Несмотря на то, что протоколу **FTP**, являющемуся  одним из старейших протоколов, уже исполнилось больше 40 лет, он продолжает использоваться повсеместно там, где требуется простой протокол передачи файлов. Сервер FTP – возможно установить на всех операционных системах Microsoft. Последняя глубокая модернизация этой службы была произведена в Windows 7 / Server 2008 R2 (по сути код сервиса был переписан заново).  Была существенно улучшена безопасность службы, и появился ряд новых возможностей. В частности, в FTP сервере на Windows появилась возможность настроить **изоляцию FTP пользователей**, позволяющая разграничить доступ множества пользователей к собственным папкам на одном FTP сервере.

Благодаря возможности изоляции пользователи могут работать только со своими каталогами, и не могут  подняться выше по дереву каталогов FTP, т.к. каталог верхнего уровня пользователя отображается для него как корень службы FTP. Таким образом можно предотвратить доступ пользователей к чужим данным на FTP сервере. Изоляция FTP пользователей широко применяется ISP/ASP провайдерами, когда нужно предоставить индивидуальный доступ различным пользователям к одному файловому хранилищу.

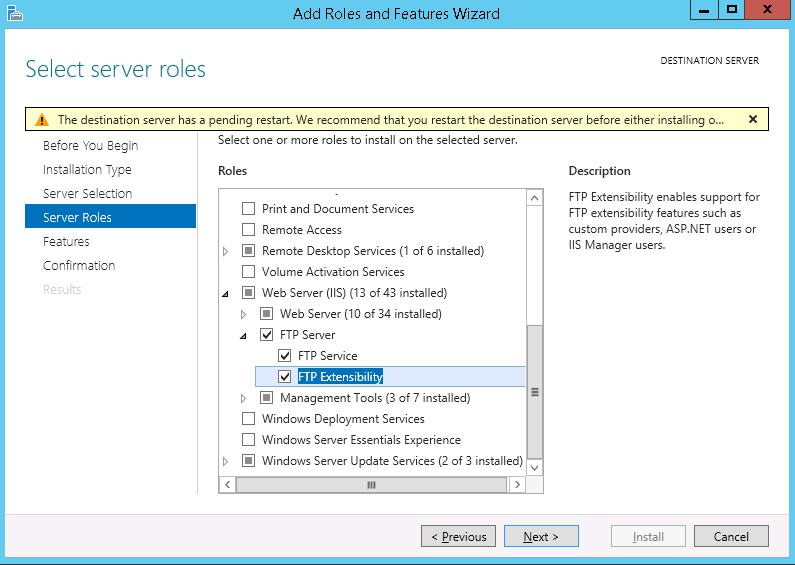
Как и в предыдущих версиях Windows, служба FTP в Windows Server 2012  R2 основана и глубоко интегрирована в сервис IIS, и имеет единый административный интерфейс управления.

В этой статье мы покажем, как **установить сервер FTP на базе IIS 8 в Windows Server 2012 R2 и настроить на нем изоляцию пользователей** (инструкция также применима и к Windows 8).

Содержание:

* Установка сервиса FTP в Windows Server 2012 R2
* Создаем FTP сайт,  заводим пользователей, настраиваем права
* Настройка изоляции FTP пользователей в Windows Server 2012 R2

**Установка сервиса FTP в Windows Server 2012 R2**

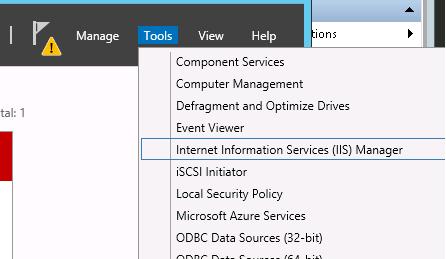
Установить сервис FTP можно через консоль Server Manager, отметив опции **FTP Service** и **FTP Extensibility** в разделе **Web Server(IIS) -> FTServer**. [](http://winitpro.ru/wp-content/uploads/2014/10/1-install-ftp-server-windows2012r2.jpg)

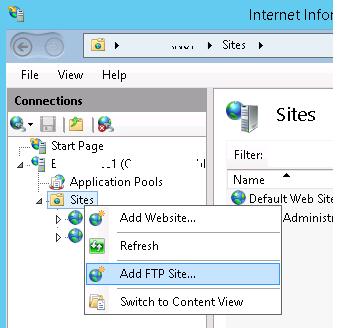
Также можно установить роль FTP сервера одной командой Powershell:

Install-WindowsFeature Web-FTP-Server

[](http://winitpro.ru/wp-content/uploads/2014/10/2-Install-WindowsFeature-Web-FTP-Server.jpg)

