Infor PLM Accelerate 11

Windows Authentication Setup

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

Publication Information

Publication date: May 30, 2018

Contents

About this guide

Infor PLM Accelerate provides the flexibility to allow administrators many options when controlling the maintenance of user logins to Infor PLM Accelerate. This document provides information about the most common deployments using Windows Authentication.

Intended audience

This guide is intended for system administrators. This document assumes that you have at least some knowledge in:

- System architecture and function for your Infor system
- SQL Server database

For the most up-to-date list of software and hardware requirements for Infor products, see the documentation for your system.

Related documents

You can find the documents in the product documentation section of the Infor Xtreme Support portal, as described in the "Contacting Infor" section below.

Contacting Infor

If you have questions about Infor products, go to the Infor Xtreme Support portal at www.infor.com/inforxtreme.

If we update this document after the product release, we will post the new version on this Web site. We recommend that you check this Web site periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1. Overview

Infor PLM Accelerate provides the flexibility to allow administrators many options when controlling the maintenance of user logins to Infor PLM Accelerate.

One method is through the use of logon hooks. These hooks provide a way to implement specialized requirements for single-sign-on, authorization control and auditing. These configurations can include standard Infor PLM Accelerate connections, leverage Web Server authentication, or use client portals for authentication.

This document concentrates on the use of logon hooks for Active Directory authentication, but is not the limit of the possible configurations. Many implementations are possible, but this document should help with one of the most common deployments using Windows Authentication.

Note: Changes outlined in this document should not be made to a production instance of Infor PLM Accelerate while it is running. Plan to implement these features only when users are not connected to the system, in a controlled deployment.

Chapter 2. Infor PLM Accelerate Login Hooks for External Authentication

The Infor PLM Accelerate client logon may be customized through the use of logon hooks described in this section. These hooks provide a way to implement specialized requirements for single-sign-on, authorization control, and auditing for example. The customization is delivered as a Microsoft.NET assembly that must be installed in the Client/bin folder of the Infor PLM Accelerate code tree. In reading this section it helps to keep in mind that this is only one possible implementation of this feature.

The `Aras.LogonHooks.WindowsAuth.dll` and the `Aras.LogonHooks.WindowsAuth.pdb` provide single-sign-on capability with Microsoft Active Directory for most customer requirements. It can be set up without programming knowledge.

Administrative Setup

This section outlines a series of options that the administrator can enable in an Infor PLM Accelerate instance.

Customizing the Client section of the Innovator Server

The /Client web-application portion of Infor PLM Accelerate may have its own private configuration file or it may share the configuration file with the /Server. For more detail on how to deploy distributed /Client folders, see the *Infor PLM Accelerate – Installation Guide*.

If you have a distributed Client setup, then this could have some technical architecture implications for the operation of client logon hooks that pre-fill some of the logon form input elements.

Enabling the Logon hooks

In order to enable the logon hooks, you must first include the `ClientConfig` tag in the `InnovatorServerConfig.xml` configuration file. Found in the root of your install directory, by default.

```
<ClientConfig
  AssemblyName="Aras.LogonHooks.WindowsAuth"
  AssemblyNameType="partial"
  TypeName=" Aras.LogonHooks.WindowsAuth" />
```

The `AssemblyName` and `TypeName` attributes depend on the how the customized library was developed. An example provided by Infor and described in this document is called `Aras.LogonHooks.WinAuth`. Other customizations should be called by other names. These names are arbitrary. For example, `AcmeOrientalRugs.InnovatorClientConfig` would be a reasonable name.

There can be more than one such assembly (dll) provided in the Client/bin folder. However, the type names should be distinct, and only one `ClientConfig` element should be declared in the application configuration file.

Configuring the Logon hooks

After enabling the logon hooks, the keys for these hooks must be configured based on the assembly specified in the `ClientConfig` tag. The standard Infor PLM Accelerate login page uses various parameters/keys for screen customization and user authorization. The assembly defined in the <`ClientConfig`> implements a function that returns key value to the login page when a key parameter is passed to the function. This allows you to customize, for example, authentication process by providing a custom assembly. These keys can vary based on assembly, but in this section we outline how to configure the keys for the "`Aras.Login.WindowsAuth`" assembly used when Microsoft Active Directory single sign-on is desired. This extension is used to leverage the Integrated Windows Authentication and Digest Authentication for Windows Domain Servers, or any other method in the web server which ends up establishing a trusted value of the server variable LOGON_USER in the form DomainName\UserName. In order to use it you must disable anonymous access to the page /Client/Scripts/login.aspx and allow only authenticated access. This method of authentication is diagrammed in the section Client Logon Hooks Authentication Sequence, Web Server Mode.

