

Implementing Kerberos in a Citrix environment

Distribution

Amount	Receivers	Location
All rights reserved.		
Contents of this publication may not be duplicated and/or made public in any way nor by any medium including; printing, photocopying and microfilm or otherwise, without the prior written permission of bjornbats.nl .		

Table of Contents

Table of Contents	3
1.1 Overview	4
1.1.1 Definition of Kerberos	4
1.1.2 Security.....	4
1.1.3 Citrix Pass-through Authentication.....	4
1.2 Presentation Server.....	5
1.3 Web Interface	5
1.4 ICA Client	6
1.5 ICA Client Initialization Files	6
2 Configuration data	8
2.1 Presentation Server Settings	8
2.2 Web Interface Settings	8
2.3 ICA Client Settings.....	8
2.4 ICA Client Initialization Files Settings	8
3 Installation summary.....	9
3.1 Server Side Kerberos Implementation.....	9
3.2 Client Side Kerberos Implementation	9
4 Step-by-step guide.....	10
4.1 Presentation Server.....	10
4.1.1 Prerequisites	10
4.2 Web Interface	12
4.2.1 Prerequisites	12
4.3 Client	15
4.3.1 Prerequisites	15
4.3.2 Procedures.....	15

1.1 Overview

1.1.1 Definition of Kerberos

Kerberos is a safe way to authenticate users in a computer network. Kerberos is developed by the Massachusetts Institute of Technology. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

1.1.2 Security

Kerberos is used in a Windows 2000 or higher domain by default. An important reason to use Kerberos is that passwords will not go over the wire. Instead, an encryption key derived from the password initiating the Kerberos ticket request will go over the wire. This way a high level of security will be achieved. Keep in mind that an unauthorized user can still gain access if he or she knows a valid username and password. To gain a higher level of security, smart card logon (certificate based logon) can be used. The use of a certificate is more secure than using name and password because it is impossible for a hacker to crack the password.

Kerberos is used in combination with Security Support Provider Interface (SSPI) security exchange mechanisms.

1.1.3 Citrix Pass-through Authentication

Kerberos can be used in combination with pass-through authentication. Kerberos with pass-through authentication works with any client logon method, e.g. smartcard, biometrics or password. Using Kerberos pass-through, the Kerberos ticket derived from the initial logon is used for Citrix pass-through authentication. If needed, this solution can be used in high level security environments.

To use Kerberos in combination with Citrix pass-through authentication a number of settings has to be made for both server and client.

It is important to note that if you want to use Kerberos in combination with Citrix pass-through authentication, you have to use the Citrix client provided on the Citrix Presentation Server component CD-ROM. Do not use a downloaded client.

1.2 Presentation Server

Kerberos logon requires Presentation Server 3.0 or higher. Kerberos works only between clients and servers that belong to the same or to trusted Windows 2000 or Windows 2003 domains. Servers must also be trusted for delegation.

Kerberos logon is not available in the following circumstances:

- Connections for which you select any of the following options in Terminal Services Configuration:
 - On the **general** tab, the **Use standard Windows Authentication** option
 - On the **logon Settings** tab, the **Always use the following logon**
- Connections you route through Secure Gateway
- If the server running Presentation Server requires smart card logon
- If the authenticated user account requires a smart card for interactive logon

SSPI requires XML Service DNS address resolution to be enabled for the server farm, or reverse DNS resolution to be enabled for the Active Directory domain.

To disable Kerberos Logon to a particular server, set the following registry key on the server:

```
HKEY_LOCAL_MACHINE_\SOFTWARE\Citrix\Logon\DisableSSPI=1
```

1.3 Web Interface

Kerberos pass-through can be used in high level security environments in combination with Citrix Web Interface or Citrix Program Neighborhood Agent. The following settings have to be made:

- Enable Kerberos pass-through authentication using the Access Suite Console
- Add the url of both the Citrix Web Interface and Citrix Program Neighborhood Agent (if different) to the local intranet zone in Internet Explorer
- Trust the Citrix Web Interface Server for delegation

This results in applications enumerated automatically in Citrix Web Interface or Citrix Program Neighborhood Agent.

