pGina Handbuch

http://pgina.xpasystems.com

http://www.xpasystems.com

Einleitung

pGina ist - einfach gesagt - ein Ersatz für die Domänen Anmeldung in einer Windows Umgebung. pGina erlaubt, durch den Einsatz von Plugin Technik, einem Administrator aus einer Vielzahl von existierenden Anmeldungsarten und -methoden auszuwählen. Wünscht sich ein Administrator zum Beispiel eine individuelle Authentifizierungsmethode zu implementieren, oder eine bestehende zu erweitern, kann er ein eigenes Plugin erstellen. Dazu steht ihm ein fertiger Beispielcode und eine pGina Plugin API zur Verfügung.

Um diese Funktion zu erfüllen, fügt sich pGina in das Windows Betriebssystem als GINA Modul (Grafische Identifikation und Authentifizierung) ein, daher auch der Name. Ohne pGina, lädt ein Windows System beim Start einen Prozess namens Winlogon, der wiederum die Microsoft GINA lädt. Diese ist verantwortlich für Systemereignisse wie das Drücken von STRG+ALT+ENTF, den Bildschirmschoner, Anmeldeversuche und ähnliches. Wenn pGina installiert ist, fügt es sich zwischen den Winlogon Prozess und die Microsoft GINA. Dann übernimmt pGina alles, was mit seiner direkten Funktion zusammenhängt (Logon, Sperren, etc.), übergibt aber alles andere transparent zu den Microsoft Modulen.

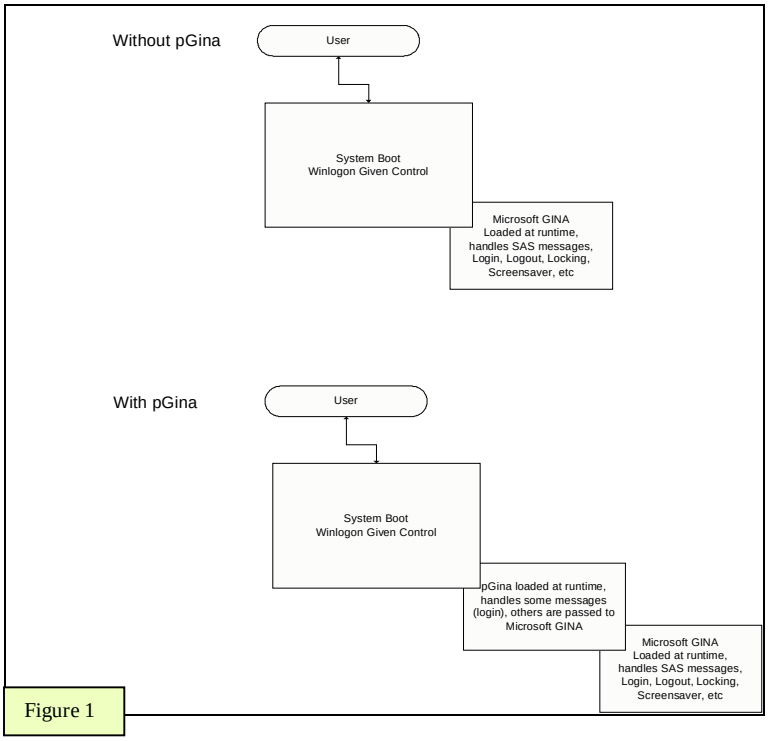


Figure 1

Nachdem Winlogon pGina gestartet hat, lädt pGina das Plugin, das vom Administrator zuvor ausgewählt wurde. Wenn sich ein Benutzer anmelden möchte, benutzt pGina das ausgewählte Plugin um zu entscheiden ob der Benutzer authentifiziert werden darf, oder nicht. Erlaubt das Plugin dem Benutzer sich anzumelden, erstellt pGina ein Benutzerkonto auf dem lokalen Computer und fügt ihn in die – vom Administrator vorher festgelegten – Gruppen ein, bindet allgemeine und Benutzer-Netzlaufwerke ein und viele andere Dinge, abhängig von der Konfiguration und dem jeweilig angepassten Plugin.