The ClientLogon attributes

The `ClientLogon` tag is used in the InnovatorServerConfig.xml to configure the various options available through the '`Aras.Login.WindowsAuth`' extension. Below is an example of various options available, as well as the purpose of each one.

```
<ClientLogon  allowed_domain_names="^DOMAINNAMEHERE$"
    allowed_domain_users=".+"
    denied_domain_users="^admin$|^root$|^vadmin$|^pdftron_user$|^esadmin
    $"
    allowed_direct_users="^admin$|^root$|^pdftron_user$|^esadmin$"
    shared_secret="Your shared secret here"
    empty_logon_user_allow_direct="false" />
```

- `allowed_domain_names` – This is a regular expression. The domain portion of the LOGON_USER must match this expression in order to be allowed into Infor PLM Accelerate. If there is a finite list of domains to recognize then it is best to use a fixed list with the or "|" operator, for example, '^europe$|^usa$|^fareast$'. The '^' character in this context means to match at the start of a string, and the '$' character means to match at the end of the string. A string without these, e.g. 'east' would match 'FarEast' and also 'EasterIsland' and any string containing the sequence 'east'. The match is case insensitive.
- `allowed_domain_users` – This is a regular expression. Usually it is best to keep it at '.+' which means to match one or more characters. This expression must match in order for the logon to Infor PLM Accelerate to be allowed. The username portion of the LOGON_USER is matched against this. If it matches then it becomes the login_name used to log onto Infor PLM Accelerate.

- `denied_domain_users` – This is matched against the username if it passes the allowed_domain_users test. If the match is true, then access to Infor PLM Accelerate is denied. This prevents domain users from logging in as Infor PLM Accelerate users with the same username. This option should be set to a list of special purpose Infor PLM Accelerate users. The ‘Innovator Admin’ (username=admin) user for example is often used when batch loading data or managing AML upgrades. The ‘Super User’ (username=root) user must be used when applying database upgrade patches to the Infor PLM Accelerate database. The ‘Vault Admin’ (username=vadmin) user is used only by the vault server in order to access the mime type database. Other denied_domain_users might include the user used by the Infor PLM Accelerate Scheduler Service, or a test user used to review upgrades in functionality.
- `allowed_direct_users` – This option limits the users allowed access to the normal logon form. These users should have known passwords. If they have a ‘Secret Password’ then it is impossible for these users to logon to Infor PLM Accelerate. These user accounts are often disabled except during limited periods of administrative maintenance.
- `debugging_password` – This is only used during debugging. It is an alternative to the computed ‘Secret Password’ internal to web server validated users. During debugging of the logon process you can assign specific test users this debugging password. These users could then obtain access via web server validated authentication and/or function as `allowed_direct_users`, if so configured. Of course, any user with a ‘Secret Password’ is denied access.
- `shared_secret` – This is the key to the web server validation logon process. Once a user has been authenticated by the web server, and has passed all the regular expression checks, the shared_secret is used to compute an inscrutable ‘Secret Password’ which is used as a ticket to gain access to the other Infor PLM Accelerate server functions, including the vault server. The shared_secret is shared by the Innovator /Client and /Server applications.
- `logon_user_server_variable` – This is the name of the server variable that the authentication mechanism trusts to be an authenticated user. This defaults to ‘LOGON_USER’.
- `logon_user_domain_delimiter` – This is the character that separates the domain name and user name portion of the string from the domain name portion. This defaults to ‘\’.
- `logon_user_domain_first` – This should be true when the LOGON_USER is of the form Domain\Username, but it should be false if the string is of the form Username@Domain. This defaults to ‘true’.
- `empty_logon_user_allow_direct` – This can be set to true to cause the regular login box to appear when the LOGON_USER variable is blank.
- `bypass_logon_form` – This controls if the login form is shown or not. This key defaults to ‘false’. If ‘true’, then a logon form is not shown if integrated authentication information is available. The query string ?bypass_logon_form=value can over-ride a true or false value given in the configuration file. If there are multiple database choices available in the logon form then it make sense to specify a database in the query string with ?database=value, otherwise the first database in the list is chosen.
- `bypass_logon_wait` – This is the number of milliseconds to display the logon form before automatically submitting the logon credentials, in the case of bypass_logon_form=‘true’.