1.4 ICA Client

Kerberos logon requires Presentation Server Clients for 32-bit Windows Version 8.x or higher. You have to use the Citrix ICA client provided on the Citrix Presentation Server component CD-ROM. Do not use a downloaded client.

The application settings of the Presentation Server Program Neighborhood Client for 32-bit Windows are controlled by a number of initialization (.ini) files. These settings can also include Kerberos settings.

The Web Client does not use .ini files. All connection properties for the Web Client are specified in .ica files.

1.5 ICA Client Initialization Files

This section explains the initialization files settings. The **appsrv.ini** file describes each custom ICA Connection and user interface settings. The **WFClient** section within the **appsrv.ini** file describes connection and session properties that serve as defaults for all custom ICA connections and also describes user interface settings. The **wfclient.ini** file describes the properties of the client device. These settings must be placed under the **WFClient** section of this initialization file.

You can customize the initialization files at the installer level. To do so, these initialization files could be included in a single package and automatically distributed to clients, along with the installer files. You can create a package using the following method:

- Extract the contents of the installer file to a new folder, A
- Install the client using the installer file
- After installation of the client, modify the initialization files
- Save the modified initialization files to a new folder, B. Replace the .ini file extensions with .src extensions
- Replace all .src files in folder A with their modified equivalents from folder B
- Repackage the contents of folder A for distribution to users

The detailed procedure of creating an ICA client package is beyond the scope of this document.

Setting	Explanation	Initialization File
SSPIEnabled	Enables Kerberos authentication	Wfclient.ini
UseSSPIOnly	Use Kerberos authentication only. Authentication will fail if Kerberos authentication fails	Wfclient.ini

BjornBats.nl

All SBC & Virtual info

These settings correspond to **ICA Settings** dialog box > **General** tab > **Pass-Through Authentication** option.

Setting	Explanation	Initialization File
EnableSSOnThruICAFile	Specifies whether (On) or not (Off) to use the same user name and password the user used to log on tot the client device for authentication through .ica files. For security reasons, users can not be authenticated tot the server unless this parameter is present and its value set to On, even if UseLocalUserAndPassword and SSONUserSetting are specified in the .ica file.	Appsrv.ini
SSOnUserSetting	Selects (On) or clears (Off) the Use local credentials to log on option	Appsrv.ini

This last setting correspond to **ICA Settings** dialog box > **General** tab > **Use local credentials to log on** option.

2 Configuration data

2.1 Presentation Server Settings

Setting	Value
Preferred version	Presentation Server 3.0 or higher
Delegation	Trust this computer for delegation to any service (Kerberos only)
Citrix Farm MetaFrame Settings	Enable XML Service DNS address resolution
Reverse DNS resolution	enabled

2.2 Web Interface Settings

Setting	Value
Preferred version	Web Interface 3.0 or higher
Delegation	Trust this computer for delegation to any service (Kerberos only)
Kerberos pass-through authentication	enabled

2.3 ICA Client Settings

Setting	Value
Preferred version	Presentation Server Clients for 32-bit Windows Version 8.x or higher (use version from CD-ROM only!)
Location of url in Internet Explorer	Local Intranet

2.4 ICA Client Initialization Files Settings

Setting	Value
SSPIEnabled	On
UseSSPIOnly	On
EnableSSOnThruICAFile	On
SSOnUserSetting	On

3 Installation summary

3.1 Server Side Kerberos Implementation

The following steps have to be taken to implement Kerberos on the server side:

- Trust servers for delegation
- Enable XML Service DNS resolution or reversed DNS resolution
- Enable Kerberos pass-through for the Web Interface or Program Neighborhood Agent

3.2 Client Side Kerberos Implementation

- Edit and package the appropriate initialization files
 - Add the url for the Web Interface or Program Neighborhood configuration file to the local intranet zone of Internet Explorer
-