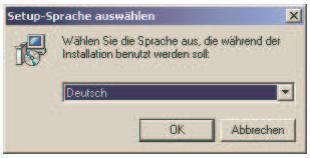
Um genau zu verstehen wie pGina Ihnen helfen kann, Ihr spezifisches Problem zu lösen, lassen Sie uns schauen wie sich die Situation für den Administrator Hans darstellt. Hans ist verantwortlich für eine Umgebung mit 2000 Windows Computern und einer größeren Anzahl von Linux Computern. Im Moment muss Hans Benutzernamen und Passwörter in beiden Umgebungen pflegen. Darüber hinaus ist der zentrale Dateiserver ein UNIX Server, so dass die Windows Server nur die Benutzeranmeldung durchführen. Im Moment melden sich die Linux Clients über das LDAP Protokoll an. Hans kann nun pGina benutzen, um alle seine Windows Benutzer von demselben UNIX Server authentifizieren zu lassen, indem er einfach pGina installiert, und dann das LDAP Plugin. Nun muss Hans nur einen Namen und ein Passwort pro

Benutzer pflegen und braucht die Windows Server nicht mehr. Das spart ihm einen Menge Zeit, die er nun für andere Dinge nutzen kann, und reduziert die Kosten, denn die Windows Server und die Clientlizenzen werden nun nicht mehr benötigt.

Installation

Die Installation von pGina ist denkbar einfach und folgt demselben System, das alle anderen Windows Installationsprogramme nutzen. ***Aber bitte beachten Sie: Sollte pGina abstürzen, oder sonst irgendwie unbenutzbar werden, haben Sie keine Möglichkeit mehr sich am System anzumelden. Aus diesem Grund ist es wichtig zu wissen, wie Sie im „Safe Mode" starten, sich eine passende Notfalldiskette erstellen oder die Registrierungseinstellungen von außen ändern können.***

Aber erst einmal Schritt für Schritt: als erstes müssen Sie sich das Installationsprogramm von der Webseite http://pgina.xpasystems.com herunterladen. Nach dem Herunterladen stellen Sie sicher, dass Sie als Administrator (oder mit administrativen Rechten) angemeldet sind, Ihr Computer nicht in einer Domäne ist (ausgenommen Sie benutzen ein Plugin, das dieses erlaubt bzw. nutzen die Domänenfunktionalität von pGina) und starten das Installationsprogramm.



Zuerst wählen Sie die Sprache aus, die während der Installation benutzt wird. Die Voreinstellung wird von der Sprachversion Ihres Betriebssystems übernommen.

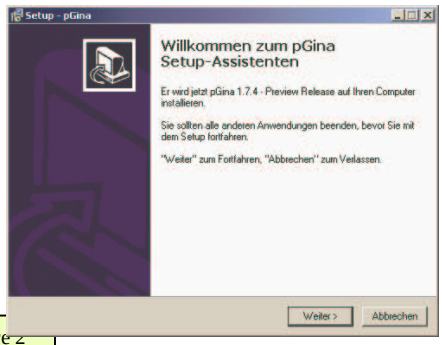


Figure 2

Wenn Sie pGina installieren wollen, klicken Sie auf „Weiter", um zu Bild 3 zu kommen.

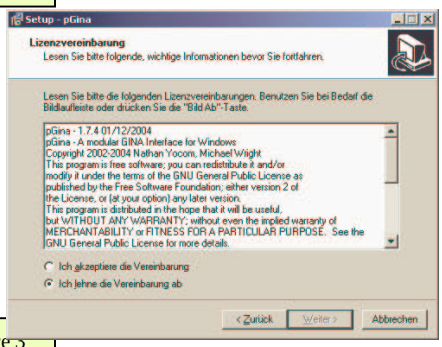
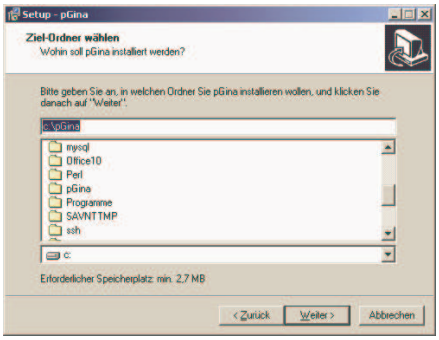


