

BitLocker Drive Encryption

Server 2012

What is BitLocker?

BitLocker is a tool that allows you to encrypt both the operating system volume and additional data volumes within the same server.

New files added to the encrypted drives are encrypted automatically, and files moved from this drive to another drive or computers are decrypted automatically

Benefits of BitLocker

- Enhanced protection against data theft
- BitLocker will protect your data in the event of a lost or stolen hard disk.
- If your disk is lost or stolen, the encryption prevents unauthorized access to the data.

Operating systems that can use BitLocker

- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows 8 Pro
- Windows 8 Enterprise
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012 & 2012R2

Removable media such as external hard disks or USB drives use **BitLocker To Go**

Security Technology behind BitLocker

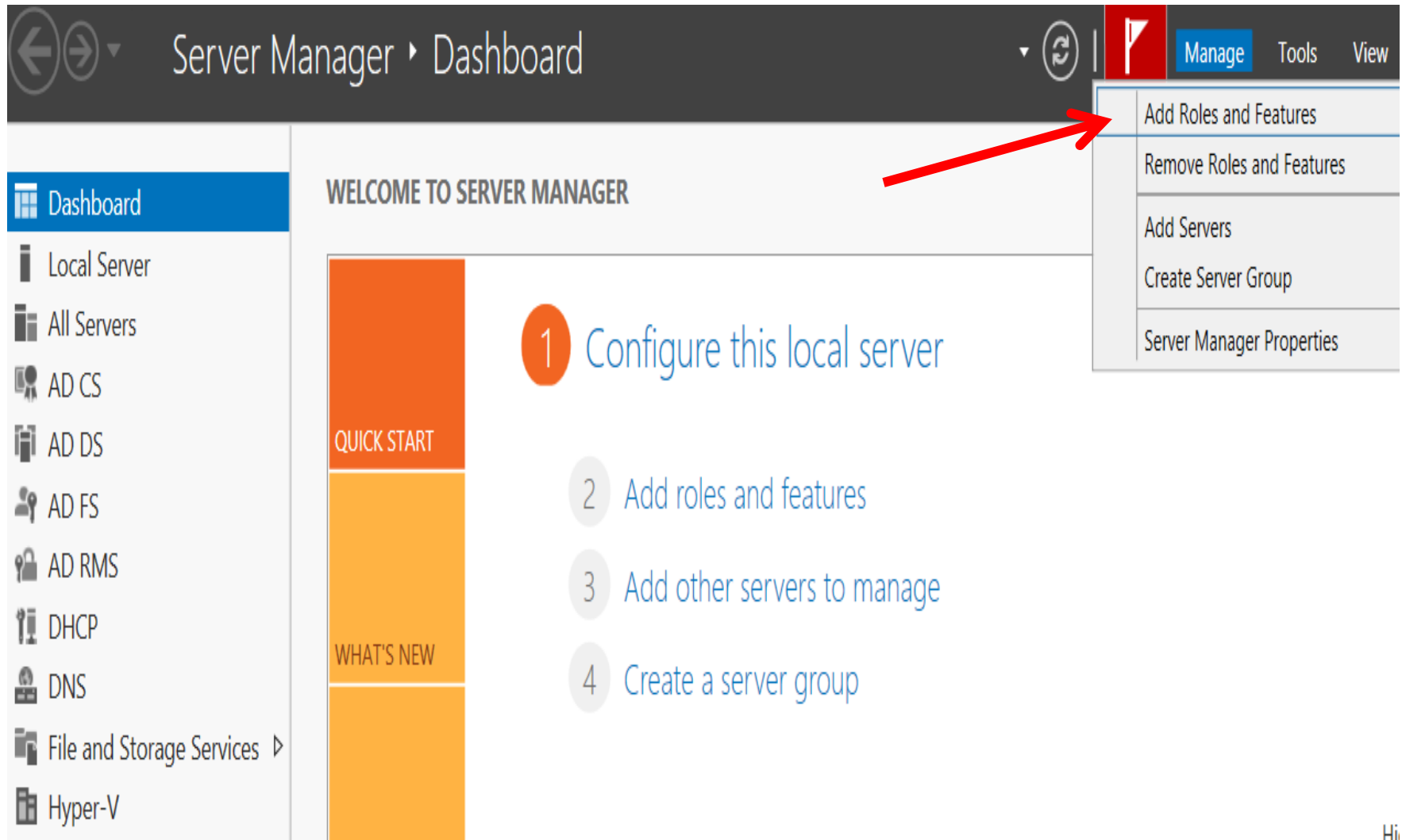
- BitLocker uses a Trusted Platform Module (TPM) chip to store the security key.
- If your computer does not have a TPM chip, you can store the key on a removable USB drive.