4 Step-by-step guide

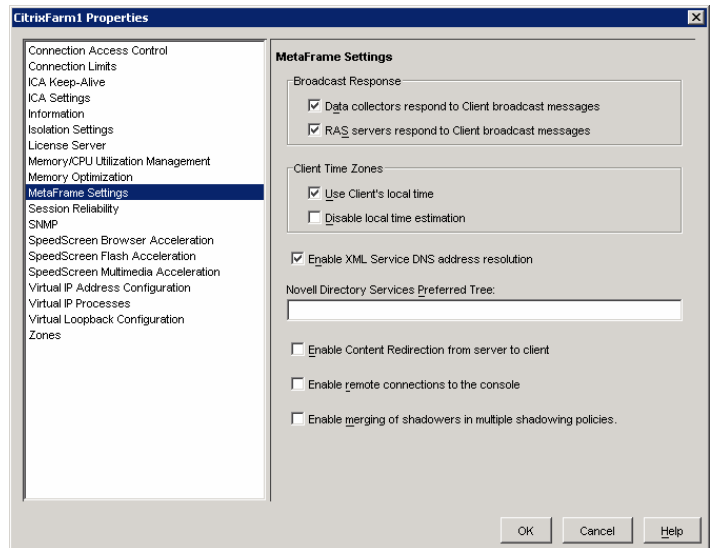
4.1 Presentation Server

4.1.1 Prerequisites

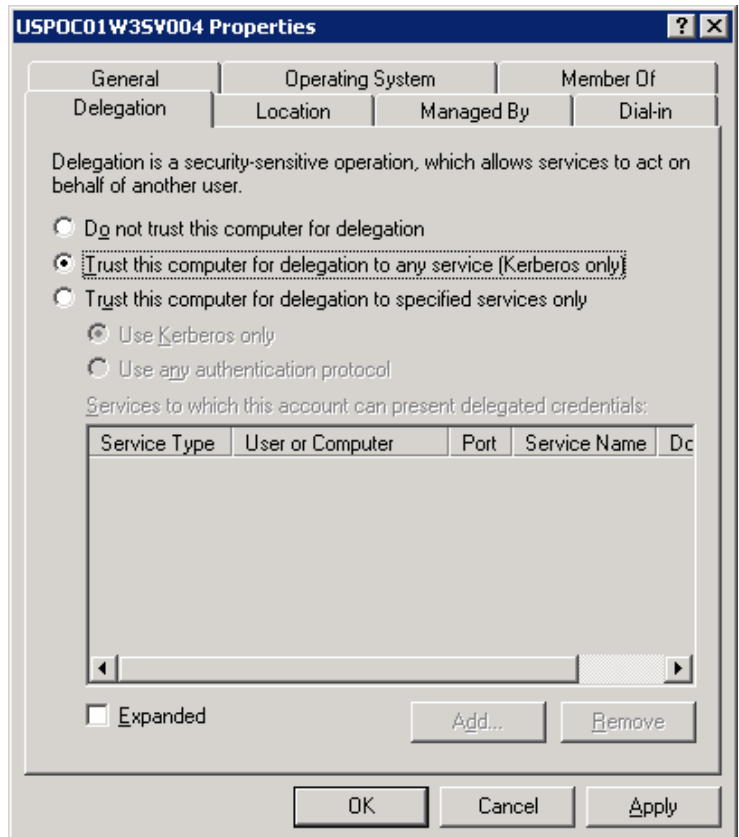
- Citrix Presentation server is installed

Action	Screenshot (if available)
NOTE: <i>Settings in the text are leading. Settings in the pictures are only informational</i>	Intentionally left blank

- 1) Right-click "CitrixFarm1"
- 2) Select "Properties"
- 3) Select the tab "MetaFrame Settings"
- 4) Check "Enable XML Service DNS address resolution"
- 5) Make sure that reverse lookup will work for every involved server (pointer records should be in DNS)



- 1) Open "Active Directory Users and Computers"
- 2) Right-click on the Citrix Server
- 3) Select "Properties"
- 4) Select the tab "delegation"
- 5) Select "Trust this computer for delegation to any service (Kerberos only)"