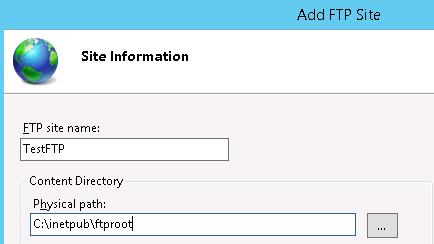
**Создаем FTP сайт,  заводим пользователей, настраиваем права**

Откроем консоль управления IIS (Internet Information Service Manager). [](http://winitpro.ru/wp-content/uploads/2014/10/3-iismanager.jpg)

И создадим новый FTP сайт (**Sites ->Add FTP Site**). [](http://winitpro.ru/wp-content/uploads/2014/10/4-add-ftp-site.jpg)

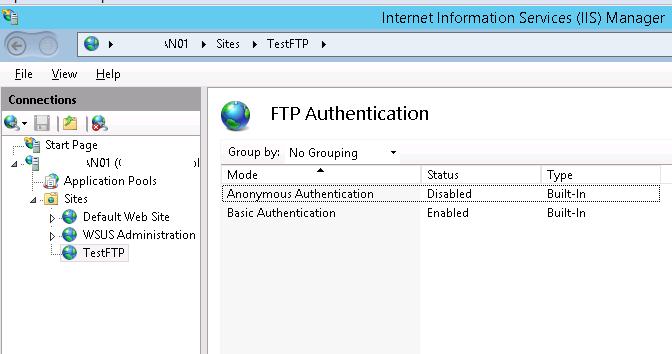
Имя FTP сайта: **MyTestSite**

Корневой каталог FTP сайта: **C:\inetpub\ftproot**

[](http://winitpro.ru/wp-content/uploads/2014/10/5-ftp-site-name.jpg)

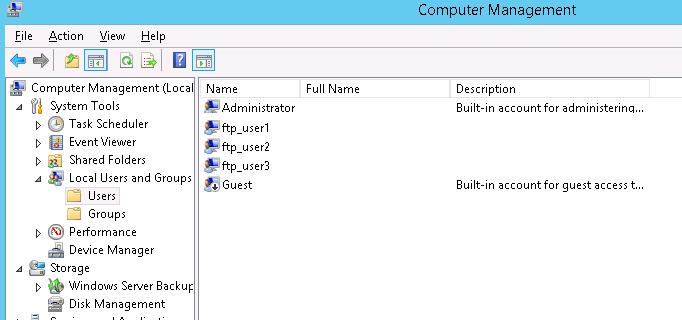
Для защиты передаваемых данных возможно настроить SSL (в этом случае все передаваемые по сети данные и пароли/учетки ftp-пользователей будут зашифрованы), но в нашей демонстрации это не обязательно. Все остальные настройки оставляем  стандартными.

Выберем наш FTP сайт и в секции **FTP Authentication** (Аутентификация) отключим анонимную аутентификацию **Anonymous Authentication**. **Basic Authentication** должна быть включена.

[](http://winitpro.ru/wp-content/uploads/2014/10/6-ftp-authentification.jpg)

FTP сервис на Windows 2012 R2 может использовать два типа учетных записей: доменные или локальные. В зависимости от типа учетной записи есть различия в структуре каталогов FTP и настройках изоляции. С целью упрощения описания мы будем использовать локальные учетные записи Windows.

Создадим пользователей FTP, допустим, это будут учетные записи ftp\_user1, ftp\_user2 и ftp\_user3. Также создадим группу ftp\_users , в которую включим этих пользователей . Создать пользователей можно в разделе **Local Users and Groups** консоли **Computer Management.**

[](http://winitpro.ru/wp-content/uploads/2014/10/7-ftp-users.jpg)

Или из командной строки:

net localgroup ftp\_users /add

[](http://winitpro.ru/wp-content/uploads/2014/10/8-create-ftp-group.jpg)

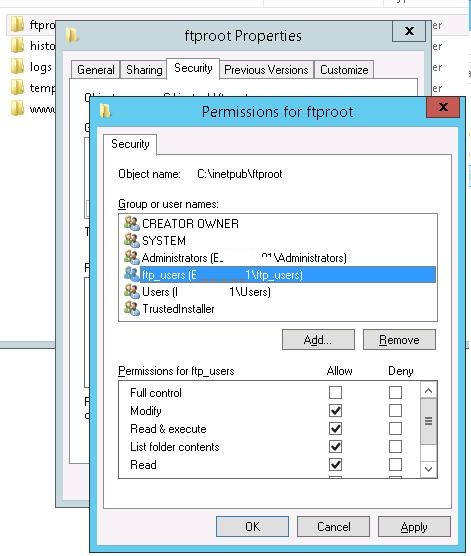
net user ftp\_user1 /add \*

[](http://winitpro.ru/wp-content/uploads/2014/10/9-create-ftp-user.jpg)

net localgroup ftp\_users ftp\_user1 /add

[](http://winitpro.ru/wp-content/uploads/2014/10/10-add-user-to-group.jpg)

