Quest

Password Propagation Service for Directory Sync Pro

User Guide

© 2025 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Password Propagation Service for Directory Sync Pro User Guide
Updated - March 2025
Version - 20.11.3

Contents

Introduction **4**
About Password Propagation Service 4
Requirements 4
Security 4
For Password Change Service 4
For Password Filter 5
Network Ports 5

Installation and Configuration **6**
Enabling Password Propagation Service 6
Installing Password Change Service 7
Configuring Password Propagation Server 15
Installing Password Filter 18

View Logs **25**

Frequently Asked Questions **26**
General FAQs 26

About us **28**
Technical support resources 28

Introduction

About Password Propagation Service

Password Propagation Service is a component of Directory Sync that allows password synchronization in environments without RC4 Encryption. Unlike the Legacy Password Monitor Service, which requires RC4 Encryption, Password Propagation Service simply copies the password from the source to the target.

When a password changes in the source, the password filter installed on every domain controller in the source environment will capture the password and use the Password Propagation Service to set the password in the target using LDAPS security.

Requirements

Security

- LDAPS must be configured. See Enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) - Windows Server from Microsoft for more information.

For Password Change Service

- Windows Server 2019 or 2022
- 4 vCore, 16GB RAM
- An Administrator Account to install and configure the Password Change Service. It must have access rights to all domains and objects in scope for all users require the password propagation service.
- An Account has with Full Write access to the target user objects in-scope for the password changes.
- Windows Internet Information Server (IIS) must be preconfigured with certificate provisioned.
- TLS 1.2 or higher. Note, for the Password Propagation Service, TLS 1.2 will need to be enabled to communicate with the Directory Sync Server as TLS 1.2 is still required for SQL Server.
- .NET Framework 4.7.2
- Third-party anti-virus or threat prevention programs may block the execution of password tasks. These programs may need to be uninstalled from both the Domain Controller and otherwise carefully whitelist all files related to Password Filter to allow proper operation.

  C:\ProgramData\Quest\DS Password Change Service

For Password Filter

- Windows Server 2019 or 2022
- An Administrator Account to install and configure the Password Change Service
- Must be installed on all domain controllers in the source environment
  Note, Read Only Domain Controllers can be excluded.
- Third-party anti-virus or threat prevention programs may block the execution of password tasks. These programs may need to be uninstalled from both the Domain Controller and otherwise carefully whitelisted to allow proper operation.
  C:\Program Files\Quest\DS Password Change Relay Service
- TLS 1.2 or higher. Note, for the Password Propagation Service, TLS 1.2 will need to be enabled to communicate with the Directory Sync Server as TLS 1.2 is still required for SQL Server.
- .NET Framework 4.7.2

Network Ports

The general requirements for Directory Sync Pro are available in the Directory Sync Pro for Active Directory Requirements and Installation Guide.

Below are the general requirements for Password Propagation Service:

- Port 443 is required for Password Filter, Password Change Service.
- Port 636, 3269 is required for LDAPs. Please refer to Enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) - Windows Server | Microsoft Learn for LDAPs requirement

Installation and Configuration

Installing and configuring the Password Propagation Service requires the following actions:

1. When configuring Password Propagation Service with On Demand Migration Active Directory, enabling the Password Propagation Service option on the Environment Passwords Setting page and downloading the Password Propagation Service Download.

   When configuring Password Propagation Service with Directory Sync and Migrator Pro for Active Directory, enabling the Password Propagation Service option on API Keys link under the menu in the top right corner.

2. Installing the Password Change Service (Both Password Change Service and DS Password Change Web Service components) on a dedicated server or on the Directory Sync Agent Server in the source environment.