Logon URL

The normal URLs for accessing Infor PLM Accelerate remain unchanged for end users. The username derived from the LOGON_USER, and is visible but not editable. The user is not prompted a password, however, a choice of database is possible.

For user who must authenticate using the standard inputs, a logon URL in the form of /Client/default.aspx?username=X is also possible. For a limited configured number of names X this provides the normal logon form. In this case there is a password input. The password is validated against the password in the Innovator database for the user X. (See '`allowed_direct_users`' attribute of <`ClientLogon`> tag in the section 0 The ClientLogon attributes.)

Infor PLM Accelerate User Setup

In order to use these login hook features, a user Item with the required login_name must exist in the Infor PLM Accelerate database, with logon_enabled = true. The special secret password must then be set in order for a web server authenticated LOGON_USER to gain access to Infor PLM Accelerate. If no such user exists, then the Logon Form is displayed, but upon pressing the Login button the error message 'Authentication failed for X' is seen.

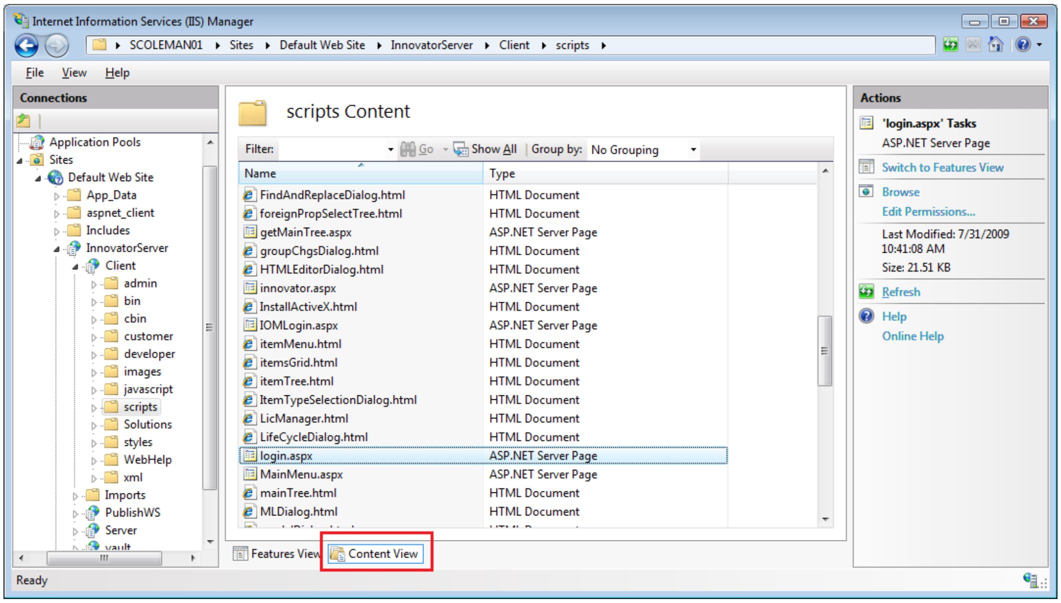
After creating a user Item, the administrator uses the 'Reset Authentication Password' action to set the user's password.

If the `shared_secret` attribute in the `ClientLogon` configuration element is changed then the 'Reset Authentication Password' action must be run or no users are able to logon except for these configured for direct logon.

Initial Setup with Active Directory

The following steps walk through the initial setup for using Active Directory authentication integrated with Infor PLM Accelerate where the Innovator Server is installed on Windows Server machine. The server must have access to the domain, and domain users must have permissions to read the /Client/scripts/login.aspx.

1. Make sure the Infor PLM Accelerate Admin login (admin) is enabled before proceeding, to make the process a little easier. Remember to disable it after completion if you haven't been using it.
2. Ensure the user information is loaded into the database. (login, firstname, lastname, email, etc.)
3. Obtain the Aras.LogonHooks.WindowsAuth.dll and Aras.LogonHooks.WindowsAuth.pdb files from the `Utilities\Aras.LogonHooks.WindowsAuth.zip` folder of the CD Image.
4. Copy the Aras.LogonHooks.WindowsAuth.dll and Aras.LogonHooks.WindowsAuth.pdb files to the \Innovator\Client\bin and \Innovator\Client\cbin folders of your installation.
5. Open up the IIS Manager on the Windows Server machine.
6. Browse to the /Client/Scripts folder.
7. Select 'Content View' from the bottom of the window pane.