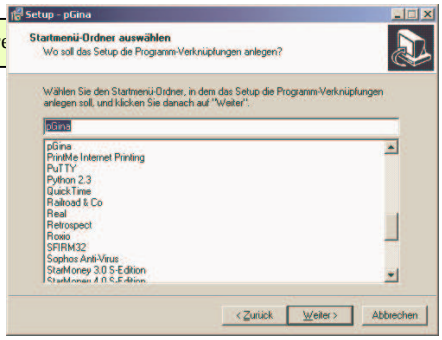
Figure 3

Dieser Dialog zeigt eine Kopie der „Gnu Public License". Wenn Sie dem zustimmen, wählen Sie „Ich aktzeptiere die Vereinbarung" und klicken dann „Weiter" um zu Bild 4 zu kommen.



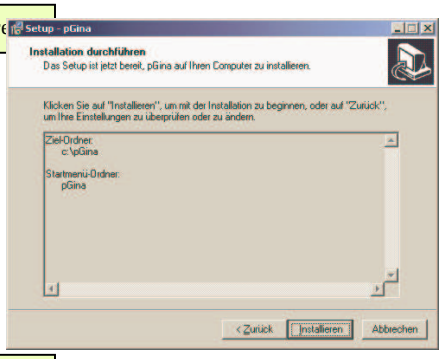
Nun können Sie auswählen wohin Sie pGina und die nötigen Dateien installieren wollen. Wählen Sie den vorgegebenen Pfad oder wählen Sie einen anderen aus, und klicken Sie „Weiter", um zu Bild 5 zu kommen.
(Wir gehen ab hier davon aus, dass Sie die Standardpfade und Einstellungen gewählt haben.)

Figure



Hier wählen Sie aus, in welchem Ordner im Startmenü die Verknüpfungen zu pGina erstellt werden sollen. Nach der Auswahl klicken Sie auf „Weiter", um zu Bild 6 zu kommen.

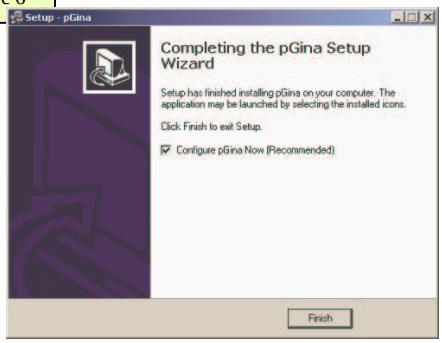
Figure



Dieser Dialog fasst Ihre vorherigen Einstellungen zusammen. Benutzen Sie die „Back" Schaltfläche, um zurück zu gehen, um Änderungen vornehmen zu können. Nachdem Sie „Installieren" angeklickt haben, werden die notwendigen Dateien entpackt und auf Ihrem System im gewünschten Pfad installiert.

Normalerweise sollten Sie pGina ohne Neustart benutzen können. Trotzdem ist es nicht empfehlenswert, ohne Neustart weiterzumachen. Bild 7 zeigt dann den letzen Dialog des Installationsprozesses.

Figure 6



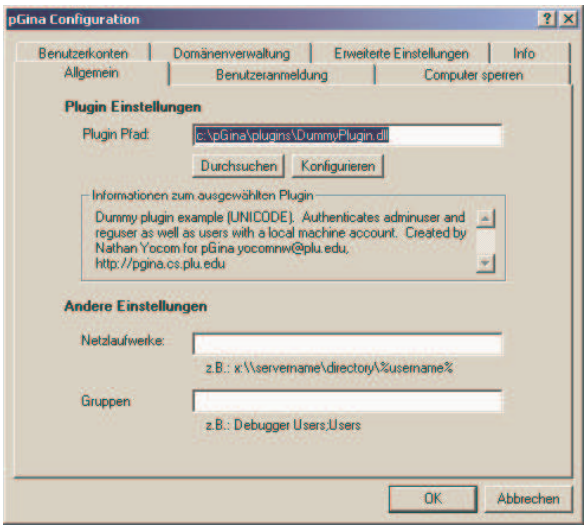
Um die Konfiguration zu überspringen, deaktivieren Sie auf das „Configure pGina Now" Kästchen und wählen „Finish". Ansonsten wählen Sie „Finish", um das Installationsprogramm zu beenden und das Konfigurationswerkzeug zu starten.

