

IIS Easy Migration Tool (For IIS 7, 8, 10) – Quick Start Guide

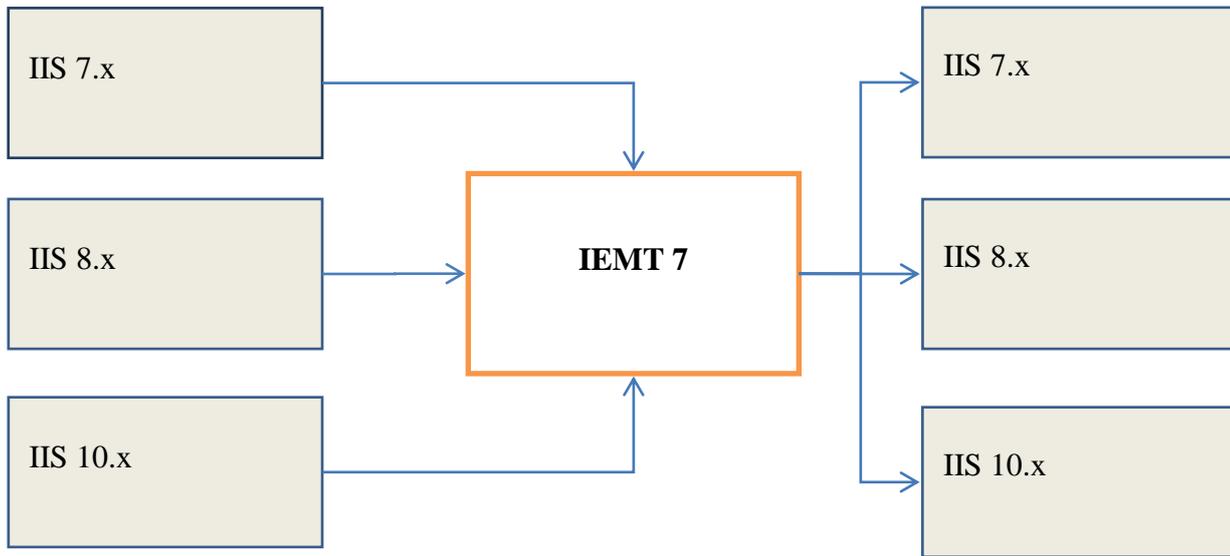
Table of contents

The purpose of this software and its parts	1
Data sources.....	2
System requirements:	3
Software registration and evaluation	3
Source server: The first way of data collection – using the Gathering Agent.....	4
Source server: The second way of data collection – using the APPLICATIONHOST.CONFIG file.....	8
The command line version of the Gathering Agent	8
Destination server: The migration procedure	8
Step 1	10
IIS Security Scan	13
Step 2.....	15
Step 3.....	23
Step 4.....	24
Step 5.....	26
Step 6.....	27
Step 7.....	28
Step 8.....	29
Step 9.....	30
The IEMT Remote Connection function.....	32
Description and prerequisites.....	32
How to use the IEMT Remote Connection function	36
How to create the firewall rules for remote IEMT connection on the destination server	38
Troubleshooting.....	39

The purpose of this software and its parts

IIS Easy Migration Tool (IEMT) software helps with the *migration* from one Microsoft IIS server to another. It can also be used as IIS *backup, recovery and consolidation* tool.

IIS Easy Migration Tool for IIS 7, 8, 10 (IEMT 7) is able to migrate websites from IIS 7.0, 7.5, 8.0, 8.5 and 10.0 servers to IIS 7.0, 7.5, 8.0, 8.5 and 10.0 servers. It does not work with IIS 6.



(The former version of the IIS Easy Migration Tool (IEMT for IIS 6) is able to migrate websites from IIS 6.0 to IIS 6.0, 7.0, 7.5, 8.0, 8.5, 10.0. It is available at our website. You can purchase it if you are going to transfer websites from IIS 6 (Windows 2003).)

This application is portable, no installation is required.

The **IEMT 7** can:

- Transfer and consolidate items (websites, SSL certificates, FTP accounts, etc.) and data (website settings, etc.) between IIS 7/8/10 servers.
- Recover and consolidate IIS settings (IIS server itself and its websites etc.) from applicationHost.config file.
- Backup and recovery of IIS settings and items with **Gathering Agent (GA)** utility.

Data sources

The **IEMT 7** uses 2 data sources: applicationHost.config file and a data file created by Gathering Agent (GA) utility.

The **preferable** data source is the GA data file. This file contains all the needed data about the IIS items and settings. To get this file you should run Gathering Agent (GA) software on the source IIS server.

The applicationHost.config file contains incomplete information about the websites (and other IIS items like applications, virtual directories etc.), but it may be used for the IIS migration and/or recovery in case you do not have a GA data file for some reason.

Please note that applicationHost.config file does not contain any information about SSL certificates, Windows users and groups, NTFS permissions, thus these items cannot be migrated/recovered in full in case you use applicationHost.config file as the data source.

The applicationHost.config file can be used in disaster recovery cases, when the source server is offline and you cannot run the Gathering Agent utility on that server. **In all other cases we recommend using of the Gathering Agent utility.**

We also provide a command line version of the GA, it is designed to help with IIS related backup, recovery and consolidation tasks. Files created by this command line utility can be used for recovery and/or consolidation of IIS data (settings, items) on the same server or other servers.

*The Gathering Agent does not change anything on the server. It does not stop any websites, does not change any settings. It just collects the needed IIS related information. So, **it is safe to use the Gathering Agent on production servers.** The websites on your source server stay intact and unaltered.*

System requirements:

Source server: .NET framework 4.x is required for the Gathering Agent

Destination server: .NET framework 4.x is required for the IIS Easy Migration Tool.

*Note: The IEMT 7 is a GUI application, so currently it is not compatible with Server Core installation of Windows. You should either have **Full Installation** of Windows 2008, 2012 or Windows Server 2016 with **Desktop Experience**.*

Software registration and evaluation

It is possible to try the IEMT 7 for free. It works without a license key, but in the evaluation mode it allows to migrate only a few items of each kind during a single migration session. (For example, it may allow to migrate 3 websites, 4 virtual directories, 5 FTP accounts, 2 SSL certificates and 1 Windows User Group during the evaluation session.)

To register the software you need to buy a license key and write it to appropriate section of IEMT.exe.Config file. You can buy a key at <http://www.hoststools.com> The license key makes the software fully-functional and allows to migrate thousands of websites, Windows users etc. The amount depends on the license key you purchased. For example, a license key can have the following limit: “10000 websites, 10000 web applications, 10000 Windows users, 10000 SSL certificates, 10000 FTP accounts, 10000 virtual directories”.

Please note that IEMT connects to <http://keysys.hoststools.com/> (online licensing system) at the beginning of each session. So, please be sure the destination server firewall does not block port 80. IEMT sends its license key and gets a response (“valid” or “not valid”). Nothing else is sent or received.

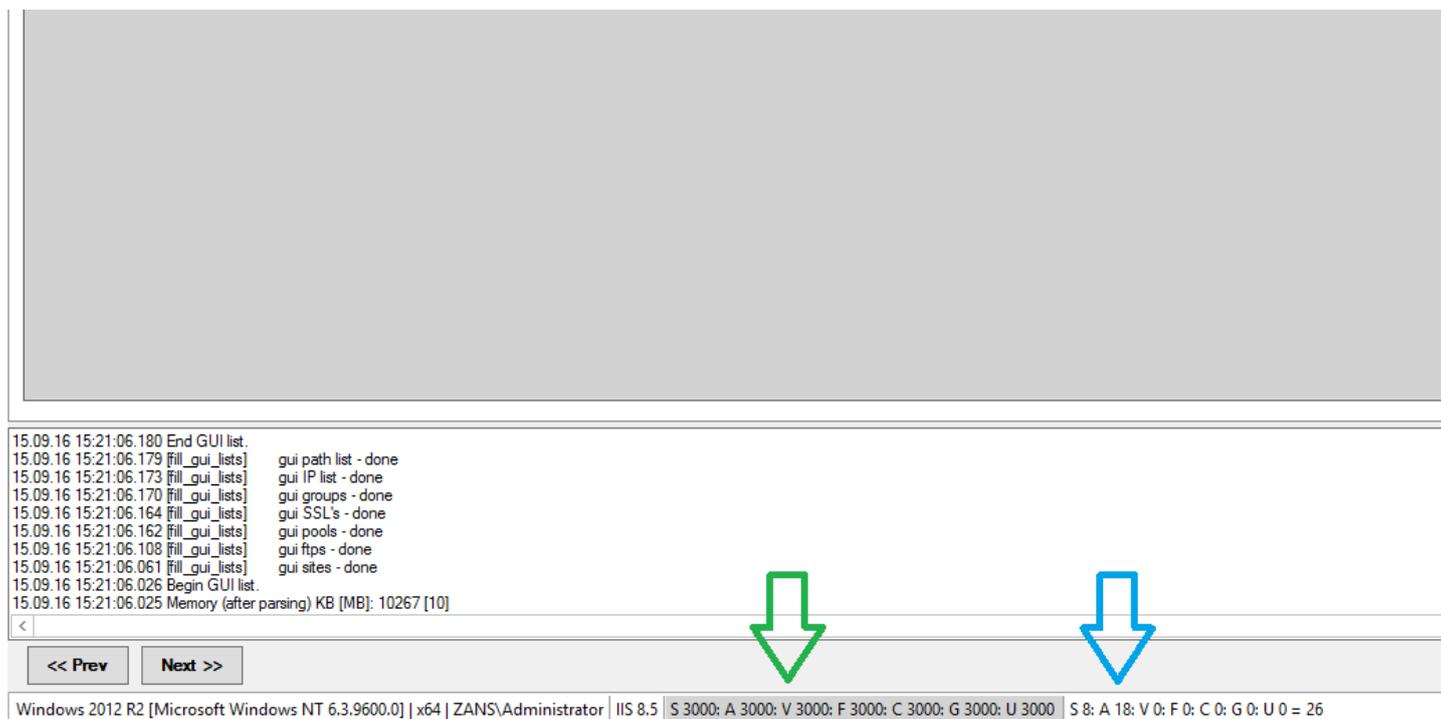
Please contact us if your destination server does not have Internet access. We have a solution.

When you have a key, please open **IEMT.exe.Config** file with the Notepad, find **1234** (between <value> and </value> tags of **ks_key** section) and replace the **1234** with your license key. **Then restart the IEMT 7.**

If there is “**Trial**” word in the IEMT window caption, the program is not registered and works in the evaluation mode.

During the migration process you select items to be migrated. The items are: websites, web applications, virtual directories, FTP accounts, SSL certificates, Windows users, Windows user groups. The IEMT status bar indicates how many items of each kind you selected and how many items you can migrate with your license key.

For example:



```
15.09.16 15:21:06.180 End GUI list.
15.09.16 15:21:06.179 [fill_gui_lists] gui path list - done
15.09.16 15:21:06.173 [fill_gui_lists] gui IP list - done
15.09.16 15:21:06.170 [fill_gui_lists] gui groups - done
15.09.16 15:21:06.164 [fill_gui_lists] gui SSL's - done
15.09.16 15:21:06.162 [fill_gui_lists] gui pools - done
15.09.16 15:21:06.108 [fill_gui_lists] gui ftps - done
15.09.16 15:21:06.061 [fill_gui_lists] gui sites - done
15.09.16 15:21:06.026 Begin GUI list.
15.09.16 15:21:06.025 Memory (after parsing) KB [MB]: 10267 [10]
```

< << Prev Next >>

Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | IIS 8.5 | S 3000: A 3000: V 3000: F 3000: C 3000: G 3000: U 3000 | S 8: A 18: V 0: F 0: C 0: G 0: U 0 = 26

The IEMT status bar shows that the license key allows to migrate 3000 websites, 3000 web applications and so on (the green arrow). It also shows that 8 websites and 18 web applications are going to be migrated during the current session (the blue arrow).

The Gathering Agent does not need any license key. Only the IEMT needs it.

Source server: The first way of data collection – using the Gathering Agent

Log in to your source IIS server and place the Gathering agent files to some folder. Then start **ga.exe as Administrator**. (There is also a command line version of the Gathering Agent – **gacmd.exe**)

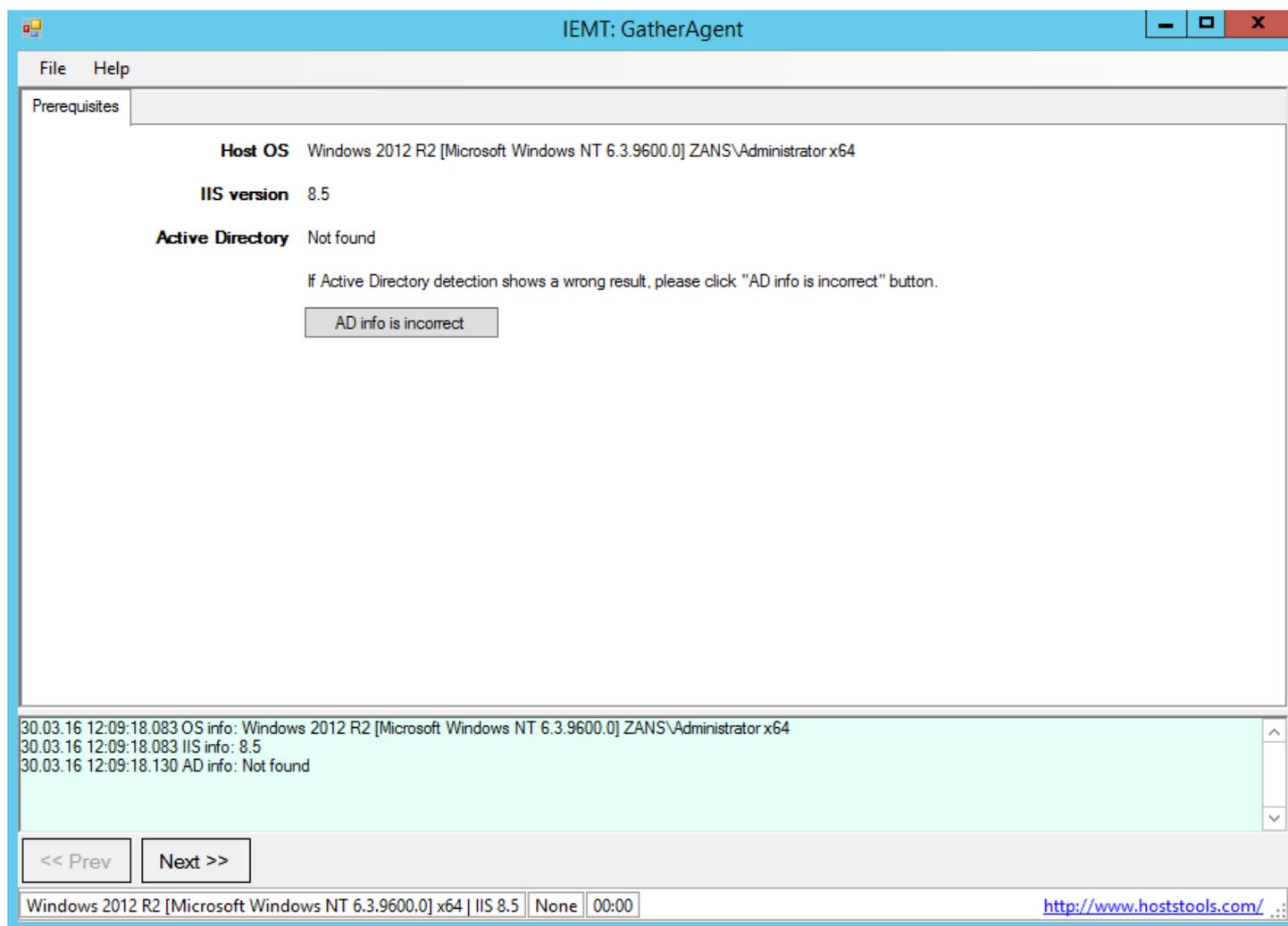
*It is important to run the Gathering Agent as Administrator. You must be logged on as a local administrator or provide the credentials of a member of the **local Administrators group**.*

You can log on as a domain administrator too. Usually it works. But it depends on your domain/server settings and is not guaranteed. So, it is better to use a local admin account.