Last Modified: 7/31/2009 10:41:08 AM

Size: 21.51 KB

Name	Type
FindAndReplaceDialog.html	HTML Document
foreignPropSelectTree.html	HTML Document
getMainTree.aspx	ASP.NET Server Page
groupChgsDialog.html	HTML Document
HTMLEditorDialog.html	HTML Document
innovator.aspx	ASP.NET Server Page
InstallActiveX.html	HTML Document
IOMLogin.aspx	ASP.NET Server Page
itemMenu.html	HTML Document
itemsGrid.html	HTML Document
itemTree.html	HTML Document
ItemTypeSelectionDialog.html	HTML Document
LicManager.html	HTML Document
LifeCycleDialog.html	HTML Document
login.aspx	ASP.NET Server Page
MainMenu.aspx	ASP.NET Server Page
mainTree.html	HTML Document
MLDialog.html	HTML Document

Figure 1.

8. Highlight login.aspx.
9. Right click Login.aspx and select **Switch to Features View**.

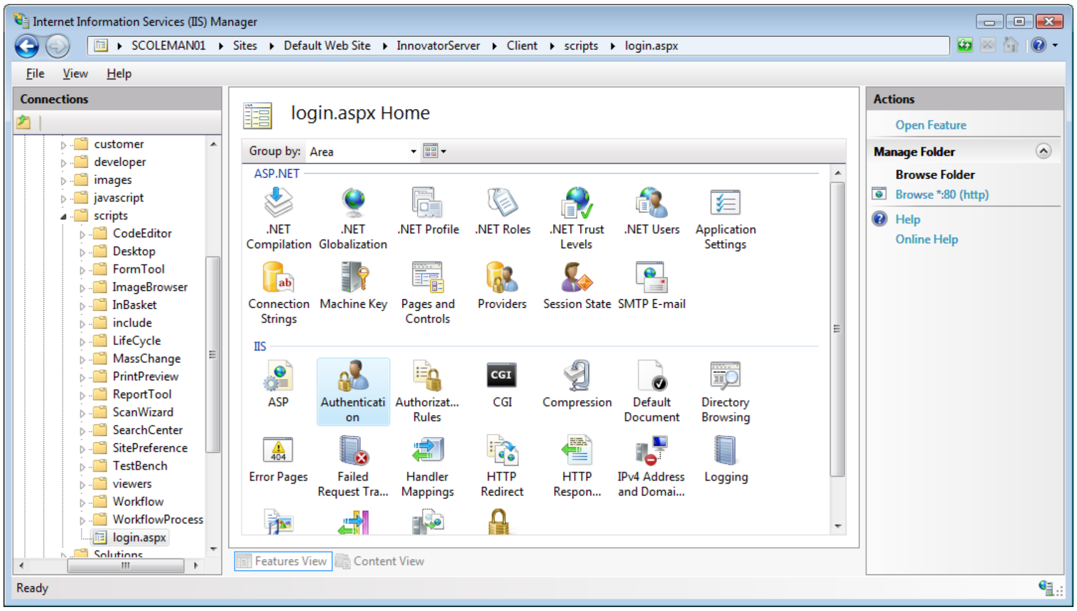
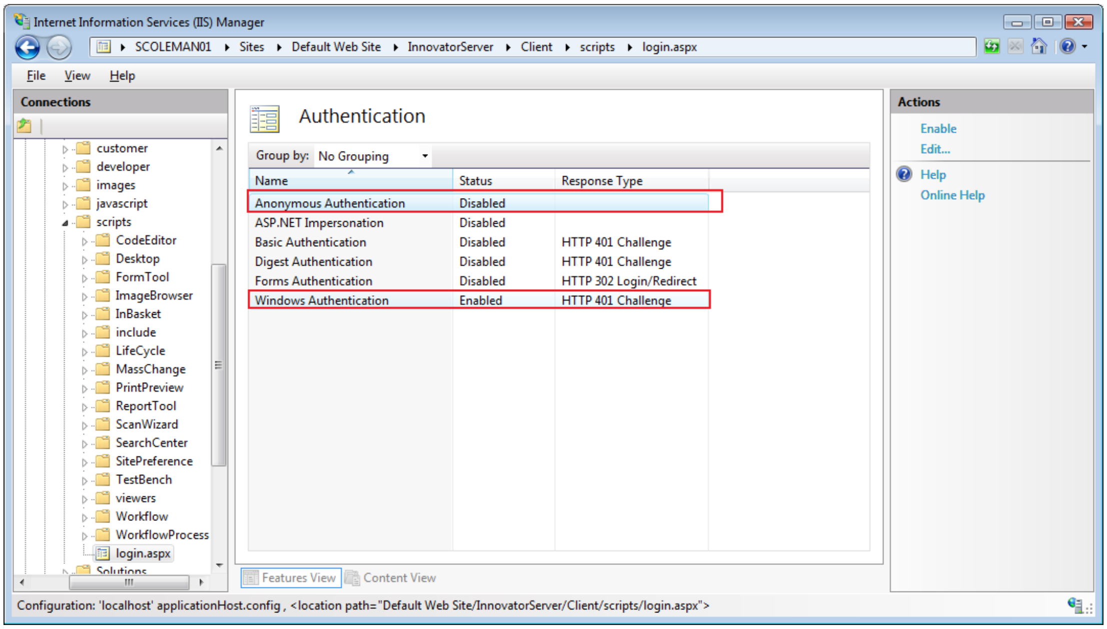