Figure 7

Konfiguration von pGina

Um pGina konfigurieren zu können, stellen Sie sicher, dass Sie als Administrator oder mit administrativen Rechten angemeldet sind. Starten Sie dann das pGina Konfigurationsprogramm, indem Sie auf Start → Programme → pGina → Configure pGina klicken. Nachdem kurz ein Startbild angezeigt wird, kommt ein Konfigurationsdialog, der so ähnlich aussieht wie in Bild 8 gezeigt. In diesem Dialog können Sie Einstellungen ändern und Optionen auswählen, die das Verhalten von pGina ändern. Lassen Sie uns mal sehen, welche Effekte die individuellen Optionen von pGina haben:

ALLGEMEINE KONFIGURATION



Die am häufigsten benutzten Einstellungen sind im Reiter „Allgemein“ enthalten. Diese sind das Plugin, das pGina für die Authentifizierung benutzten soll, Netzlaufwerke und Gruppen-mitgliedschaften, die für alle Benutzer gelten sollen.

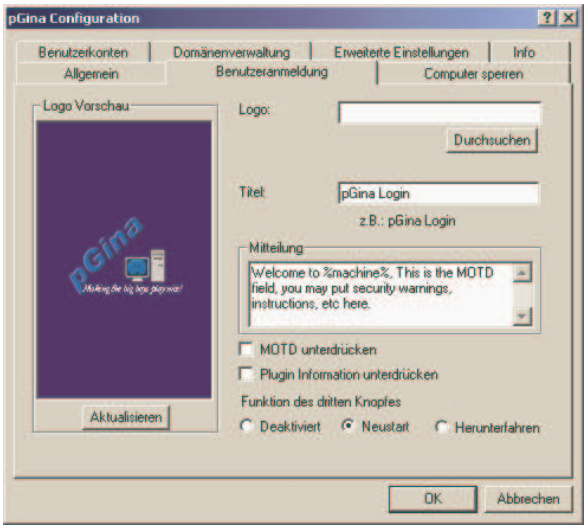
Plugin Einstellungen
Um ein Plugin auszuwählen oder zu ändern klicken auf die Schaltfläche „Durchsuchen“ und wählen das gewünschte Plugin aus. Im darunter befindlichen Fenster werden Informationen zum ausgewählten Plugin angezeigt. Wenn für das ausgewählte Plugin über weitere Einstellungen vorgenommen werden können, können Sie es konfigurieren, indem Sie auf die „Konfigurieren” Schaltfläche klicken.

Andere Einstellungen
Hier können Sie festlegen, welche Netzwerklaufwerke und Freigaben Sie bei erfolgreichem Anmelden zuordnen wollen. Wenn Sie möchten, dass alle Benutzer, die sich anmelden, die Freigabe `\\einserver\freigabe` als Laufwerk `X:` zugeordnet bekommen sollen, dann müssen Sie hier `X:\\einserver\freigabe` eintragen. Trennen Sie mehrere Laufwerkszuordnungen mit einem Semikolon. Sie können pGina auch den Benutzernamen benutzen lassen, indem Sie die Variable `%username%` in den Eintrag einfügen. Wenn Sie also wollen, dass das Laufwerk X: der Freigabe `\\einserver\freigabe` für alle Benutzer zugeordnet wird, aber außerdem wollen, dass das Laufwerk Y: dem Benutzerlaufwerk auf einem Samba Server `\\sambaserver\` des jeweiligen Benutzers zugeordnet wird, tragen Sie in die *„Drive Maps“* Option `X:\\einserver\freigabe;Y:\\sambaserver\%username%` ein.