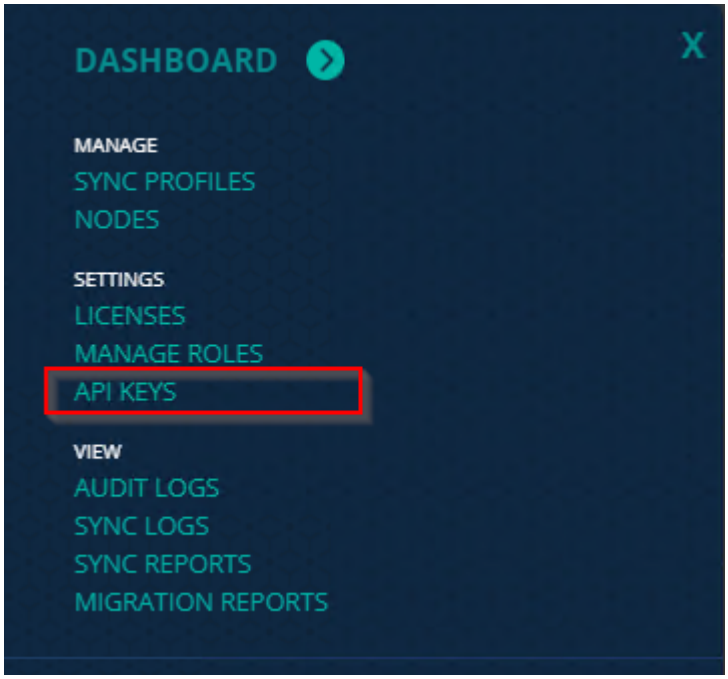
3. Configuring the Password Propagation Server for the target environment where the passwords will be changed.

   Note: The Password Propagation Service must be preconfigured with Windows Internet Information Server (IIS) with certificate provisioned.

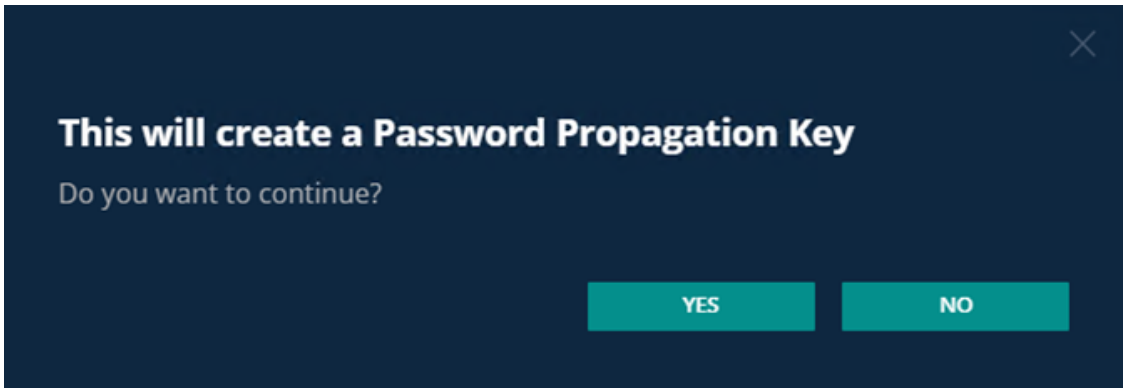
4. Manually installing Password Filter on every Domain Controller in the source Active Directory forest.