To run an application with a full administrator access token:

1. Locate the program icon or a shortcut in Windows Explorer.
2. Right-click the program icon or shortcut, and then click **Run as administrator**.
3. When the UAC message is displayed, do one of the following:
 - If you are logged on as a standard user, or if UAC is configured to always require credentials, enter the appropriate administrative credentials, and then click **OK**.
 - If you are logged on as an administrator and UAC is not configured to always require credentials, click **Yes** to start the application.

When you start GA.EXE (the GUI version of the Gathering Agent) it first collects and shows the server system information. IIS and OS along with Active Directory information can be found there.

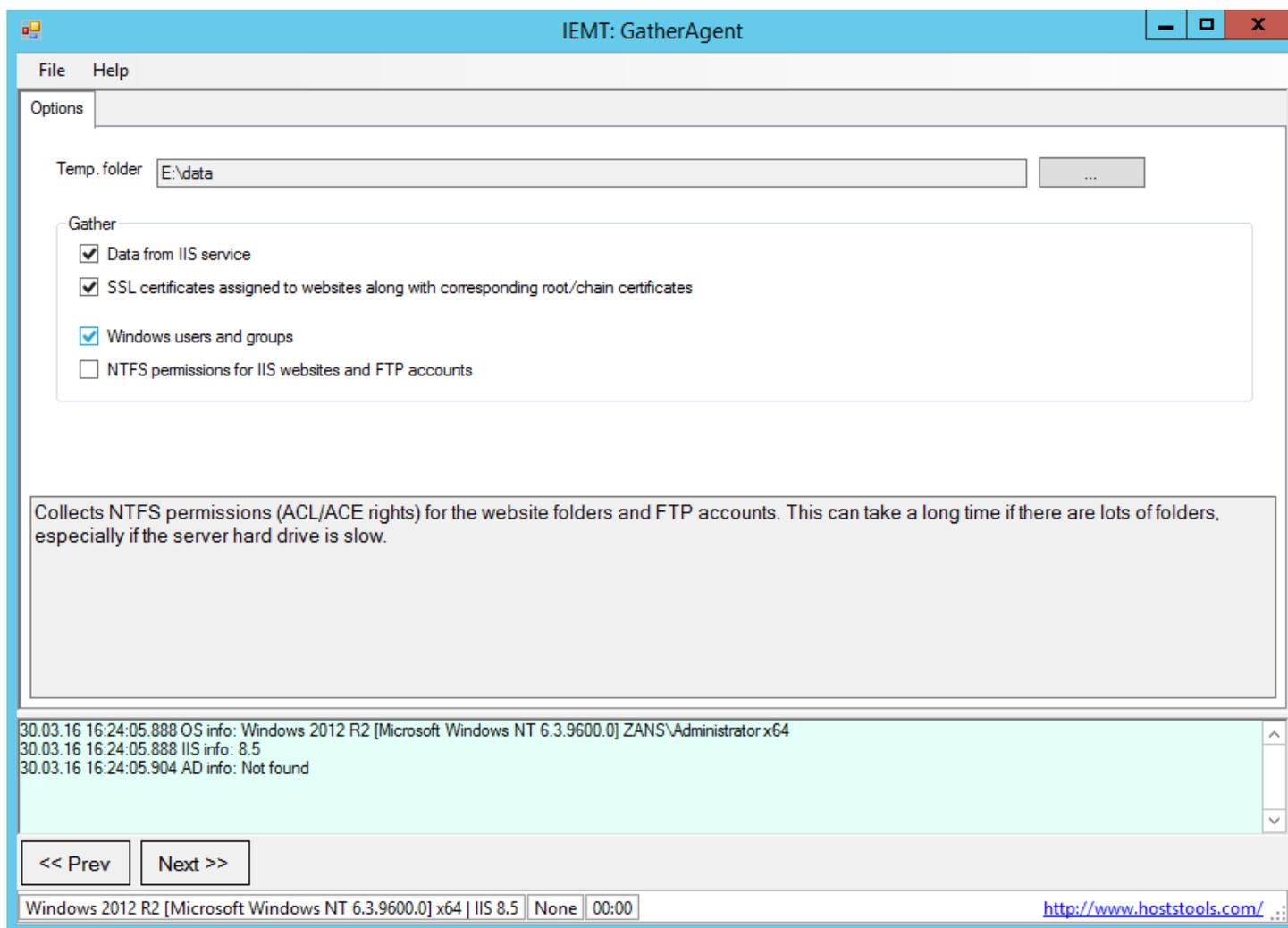


Pay attention to the Active Directory information displayed by the Gathering Agent. If it is incorrect, click [AD info is incorrect] button. It is an **important step** needed for the correct Windows/FTP account migration and also anonymous website user assignments on the destination IIS server.

*NOTE: If there are Active Directory users assigned to any websites and/or FTP accounts/directories it may take **noticeable amount of time** to collect the data. Please wait till the Gathering Agent finishes its job.*

***Do not interrupt it!** We know the cases when the data collection took 12 and more hours. It is normal if Active Directory is involved.*

Click **Next** button to go to the next step.



Here you select the data collection options:

Temp. Folder – directory for temporary files.

Data from IIS service – collect data from IIS service.

SSL certificates assigned to websites along with corresponding root/chain certificates – collect SSL certificates assigned to websites and also the corresponding root/chain SSL certificates (if needed).

Windows users and groups – collect Windows users and groups related data.

NOTE: There is no way to collect the current passwords of Windows (and FTP) users! (Because Windows keeps only hashes, not the passwords.) The IEMT will generate new strong passwords for all the migrated users and saves the list of those users and their new passwords in a file. (See below in this document for more information.)

*NOTE: If there are Active Directory users assigned to any websites and/or FTP accounts/directories it may take **noticeable amount of time** to collect the data. Please wait till the Gathering Agent finishes its job. **Do not interrupt it!** We know the cases when the data collection took 12 and more **hours**. It is normal if Active Directory is involved.*

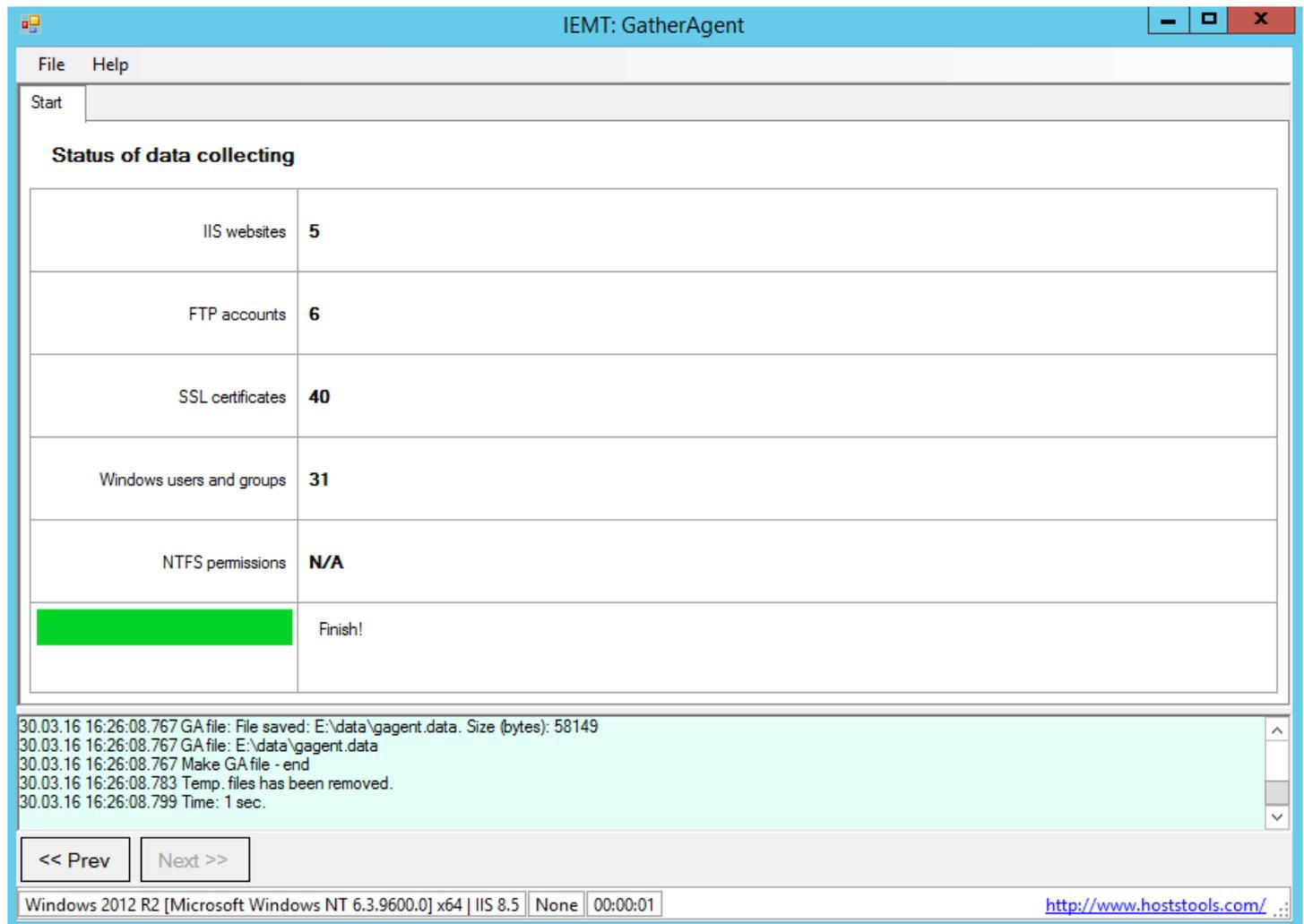
NTFS permissions for IIS websites and FTP accounts – collect all NTFS permissions for directories of IIS websites and FTP accounts.

NOTE: If there are many directories and files the GA may need few hours to collect the data. Also the resulting data file can be huge.

Select the needed options and click **Next** button. At the next page click **Start** button and wait till the Gathering Agent finishes the data collection task.

The Gathering Agent analyzes data of **all available** web.config files of websites on the source server. Thus, the IEMT can copy the websites settings to the destination server or recover them on the source server.

However some collisions may happen in rare cases. For example, if Microsoft SharePoint has different settings on the source and destination servers, the migrated website (or its part) may show error messages.



The screenshot shows the IEMT: GatherAgent application window. The title bar reads "IEMT: GatherAgent". The window has a menu bar with "File" and "Help". Below the menu bar is a "Start" button. The main area is titled "Status of data collecting" and contains a table with the following data:

IIS websites	5
FTP accounts	6
SSL certificates	40
Windows users and groups	31
NTFS permissions	N/A
	Finish!

Below the table is a log window showing the following text:

```
30.03.16 16:26:08.767 GA file: File saved: E:\data\gagent.data. Size (bytes): 58149
30.03.16 16:26:08.767 GA file: E:\data\gagent.data
30.03.16 16:26:08.767 Make GA file - end
30.03.16 16:26:08.783 Temp. files has been removed.
30.03.16 16:26:08.799 Time: 1 sec.
```

At the bottom of the window, there are navigation buttons: "<< Prev" and "Next >>". The status bar at the very bottom shows "Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] x64 | IIS 8.5 | None | 00:00:01" and a URL "http://www.hoststools.com/".

When the Gathering Agent finished its job, it shows “Finish!” word at the right column near the progress bar. Also it shows the time spent for the data collection in the log.

The resulting data file with collected IIS information – **gagent.data** – will be saved in the same folder with the EXE file of the Gathering Agent. You need to copy this file to the destination server for the websites (FTP etc.) migration or to a backup server if just need a backup copy of your IIS server data.

NOTE: The Gathering Agent (nor the IEMT) does not backup any files (except SSL certificates if that option is turned on)! It just collects IIS server and related items settings. If you need to backup, restore and copy website files (ASPX, HTML, JPG etc.) you need to use specialized backup and recovery software.

Source server: The second way of data collection – using the APPLICATIONHOST.CONFIG file

This way should be used only if there is no possibility to use the first way. For example, if the source server is down.

It is a 1-stage way: Just copy **APPLICATIONHOST.CONFIG** file from the source server (or a backup copy) to the destination server. This file can be found in C:\Windows\System32\inetsrv\config\ folder usually. This file will be used by IEMT as a source data file.

Please note that SSL certificates and bindings for HTTPS parameters of web sites will not be migrated if you use applicationHost.config file. If you need to migrate them you must use the Gathering Agent.

The command line version of the Gathering Agent

There is also a command line version of the Gathering Agent – **gacmd.exe**

Usage:

```
gacmd.exe [/f=path-to-agent.data] {/i | /s | /u | /n | /a=y|n}
```

Command line switches:

/f - path and file name where the collected data should be saved. Default: [CURRENT-FOLDER]\gagent.data

/i - get data from IIS service

/s - get SSL cert. assigned to websites along with corresponding root/chain cert.

/u - get Windows users and groups

/n - get NTFS permissions for IIS websites and FTP accounts

/a - is this server connected to ActiveDirectory or not. Possible values: y - Yes, n - No. Default: n

Destination server: The migration procedure

To start the migration you should have either **gagent.data** or **applicationHost.config** file. Please read above how to get them.

***Very Important Note:** The IEMT does not copy any files (.html, .aspx, .php, etc.) from the source server to the destination one! It does lots of useful things (creates the web sites and Windows users, sets the ACL/NTFS permissions and so on), but it does not copy the files. So, please, use some other software to copy the files first. It is possible to use WinZIP or WinRAR to zip the files/folders on the source server, copy the archive by FTP and unzip/unrar it on the destination server. Then run the IEMT, it will create the sites and set the permissions on those folders.*

*So, please, **first copy the files** (with any backup/restore software) **then run the IEMT.***

Important Note:

The IEMT does not install frameworks and applications to servers. It will not install ASP.NET, .NET, PHP, ColdFusion, TomCat (Java) etc. So, if your websites need such frameworks, you should install them yourself.

Also the IEMT does not update installed frameworks.

For example, if you have PHP 5 installed on your destination server but a migrated website needs PHP 7, the IEMT will specify "PHP 7" handler in that website properties, but it will not install PHP 7 on your server. You should install it yourself.

Copy the IEMT files to some folder on the destination server and start IEMT.

