarlig for at håndtere systembegivenheder som f.eks. CTRL+ALT+DEL, pauseskærms aktivering og ”log på” forsøg. Når pGina er installeret, lægger det sig selv mellem Winlogon processen og Microsofts GINA og håndterer de ting der er direkte relateret til dets egen virke (log på, låsning, osv.) og sender transparent andet videre til Microsoft modulet.



Når Winlogon har startet pGina, starter pGina derefter det plug-in som administratoren har valgt. Når en bruger forsøger at logge på, bruger pGina det valgte plug-in til at bestemme om brugeren kan autentificeres eller ej.

Hvis brugeren godkendes af plug-in'et laver pGina en brugerkonto til denne på den lokale maskine, tilføjer det til grupper som angivet af plug-in'et, tilknytter drev, både globalt og specifikt for brugeren. Mange andre ting er mulige, afhængig af konfigurationen og udvidelser.

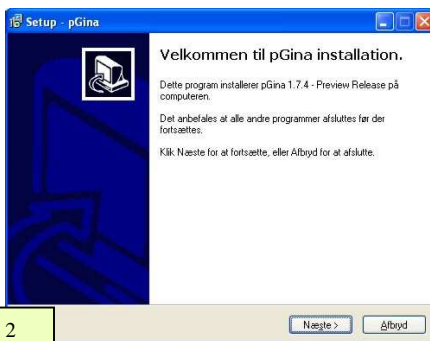
For nøje at forstå hvordan pGina kan hjælpe vil vi undersøge situationen for en generisk administrator kaldet Jørgen. Jørgen er ansvarlig for både et antal Windows 2000 maskiner og et stort antal Linux maskiner. Som det er nu er Jørgen tvunget til at vedligeholde brugernavn og kodeord på både hans Windows og UNIX server, dvs. dobbelte brugernavne og kodeord. Derudover er UNIX serveren også central fil server, så i realiteten er det eneste Windows serveren laver brugerautentifikation. Linuxklienterne bruger LDAP protokollen til autentifikation. Jørgen kan bruge pGina til at autentificere alle hans Windows brugere fra den samme UNIX server ved blot at installere pGina og LDAP plug-in'et. Nu behøver Jørgen kun at administrere brugernavne og kodeord ét sted, der er altså ikke længere brug for Windows serveren.

Dette frigør en stor del af Jørgens tid til andre opgaver og reducerer omkostningerne til Windows servere og de tilhørende klientlicenser.

Installation

Installering af pGina er nogenlunde ligetil og følger mange af de samme rutiner som andre Windows programmer bruger. **OBS: Skulle pGina nogensinde gå ned eller på anden måde blive ustabil vil det forhindre al adgang til systemet. Af denne grund er det vigtigt at vide hvordan man booter til Safe Mode, har en rescue diskette eller på anden måde være bekendt med remote registry redigering.**

Som det første: Du skal downloade den nyeste installer fra <http://pgina.xpasystems.com>. Herefter skal du sikre dig at du er logget på som lokal administrator (eller at du har lokal administrator privilegier), at din maskine IKKE er del af et domæne (medmindre du bruger et plug-in som har domæne interaktion). Kør herefter installeren. Vælg sprog og klik "OK", herefter bliver du præsenteret for et skærbillede som det på Figur 2.



Figur 2

Afslut andre programmer og klik "Næste" for at fortsætte til figur 3.



Figur 3

Dette vindue viser "Gnu Public License" på engelsk. Vær sikker på at du forstår og er indforstået med licensen før du vælger "Jeg accepterer aftalen". Klik derefter "Næste" for at fortsætte til figur 4.



Figur 4

Du får nu muligheden for at vælge hvor du vil installere pGina. Vælg evt. en anden sti eller folder. Klik "Næste" for at fortsætte til figur 5.



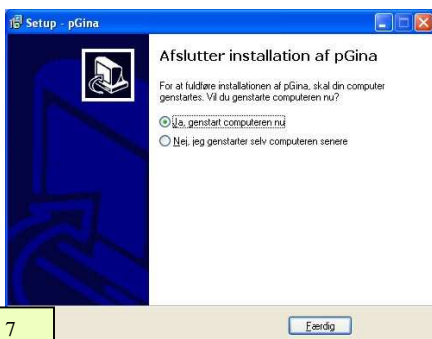
Figur 5

Du kan nu vælge hvor i start menuen pGina menuen skal laves. Klik "Næste" for at fortsætte til figur 6



Figur 6

Dette billede viser dig dine hidtidige valg. Hvis du ikke er tilfreds med dem, brug da "tilbage" knappen for at gå tilbage og ændre dine valg. Ellers vælg "Installer", hvorefter pGina vil blive installeret.



