Setting up Kerberos, AFS, and Putty on Windows Vista/Windows 7

Note on 64-bit Windows systems:

On 64-bit Windows systems you will need to install both 32-bit *and* 64-bit distributions of both Kerberos and AFS. Installing just 64-bit editions will not work properly.

Installing Kerberos

The recommended version of Kerberos for use with AFS 1.7+ is now Heimdal.

1) Download the appropriate installer from here:

https://www.secure-endpoints.com/heimdal/

Note: For Kerberos + AFS on 64-bit Windows, download the combined 64-bit and 32-bit installer.

2) Run the installer that you downloaded:

Note: You may encounter an open file security prompt depending on your system configuration.



Accept the license agreement:

Heimdal 1.5.100.930 Setup	
End-User License Agreement Please read the following license agreement carefully	
License Agreement	^
Copyright (c) 1995 - 2009 Kungliga Tekniska högskolan	E
(Royal Institute of Technology, Stockholm, Sweden).	
All rights reserved.	
Redistribution and use in source and binary forms, with o	r without 🔻
☑ I accept the terms in the License Agreement	
Print Back Next	Cancel

Leave the install options at default:

📸 Heimdal 1.5.100.930 Setup			
Custom Setup Select the way you want features to be installed.			
Click the icons in the tree below to change the way features will be installed.			
Heimdal	Command line tools and libraries for Heimdal Kerberos		
	This feature requires 10MB on your hard drive. It has 1 of 1 subfeatures selected. The subfeatures require 5559KB on your hard drive.		
Location: C:\Program Files\Heimdal\	Browse		
Re <u>s</u> et Disk <u>U</u> sage	Back Next Cancel		

Finally, confirm that you wish to proceed



Once installation has completed, click Finish:

Heimdal 1.5.100.930 Setup	
	Completed the Heimdal 1.5.100.930 Setup Wizard
	Click the Finish button to exit the Setup Wizard.
	Back Finish Cancel

Note that the Heimdall installer does **not** include a user interface. You will need to download and install one as detailed below:

3) Download the Network Identity Manager installer from here:

https://www.secure-endpoints.com/netidmgr/v2/

Note: For 64-bit installs, only download the 64-bit installer (non-SDK).

4) Run the installer that just downloaded:



Accept the license agreement:

Network Identity Manager Setup
End-User License Agreement Please read the following license agreement carefully
Copyright Notice and Legal Administrivia
Copyright (C) 2010 by Secure-Endpoints Inc.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
✓ I accept the terms in the License Agreement:
Print Back Next Cancel

Select Typical install:

🔡 Network Identity Manager Setup	X
Choose Setup Type Choose the setup type that best suits your needs	Ţ
Typical Installs the most common program features. Recommended for most users.	
Custom Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.	
Complete All program features will be installed. Requires the most disk space.	
<u>B</u> ack <u>N</u> ext Cancel	

Click Install to proceed:



Finally, click Finish once the installer completes.

5) Run Network Identity Manager from the Start Menu:



6) Open the Network Identity Manager main window:

Right click the Kerberos for Windows icon in the system tray (you may need to click the up or left arrow first) and click Show Network Identity Manager window. You may have to do this twice the first time:

Show Network Identity Manager window		
CObtain ne	Ctrl+N	
Renew Mimport Cr Destroy	Ctrl+I	
Set defaul	t	F
😿 Change p	assword	
Melp Contents About Network Identity Manager		
Exit		Ctrl+X
	0	
	Customize	-) •
A:11 PM		

7) Setup your account and obtain tickets for the first time

Click the "Obtain new credentials ..." icon in the toolbar:

🔊 Network Identity Manager	• X
File Credential View Options Help	
🔃 👒 - 🞦 👒 - 💌 💿	
Obtain new credentials	KeyStore

Enter your DICE username in the Username box, and INF.ED.AC.UK (case sensitive) in the Realm box:

Obtain ne	w credentials			? X
Kerber Princip	ros pal			
Kerbe	ros v5 Principal Sele	ction		
	Username	yhuang		•
	Realm	INF.ED.AC.UK		•
			Next >	Cancel

The first time after you click "Next" the following window should appear. Tick the "Proxiable" and "Make this the default identity" boxes and click "Next" (do not click "Finish"):