Figure 2.

10. Open **Authentication** under the **IIS** section.

11. Disable **Anonymous Authentication**.

12. Enable **Windows Authentication**.



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/InnovatorServer/Client/scripts/login.aspx">

Figure 3.

13. Browse to the /Client/Scripts folder.

14. Select ‘Content View’ from the bottom of the window pane.

15. Highlight `IOMLogin.aspx`.

16. Repeat steps 9-12 for IOMlogin.aspx.
17. Set the `<ClientConfig>` and `<ClientLogon>` tags in the InnovatorServerConfig.xml file (Sample below)

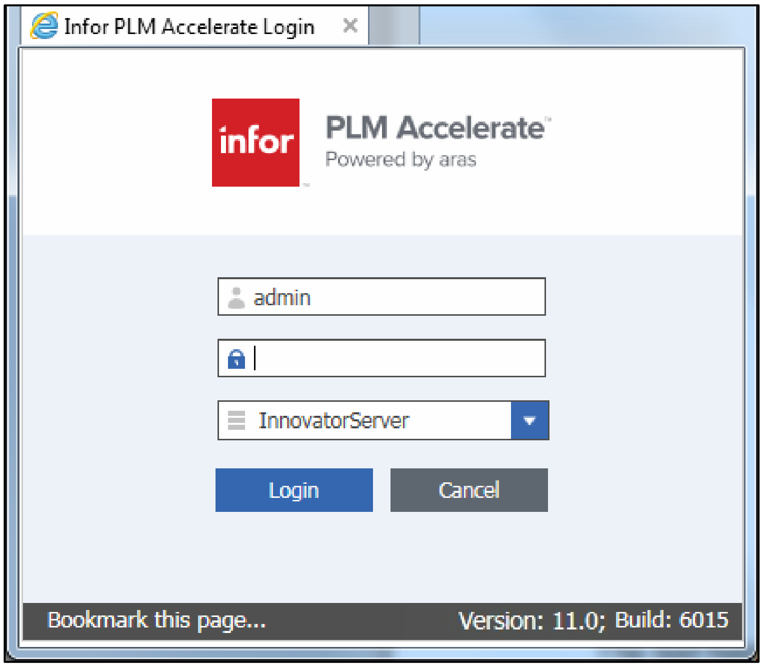
```
<ClientConfig
   AssemblyName="Aras.LogonHooks.WindowsAuth"
   AssemblyNameType="partial"
   TypeName="Aras.LogonHooks.WindowsAuth" />

<ClientLogon  allowed_domain_names="^DOMAINNAMEHERE$"
   allowed_domain_users=".+"
   denied_domain_users="^admin$|^root$|^vadmin$|^PLM$|^pdftron_user$
   |^esadmin$"
   allowed_direct_users="^admin$|^root$|^pdftron_user$|^esadmin$"
   shared_secret="Your shared secret here"
   empty_logon_user_allow_direct="false" />
```

18. In the web.config file, located in the Client folder, increment the “filesRevision” attribute by 1:

```
     ...
   </runtime>
  <cachingModule moduleEnabled="true" filesRevision="2" />
</configuration>
```