*It is important to run the IIS Easy Migration Tool as Administrator. You must be logged on as a local administrator or provide the credentials of a member of the **local Administrators group**.*

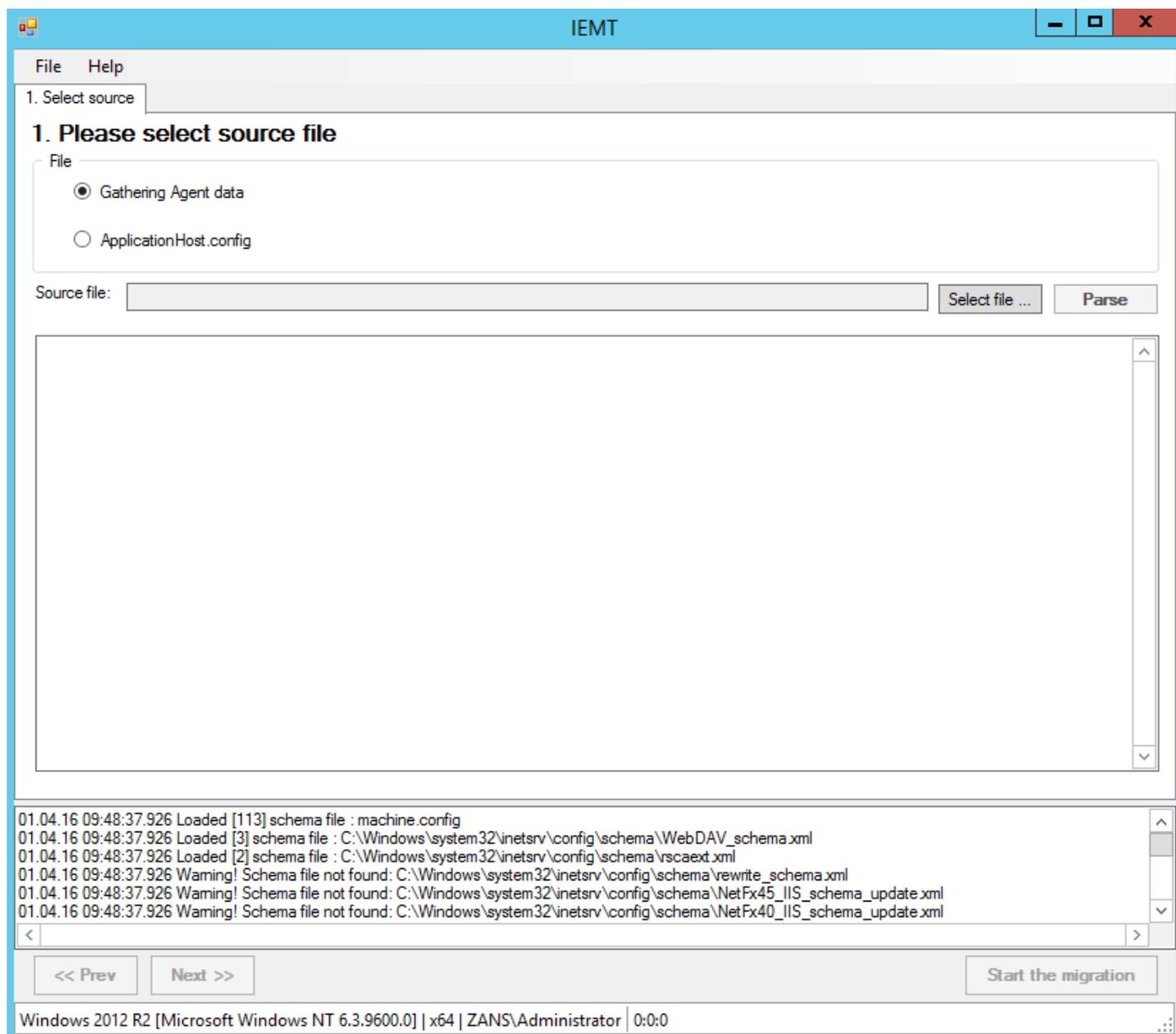
You can log on as a domain administrator too. Usually it works. But it depends on your domain/server settings and is not guaranteed. So, it is better to use a local admin account.

To run an application with a full administrator access token:

1. Locate the program icon or a shortcut in Windows Explorer.
2. Right-click the program icon or shortcut, and then click **Run as administrator**.
3. When the UAC message is displayed, do one of the following:
 - If you are logged on as a standard user, or if UAC is configured to always require credentials, enter the appropriate administrative credentials, and then click **OK**.
 - If you are logged on as an administrator and UAC is not configured to always require credentials, click **Yes** to start the application.

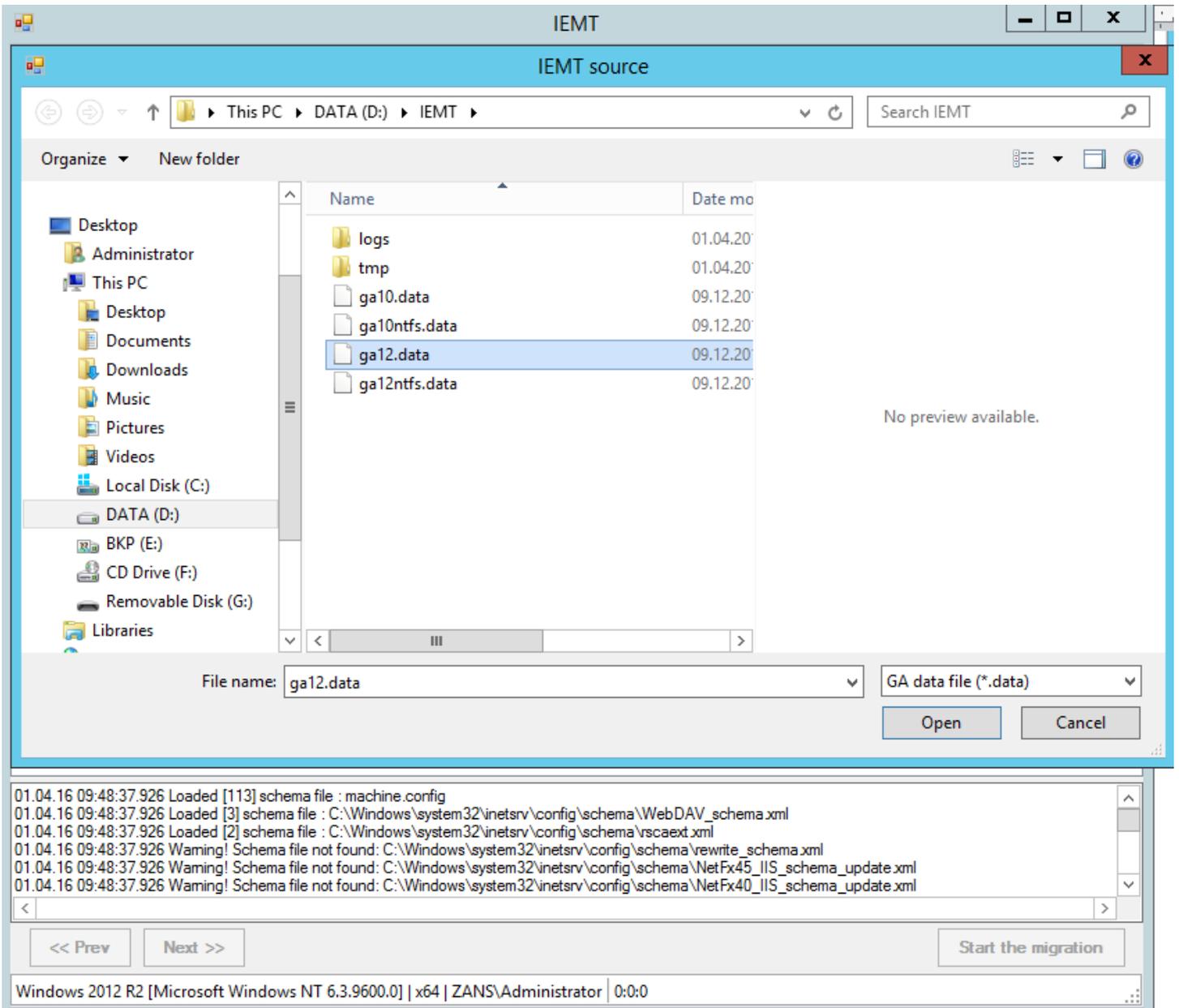
The program will detect the OS version and show it in the status bar.

Step 1

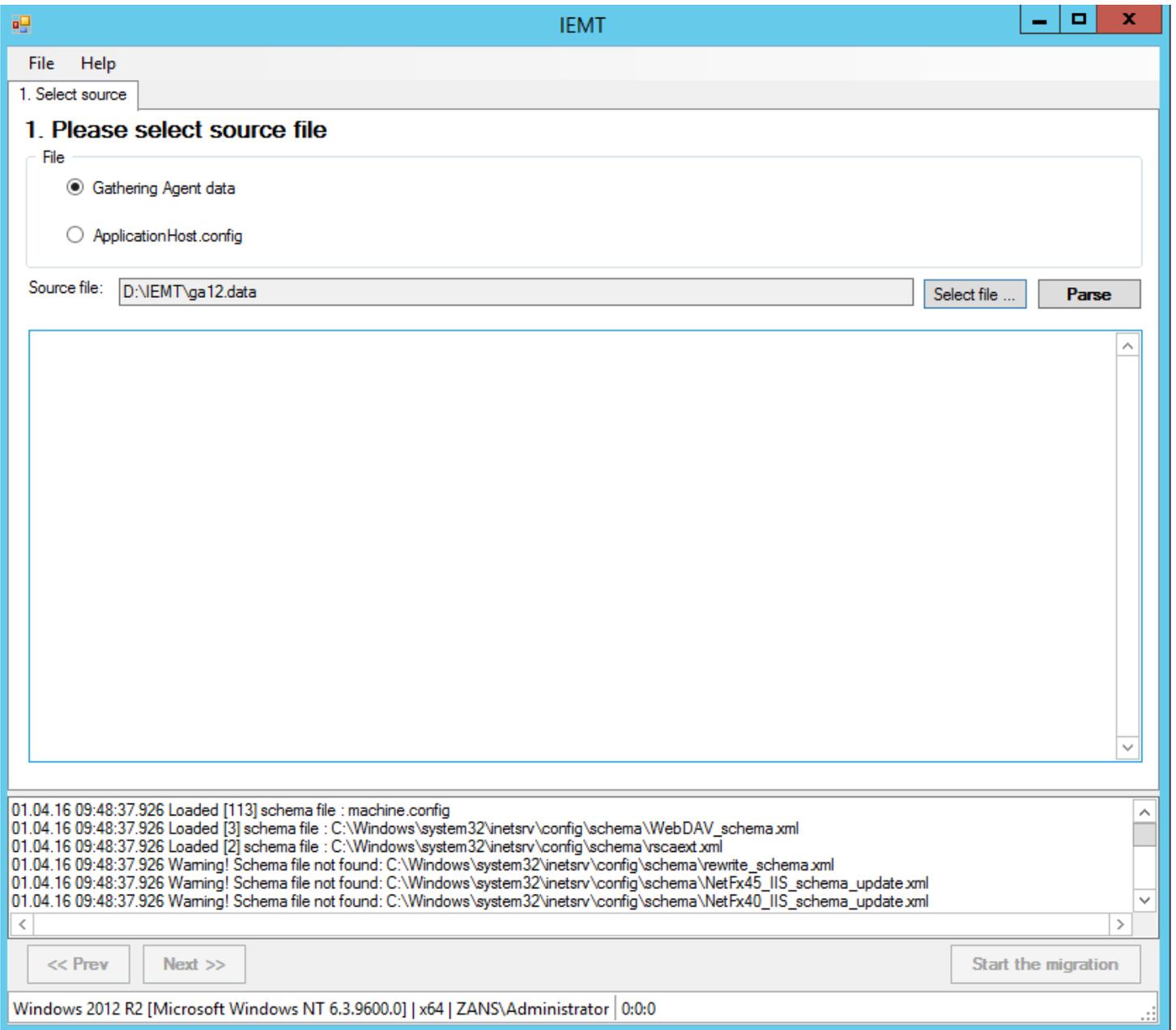


At the beginning the GA software analyzes all available configuration files of IIS and Microsoft .NET Framework installed on the server. It may take a noticeable amount of time, but it is a necessary step for the correct migration. It also allows using the new features of IIS and .NET Framework in full.

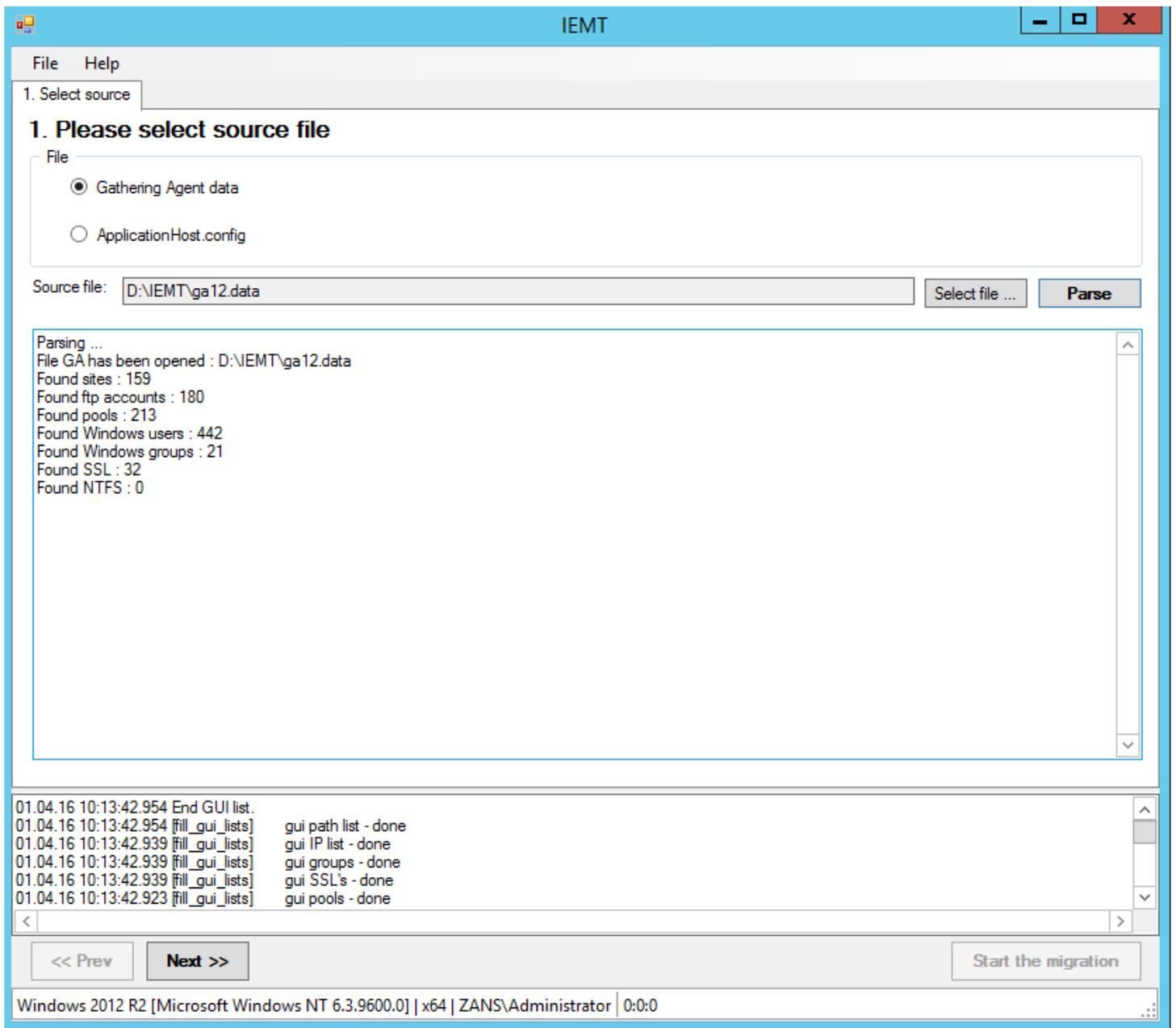
Select the data source type and click *Select file ...* button.



Select the data source file and click *Open*.



Click ***Parse*** button to start the source data analysis.