Oł	otain new credentials			8 ×
4	yhuang@INF.ED.AC	.UK	Kerbero	s Principal
	•			
	Kerberos v5 Credentia	Ontions		
	Lifetime			
	Fuedule	10 hours		
	Renewable for	7 days		
	📝 Can be <u>f</u> orwarded t	o other machines		
	Addressless			
	Proxiable			
	Make this the default id	entity		
			Next > Finish	<u>C</u> ancel

Enter your password in the Password box, then click "Make this the default identity". Optionally, select "Save password in My Keystore" if you want the password stored on your machine:

Obtain new credentials	8 x
whuang@INF.ED.AC.UK	Kerberos Principal
•	
Identity	
yhuang@INF.ED.AC.UK's Password:	•••••
Save password in My Keystore	
Saving your password in this location allows using this single key store. You may be aske	you to obtain credentials for multiple identities d to enter a password for the keystore.
Make this the default identity	
< <u>B</u> ack	Next >

Finally, click Finish. You should see a status dialog for a few seconds.

Note: If you have chosen to save your password, click "Next" instead, and follow the prompts to setup a keystore password to protect it.

Obtain new credentials	? ×
whuang@INF.ED.AC.UK	Kerberos Principal
Obtaining new credentials for yhuang@INF.ED.AC.UK	
Obtaining initial Kerberos v5 tickets	
☑ Close this window after operation is complete ≦Back	<u>E</u> inish <u>A</u> bort

You'll then be returned to the main Network Identity Manager window where there should be a new entry indicating your credentials have been successfully validated and a Kerberos ticket obtained:

🚺 Network Identity Manager	
<u>File Credential View Options H</u> elp	
🔁 • 🖄 • 🚬 💁 • 💌 🕥	٥
My Keystore -(⊃	KeyStore
 ☆ yhuang@INF.ED.AC.UK ↓ Valid for 9 hours 59 Kerberos v5 tickets (1) 	Kerberos Principal

Installing PuTTY

PuTTY can be used to remotely login to Informatics machines and servers from anywhere on the internet using SSH. Where possible, you should use Kerberos authentication instead of keyboard-interactive by setting up Putty to use your Kerberos credentials.

1) Download PuTTY or its automated installer:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The easiest option is to just save putty.exe on its own to a location of your choice, though there is also a Windows installer package.

2) Setup PuTTY to work with Kerberos:

To start off, run the PuTTY executable, and then enter one of the following into the **Host Name** box. Put whatever you want the connection to be called in the **Saved Sessions** box, though we'd recommend keeping it the same as the Host Name:

student.ssh.inf.ed.ac.uk

for taught students

staff.ssh.inf.ed.ac.uk

for staff and research students

Reputity Configuration		? ×
Category:		
Session	Basic options for your PuTTY se	ssion
	Specify the destination you want to conne	ct to
	Host <u>N</u> ame (or IP address)	Port
Bell	staff.ssh.inf.ed.ac.uk	22
Features Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial	Connection type: ◎ Ra <u>w</u> ◎ <u>T</u> elnet ◎ Rlogin ● <u>S</u> SH	l 🔘 Se <u>r</u> ial
	Load, save or delete a stored session Sav <u>e</u> d Sessions staff.ssh.inf.ed.ac.uk	
	Default Settings	Load Sa <u>v</u> e Delete
	Close window on e <u>x</u> it: ◎ Always ◎ Never ◎ Only on d	lean exit
<u>A</u> bout <u>H</u> elp		<u>C</u> ancel

Leave the remaining options as-is for now.

From the Category menu on the left, select **Data** under **Connection**. If you are the only user of your machine, enter your DICE username in the **Auto-login username** box. If the user account on your machine is used by multiple people, it's best to leave this box blank.

😵 PuTTY Configuration		? <mark>×</mark>
Category:		
Category: Session Logging Terminal Keyboard Bell Features Window Behaviour Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Serial	Data to see Login details Auto-login usemame When usemame is not sp Prompt OUse system Terminal details Terminal details Terminal speeds Environment variables Value	end to the server yhuang eccified: stem usemame (Administrator) xtem 38400,38400 Add Remove
About <u>H</u> elp		Open Cancel

Again from the Category box, expand the **SSH** group, then the **Auth** group and finally select **GSSAPI**. In this window, tick the **"Allow GSSAPI credential delegation"** box.