19. Log into Infor PLM Accelerate using a string such as:

```
http://localhost/InnovatorServer/Client/default.aspx?username=admin
```



admin

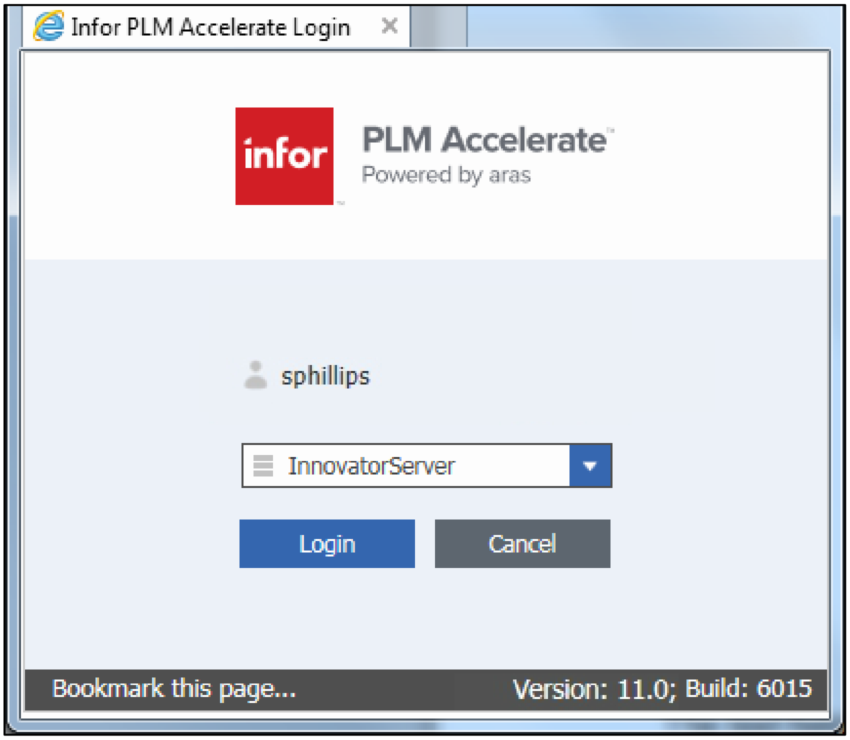
InnovatorServer

Bookmark this page...

Version: 11.0; Build: 6015

Figure 4.

20. From the TOC, select **Administration --> Users**.
21. Run search to confirm users are displayed.
22. From the main menu, select **Actions --> Reset Authentication Passwords.**
23. Logout.
24. Re-start IIS to flush the server cache.
25. Login using a normal URL.



sphillips

InnovatorServer

Figure 5.

Chapter 3. Securing built-in Infor PLM Accelerate Accounts

It should be noted that the core Infor PLM Accelerate database comes with 3 built-in accounts. These are ‘Innovator Admin’ (username=admin), ‘Super User’ (username=root), and ‘Vault Admin’ (username=vadmin).

The Innovator Admin and Super User accounts should be changed to prevent them being used by persons who know something about the default values of these passwords by disabling these accounts and only enabling logon during periods controlled by strict configuration management principals. Users should be made members of the Administrators Identity to have administrative privileges assigned on their own account, rather than using the Innovator Admin or Super User accounts.

The Vault Admin user cannot be disabled if the VaultServer feature of Infor PLM Accelerate is being used. The best way to restrict access to this account is to generate a random, sufficiently long password as to be astronomically improbable to guess, and to store this password in encrypted form in the VaultServerConfig.xml file.

The Visual Collaboration solution also uses a designated user called pdftron_user. This user should be accommodated in Windows Authentication setup as well.

Chapter 4. Mixing Authentication Methods

Infor PLM Accelerate allows for a flexible set of configurations for authentication, and for site structure. By combining the ability to distribute the different tiers of innovator with the different authentication modes, administrators can create a deployment that leverages more than one authentication method.

The following is an example of an existing production deployment of multi-tier mixed authentication control.