Weiterhin kann angegeben werden, zu welchen Gruppen ein Benutzer, der gegebenenfalls von pGina erstellt wird, beim Login hinzugefügt wird. Sie sollten die Gruppen in der Reihenfolge angeben, in der sie pGina eintragen soll. Trennen Sie mehrere unterschiedliche Gruppen durch ein Semikolon. Beispiel: „`Test Benutzer;Benutzer`“. Beachten Sie, dass die Gruppen, die Sie angeben, auf dem System existieren müssen – pGina erstellt Gruppen die nicht existieren NICHT.

Also available on the General tab is the Drive Maps option. If set, any and all indicated drives will be mapped for all users who successfully log in. Drives are specified as DRIVE:UNC-PATH, for instance: to map drive J to \\jack\nate\working this is set to J:\\jack\nate\working. Multiple drives can be specified by separating entries with a semicolon.

"BENUTZERANMELDUNG" KONFIGURIEREN



Wenn Sie auf den Reiter Benutzeranmeldung klicken, erhalten Sie Zugriff auf alle Einstellungen des Anmeldefensters.

Sie können die Schaltfäche Durchsuchen nutzen, um ein eigenes *Logo* im Anmeldefenster zu verwenden. Wenn Sie ein gültiges Bild ausgewählt haben, wird es in der Vorschau im linken Teil angezeigt. Zum Vergleich: das Standard-Logo von pGina ist 100 Pixel breit, 146 Pixel hoch und hat eine Auflösung von 300x300 Punkten bei einer Farbtiefe von 24 Bit. Es können nur Bitmaps verwendet werden.

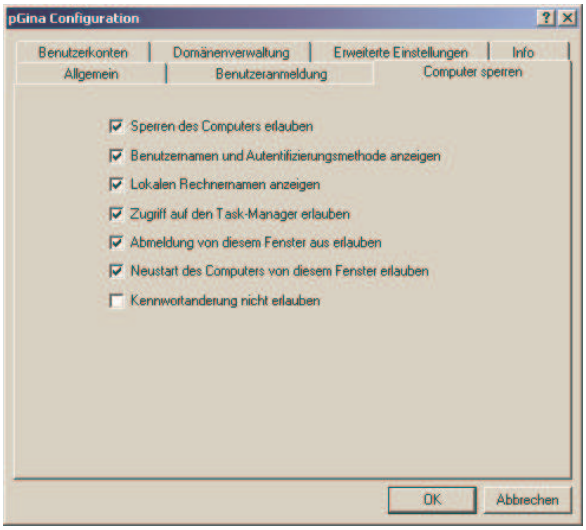
Mit der Einstellung *Titel* können Sie einen beliebigen Titeltext für das Anmeldefenster festlegen.

Die *Mitteilung* (Message of the day) wird oberhalb des Benutzernamens im Anmeldefenster angezeigt. Der Text %machine% wird zur Laufzeit durch den Namen des Computers (ohne DNS Suffix) ausgetauscht. Wenn Sie die MOTD unterdrücken wollen, wählen Sie die Option aus.

Wenn die Option *Plugin Information unterdrücken* ausgewählt ist, zeigt der Login Dialog die Plugin Information nicht an. Wenn deaktiviert (Standard), wird der Text angezeigt.

Schließlich kann die *Funktion des dritten Knopfes* des Login Dialoges festgelegt werden. Ist hier „Neustart" ausgewählt, wird die dritte Schaltfläche mit „Neustart" beschriftet, und der Computer wird neu gestartet, wenn sie angeklickt wird. Alternativ kann man hier „Herunterfahren" wählen, dann zeigt die dritte Schaltfläche „Herunterfahren", und der Computer wird heruntergefahren, wenn sie angeklickt wird. Als dritte Option kann man hier „Deaktiviert" auswählen, dann wird die Schaltfläche deaktiviert, und man kann sie nicht anklicken.

"COMPUTER SPERREN" KONFIGURIEREN



Das Fenster, das angezeigt wird, wenn der Benutzer CTRL+ALT+DEL drückt ist auch konfigurierbar.