Reputity Configuration	? <mark>×</mark>
Category:	
Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Flogin SSH Kex GSSAPI TTY X11 Tunnels Bugs Serial TT	Options controlling GSSAPI authentication
About <u>H</u> elp	Open <u>C</u> ancel

Then, click **Browse** and select the **gssapi32.dll** of your Kerberos installation. On 32-bit systems this will normally be **C:\Program Files\Heimdal\bin\gssapi32.dll**. On 64-bit Windows, this file will normally be **C:\Program Files (x86)\Heimdal\bin\gssapi32.dll**. Finally, select the **User-specified GSSAPI DLL** entry in the **Preference order** box and then click **Up** twice so it is top of the list:

Real PuTTY Configuration	? ×
Category:	
Logging 🔺	Options controlling GSSAPI authentication
En Terminal Keyboard Bell	 Attempt GSSAPI authentication (SSH-2 only) Allow GSSAPI credential delegation
Window	Preference order for GSSAPI libraries: User-specified GSSAPI DLL MIT Kerberos GSSAPI32.DLL
Behaviour Translation	Microsoft SSPI SECUR32.DLL <u>D</u> own User-supplied GSSAPI library path:
Colours	C:\Program Files (x86)\Heimdal\bin\gssa Browse
··· Data ··· Proxy	
Telnet Rlogin	
E SSH	
GSSAPI	
About <u>H</u> elp	Qpen Cancel

If you wish to use X11 forwarding (i.e. running graphical X window applications remotely), navigate down to the **X11** entry under **SSH**, select the **Enable X11 forwarding** checkbox and enter **localhost:0** for **X display location**. You will need to have an X11 server installed on your local computer first.

Reputity Configuration		? ×
Category:		
🖻 ·· Window 🗛	Options controlling	SSH X11 forwarding
- Appearance	X11 forwarding	
Translation	Enable X11 forwarding	
Selection	X display location	localhost:0
Colours	Remote X11 authentication MIT-Magic-Cookie-1	n protocol
···· Data ···· Proxy	X authority file for local disp	Browse
Telnet		
⊡. SSH		
- Kex =		
Auth		
TTY		
<mark>X11</mark>		
Tunnels		
Serial		
	-	
Image: Image		
About <u>H</u> e	lp	Open Cancel

If you wish to use port-forwarding and tunnelling, e.g. for remote VNC access, navigate to the **Tunnels** page under **SSH** and enter the ports as required (the following is only an example):

Reputry Configuration		१ <mark>×</mark>
Category:		
📄 Window 🔺	Options controlling SSH	port forwarding
Appearance Behaviour Translation Selection Colours Connection Data Proxy	Port forwarding Local ports accept connectio Remote ports do the same (S Forwarded ports:	ns from other hosts SH-2 only) <u>R</u> emove
Telnet Rlogin SSH Kex ≡	Add new forwarded port: <u>S</u> ource port 5900 Destination localhost:590	A <u>d</u> d
	● Local ○ Remote ● Auto ○ IPv4	© Dynamic © IPv <u>6</u>
4 <u> </u>		
About <u>H</u> elp	Оре	n <u>C</u> ancel

Finally, navigate back to the **Session** page and click **Save**:

Reputity Configuration	8 ×
Category:	
Session 🔺	Basic options for your PuTTY session
···· Logging ⊡·· Terminal ···· Keyboard	Specify the destination you want to connect to Host Name (or IP address) Port
Bell Features Window	Connection type: Raw O Telnet Rlogin O Serial
···· Appearance ···· Behaviour ⋿ ···· Translation ···· Selection	Load, save or delete a stored session Sav <u>e</u> d Sessions staff.ssh.inf.ed.ac.uk
Colours ⊡Connection Data	Default Settings staff.ssh.inf.ed.ac.uk
Proxy Telnet Rlogin	Delete
GSSAPI ▼	Close window on exit: ⊚ Always ⊚ Never
About <u>H</u> el	p <u>O</u> pen <u>C</u> ancel

From now on, when you start PuTTY, you can just double-click your connection entry in the **Saved Sessions** list to automatically connect, authenticate, and open a terminal session, without you having to type your username and password each time:



Note that if you haven't already authenticated via Kerberos you'll be asked to enter your Kerberos credentials the first time you run PuTTY after you start your computer.