Note: The USB drive will be required each time you start the computer so that the system drive can be decrypted.

How does it work?

If the TPM discovers a potential security risk, such as a disk error or changes made to BIOS, hardware, system files, or startup components, the system drive will not be unlocked until you enter the 48-digit BitLocker recovery password or use a USB drive with a recovery key as a recovery agent.

Enabling BitLocker in Windows Server 2012



The screenshot shows the Windows Server 2012 Server Manager interface. The top navigation bar includes navigation arrows, the text "Server Manager Dashboard", a refresh icon, and a red flag icon. Below the navigation bar, there are three tabs: "Manage" (selected), "Tools", and "View". A red arrow points from the "Manage" tab to a context menu that is open, showing the following options: "Add Roles and Features", "Remove Roles and Features", "Add Servers", "Create Server Group", and "Server Manager Properties".

On the left side, there is a navigation pane with the following items: "Dashboard", "Local Server", "All Servers", "AD CS", "AD DS", "AD FS", "AD RMS", "DHCP", "DNS", "File and Storage Services", and "Hyper-V".

The main content area displays "WELCOME TO SERVER MANAGER" and a "QUICK START" section with the following steps:

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group

Below the "QUICK START" section, there is a "WHAT'S NEW" section.



Add Roles and Features Wizard



Before you begin

DESTINATION SERVER
WIN-R44O8GIKKQK.DeanLashley.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default



< Previous

Next >

Install

Cancel



Add Roles and Features Wizard



Select installation type

DESTINATION SERVER
WIN-R44O8GIKKQK.DeanLashley.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



< Previous

Next >

Install

Cancel

Add Roles and Features Wizard



Select destination server

DESTINATION SERVER
WIN-R44O8GIKKQK.DeanLashley.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
WIN-R44O8GIKKQK.Dea...	169.254.241.15...	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard



Select server roles

DESTINATION SERVER
WIN-R44O8GIKKQK.DeanLashley.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services (Installed)
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services (Installed)
- Application Server
- DHCP Server (Installed)
- DNS Server (Installed)
- Fax Server
- File And Storage Services (Installed)
- Hyper-V (Installed)
- Network Policy and Access Services (Installed)
- Print and Document Services (Installed)
- Remote Access (Installed)
- Remote Desktop Services