Sie können es dem Benutzer erlauben, den Computer zu sperren (*Sperren des Computers erlauben*).

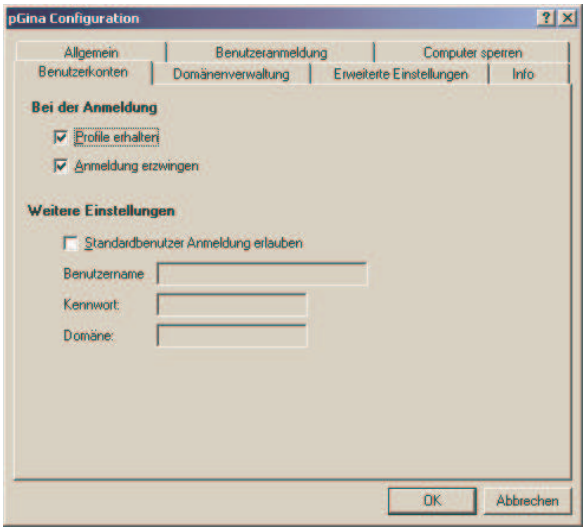
Mit der zweiten Option wird ausgewählt, ob die Art der Authentifikation, Benutzername und Paßwort in diesem Fenster angezeigt werden (*Benutzernamen und Authentifizierungsmethode anzeigen*).

Mit der dritten Option wählen Sie aus, ob der Name des Computers in diesem Fenster angezeigt wird (*lokalen Rechnernamen anzeigen*).

Mit der vierten Einstellung können Sie den Zugriff auf den Task-Manager kontrollieren. (Das beeinflußt keine anderen Zugriffsarten wie z.B. CTRL+SHIFT+ESC).

Die letzten drei Optionen beeinflussen die Möglichkeit des Benutzers sich von diesem Fenster aus abzumelden, den Rechner neu zu starten und das Kennwort zu ändern.

"BENUTZERKONTEN" KONFIGURIEREN



Normalerweise werden nach dem Login lokale Konten entsprechend der Authentifizierung durch das Plugin angelegt. Dadurch wird auf der Festplatte ein Profil erzeugt (entsprechend der machine policy und den Profil-Einstellungen von Windows). Dieses Verhalten kann mit den Einstellungen im Reiter „Benutzerkonten" beeinflusst werden.

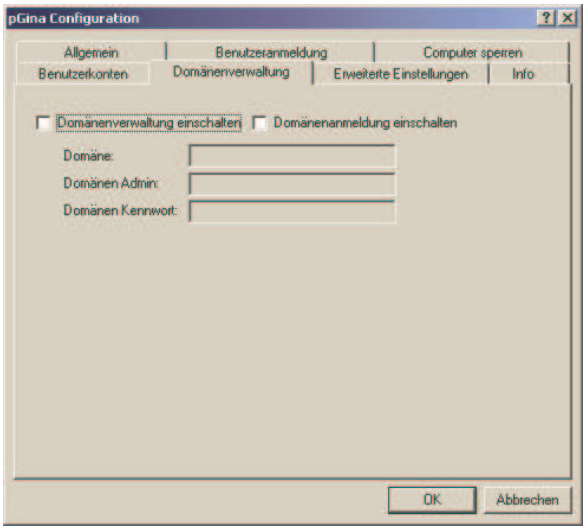
Wenn ein Benutzer von einem pGina Plugin authentifiziert wird, erstellt pGina normalerweise ein lokales Konto mit dem Benutzernamen und dem Passwort des Benutzers und meldet ihn damit beim Windows System an. Dabei benutzt pGina eine Kopie des Standard Benutzer (=Default User) Profils. Die Option „Profile erhalten" ermöglicht Ihnen festzulegen, ob dieses Profil beim Abmelden bestehen bleiben, oder gelöscht werden soll. Wenn Sie diese Option auswählen, bleibt das Profil erhalten. Der Benutzer kann seine Desktopumgebung verändern und die Änderungen bleiben erhalten, wenn er sich erneut anmeldet. Wenn Sie diese Option ausschalten wird das Profil beim Abmelden gelöscht und alle Änderungen gehen verloren, was sinnvoll sein kann, wenn Sie ein Standardprofil nutzen wollen.