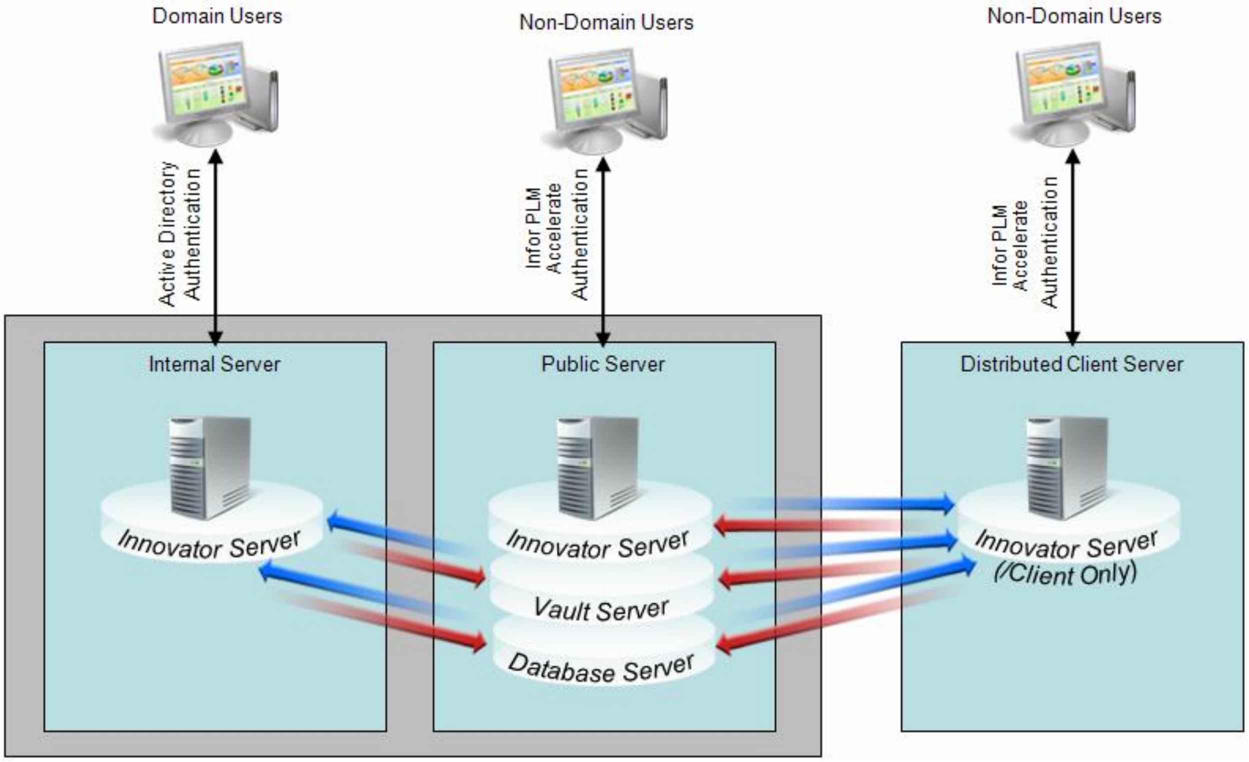

Domain Users
Non-Domain Users
Non-Domain Users
Active Directory Authentication
Infor PLM Accelerate Authentication
Infor PLM Accelerate Authentication
Internal Server
Public Server
Distributed Client Server
Innovator Server
Innovator Server
Vault Server
Database Server
Innovator Server (/Client Only)

Figure 6.

In this diagram we have three servers running Infor PLM Accelerate.

- **Public Server** - This server represents the main instance of Infor PLM Accelerate. This server runs the Innovator Server, Database Server, and Vault Server tiers of Infor PLM Accelerate. The URL for this server would be used by internal and external users of Infor PLM Accelerate, and would deploy the Infor PLM Accelerate Security features. Users would authenticate against this server using standard Infor PLM Accelerate authentication methods.
- **Internal Server** – This server represents a second instance of Infor PLM Accelerate on the same network as the Public Server, but does not stand alone. This server only consists of the Innovator Server tier of Infor PLM Accelerate, and would refer back to the Public Server when calling the Database Server tier or the Vault Server tier. The URL for this server would be used by internal and external users of Infor PLM Accelerate, and would deploy the logon hooks. Users would authenticate against this server using Active Directory, and would not