Enabling Password Propagation Service

1. Navigate to the **API Keys** link from the right navigation menu.



2. On the API page, click on **Create**.
3. Click **Yes** to create the Password Propagation Key.

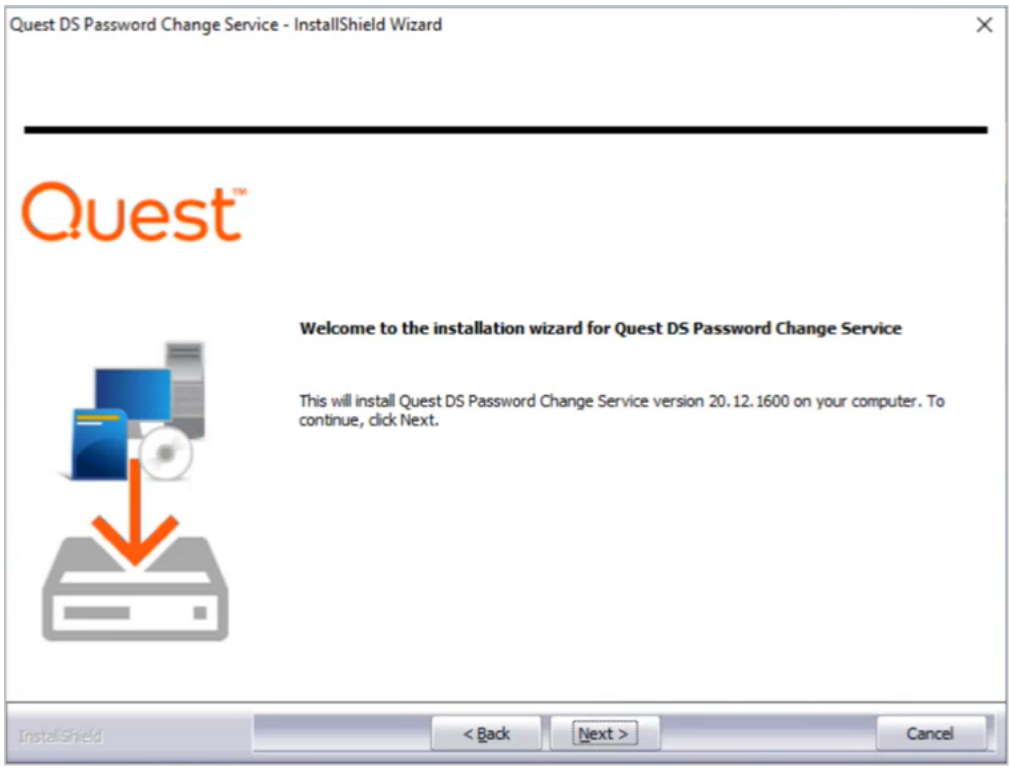


4. Copy the API Key for later use when installing the Password Propagation Service.