Die Einstellung *Anmeldung erzwingen* ist eine Ergänzung der Option *Profile erhalten* und zum Problem des unterschiedlichen Passwortes gedacht. Wenn diese Option aktiviert ist, und ein pGina Plugin eine Benutzer authentifiziert hat, wird dieser, egal ob ein lokales Konto besteht oder nicht, unter dem angegebenen Benutzernamen angemeldet. Findet pGina ein lokales Konto mit dem gleichem Benutzernamen, wird das lokale Passwort mit dem überschrieben, das vom Plugin genutzt wurde. Wenn diese Option deaktiviert ist, und ein lokales Konto mit gleichem Benutzernamen gefunden wird, zeigt pGina den Microsoft Anmeldedialog, und der Benutzer kann sein lokales Passwort eingeben. Dies kann sinnvoll sein, wenn man den Benutzern ermöglichen will, lokale Konten zu pflegen, egal wann und wie sie ihr Passwort ändern.

Standardbenutzer Anmeldung ist sinnvoll, wenn Sie die Benutzer über ein Plugin authentifizieren wollen, sie aber lokal über ***ein*** Konto anmelden wollen. Vielleicht ist dieses Konto ein spezielles Domänenkonto mit bestimmten Richtlinien (Policies) oder einer anderen speziellen Anpassung. Wenn sie das Kontrollkästchen aktivieren, können Sie einen Benutzernamen und ein Passwort eingeben, mit dem pGina die Anmeldung lokal (oder an der Domäne, wenn die Domänenoption aktiviert ist) vornehmen soll, **nachdem die Authentifizierung durch das Plug-In erfolgreich war**. Es ist wichtig zu wissen, dass ein Authentifizierungsfehler des Plugins immer einen Fehler provozieren wird, egal ob die Standardbenutzer Anmeldung aktiviert worden ist, um den Zugriff von nicht authentifizierten Benutzern zu verhindern. Wie auch immer: wenn ein Benutzer den Benutzernamen und das Passwort kennt, das hier eingetragen ist, kann er sich an dem Computer anmelden, so lange nicht das Plugin als erforderlich für die Anmeldung eingestellt ist. Es ist dringend angeraten, die Registrierungsschlüssel, die pGina benutzt (HKLM\Software\pGina) zu schützen, so dass NUR das System- und das Administratorkonto Zugriff darauf haben.

In Verbindung mit dieser Einstellung haben die Optionen *Profile erhalten* und *Anmeldung erzwingen* keine Funktion.

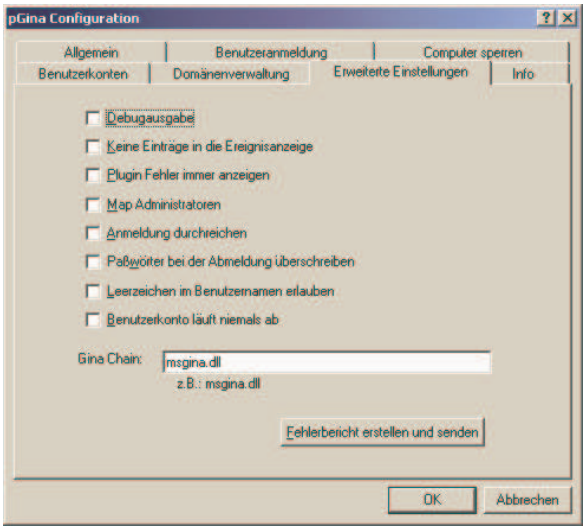
"DOMÄNENVERWALTUNG" KONFIGURIEREN



pGina besitzt verschiedene Möglichkeiten zur Integration in eine vorhandene Domänenstruktur. Wenn die Einstellung *Domänenverwaltung einschalten* ausgewählt ist, wird die Domäne in die Authentifizierung aufgenommen. PGina wird dann zuerst das ausgewählte Plugin verwenden, dann die Domäne und zuletzt den lokalen Computer.