Figur 7

Figur 7 viser det sidste billede i installations processen.

Standard installationen vil fungere uden yderligere konfiguration på de fleste systemer, men det er ikke anbefalet at undlade konfiguration før genstart.

Klik på "Færdig".

Konfigurering af pGina

For at konfigurere pGina, skal du være sikker på at du er logget på som administrator eller har fulde administrator rettigheder. Kør herefter "Configure pGina" fra den start menu som du valgte under installationen. Efter et kort præsentations billede vil et konfigurations vindue fremkomme. Det er via dette vindue at du kan ændre opsætningen af pGina. Nedenfor er de forskellige muligheder beskrevet.

OVERORDNET KONFIGURATION

De oftest benyttede indstillinger er placeret under fanebladet "Generelt". Dette omfatter valg af autentifikations plug-in, hvilke drev der skal tilkobles, samt gruppedlemskab for alle brugere.

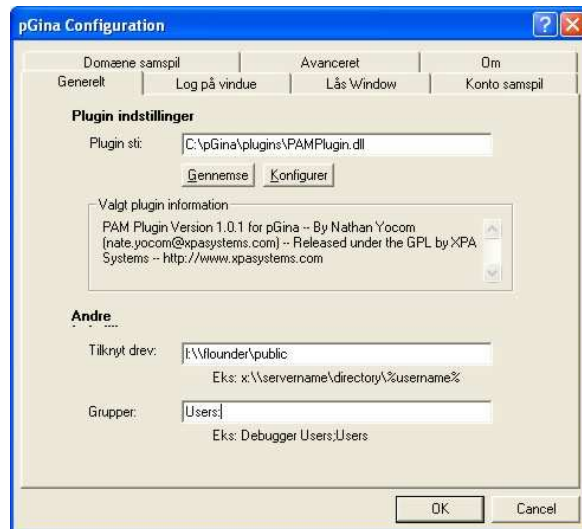
Plugin Indstillinger

For at vælge eller ændre et plugin skal du klikke på "Gennemse" knappen og vælge det plugin du vil benytte. I boksen "Valgt plugin information" kan du læse mere om det plugin du har valgt.

Hvis et plugin tillader yderligere konfiguration vil et klik på "Konfigurer" åbne en dialogboks.

Andre indstillinger

Hvis "Tilknyt drev" er udfyldt vil de angivne drev blive tilknyttet for alle brugere der logger på. Feltet skal udfyldes som DREV:UNC-STI, f.eks. for at tilknytte drev L: til [\\flounder\\public](#) skal der stå L:\\flounder\\public. Flere drev kan angives med et semikolon som adskillelse.



Derudover er det muligt at angive hvilke grupper alle brugere skal tilhøre. Hvis du, for eksempel, ønsker at alle brugere skal tilhøre gruppen "Brugere" skal der stå "Brugere" i feltet. Flere grupper kan angives med et semikolon som adskillelse.

LOG PÅ VINDUE

Ved at klikke på "Log på vindue" fanebladet ser du alle de indstillinger, som påvirker udseende og opførsel af "Log på vinduet".

Du kan bruge "Gennemse"-knappen til vælge dit eget logo.

Når du har valgt et logo vil det blive vist i "Vis special logo" boksen til venstre. Hvis det ikke vises automatisk så tryk på "Opdatér".

Denne viser logoet præcis som det vil se ud på "Log på vinduet".

Standard logoet som er inkluderet med pGina er 100 pixels bredt og 146 pixels højt i 24 bit farver. Kun billeder i bmp-formatet er brugbare.

"Vindue titel" feltet giver dig mulighed for at give "log på" vinduet en anden titel.



”Tekst meddelelse” boksen (MOTD, Message of the day) indeholder den tekst som vil blive vist ovenover brugernavn og adgangskode felterne i ”log på” vinduet. Teksten %machine% vil blive erstattet med maskinens lokale navn, uden DNS suffiks.

Det er ikke muligt at redigere i teksten, såfremt ”Skjul MOTD” er markeret, da teksten ikke vil blive vist alligevel.

Hvis ”Skjul Plugin info” er markeret vil informationen omkring pluginet ikke blive vist nedenunder brugernavn og adgangskode felterne på ”Log på vinduet”

Den 3. knap på ”Log på vinduet” kan konfigureres. Den kan være slået fra, sat til ”Genstart” eller til ”Luk Computer”

LÅS VINDUE

Det vindue som brugeren præsenteres for når han trykker på CTRL+ALT+DEL mens han er logget på kan konfigureres.