Description

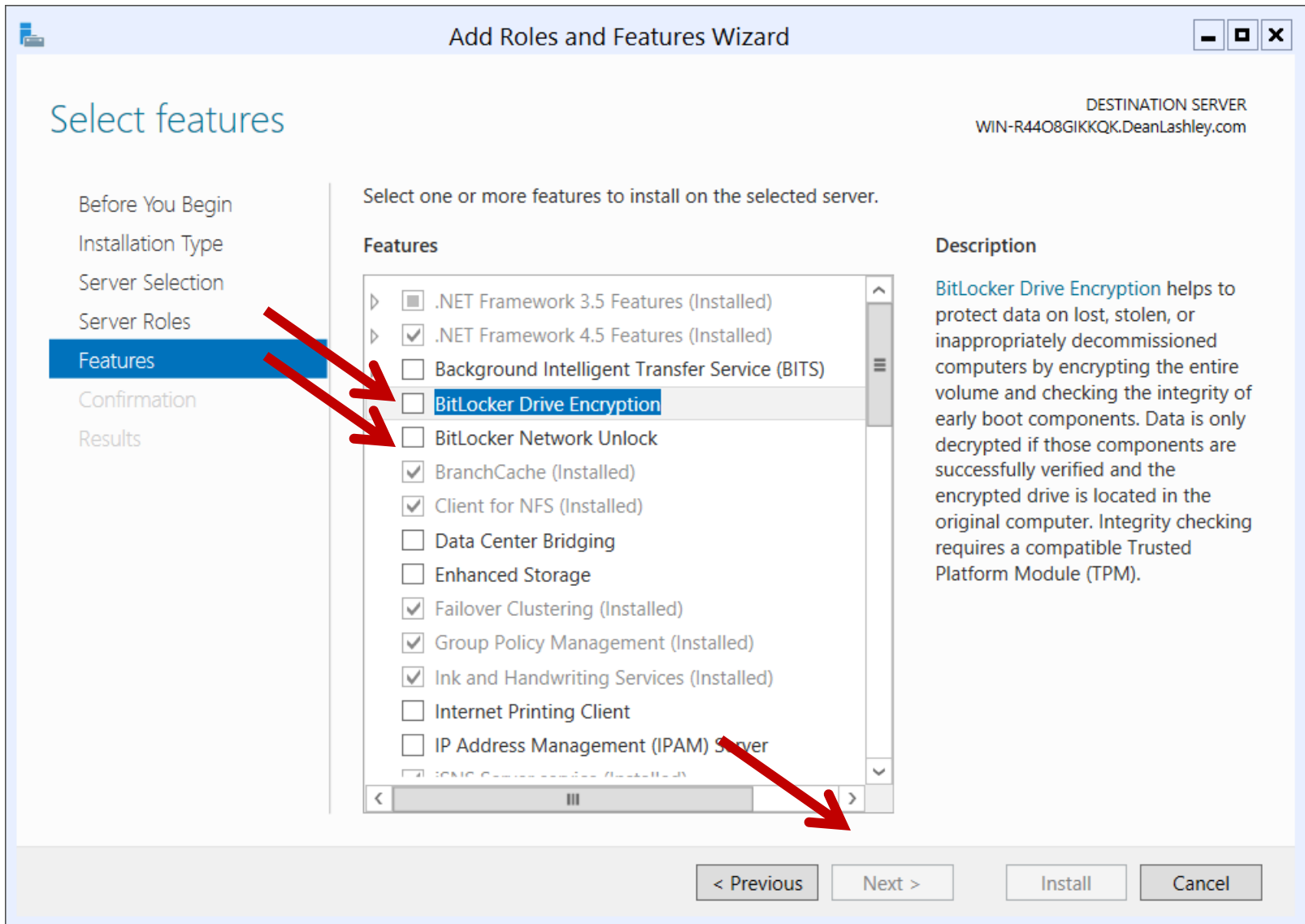
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