Mit der Einstellung *Domänenanmeldung einschalten* wird die Verwaltung der Benutzerkonten an die Domäne übergeben. Auf diese Weise kann pGina automatisch und transparent Konten auf einem Domänenserver verwalten, während trotzdem noch andere Authentifizierungen durchgeführt werden (über das Plugin). Um das zu ermöglichen, braucht pGina ein Konto, das die Berechtigung hat, Konten in der Domäne zu verwalten. Dafür sind die Felder „Username" und „Password". Beachten Sie, dass bei Anmeldung an einer Windows NT 4.0 Domäne der Servername mit „\\" anfangen muss wie in „\\servername".

ERWEITERTE EINSTELLUNGEN



Der letzte Reiter enthält die "Erweiterten Einstellungen".

Wenn Sie die Option *Debugausgabe* wählen, wird pGina extrem viele Mitteilungen als Fehlerhilfe in die Ereignisanzeige schreiben. Diese Option sollte normalerweise ausgeschaltet bleiben, ansonsten wird die Ereignisanzeige sehr schnell anwachsen. Natürlich ist es sinnvoll, diese Option zu nutzen, wenn Sie Programmfehler suchen oder eine Fehlerquelle ausschließen wollen. Ein solches Protokoll kann evtl. von pGina Entwicklern angefordert werden, wenn Sie einen Fehler oder ein Problem gelöst haben möchten.

Mit der Option *Keine Einträge in die Ereignisanzeige* könne Sie alle normalen Ausgaben in den Ereignisanzeige ausschalten.

Wenn Sie die Option *Plugin Fehler immer anzeigen* auswählen, werden alle Fehler im Plugin angezeigt, auch wenn die Anmeldung anschließend über die Domäne oder einen lokalen Benutzer gelingt. Wenn abgeschaltet, wird nur ein Fehler ausgegeben, wenn die Authentifizierung komplett fehlgeschlagen ist.

Standardmäßig werden Netzlaufwerke (aus dem Reiter „Allgemeine Konfiguration") nur bei Benutzern angewendet, die durch das ausgewählte Plugin authentifiziert wurden. Wenn die Option *Map Administrator* eingeschaltet wird, dann erhalten auch lokale Administratoren die angegebenen Netzlaufwerke.

Wenn dies Option *Anmeldung durchreichen* eingeschaltet ist, wird pGina in keinen Prozess eingreifen und alle Daten direkt an die Microsoft GINA Schnittstelle (oder die angegebene GINA, siehe „Gina Chain") weitergeben. Wenn diese Option nicht eingeschaltet ist, verhält sich pGina wie angegeben. Diese Einstellung mag sinnvoll sein, wenn Sie Fehler suchen oder pGina abschalten wollen, ohne das Programm zu deinstallieren.

Wenn die Option *Paßwörter bei der Abmeldung überschreiben* aktiviert ist, wird das Passwort des lokalen Kontos beim Abmelden mit Zufallszeichen überschrieben. Es ist dringend angeraten, diese Option zusammen mit den „Profile erhalten" und „Anmeldung erzwingen" Optionen zu benutzen. Falls ein Benutzer sein Passwort auf dem Server ändert, kann er die lokalen Ressourcen nicht mit dem alten Passwort benutzen. Das verhindert einen Zugriff auf die lokalen Ressourcen, falls die Authentifizierung des Plugin fehlschlägt.

Einige Protokolle wie z.B. LDAP ignorieren automatisch führende Leerzeichen, wenn die Option *Leerzeichen im Benutzernamen erlauben* nicht ausgewählt ist.

Weiterführende Literatur (auf Englisch)

Microsoft Support Article on "Setting up a custom default user profile":
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q305709

Other pGina Documentation
http://pgina.xpasystems.com

Online Discussion Forums
http://forums.xpasystems.com/

Professional Consultation, Implementation and Support
http://www.xpasystems.com

Mailing Lists:
General: http://lists.sourceforge.net/mailman/listinfo/pgina-general
Updates: http://lists.sourceforge.net/mailman/listinfo/pgina-updates
Developers: http://lists.sourceforge.net/mailman/listinfo/pgina-devel

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