Hvis ”Tillad brugere at låse deres skrivebord” ikke er markeret deaktiveres ”Lås” knappen.

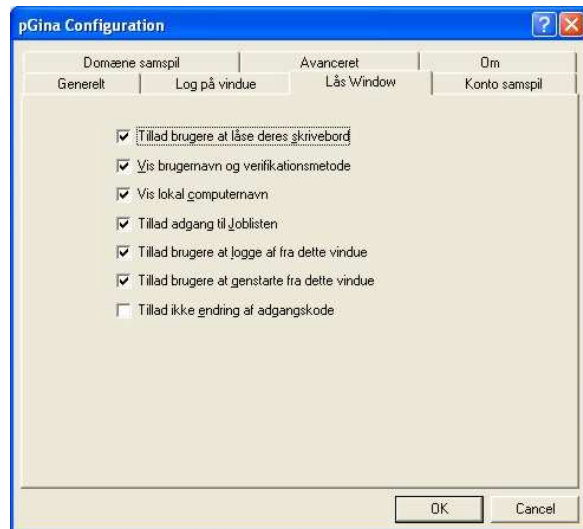
Hvis ”Vis brugernavn og verifikationsmetode” er markeret vil denne information blive vist.

”Vis lokal computernavn” påvirker hvorvidt navnet på computeren vises.

”Tillad adgang til Joblisten” kontrollerer hvorvidt ”Joblisten”-knappen kan vælges. (Dette påvirker ikke andre genveje til Joblisten.)

”Tillad brugere at logge af fra dette vindue” og ”Tillad brugere at genstarte fra dette vindue” påvirker brugernes mulighed for at logge af og genstarte computeren fra ”lås vinduet”.

Hvis ”Tillad ikke ændring af adgangskode” er markeret kan brugere ikke ændre deres adgangskode.



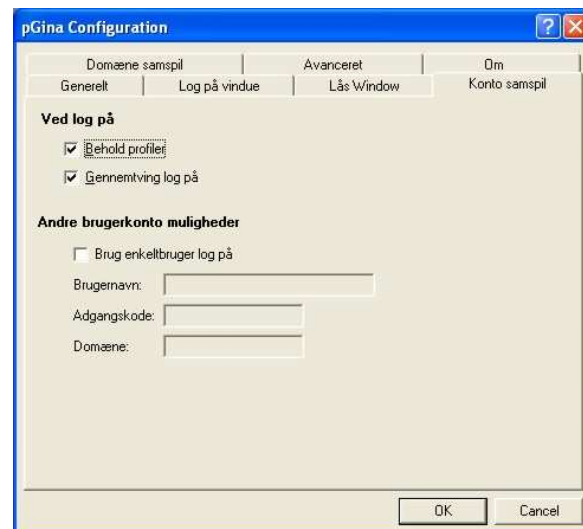
KONTO SAMSPIL

Under normale omstændigheder håndterer pGina log på ved at lave en lokal brugerkonto ud fra de autentificerede informationer fra pluginet. Dette resulterer i at der laves en profil på disken i overensstemmelse med maskin-politik og standard profil-politik i Windows. Indstilling for denne opførsel sker på ”Konto Samspil” fane-bladet.

Når ”Behold profil” er afkrydset bliver brugerkonto og profil ikke fjernet ved log af. Dette medfører at ændringer i profilen beholdes fra gang til gang.

Når ”Behold profil” ikke er afkrydset slettes profiler og lokale brugerkonti ved hvert log af. Dette resulterer i en ny profil ved hvert log på.

Når behold profiler er afkrydset, er det muligt at en brugers adgangskode er ændret andet steds, hvilket



medfører uoverensstemmelse med den lokale konto. Når "Gennemtvung log på" er afkrydset fjernes dette problem ved at den lokale adgangskode sættes til den der blev verificeret af pluginet ved log på.

"Brug enkeltbruger log på" giver mulighed for at benytte pGina med tilhørende plugins til at verificere om en bruger har adgang til en maskine, og derefter benytte det angivne brugernavn og den angivne adgangskode samt evt. angivne domæne, til at logge på maskinen. Man kan således give brugere, der er autentificerede ved hjælp af et plugin, adgang til en brugerkonto uden det er nødvendigt, at de kender brugerkontoens adgangskode.