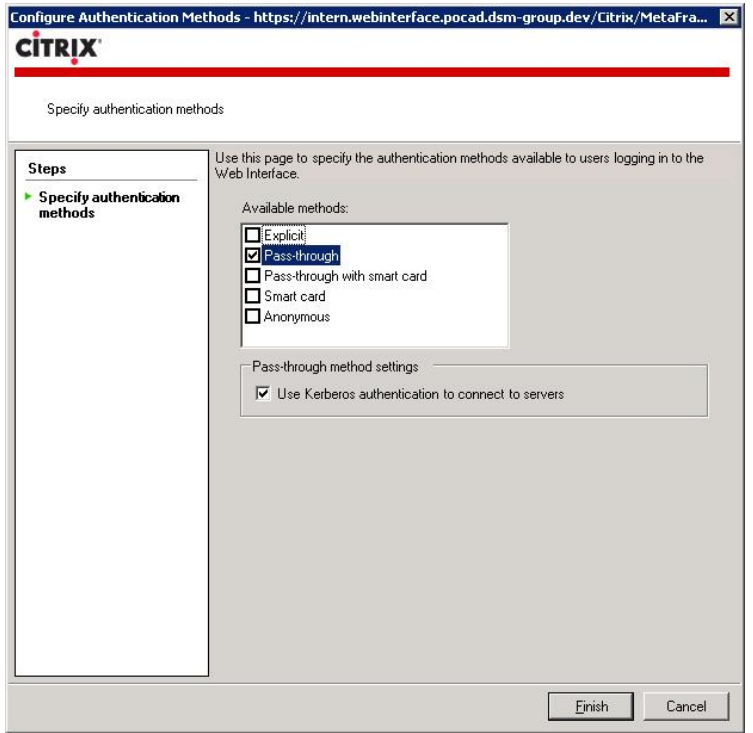


4.2 Web Interface

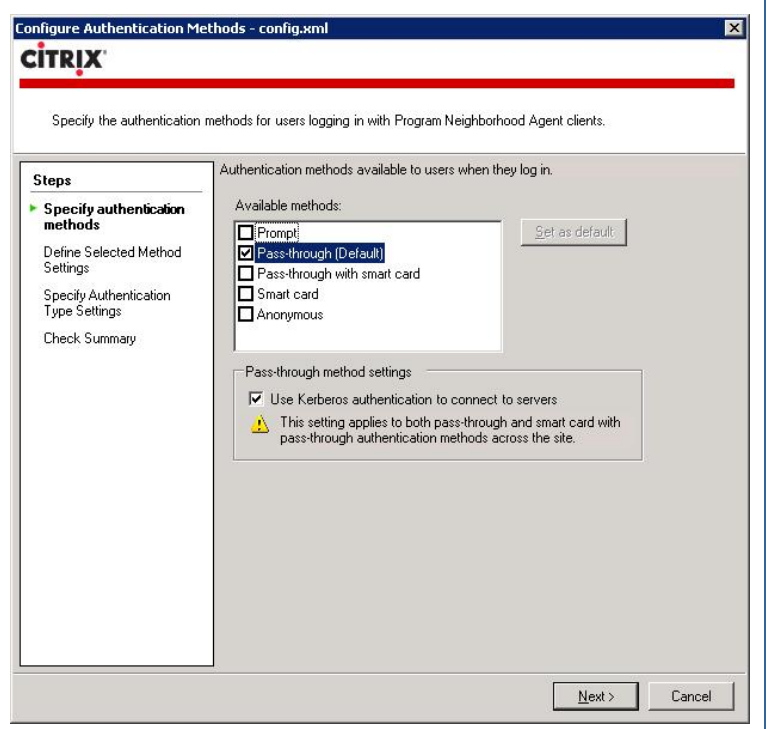
4.2.1 Prerequisites

- Citrix Web Interface is installed

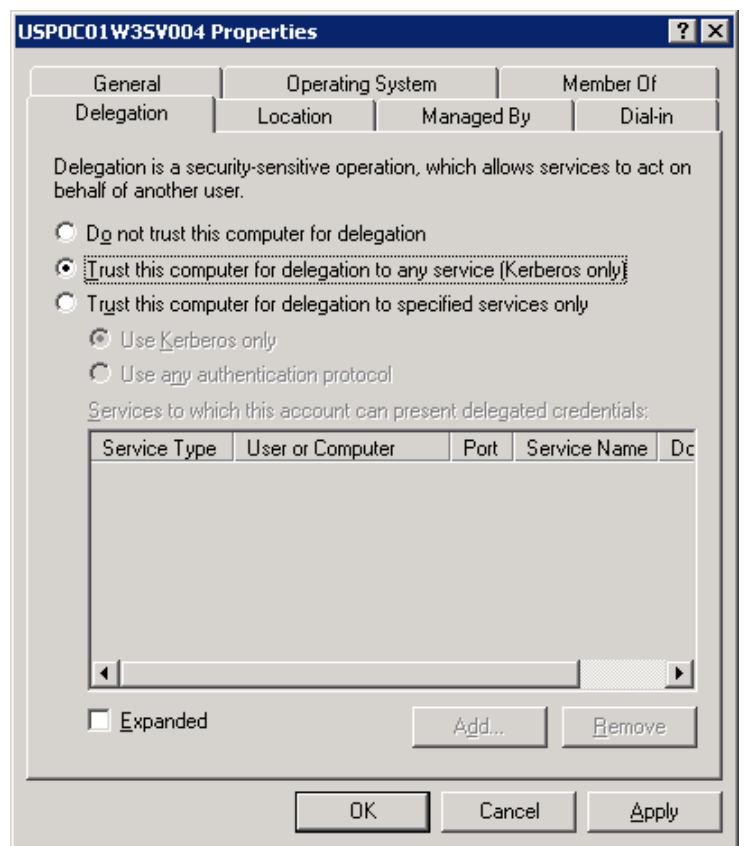
Action	Screenshot (if available)
<p>NOTE: <i>Settings in the text are leading. Settings in the pictures are only informational</i></p>	Intentionally left blank
<ol style="list-style-type: none">1) Using the Access Suite Console, select the appropriate website for which you want to enable Kerberos in the left pane.2) In the Middle Pane, choose "Configure Authentication Methods"3) A wizard will open	

<ol style="list-style-type: none">1) Check "pass-through" from available methods2) Also check "Use Kerberos authentication to connect to servers"3) Uncheck all other available methods	 <p>Configure Authentication Methods - https://intern.webinterface.pocad.dsm-group.dev/Citrix/MetaFra...</p> <p>CITRIX</p> <p>Specify authentication methods</p> <p>Use this page to specify the authentication methods available to users logging in to the Web Interface.</p> <p>Steps</p> <ul style="list-style-type: none">Specify authentication methods <p>Available methods:</p> <ul style="list-style-type: none"><input type="checkbox"/> Explicit<input checked="" type="checkbox"/> Pass-through<input type="checkbox"/> Pass-through with smart card<input type="checkbox"/> Smart card<input type="checkbox"/> Anonymous <p>Pass-through method settings</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use Kerberos authentication to connect to servers <p>Finish Cancel</p>