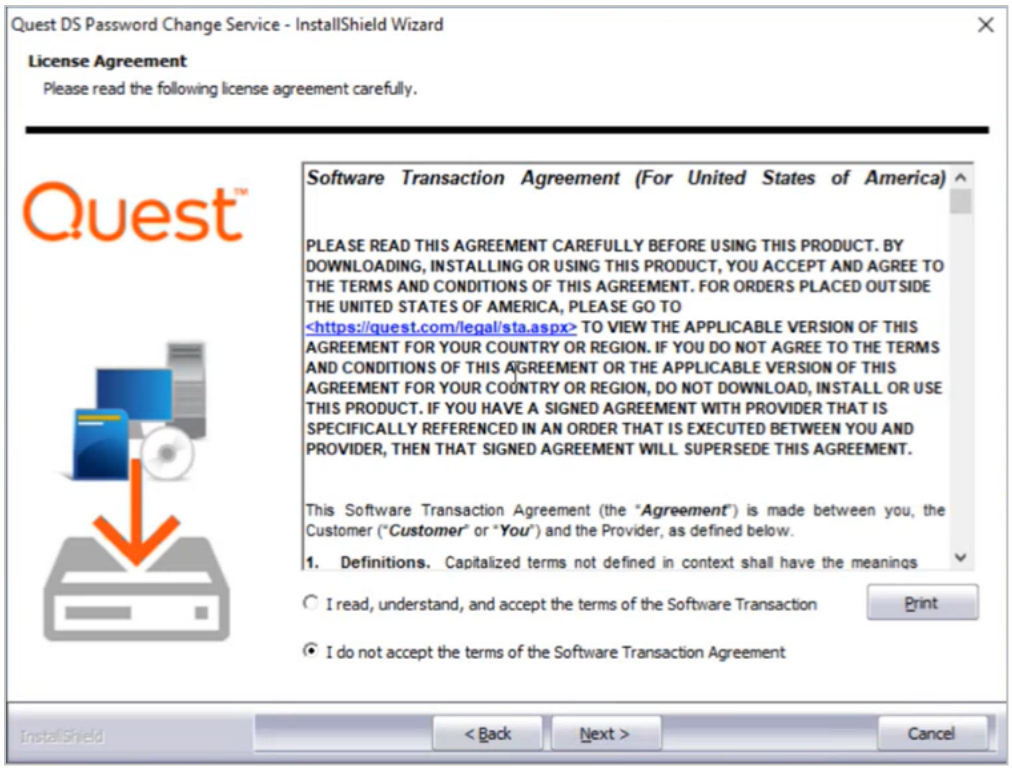
Installing Password Change Service

1. On the source environment, click the QuestPasswordPropagationService icon. The install wizard appears.

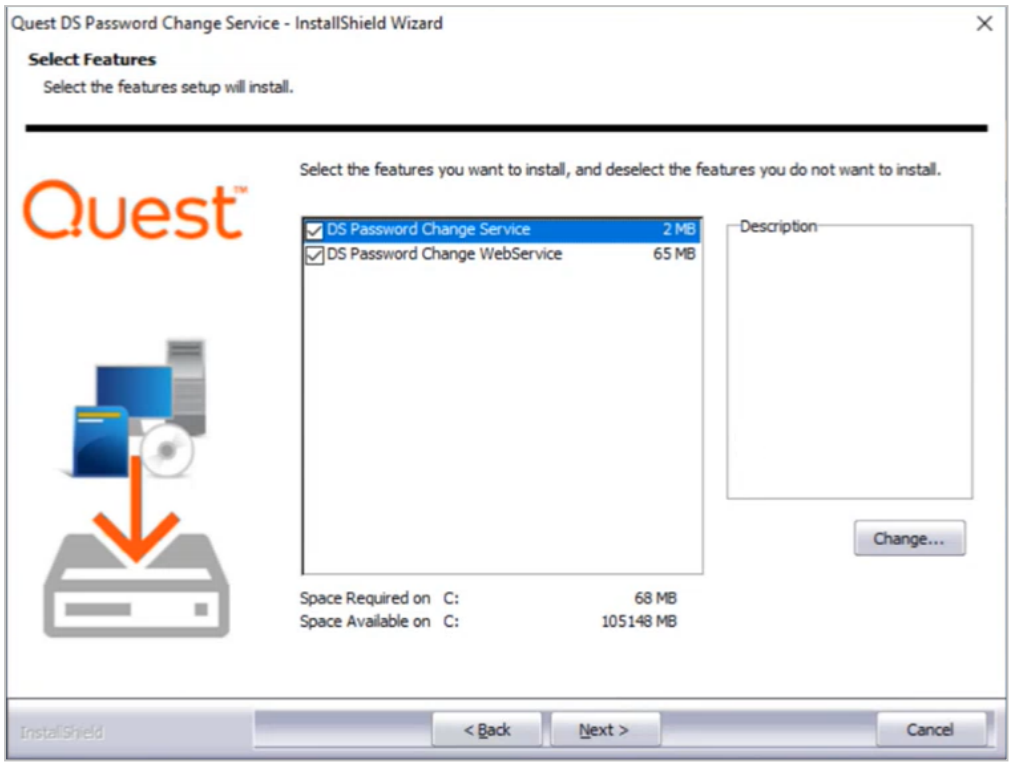
2. Click **Next** on the Welcome screen.