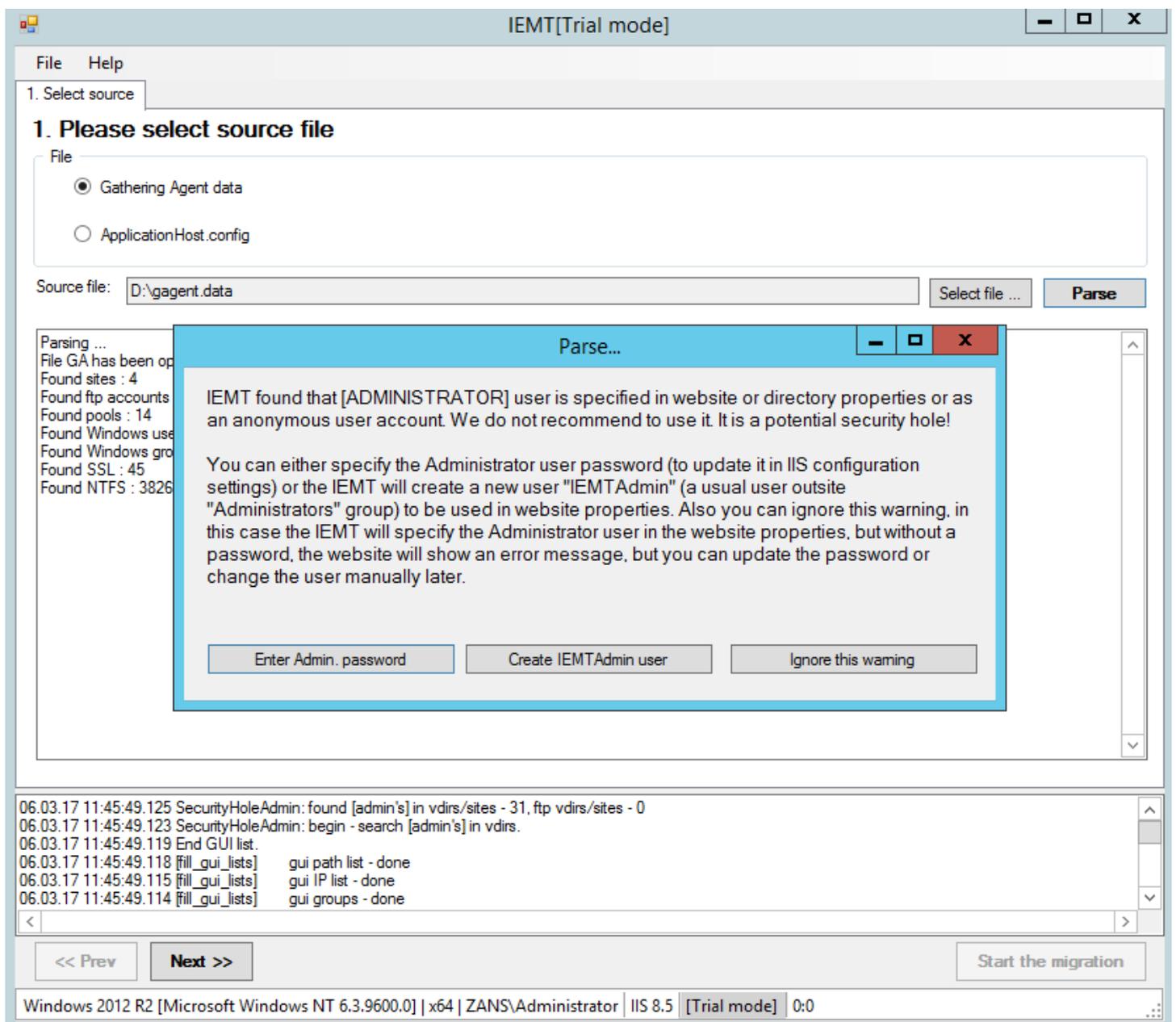
Once the parsing is finished you will see some stats. Click *Next* button to go to the next step.

IIS Security Scan

We noticed that some engineers use *Administrator* user (or other users from *Administrators* group) as an *anonymous user* or *Connect As* user.

It is a potential security hole!

If the IEMT finds that *Administrator* user is specified in website or directory properties or as an anonymous user account it shows the following dialog window and asks to make a choice.



You can either specify the *Administrator* user password (to update it in IIS configuration settings) or the IEMT will create a new user *IEMTAdmin* (a usual user outside *Administrators* group) to be used in website properties. Also you can ignore this warning, in this case the IEMT will specify the *Administrator* user in the website properties, but without a password, the website will show an error message, but you can update the password or change the user manually later.

- **Enter Admin. Password** — click this button if you want to specify the *Administrator* user password to be saved in IIS settings.

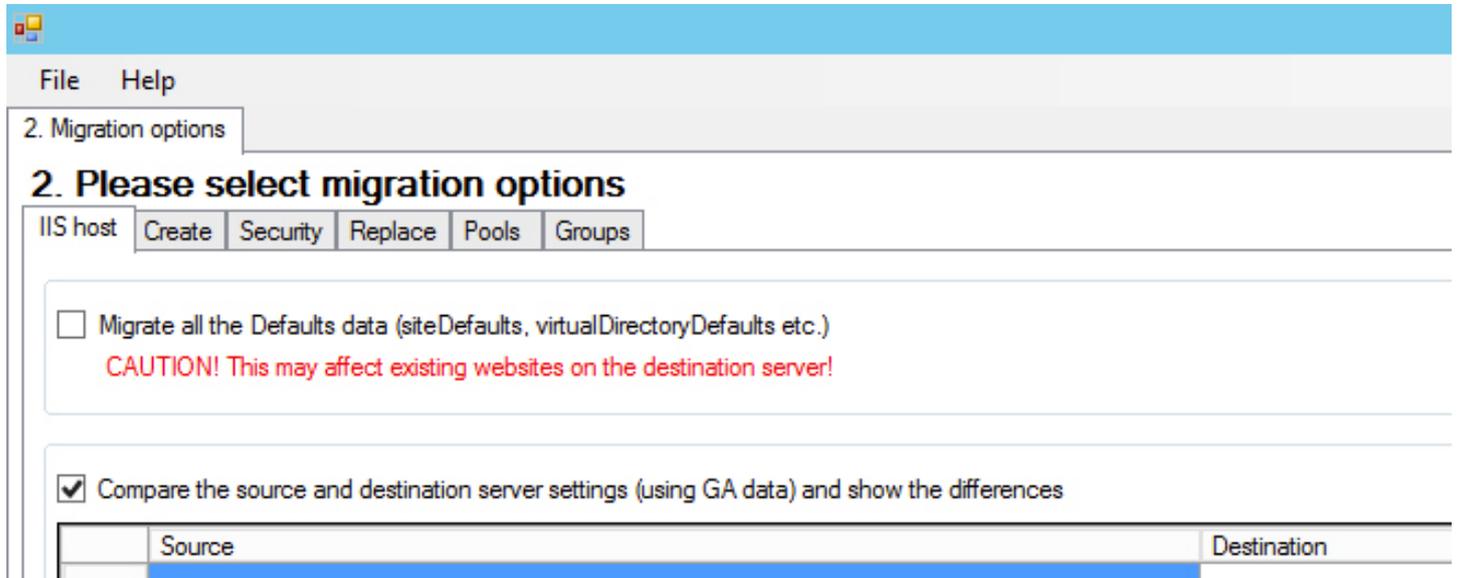
We do not recommend doing this! It is potential security hole!

- **Create IEMTAdmin user** — click this button if you want the IEMT to create a new user *IEMTAdmin* (a usual user outside *Administrators* group) to be used in website properties. This user will have **Read** NTFS permissions only (not Write or Modify). Later you can manually change the permissions. Also you can include *IEMTAdmin* user to *Administrators* group manually, but we do not recommend to do that!
- **Ignore this warning** — click this button to ignore this warning. The IEMT will copy the configuration from the source server “as is”. The *Administrator* user will be specified in appropriate website(s)

properties without a password. The website(s) will show error messages, so you should fix it manually later by assigning some other user (or specifying *Administrator* user password).

Step 2

This step is for the migration process settings and fine tuning.



There are several tabs allowing to set/select/tune multiple parameters:

- **IIS host** (server level IIS settings),
- **Create** (entities to be created on the destination server),
- **Security** (IIS security related settings),
- **Replace** (to change paths, IP addresses, etc.),
- **Pools** (Application pools related settings),
- **Groups** (Windows user groups related settings).

Step 2. IIS host tab

IIS host tab:

Turn on **Migrate all the Defaults data ...** check box if you wish to migrate server level IIS Defaults settings (siteDefaults, virtualDirectoryDefaults etc.).

CAUTION! This may affect existing websites on the destination server!

Turn on **Compare the source and destination server settings (using GA data) and show the differences** checkbox and the IEMT will show you the differences between the source and destination server settings before the migration starts. So, you can change your mind.

File Help

2. Migration options

2. Please select migration options

IIS host Create Security Replace Pools Groups

Migrate all the Defaults data (siteDefaults, virtualDirectoryDefaults etc.)
CAUTION! This may affect existing websites on the destination server!

Compare the source and destination server settings (using GA data) and show the differences 38

Source	Destination	Difference
system.webServer/defaultDocument/files/add value=index.php	not found	
system.webServer/fastCgi/application fullPath=C:\Program Files (x86)\PHP\php-cgi.exe,activityTimeout=600,requestTimeout=600,instanceMaxRequests=10000	Attr not found	File or path not found: C:\Program Files (x86)\PHP\php-cgi.exe
system.webServer/fastCgi/application/environmentVariables/environmentVariable name=PHP_FCGI_MAX_REQUESTS,value=10000	Item not found.	
system.webServer/fastCgi/application/environmentVariables/environmentVariable name=PHPRC,value=C:\Program Files (x86)\PHP\	Item not found.	
system.webServer/globalModules/add name=SharePoint14Module,image=C:\Program Files\Microsoft Shared\Web Server Extensions\14\isapi\owssvr.dll,preCondition=appPoolName=SharePoint Central Administration	Extension: not equal attrs.	preCondition=appPoolName=SharePoint Central Administration v4; intranet80
system.webServer/httpLogging dontLog=false	Item not found.	
system.webServer/isapiFilters/filter name=ASP.Net_2.0_for_V1.1,path=%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_filter.dll	not found	File or path not found: %windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_filter.dll
system.webServer/security/authentication/windowsAuthentication enabled=true	found	
system.webServer/security/isapiCgiRestriction/add path=C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll,allowed=true,groupId=ASP.NET v4.0.30319 (32-bit),description=ASP.NET v4.0.30319 (32-bit)	system.webServer/security/isapiCgiRestriction/add path=C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll,allowed=true,groupId=ASP.NET v4.0.30319 (32-bit),description=ASP.NET v4.0.30319 (32-bit)	groupId=ASP.NET v4.0.30319 (32-bit) description=ASP.NET v4.0.30319 (32-bit)
system.webServer/security/isapiCgiRestriction/add path=C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll,allowed=true,groupId=ASP.NET v4.0.30319 (32-bit),description=ASP.NET v4.0.30319 (32-bit)	system.webServer/security/isapiCgiRestriction/add path=C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll,allowed=true,groupId=ASP.NET v4.0.30319 (32-bit),description=ASP.NET v4.0.30319 (32-bit)	groupId=ASP.NET v4.0.30319 (32-bit) description=ASP.NET v4.0.30319 (32-bit)
system.webServer/staticContent/mimeMap fileExtension=.323,mimeType=text/h323		
system.webServer/staticContent/mimeMap		

```

05.04.17 14:17:40.615 SecurityHoleAdmin: end - search [admin's] in vdirs.
05.04.17 14:17:40.614 SecurityHoleAdmin: found [admin's] in vdirs/sites - 0
05.04.17 14:17:40.609 SecurityHoleAdmin: begin - search [admin's] in vdirs.
05.04.17 14:17:40.605 End GUI list.
05.04.17 14:17:40.604 fill_gui_lists) gui AD users - done
05.04.17 14:17:40.598 fill_gui_lists) gui path list - done
05.04.17 14:17:40.595 fill_gui_lists) gui IP list - done
05.04.17 14:17:40.593 fill_gui_lists) gui groups - done
05.04.17 14:17:40.587 fill_gui_lists) gui SSL's - done
05.04.17 14:17:40.586 fill_gui_lists) gui pools - done

```

<< Prev Next >>

Start the migration

Windows 2012 R2 | Microsoft Windows NT 6.3.9600.0 | x64 | ZANS\Administrator | IIS 8.5 | S 3000: A 3000

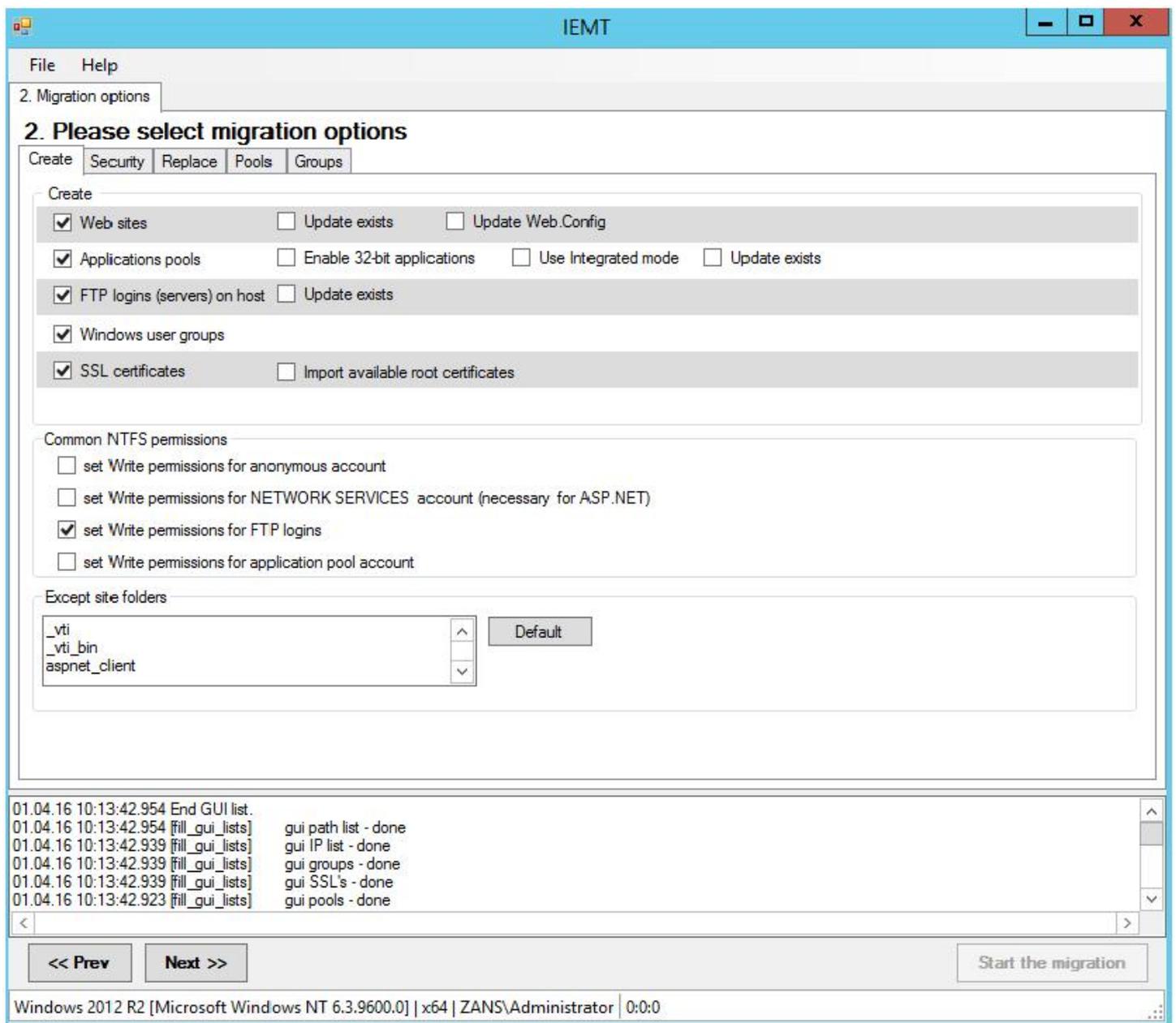
In the comparison table you can see the difference of the IIS settings between the source and destination server. Please pay attention to this list.

This list contains the server level settings only, not website (web application, virt. dir.) level!

The IEMT shows all the differences it finds, but some of them may be inessential. For example, default application pool names may be different, but it does not affect IIS work. Also some MIME types (for example, video/x-msvideo and video/avi) may look different, but work the same way. Use this comparison list as a guide, but make your own decisions based on your qualification.

The IEMT compares the server level settings of IIS and checks if appropriate files exist on the destination server. But the IEMT does not install frameworks and other software. It will not install ASP.NET, .NET, PHP, ColdFusion, TomCat (Java) etc. So, if your websites need such frameworks, you should install them yourself.

Step 2. Create tab



Create tab:

- Should IEMT create web sites?
- Should IEMT create application pools?
- Should IEMT create FTP accounts?
- Should IEMT create Windows users (and groups)? *This option is only available when Gathering Agent data is used.*
- Should IEMT migrate SSL certificates? *This option is only available when Gathering Agent data is used.*

Additional options for fine tuning:

Update existing – If this option is **off**: if some object (website, app pool, FTP account etc.) already exists on the destination server it will be removed and then recreated from scratch with the properties taken from the source server. If this option is **on**: if some object already exists on the destination server its properties will be **updated** according to the data from the source server with an “overwrite” rule. If the object does not have some property it will be **added**. If it has some new property (missing on the source server) this property stays the same.

Upgate Web.Config – **IMPORTANT! This option allows to create or update web.config files of the migrated (or recovered) websites!** If this option is **off**: The IEMT ignores data of web.config files collected on the source server.