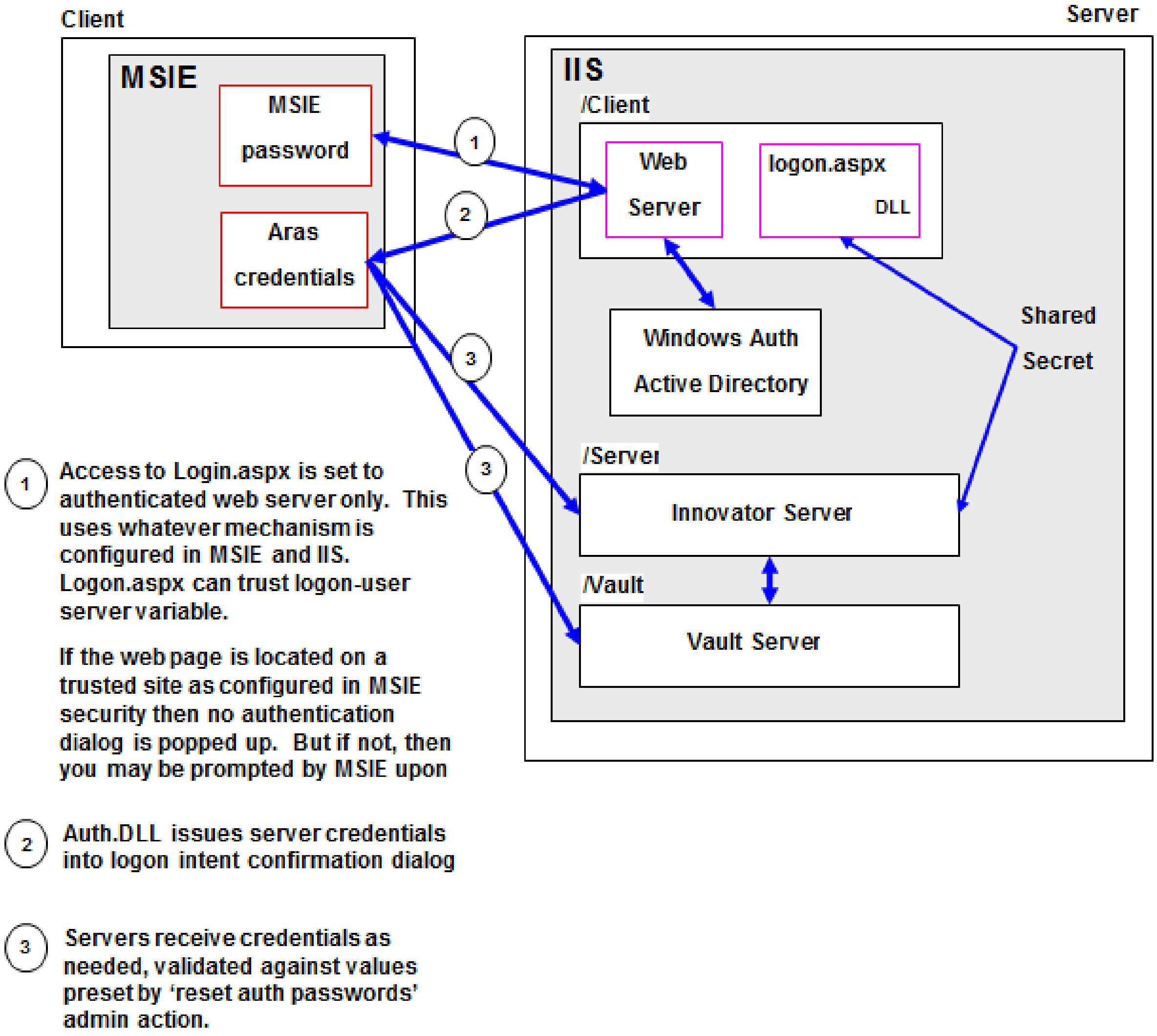
be subject to the session timeout restrictions of the Infor PLM Accelerate Security feature of the Public Server.

- **Distributed Client Server** - This server represents an instance of Infor PLM Accelerate deployed on a different LAN than the Public Server. This server only consists of the Innovator Sever tier of Infor PLM Accelerate. Furthermore, only the /Client folder would be used from this tier. When calling the /Server folder, all requests would be redirected to the Public Server. As with the Internal Server, all requests would refer back to the Public Server when calling the Database Server tier or the Vault Server tier. This deployment is for two reasons. One, all calls to the /Client folder, like for UI images, would be done on a local network at the remote site, and would help performance over a slow WAN connection. And two, this deployment allows the Public Server to control the Authentication and session management, including Infor PLM Accelerate Security features like session timeout.

While this example only represents one configuration possibility, it does represent the flexibility of access control that can be achieved with the Infor PLM Accelerate platform.

Chapter 5. Reference Diagrams

Client Logon Hooks Authentication Sequence, Web Server Mode



1 Access to Login.aspx is set to authenticated web server only. This uses whatever mechanism is configured in MSIE and IIS. Logon.aspx can trust logon-user server variable.

If the web page is located on a trusted site as configured in MSIE security then no authentication dialog is popped up. But if not, then you may be prompted by MSIE upon

2 Auth.DLL issues server credentials into logon intent confirmation dialog

3 Servers receive credentials as needed, validated against values preset by ‘reset auth passwords’ admin action.

Figure 7.