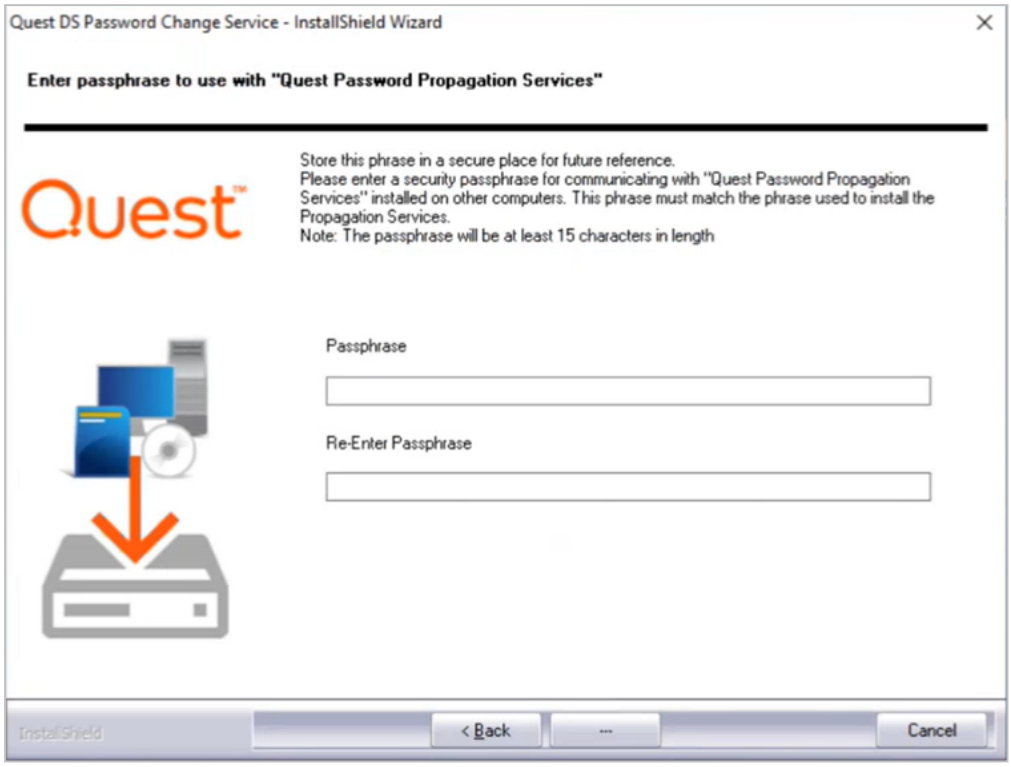
3. Read and accept the License Agreement. Click **Next**.



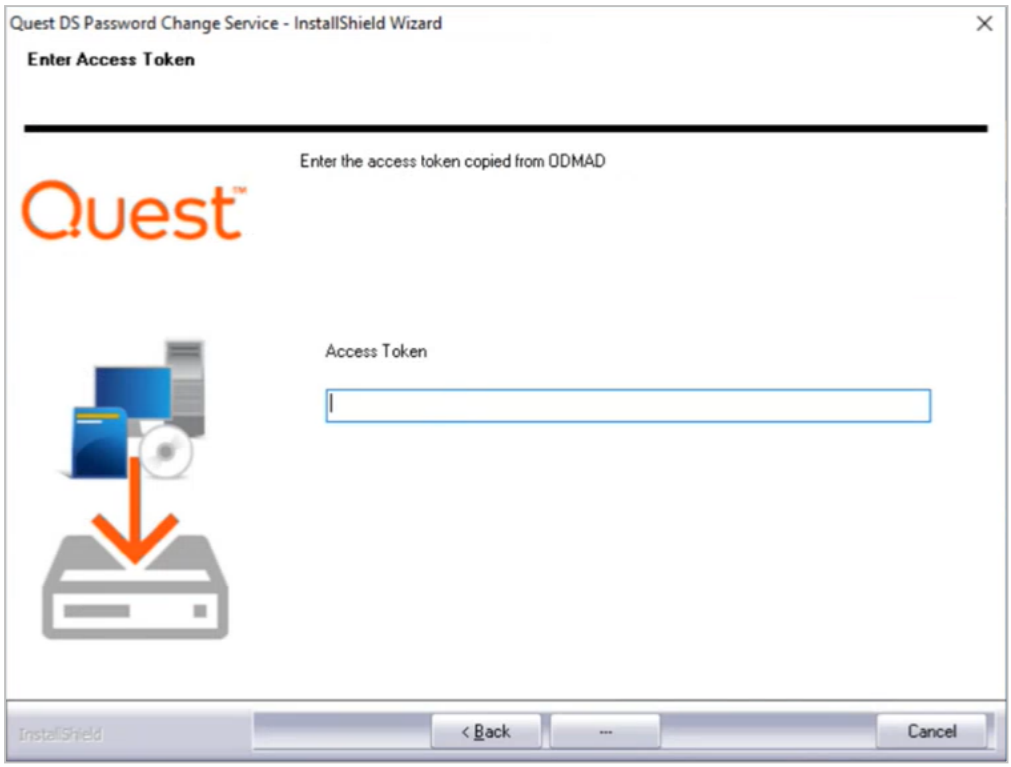
4. Check the **DS Password Change Service** and **DS Password Change WebService** features and click **Next**. Both features are required.