Enable 32-bit applications – enable (force) 32-bit mode in migrated application pools.

Use Integrated mode – enable (force) Integrated mode in migrated application pools.

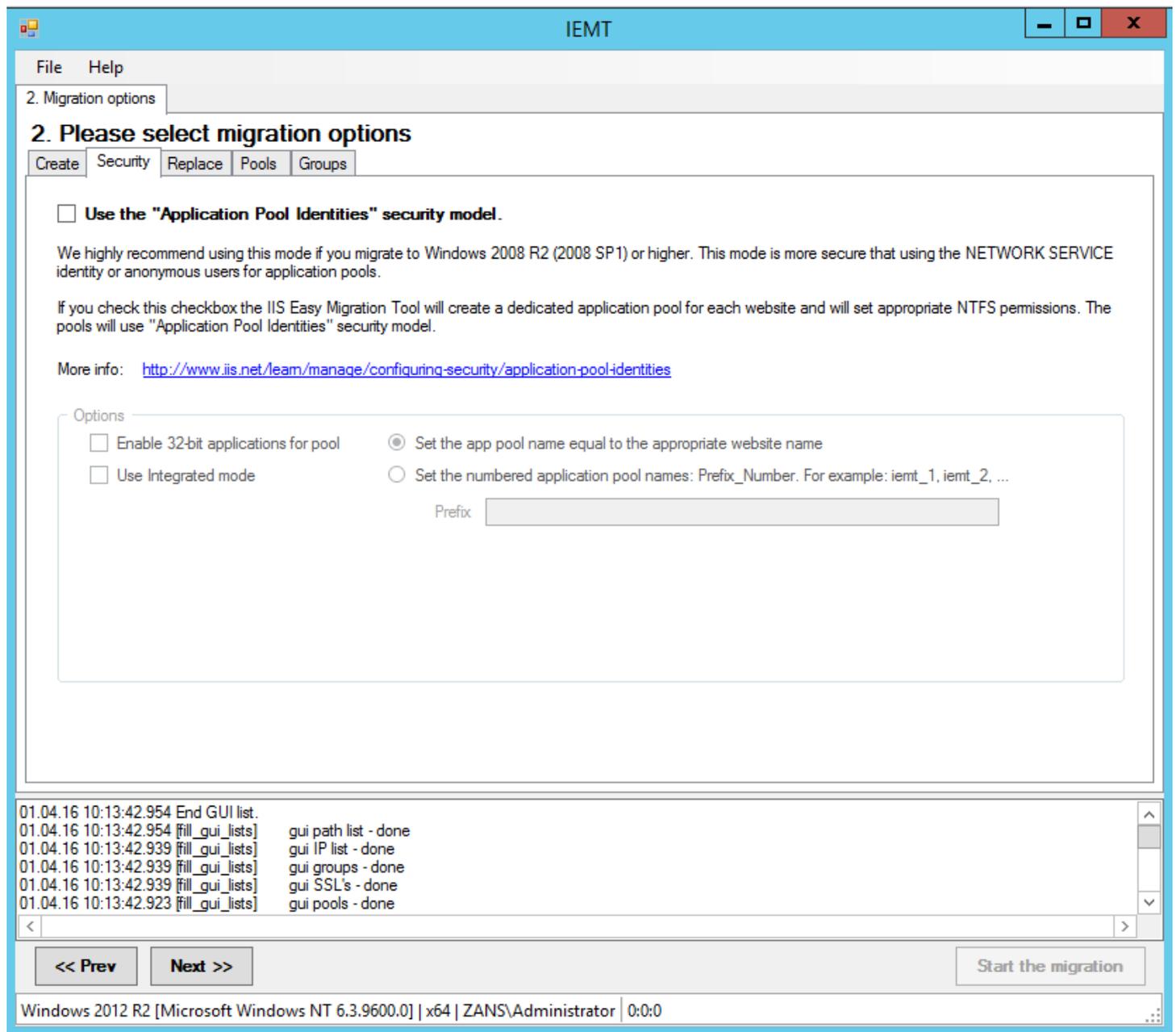
Import available root certificates – install available root SSL certificates to the destination server store.

NTFS part allows to select the permissions for site and FTP folders. Also you can set Write permissions for Application Pool account if ***Application Pool Identities*** security model was selected on ***Security*** tab.

In ***Except site folders*** list you can select those folders that should not be created. The ***Default*** button resets the list.

Step 2. Security tab

The **Security** tab helps to improve the server security by using the modern “**Application Pool Identities**” security model.



*Note! The **Security** and **Pools** tabs are mutually exclusive. If you use one of them, another one will be disabled automatically.*

If you enable the “**Application Pool Identities**” security model the IEMT will create a dedicated application pool for each web site and application. You can tune the dedicated pools properties with the **Options** group:

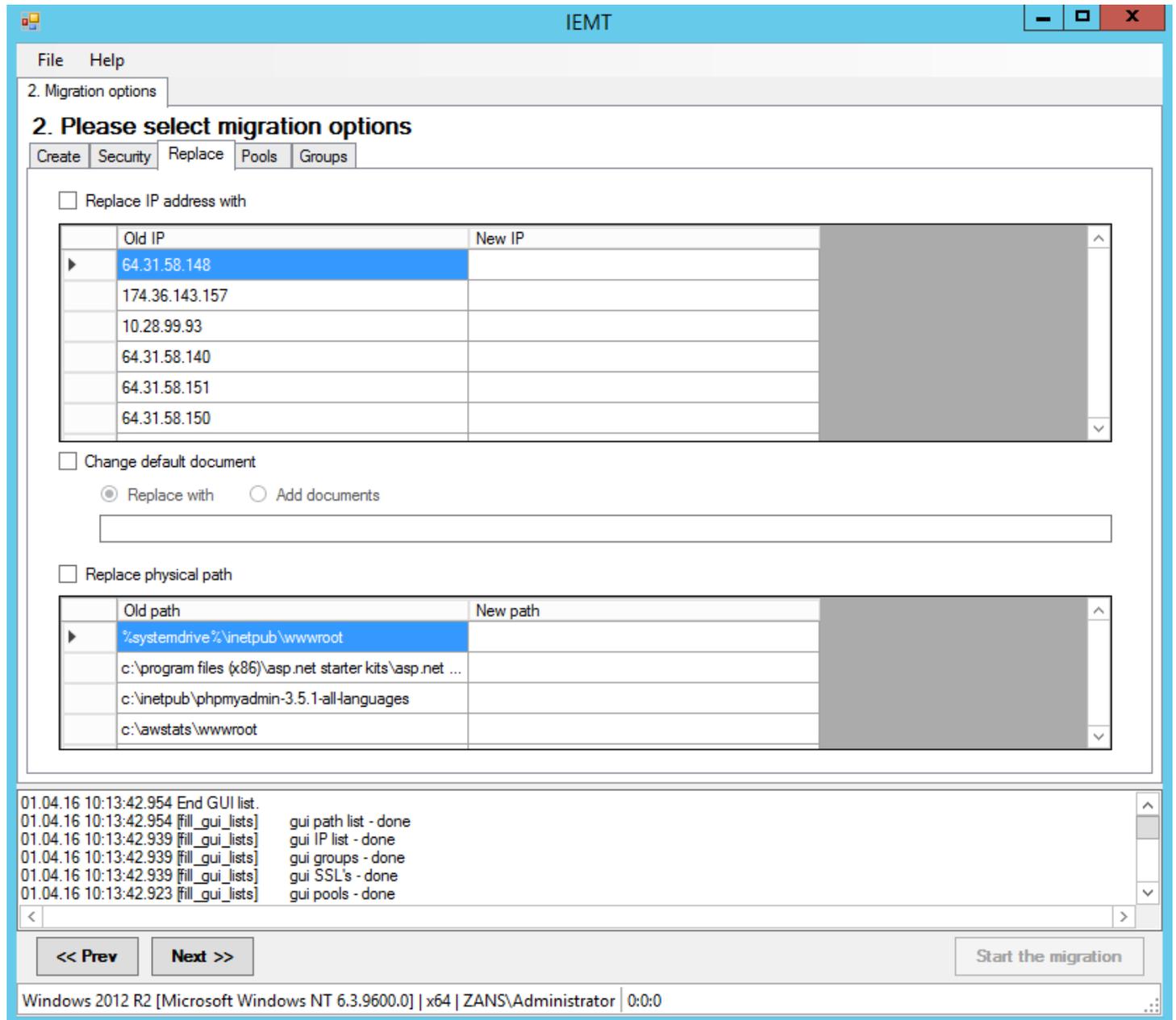
Set the app pool name equal to the appropriate website name — the dedicated pool name will be the same as the site name. E.g. “MyFunnySite.com” website will be placed to a new dedicated pool named “MyFunnySite.com”. If the pool with that name already exists, the site will be placed to that existing pool. For virtual directories the pool name contains the site name and the dir name separated by dash. E.g. “MyFunnySite.com/images” virtual directory will have “MyFunnySite.com-images” dedicated pool.

Set the numbered application pool names — the new pool names will begin with a word specified in the **Prefix** field and end with a unique number (GUID). For example, if you set the **Prefix**: *NewPools*, one of the pool names can be *NewPools_19195a5b6da011d0afd300c04fd930c9*

Enable 32-bit applications for pool — turn this on if you wish to allow 32-bit applications in these pools.

Use Integrated mode — enable “Integrated” .NET Framework mode. The default mode is “Classic”.

Step 2. Replace tab



Replace tab is for several different replacement options:

IEMT can replace old **IP addresses** (in the IIS sites properties, host headers, ...) with the new ones. At this tab you can see the list of the old IP addresses found in GA data (or applicationHost.config). Specify the new IP addresses if needed.

The **Default Documents** can also be changed. Use a comma to separate the document names.

The site **Physical path** can also be changed.

The **Physical path** will be replaced only if the **New path** field is not empty. The regular expressions in the .NET Framework style can be used in the **Old path** field. More info about the regular expressions: <https://msdn.microsoft.com/en-us/library/az24scfc%28v=vs.110%29.aspx>

Step 2. Pools tab

File Help

2. Migration options

2. Please select migration options

Create Security Replace **Pools** Groups

Assign dedicated pools to the sites. (The pools will also be renamed according to the rules specified at "Options" section.)

Options

Enable 32-bit applications for pool

Use Integrated mode

Set the app pool name equal to the appropriate website name

Set the numbered application pool names: Prefix_Number. For example: iemt_1, iemt_2, ...

Prefix

01.04.16 10:13:42.954 End GUI list.
01.04.16 10:13:42.954 [fill_gui_lists] gui path list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui IP list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui groups - done
01.04.16 10:13:42.939 [fill_gui_lists] gui SSL's - done
01.04.16 10:13:42.923 [fill_gui_lists] gui pools - done

<< Prev Next >> Start the migration

Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | 0:0:0

With the controls of the **Pools** tab you can create dedicated application pools for each web site (and virtual directory).

*To enable the **Pools** tab you can turn off **Use the Application Pool Identities** checkbox on **Security** tab. These tabs are mutually exclusive.*

The fields/controls on this tab are similar to the ones on the **Security** tab. Look at the **Security** tab description for more info, please.

Step 2. Groups tab

File Help

2. Migration options

2. Please select migration options

Create Security Replace Pools **Groups**

Windows groups for

Web accounts
IIS_IUSRS

FTP accounts
-- NONE --

Create group

Group name

Description

Create

```
01.04.16 10:13:42.954 End GUI list.
01.04.16 10:13:42.954 [fill_gui_lists] gui path list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui IP list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui groups - done
01.04.16 10:13:42.939 [fill_gui_lists] gui SSL's - done
01.04.16 10:13:42.923 [fill_gui_lists] gui pools - done
```

<< Prev Next >> Start the migration

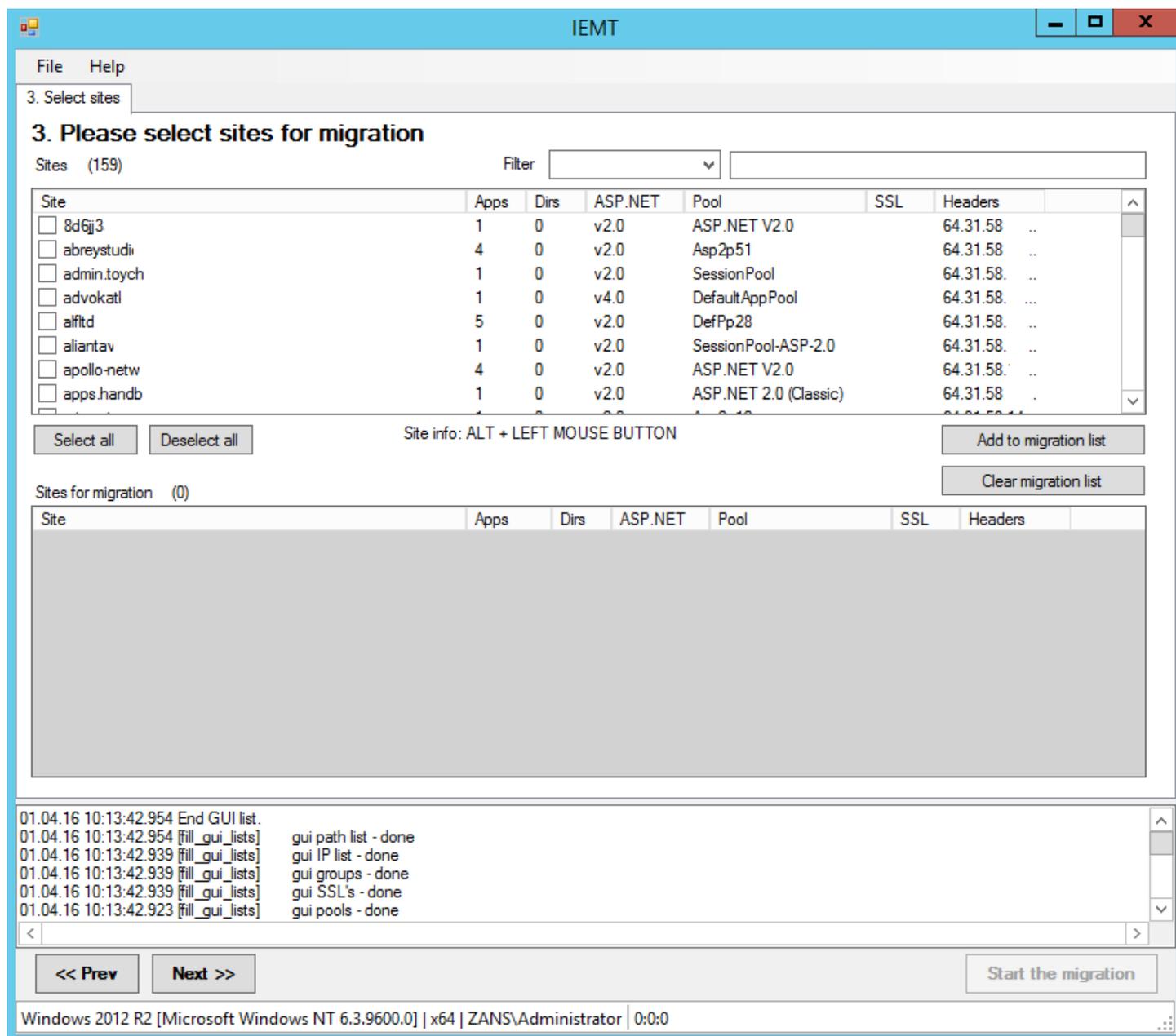
Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | 0:0:0

Groups tab is for selecting of groups for FTP accounts and anonymous web users. It is also possible to create a Windows group directly from this tab, just use **Create** button after specifying the group name.

Click **Next** button to go to the next step.

Now you can select the web sites to be migrated. If you need them all, just click **Select all** button.

Step 3



Select a site or several sites and click **Add to migration list** button. Repeat this as many times as you need. Use **Filter** fields to find sites by different criteria.

The regular expressions in the .NET Framework style can be used in the **Filter** field. More info about the regular expressions: <https://msdn.microsoft.com/en-us/library/az24scfc%28v=vs.110%29.aspx>

ALT + LEFT MOUSE BUTTON CLICK combination allows to get the extended information about any website in the list.