<ol style="list-style-type: none">1) Using the Access Suite Console, select the appropriate Program Neighborhood Agent config file for which you want to enable Kerberos in the left pane.2) In the Middle Pane, choose "Configure Authentication Methods"3) A wizard will open	

- 1) Check "pass-through" from available methods
- 2) Also check "Use Kerberos authentication to connect to servers"
- 3) Uncheck all other available methods



- 1) Open "Active Directory Users and Computers"
- 2) Right-click on the Citrix Server
- 3) Select "Properties"
- 4) Select the tab "delegation"
- 5) Select "Trust this computer for delegation to any service (Kerberos only)"



4.3 Client

4.3.1 Prerequisites

- The Citrix Presentation Server Clients for 32-bit Windows Version 8.x or higher has to be installed including the appropriate initialization files (use version from CD-ROM only!)

4.3.2 Procedures

Action	Screenshot (if available)
NOTE: <i>Settings in the text are</i>	Intentionally left blank

BjornBats.nl

All SBC & Virtual info

leading. Settings in the pictures are only informational

- 1) Open Internet Explorer and go to "Internet Options" in the Tools menu
- 2) Go to the security tab and click "local Intranet"
- 3) Click "sites", "advanced" and add the url of both the Citrix Web Interface and Citrix Program Neighborhood Agent Configuration File (if different)



BjornBats.nl

All SBC & Virtual info