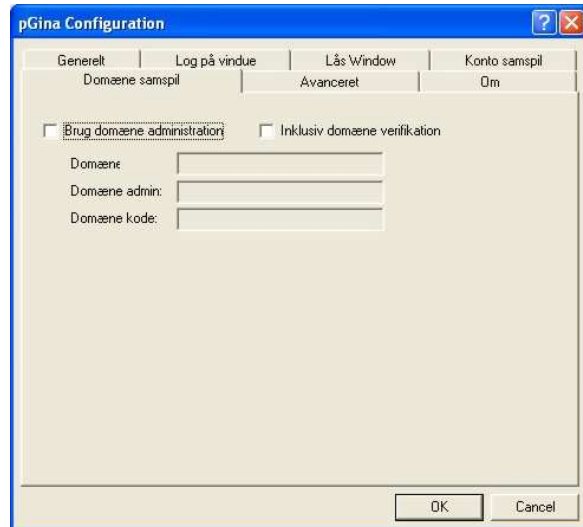
Når "Brug enkeltbruger log på" bliver brugt har "Behold Profil" og "Gennemtvung log på" ingen effekt.

DOMÆNE SAMSPIL

pGina har også muligheden for et mere avanceret samspil med en eksisterende domæne struktur. Selvom det ikke var en del af den oprindelige ide med pGina, er det i nogle tilfælde blevet en meget anvendelig og brugt funktion.

Når "inklusive domæne verifikation" er afkrydset, vil det angivne domæne også blive brugt i autentifikations kæden. Først vil pGina prøve at autentificere brugeren ved hjælp af det valgte plugin, dernæst som en domæne bruger, og til sidst som en lokal bruger.

Når "Brug domæne administration" er afkrydset sender pGina sin brugerkonto administration (se "Konto samspil" ovenfor) videre til det angivne domæne. Dette betyder at brugerkonti vil blive oprettet, slettet og administreret ligesom pGina ville gøre lokalt. Fra version 1.7.4 kræver denne funktion enten en NT4 server eller en Active Directory server der kører i mixed mode (ren AD support er planlagt i senere udgaver). En brugerkonto og adgangskode til en konto med administrator rettigheder er nødvendigt for at pGina kan lave de fornødne ændringer.



AVANCERET

Det sidste konfigurations faneblad er "Avanceret" fanebladet.

Når "Meget Output" er slået til, vil debugging output bliver logget i hændelses loggen, dette kan ses med Windows administrator værktøjet hændelseslogviser.

"Undlad al hændelseslogging" stopper, når den er slået til, al logging til hændelsesloggen.

Hvis "Vis altid plugin fejl" er afkrydset, vises alle plugin fejl, selv hvis brugeren bliver autentificeret som en lokal eller domænebruger. Hvis den er slået fra vises kun fejl hvis autentifikationen fejler totalt.

Som standard tilknytter pGina kun de drev der er angivet i "Generelt" fanebladet under "Tilknyt drev" for brugere som er autentificeret af det valgte plug-in. Når "Tilknyt også drev for administratorer" er valgt bevirker det at også lokale administratorer får drevene tilknyttet.



Når "Undlad pGina funktionalitet" er valgt bevirker det at pGina skjuler sig og lader al kontrol gå videre til Microsofts standard Gina, hvilket i praksis vil give standard Windows Gina funktionalitet.

Sommetider er den ønskede måde at håndtere profiler på, at bruge "Behold profiler" i "Konto samspil". Men profilen bliver gemt med den adgangskode som benyttes på det aktuelle tidspunkt. Hvis netværksforbindelsen tabes, eller plugin'et fejler ved autentifikationen og det lokale brugernavn og adgangskode bruges gives der adgang. "Scramble adgangskode ved log af" tillader at man beholder lokale konti uden også automatisk at give lokal adgang. Dette gøres ved at sætte adgangskoden til en tilfældig værd ved log af. Det er meget vigtigt at denne indstilling kun er sat når "Gennemtvung log på" også er sat. Hvis dette undlades vil det medføre at man ikke kan få adgang til den lokale konto. Dette er tilsigtet.

Visse protokoller, f.eks. LDAP, ignorerer automatisk foranstillede mellemrum. Når "Tillad mellemrum i brugernavn" *ikke* er valgt, vil pGina ikke forsøge at autentificere brugernavne med mellemrum i.

Andre referencer

Microsoft Support Artikel om "Setting up a custom default user profile":

<http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q305709>

Anden pGina dokumentation

<http://pgina.xpasystems.com>

Online diskussionsfora

<http://forums.xpasystems.com/>

Professionel konsultation, implementering og support.

<http://www.xpasystems.com>

Mailinglister

Generel: <http://lists.sourceforge.net/mailman/listinfo/pgina-general>

Opdateringer: <http://lists.sourceforge.net/mailman/listinfo/pgina-updates>

Udviklere: <http://lists.sourceforge.net/mailman/listinfo/pgina-devel>

Anden GINA Dokumentation

http://msdn.microsoft.com/library/en-us/security/security/winlogon_and_gina_start_page.asp