Please note that IEMT will add all the application pools assigned to the selected sites to the migration list automatically.

Before going to the next step, think if all is selected correctly. If not, you can click **Clear migration list** and repeat the steps again.

Click **Next** button to go to the next step.

Step 4

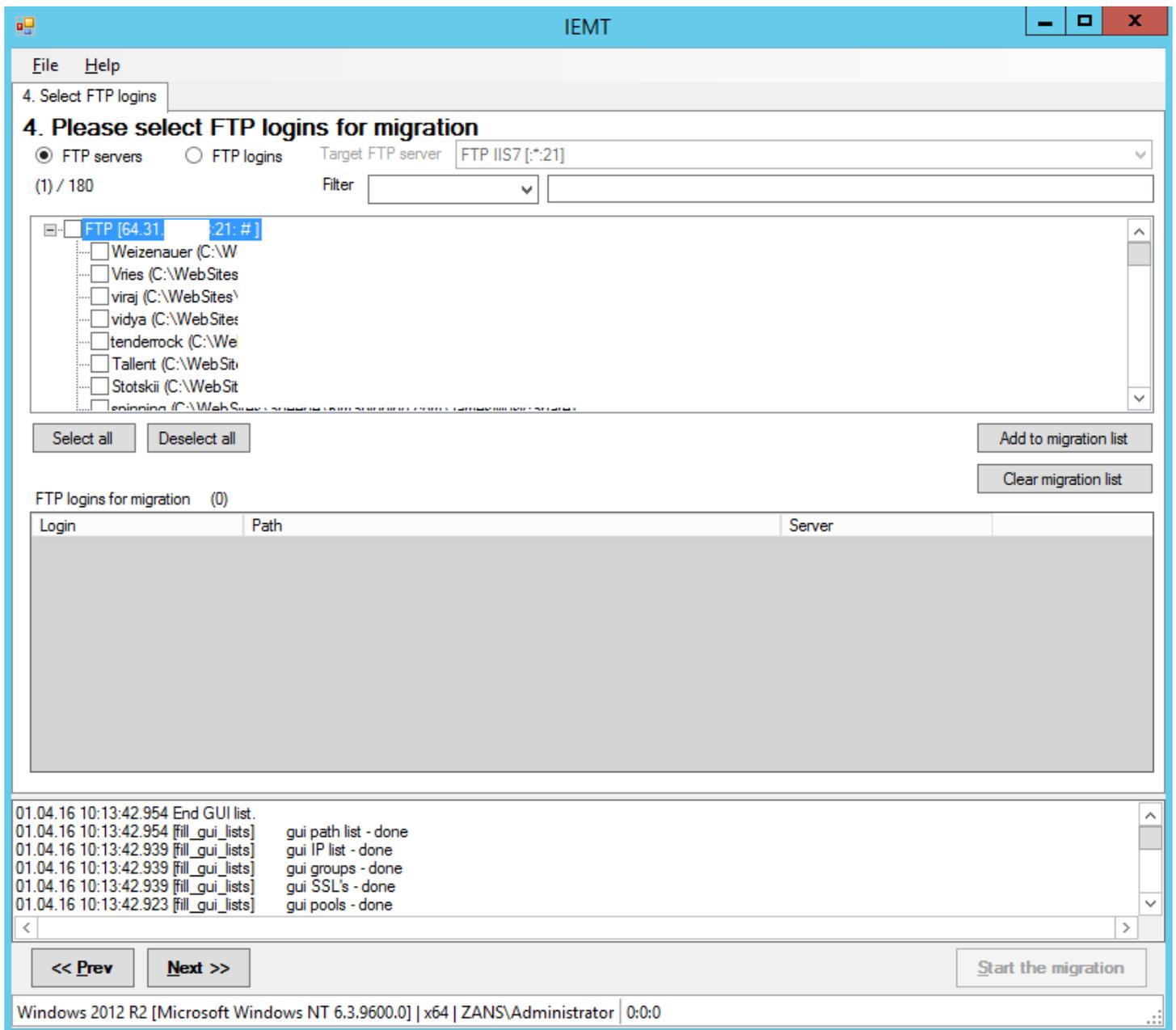
The screenshot shows the IEMT application window. The title bar reads "IEMT". The menu bar contains "File" and "Help". The main content area is titled "4. Please select FTP logins for migration". It features a radio button selection for "FTP servers" (unselected) and "FTP logins" (selected). A dropdown menu for "Target FTP server" is set to "FTP IIS7 [*:21]". Below this, a filter input field is present. A table lists 180 FTP logins, with the first few visible:

Login	Path	Server
<input type="checkbox"/> 130n41k	C:\WebSites\Df	FTP [64.31. :21: #]
<input type="checkbox"/> aaron	C:\WebSites\Sf	FTP [64.31. :21: #]
<input type="checkbox"/> AbreyFamilyAccess	C:\WebSites\At	FTP [64.31. :21: #]
<input type="checkbox"/> Adam	c:\websites\AM	FTP [64.31. :21: #]
<input type="checkbox"/> adminAbreyStudios	C:\WebSites\At	FTP [64.31. :21: #]
<input type="checkbox"/> AdminIT	C:\WebSites\Gi	FTP [64.31. :21: #]
<input type="checkbox"/> Aggarwal	C:\WebSites\Ag	FTP [64.31. :21: #]

Below the table are buttons for "Select all", "Deselect all", "Add to migration list", and "Clear migration list". A section titled "FTP logins for migration (0)" contains an empty table with columns "Login", "Path", and "Server". At the bottom, a log window shows the following entries:

```
01.04.16 10:13:42.954 End GUI list.
01.04.16 10:13:42.954 [fill_gui_lists] gui path list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui IP list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui groups - done
01.04.16 10:13:42.939 [fill_gui_lists] gui SSL's - done
01.04.16 10:13:42.923 [fill_gui_lists] gui pools - done
```

Navigation buttons include "<< Prev", "Next >>", and "Start the migration". The status bar at the bottom indicates "Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | 0:0:0".



Select FTP logins tab is for FTP accounts and FTP servers migration. It is similar to the steps 9 to 10, just select the accounts (and/or servers) and add them to the migration list by using the checkboxes, filters and **Add to migration list** button.

To migrate FTP accounts to an **existing** FTP server select **FTP logins** option and then select the destination FTP server name in **Target FTP server** list. Then click **Add to migration list** button.

To migrate a FTP server along with all (or some) of its FTP accounts, select **FTP servers** option. Then select desired FTP logins in the tree (see the screenshot above). Then click **Add to migration list** button.

Click **Next** button to go to the next step.

Step 5

5. Select pools

5. Please select pools for migration

Application pools 213

Filter

Pool	Identity	Pipeline	ASP.NET	Status
<input type="checkbox"/> 1057:	NetworkService	Classic	v2.0	Started
<input type="checkbox"/> administration.ipsl-re	SpecificUser	Classic	v2.0	Started
<input type="checkbox"/> administration.ipsl-re	SpecificUser	Integrated	v2.0	Started
<input type="checkbox"/> administration.ipsl-re	SpecificUser	Classic	v4.0	Started
<input type="checkbox"/> administration.ipsl-re	SpecificUser	Integrated	v4.0	Started
<input type="checkbox"/> aliantz v2.0 (Classic)	SpecificUser	Classic	v2.0	Started
<input type="checkbox"/> aliantz v2.0 (Integrated)	SpecificUser	Integrated	v2.0	Started
<input type="checkbox"/> aliantz v4.0 (Classic)	SpecificUser	Classic	v4.0	Started

Select all Deselect all Add to migration list

Application pools for migration (0) Clear migration list

Pool	Identity	Pipeline	ASP.NET	Status
------	----------	----------	---------	--------

01.04.16 10:13:42.954 End GUI list.
01.04.16 10:13:42.954 [fill_gui_lists] gui path list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui IP list - done
01.04.16 10:13:42.939 [fill_gui_lists] gui groups - done
01.04.16 10:13:42.939 [fill_gui_lists] gui SSL's - done
01.04.16 10:13:42.923 [fill_gui_lists] gui pools - done

<< Prev Next >> Start the migration

Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | 0:0:0

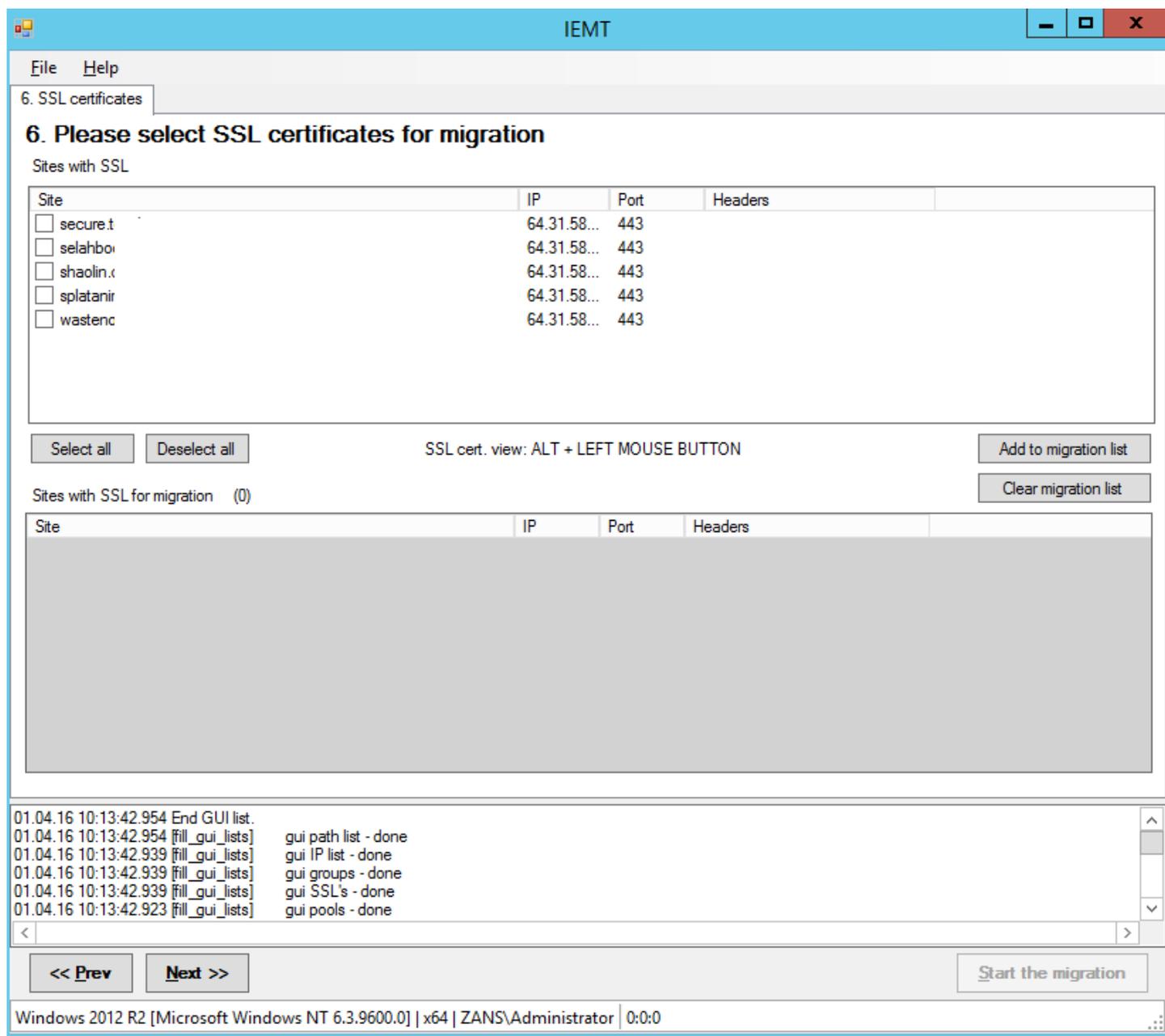
Select pools tab is for Application Pools migration. It is similar to the steps 9 to 10, just select the pools and add them to the migration list by using the checkboxes, filters and **Add to migration list** button.

Some of the pools will be added to the migration list automatically. These pools are assigned to the sites you selected at the previous steps. So, they cannot be removed from the list directly. To remove such a pool you need to go back to the sites selection step and remove the associated site from the migration list.

IEMT detects the .NET framework version for each pool automatically at the sites selection step.

Click **Next** button to go to the next step.

Step 6



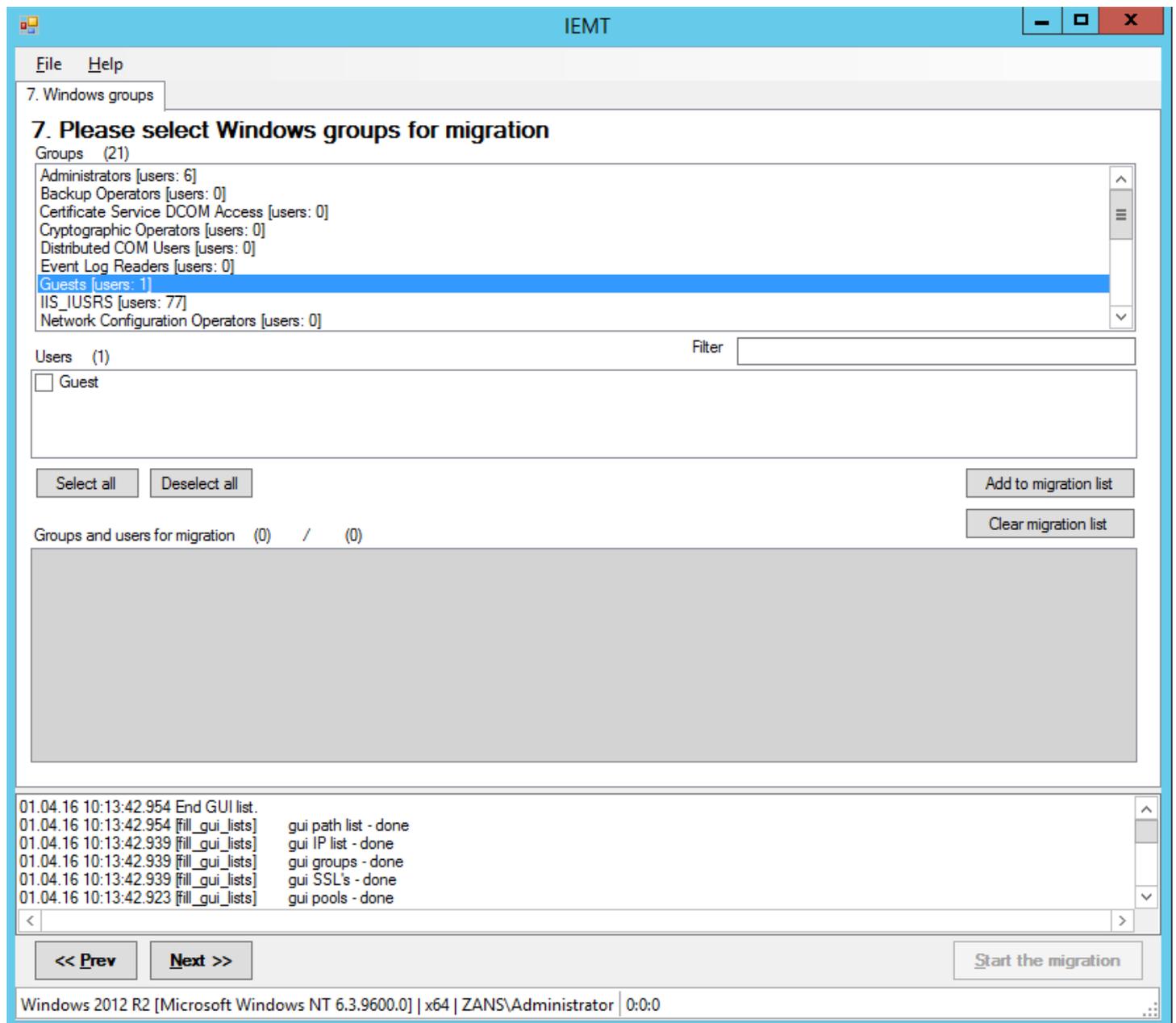
SSL certificates tab is for SSL certificates migration.