< Previous

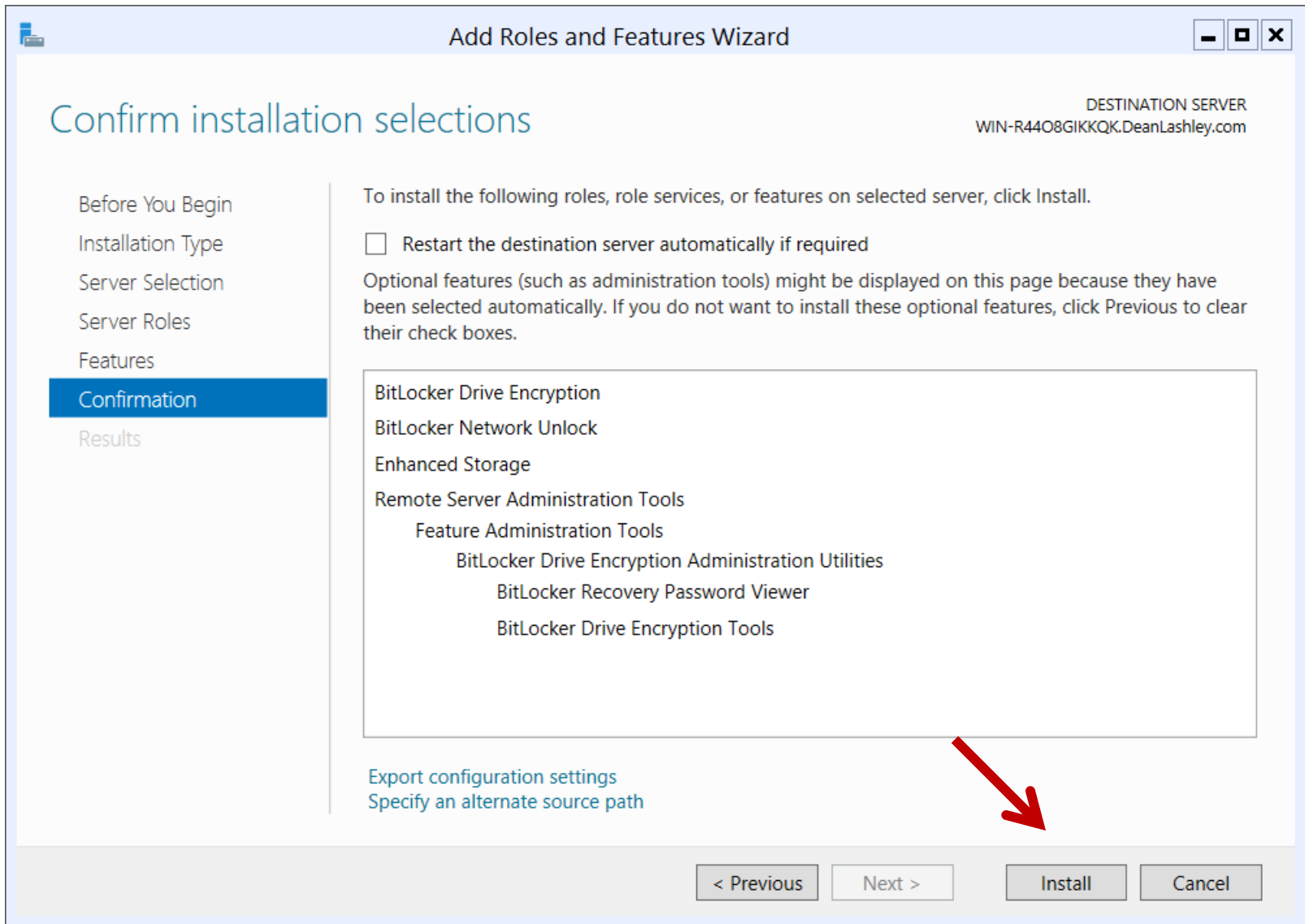
Next >

Install

Cancel



Here we want to select both BitLock Drive encryption and BitLock Network Unlock feature if we require the Network Unlock feature



The system needs to be restarted after the bitlocker install.

Install BitLocker by using the Windows PowerShell utility

To install BitLocker, use the following PowerShell commands:

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -  
IncludeManagementTools -Restart
```

Network Unlock

- Network Unlock allows an administrator to configure BitLocker to unlock automatically an encrypted hard drive during a system reboot when that hard drive is connected to their trusted corporate environment.
- For this to function properly on a machine, there has to be a DHCP driver implementation in the system's firmware.

TABLE 14.3 BitLocker then and now

Feature	Windows 7/Server 2008 R2	Windows 8/Server 2012
Reset the BitLocker PIN or password	The user's privileges must be set to an administrator if you want to reset the BitLocker PIN on an operating system drive and the password on a fixed or removable data drive.	Standard users now have the ability to reset the BitLocker PIN and password on operating system drives, fixed data drives, and removable data drives.
Disk encryption	When BitLocker is enabled, the entire disk is encrypted.	When BitLocker is enabled, users have the ability to choose whether to encrypt the entire disk or only the used space on the disk.
Hardware Encrypted Drive support	Not supported.	If the Windows logo hard drive comes pre-encrypted from the manufacturer, BitLocker is supported.
Unlocking using a network-based key to provide dual-factor authentication	Not available.	If a computer is rebooted on a trusted corporate wired network, key protector then allows a key to unlock and skip the PIN entry.
Protection for clusters	Not available.	Windows Server 2012 BitLocker includes the ability to support cluster shared volumes and failover clusters as long as they are running in a domain that was established by a Windows Server 2012 domain controller with the Kerberos Key Distribution Center Service enabled.
Linking a BitLocker key protector to an Active Directory account	Not available.	BitLocker allows a user, group, or computer account in Active Directory to be tied to a key protector. This key protector allows a protected data volumes to be unlocked.