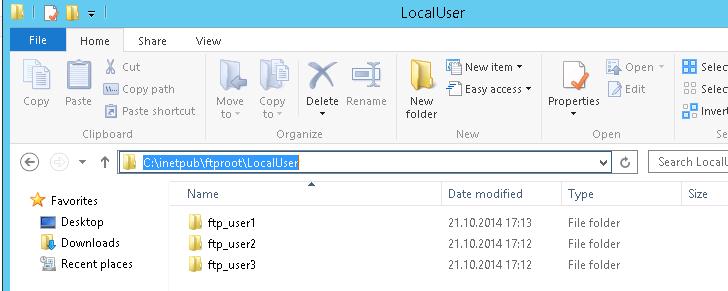
Точно так же создадим еще двух пользователей.

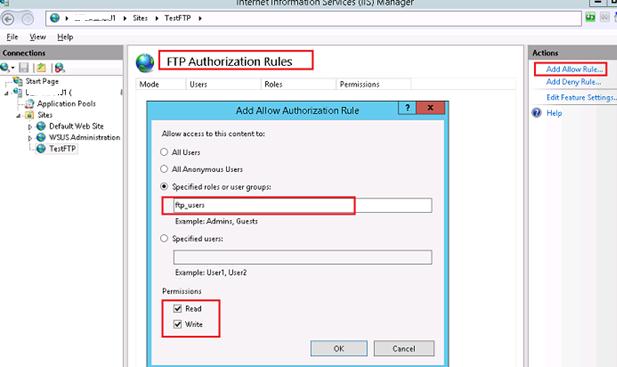
Предоставим созданной группе ftp\_users права (RW) на каталог C:\inetpub\ftproot. [](http://winitpro.ru/wp-content/uploads/2014/10/11-ftp-permissions.jpg)

Внутри каталога C:\inetpub\ftproot создадим каталог с именем **LocalUser** (имя должно полностью соответствовать, **это важно!!!**). Затем внутри C:\inetpub\ftproot\LocalUser создадим три каталога с именами созданных нами пользователей: ftp\_user1, ftp\_user2, ftp\_user3.

**Примечание**. В зависимости от типа учетных записей необходимо создать следующие структуры каталогов (под %FtpRoot%\ подразумевается корень сайта FTP, в нашем случае это C:\inetpub\ftproot\):

|  |  |
| --- | --- |
| **Тип учетной записи** | **Синтаксис именования домашних каталогов** |
| Анонимные пользователи | %FtpRoot%\LocalUser\Public |
| Локальная учетная запись Windows | %FtpRoot%\LocalUser\%UserName% |
| Доменная учетная запись Windows | %FtpRoot%\%UserDomain%\%UserName% |
| Специальные учетки IIS Manager или ASP.NET | %FtpRoot%\LocalUser\%UserName% |

[](http://winitpro.ru/wp-content/uploads/2014/10/12-ftproot-localuser-folder.jpg)

Вернемся в консоль IIS и в разделе сайта **FTP Authorization Rules** создадим новое правило (**Add AllowRules**), в котором укажем, что группа ftp\_users должна иметь права на чтение и запись (разрешения Read и Write). [](http://winitpro.ru/wp-content/uploads/2014/10/13-FTP-Authorization-Rules.jpg)

**Настройка изоляции FTP пользователей в Windows Server 2012 R2**

Перейдем к настройке изоляции пользователей FTP. Изоляция FTP пользователей настраивается на уровне сайта FTP, а не всего сервера.

В настройках FTP сайта откройте пункт **FTP User Isolation**.