ALT + LEFT MOUSE BUTTON CLICK combination allows to get the extended information about any SSL certificate in the list.

This step is available only if Gathering Agent was used for source data collection.

Click **Next** button to go to the next step.

Step 7

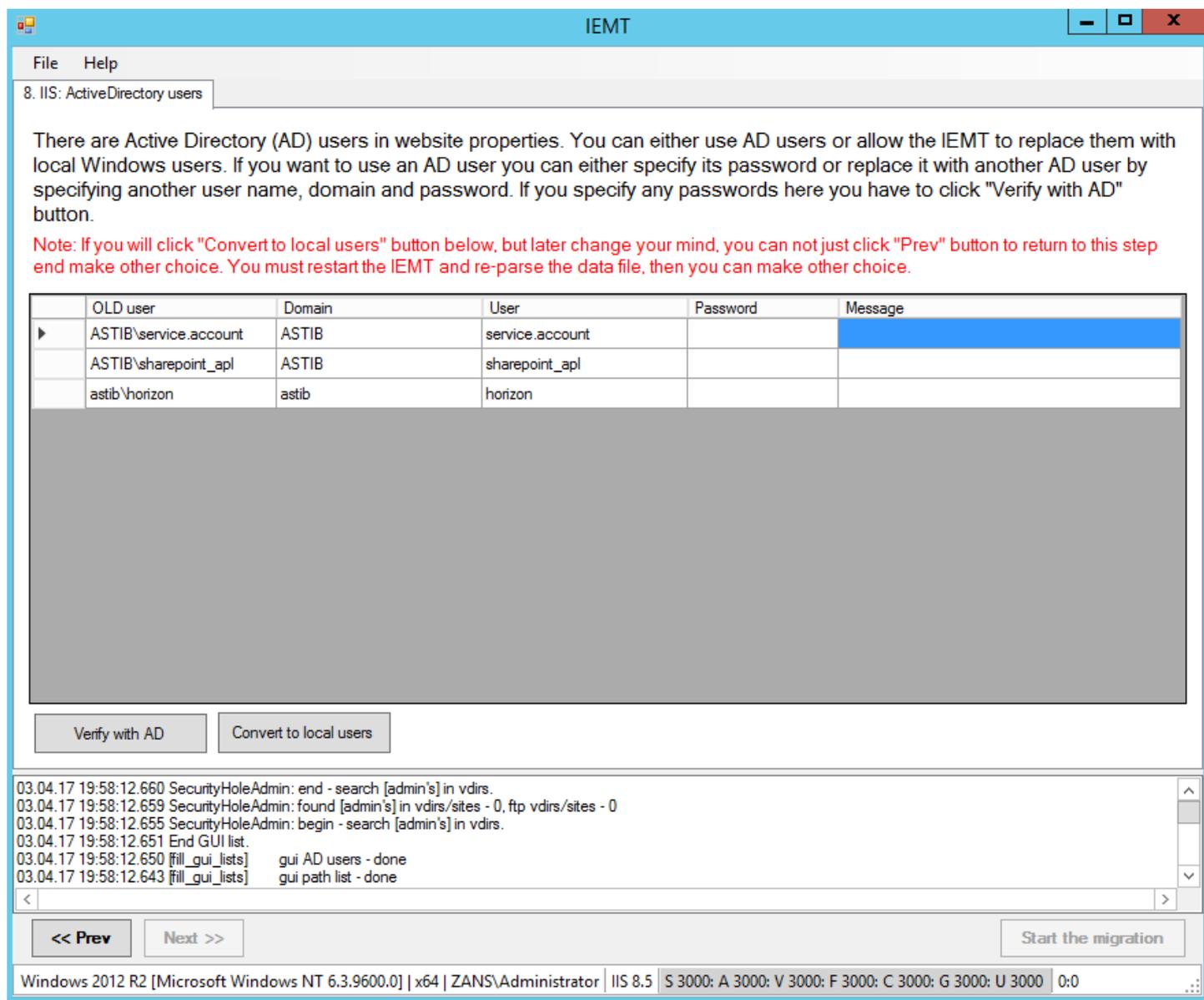


Windows groups tab is for Windows users and groups migration.

This step is available only if Gathering Agent was used for source data collection.

Click **Next** button to go to the next step.

Step 8



The screenshot shows the IEMT application window. At the top, there is a menu bar with 'File' and 'Help'. Below it, a tab is labeled '8. IIS: ActiveDirectory users'. The main area contains a text block explaining that Active Directory (AD) users are present in website properties and can be replaced with local Windows users. A red note below states: 'Note: If you will click "Convert to local users" button below, but later change your mind, you can not just click "Prev" button to return to this step end make other choice. You must restart the IEMT and re-parse the data file, then you can make other choice.'

OLD user	Domain	User	Password	Message
ASTIB\service.account	ASTIB	service.account		
ASTIB\sharepoint_apl	ASTIB	sharepoint_apl		
astib\horizon	astib	horizon		

Below the table are two buttons: 'Verify with AD' and 'Convert to local users'. At the bottom, there is a log window showing system events, a navigation bar with '<< Prev', 'Next >>', and 'Start the migration' buttons. The status bar at the very bottom displays system information: 'Windows 2012 R2 [Microsoft Windows NT 6.3.9600.0] | x64 | ZANS\Administrator | IIS 8.5 | S 3000: A 3000: V 3000: F 3000: C 3000: G 3000: U 3000 | 0:0'.

In most cases the IEMT cannot create Active Directory (AD) users, because it works as a local Administrator, but usually the local Administrator does not have enough permission to create AD users (due to security policies).

If there are Active Directory users in website (or other IIS object) properties the IEMT will show the list of those AD users.

You can either use Active Directory users or allow the IEMT to replace them with local Windows users. If you want to use an AD user you can either specify its password or replace it with another AD user by specifying another user name, domain and password.

If you specify any passwords here you have to click **Verify with AD** button.

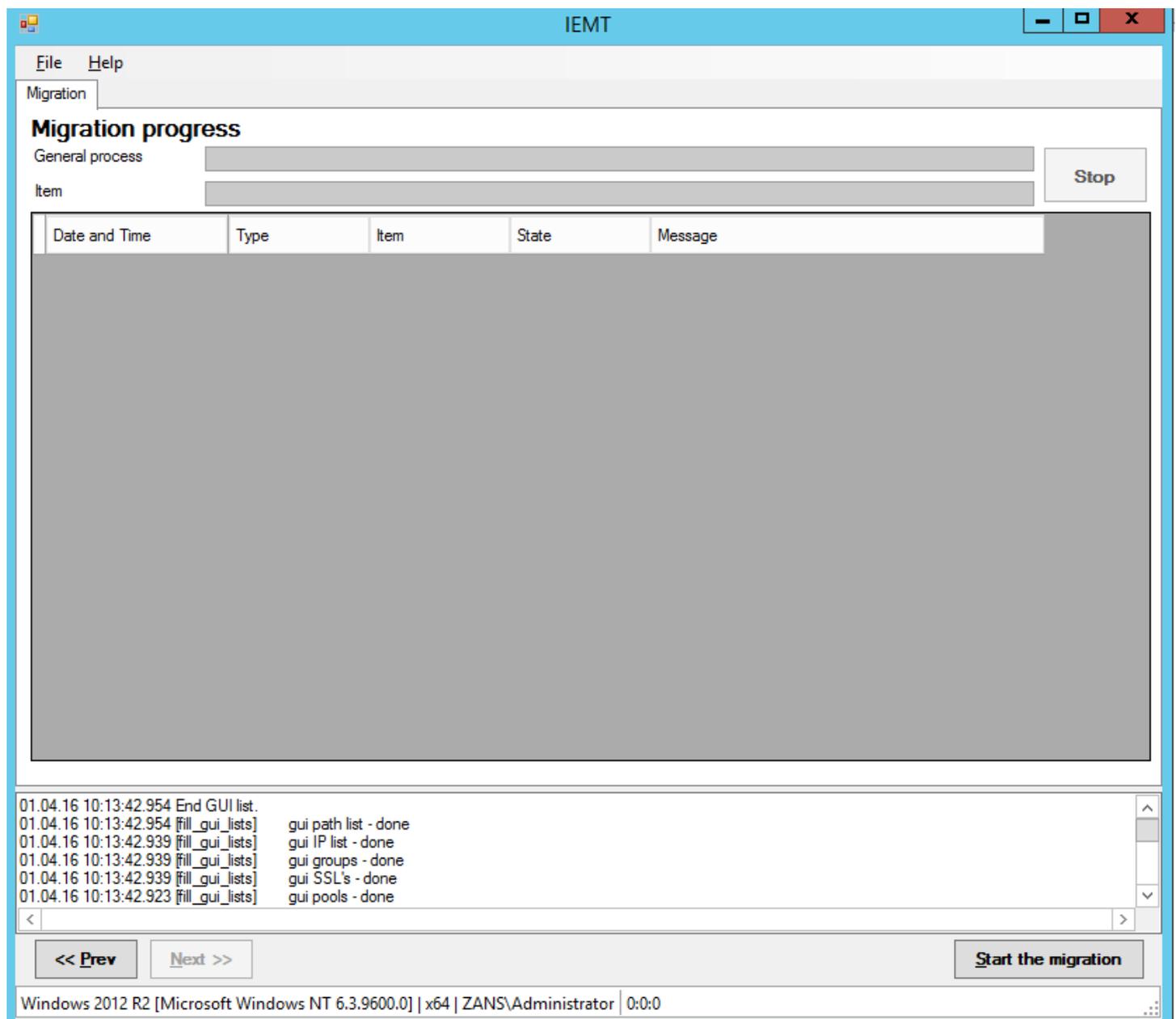
Note: The AD users must exist on the destination server and you have to specify their correct passwords. Otherwise the migrated websites will show 401 (or other similar) errors. The AD policy should allow those AD users to access website directories on the destination server, otherwise you'll get NTFS permission related errors.

Click **Convert to local users** if you want to replace Active Directory users with local Windows ones. The IEMT will create new local Windows users with strong random passwords. At the end of the migration you can find the user list (along with the passwords) in USERS-NUM.txt file (where “NUM” is some number).

*Note: If you will click **Convert to local users** button, but later change your mind, you cannot just click **Prev** button to return to this step end make other choice. You must restart the IEMT and re-parse the data file, then you can make other choice.*

Click **Next** button to go to the next step.

Step 9



The final step. You are about to start the migration process. But before you click the **Start the migration** button you have a chance to go back (using the **Prev** button) to change the settings. If all is fine with the settings, click **Start the migration** button.

The IEMT Remote Connection function

Description and prerequisites

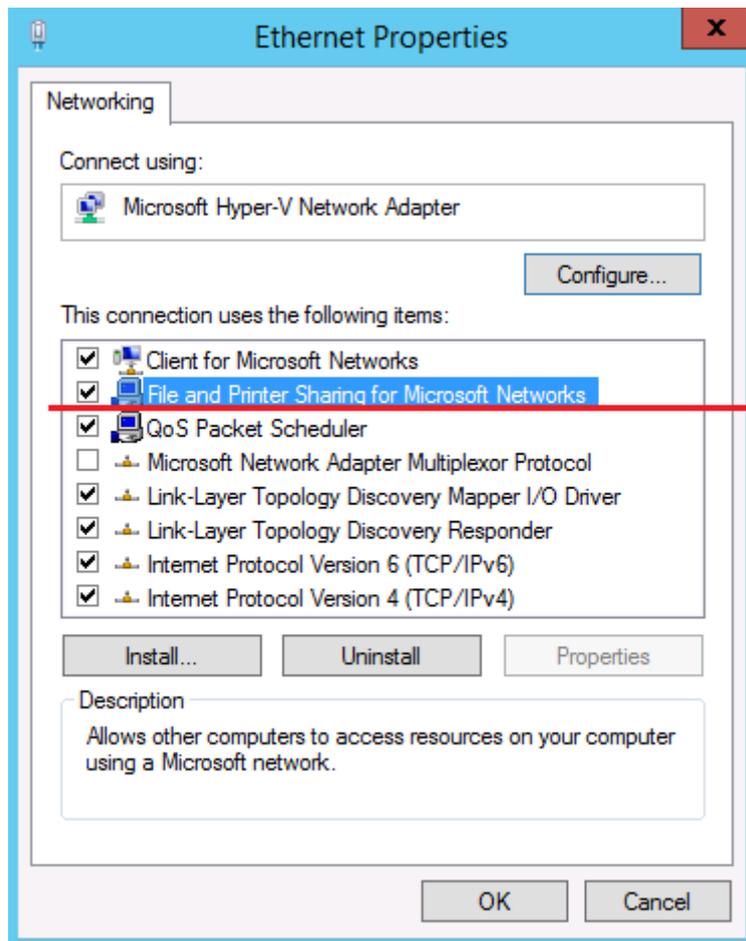
The IEMT can connect to the destination server remotely. It is a very useful function, especially for the migration to the Server Core versions of Windows. And it is useful for any version of Windows if you have multiple servers to migrate. You do not need to install the IEMT to all servers. It is enough to install it to a single one (let's call it the "central server") and migrate IIS from multiple source servers to multiple destination servers. (Please note that you still need to run the Gathering Agent on each of the source servers to get their data.)

To be able to work remotely it needs the following Windows services to be running on the destination server: **Server**, **Workstation**, **Windows Management Instrumentation (WMI)**. And **File Sharing** has to be enabled. Also the firewalls should not block the ports of those services: 135, 137, 139, 445. So, before using the remote IEMT connection you should check that:

1. Those 3 Windows services are up and running on the destination server.
2. The **Startup Type** of those 3 Windows services is **Automatic**.
3. **File Sharing** is enabled.
4. The destination server firewall has appropriate inbound rules for those 4 ports. They are open by default when you install Windows, but you could close them for security reasons. So, double check they are open before the migration, please.

Note: Once you finish the IIS migration you can turn off some of those services and/or close the ports for security reasons. For example, disable File Sharing if you do not use it. But you need them running and open during the migration.

File Sharing can be enabled in NIC properties:



The **WMI** Windows service in running state with **Automatic Startup Type** (**Server** and **Workstation** services should have the same settings and state):

The screenshot shows the Windows Computer Management console with the Services console open. The 'Windows Management Instrumentation' service is selected and highlighted in blue. The service is running and has an automatic startup type. The following table summarizes the key details for this service and its neighbors in the list.

Name	Description	Status	Startup Type	Log On As
Windows Management Instrumentation	Provides a c...	Running	Automatic	Local System...
Windows Modules Installer	Enables inst...	Manual	Manual	Local System...
Windows Presentation Foundation Font Cache 3.0.0.0	Optimizes p...	Manual	Manual	Local Service
Windows Process Activation Service	The Windo...	Running	Manual	Local System...
Windows Remote Management (WS-Management)	Windows R...	Manual	Manual	Network S...
Windows Store Service (WSService)	Provides inf...	Manual (Trig...	Manual (Trig...	Local System...
Windows Time	Maintains d...	Manual (Trig...	Manual (Trig...	Local Service
Windows Update	Enables the ...	Manual (Trig...	Manual (Trig...	Local System...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Manual	Manual	Local Service
Wired AutoConfig	The Wired ...	Manual	Manual	Local System...
WMI Performance Adapter	Provides pe...	Running	Automatic	Local System...
Workstation	Creates and...	Running	Automatic	Network S...

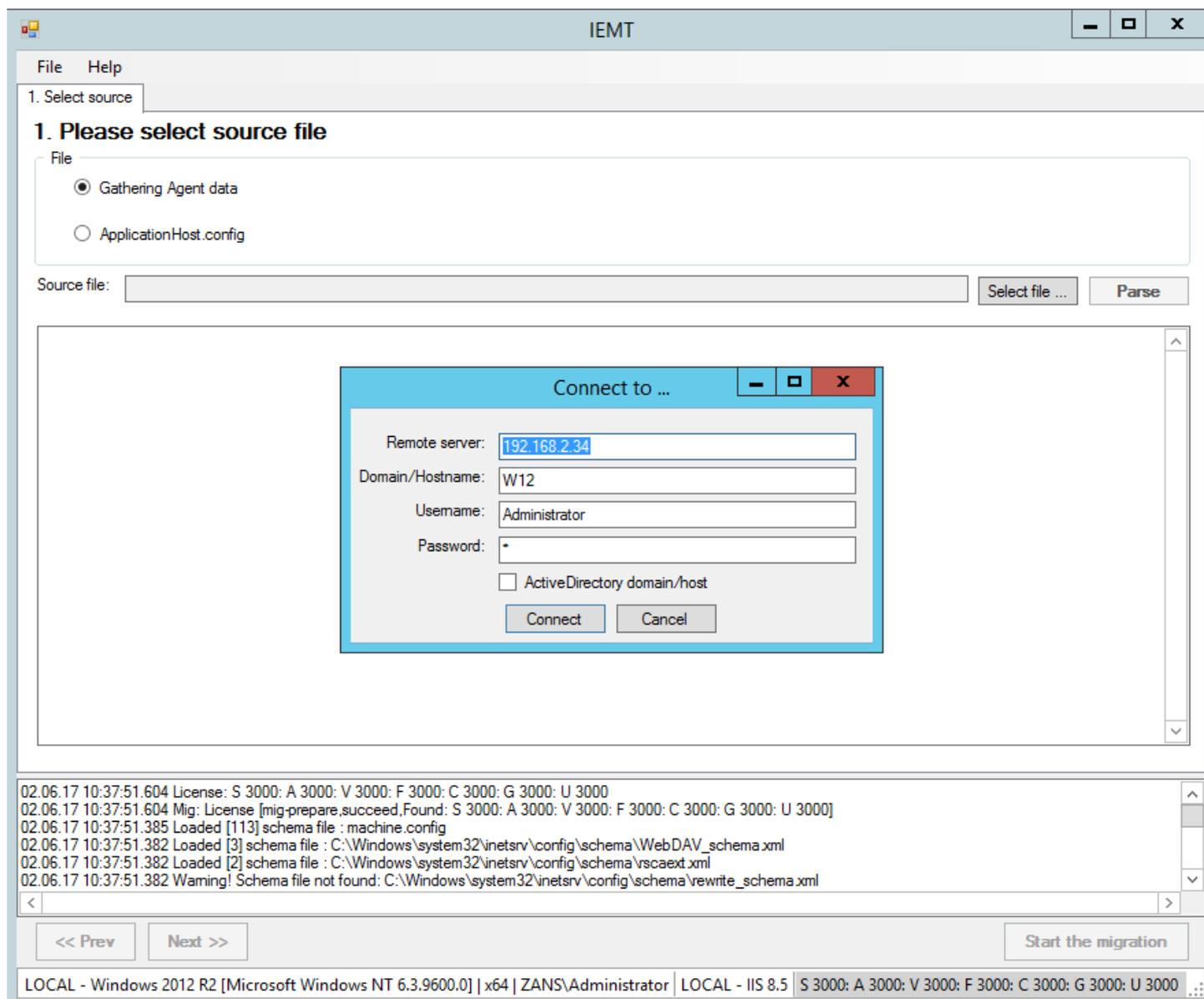
Windows Firewall rules for *File Sharing*:

The screenshot displays the Windows Firewall with Advanced Security console. The left-hand navigation pane shows the hierarchy: Windows Firewall with Advanced Security > Inbound Rules. The main pane displays a list of inbound rules. The rule 'File and Printer Sharing (SMB-In)' is highlighted in blue, indicating it is selected. Other rules in the 'File and Printer Sharing' group are also visible, including those for NB-Datagram-In, NB-Name-In, and NB-Session-In. The table below summarizes the visible rules.

Name	Group	Profile	Enabled	Action
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...)	Core Networking	All	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RP...)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TC...)	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - I...)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Echo Request - I...)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	All	No	Allow
File and Printer Sharing over SMBDirect (i...	File and Printer Sharing over...	All	No	Allow
FTP Server (FTP Traffic-In)	FTP Server	All	Yes	Allow
FTP Server Passive (FTP Passive Traffic-In)	FTP Server	All	Yes	Allow
FTP Server Secure (FTP SSL Traffic-In)	FTP Server	All	Yes	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	No	Allow
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow
Netlogon Service Authz (RPC)	Netlogon Service	All	No	Allow
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No	Allow
Network Discovery (NB-Datagram-In)	Network Discovery	All	No	Allow
Network Discovery (NB-Name-In)	Network Discovery	All	No	Allow
Network Discovery (Pub-WSD-In)	Network Discovery	All	No	Allow
Network Discovery (SSDP-In)	Network Discovery	All	No	Allow
Network Discovery (UPnP-In)	Network Discovery	All	No	Allow
Network Discovery (WSD Events-In)	Network Discovery	All	No	Allow

How to use the IEMT Remote Connection function

Run the IEMT and select **File -> Connect** menu item. You'll see the following dialog window:

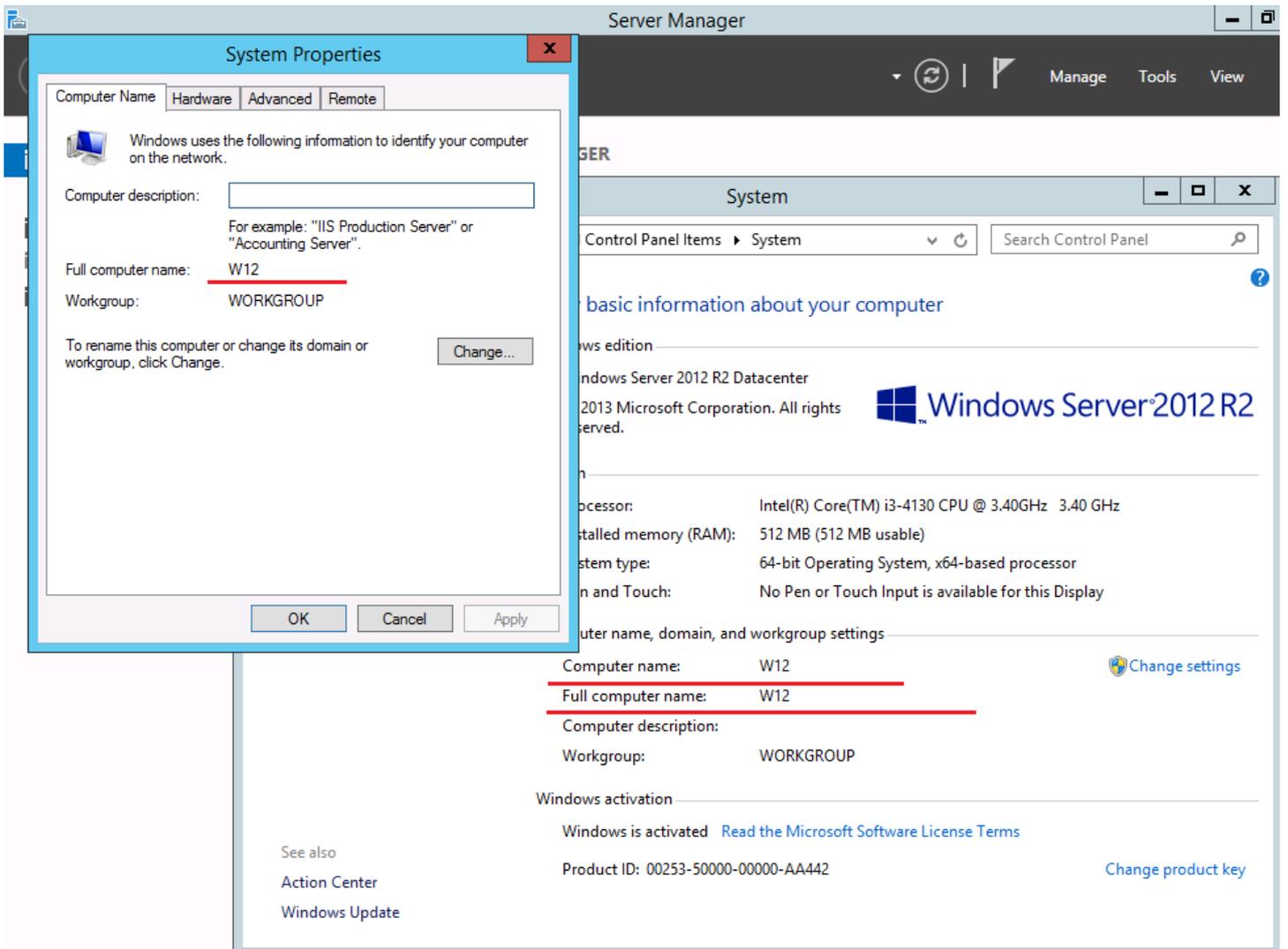


Pay attention to the status string. It starts with **LOCAL** word, that means the IEMT is in a local mode currently and is going to migrate websites to the current server.

Enter the connection parameters:

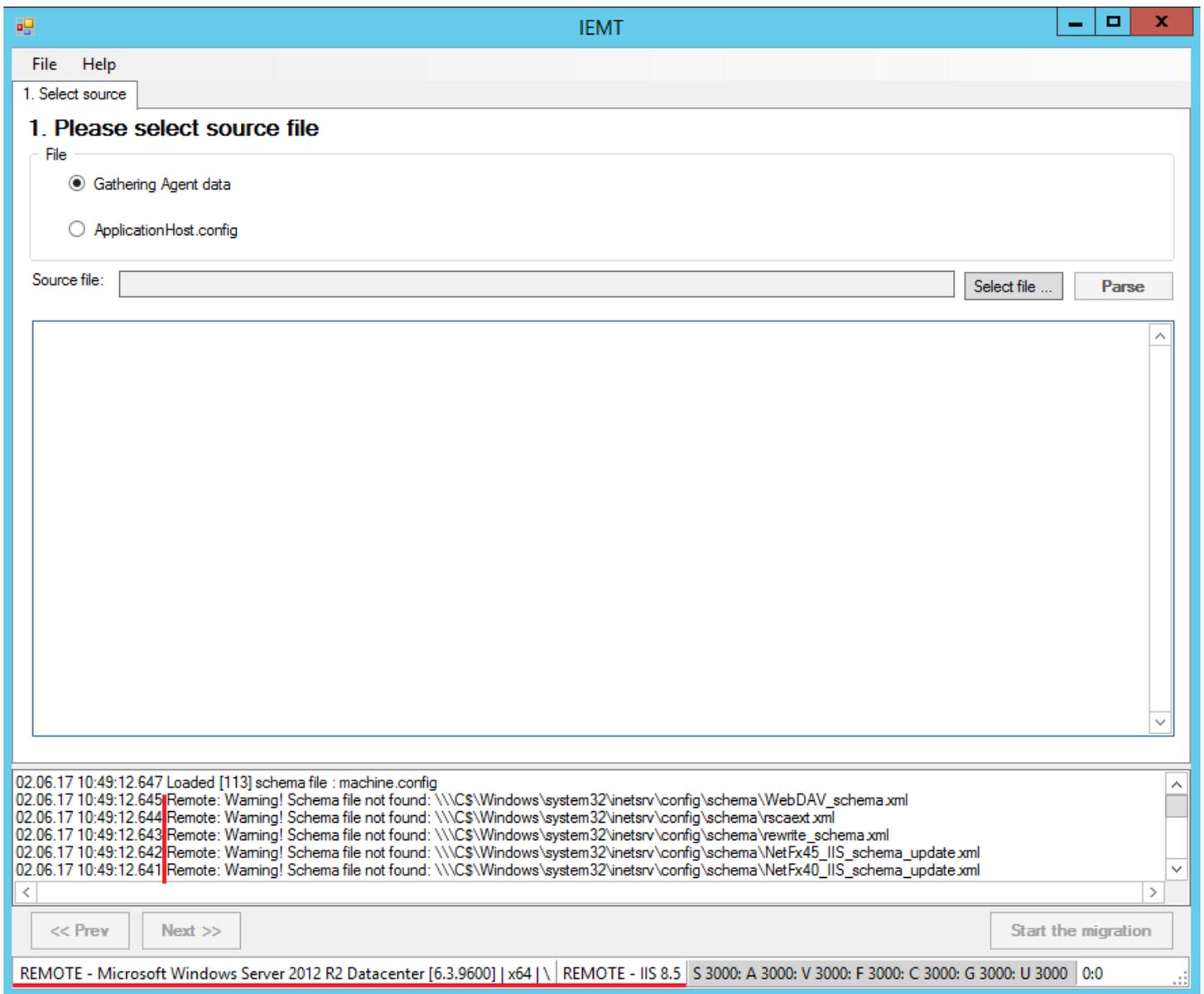
- You can use either IP address or DNS name of the destination server in **Remote server** field.
- Specify the remote server name (NETBIOS name) in **Domain/Hostname** field. You can find it in the Computer properties (Windows **Start** button -> right click on **Computer** -> **Properties**) or by executing **HOSTNAME** command in cmd.exe.

Note: Be sure you specify the name of the destination (remote) server, not the local one.



- **UserName** and **Password** – specify the credentials of a member of Administrators group. This user must have full Administrator permissions on the remote server.
- Turn on **Active Directory domain/host** checkbox if the remote server is a member of an Active Directory forest.

Click the **Connect** button and wait for the connection to be established. It takes some time; the IEMT will get the needed data from the remote server and then change the status string and the log.



The **REMOTE** word in the status string is a sign of a successful connection.

Once the connection is established you can use the IEMT to migrate websites (and other things like SSL certificates) to the remote server.

Important Note: The IEMT uses Windows services and File Sharing for the remote migration. (See the full list of the services above.) If any of them is stopped or has limited permissions then the IIS migration (or some of its steps) may fail.

How to create the firewall rules for remote IEMT connection on the destination server

As we said in the “Description and prerequisites” section above, the IEMT needs 4 ports (135, 137, 139, 445) to be open on the destination server if you wish to use its remote connection functionality. These ports are open by default, but we recommend to create a firewall rule to be 100% sure you have them open. To add the firewall rule you can either use Windows GUI or command line. Here we describe the command line way only, because it is universal for all versions of Windows, including Server Core.

To create the firewall rule you should run a **NETSH** command either in the console (cmd.exe) or PowerShell console.

Example:

```
netsh.exe advfirewall firewall add rule name="RemoteIEMT" dir=in action=allow enable=yes  
profile=any localip=any remoteip=any protocol=tcp localport="135,137,139,445"  
remoteport=any
```

This command opens ports of Windows services, so there is a potential security risk if your server is exposed to the Internet. Thus we recommend to make the ports open to your private (or a few public) IP addresses only.

Use the **remoteip** parameter to specify the IP addresses.

In the example above we used **remoteip=any**, this means "allowed from any IP address".

To allow connections only from 192.168.2.89 IP address, use this parameter:

```
remoteip=192.168.2.89
```

This is how to add 2 IP ranges (10.1.0.0/16 and 192.168.1.0/24) to the rule:

```
remoteip="10.1.0.0/16,192.168.1.0/24"
```

The full command with a single IP address:

```
netsh.exe advfirewall firewall add rule name="RemoteIEMT" dir=in action=allow enable=yes  
profile=any localip=any remoteip=192.168.2.89 protocol=tcp localport="135,137,139,445"  
remoteport=any
```

and with multiple IP addresses:

```
netsh.exe advfirewall firewall add rule name="RemoteIEMT" dir=in action=allow enable=yes  
profile=any localip=any remoteip="10.1.0.0/16,192.168.1.0/24" protocol=tcp  
localport="135,137,139,445" remoteport=any
```

To delete the firewall rule (once you finished the IIS migration) you can use this command:

```
netsh advfirewall firewall delete rule name="RemoteIEMT"
```

Troubleshooting

*Note: The IEMT 7 is a GUI application, so currently it is not compatible with Server Core installation of Windows. You should either have **Full Installation** of Windows 2008, 2012 or Windows Server 2016 with **Desktop Experience**.*

If any troubles, first of all, please take a look at the migration log. In most cases it helps to find and fix the problem. It is also a good idea to check the server Event Logs.

Also be sure you run the software *as Administrator* (you must be a member of the local Administrators group.)

And of course, you can contact support@hoststools.com for support. If you decide to contact HostTools support team, please send us all the log files, applicationHost.config file and the Gathering Agent DATA file.

Thank you for using our software!