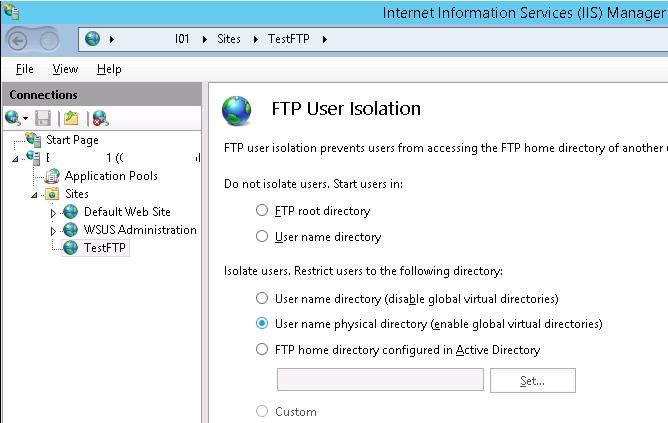
В этом разделе имеются несколько настроек. Первые две не предполагают изоляции пользователей:

* **FTP root directory** (ftp‑сессия пользователя начинается с корневого каталога ftp-сайта)
* **User name directory** (пользователь начинает работу с физического/виртуального каталога с именем пользователя. Если каталог отсутствует, сессия начинается с корневого каталога ftp-сайта)

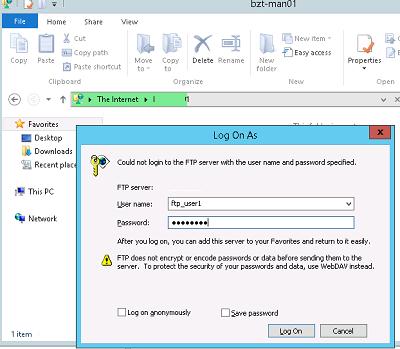
Следующие 3 опции представляют различные режимы работы изоляции пользователей:

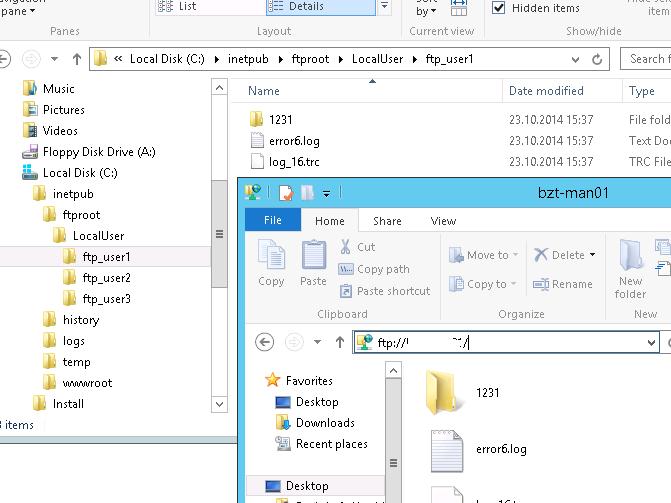
* **User name directory (disable global virtualdirectories)** – предполагает, что ftp-сессия пользователя изолирована физическим или виртуальным каталогом имя которого соответствует имени пользователя ftp. Пользователи видят только собственный каталог (для них он является корневым) и не могут выйти за его рамки (в вышестоящий каталог дерева FTP). Любые глобальные виртуальные каталоги игнорируются.
* **User name physical directory (enable global virtual directories)** – предполагается, что FTP-сессия пользователя ограничена (изолирована) физическим каталогом с именем учетной записи пользователя FTP. Пользователь не может перейти выше своего каталога по структуре FTP. Однако пользователю доступны все созданные глобальные виртуальные каталоги.
* **FTP home directory configured in Active Directory** – FTP-пользователь изолируется в рамках своего домашнего каталога, заданного в настройках его учетной записи Active Directory (свойства FTPRoot и FTPDir)

**Важно**. Если глобальные виртуальные директории активны, все пользователи могут получить доступ ко всем виртуальным каталогам, настроенным в корне FTP сайта (при наличии соответствующих NTFS прав доступа).

[](http://winitpro.ru/wp-content/uploads/2014/10/14-ftp-user-isolation.jpg)

Выберите нужный режим изоляции (вы выбрали второй вариант) и попробуйте подключиться к своему FTP сайту с помощью любого клиента FTP или непосредственно из Explorer (в адресной строке указав ftp://yourservername/.

Укажите имя и пароль пользователя [](http://winitpro.ru/wp-content/uploads/2014/10/15-logon-ftp-server.jpg)

И мы получим доступ к домашнему каталогу с данными пользователя (являющимся для пользователя корнем FTP сайта). Как мы видим, сессия пользователя является изолированной и пользователь видит только свои данные. [](http://winitpro.ru/wp-content/uploads/2014/10/16-isolate-ftp-session.jpg)

**Совет**. При анонимном подключении к FTP сайту – сессия будет ограничена каталогом LocalUser\Public (естественно каталог Public должен быть создан предварительно).

Итак, мы рассмотрели, как настроить FTP сайт с изоляцией пользователей на базе Windows Server 2012 R2. В режиме изоляции пользователи аутентифицируются на FTP со своими локальным или доменным учетными записями, после чего они получают доступ к своему корневому каталогу, соответствующему имени пользователя.