5. Enter a security passphrase for communicating with Password Propagation Services installed on other computers. This phrase must match the phrase used to install the Password Filter. The passphrase must be at least 15 characters long. Click **Next**.

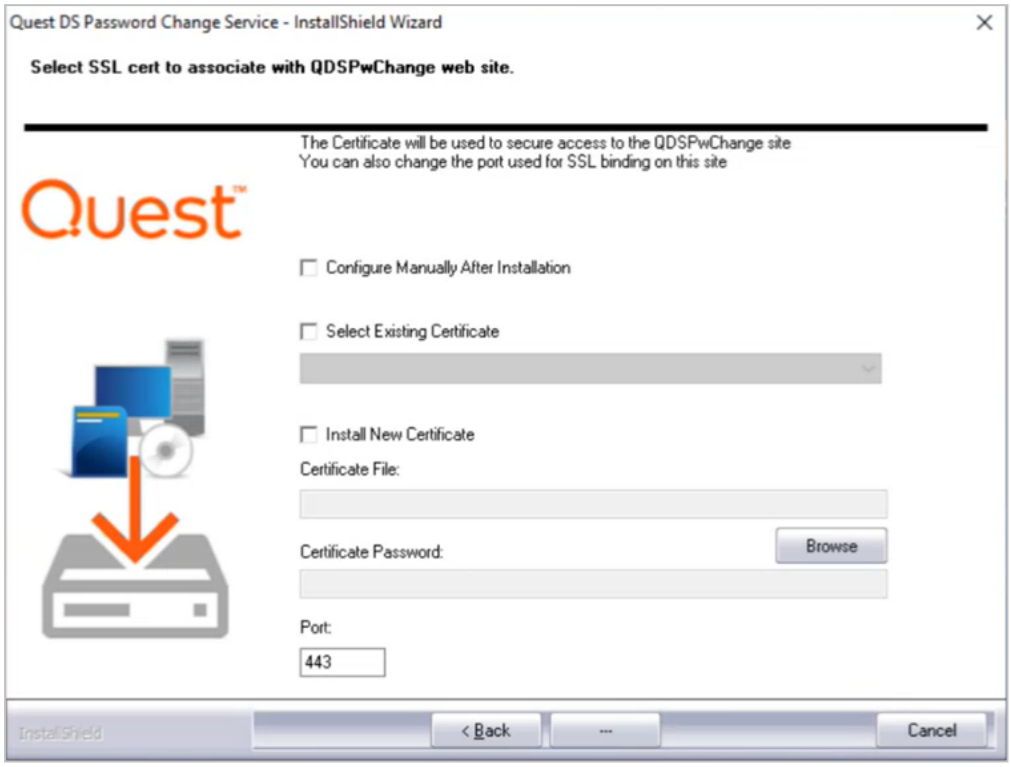


6. Enter the Password Propagation API Key found on the API Keys page. Click **Next**.

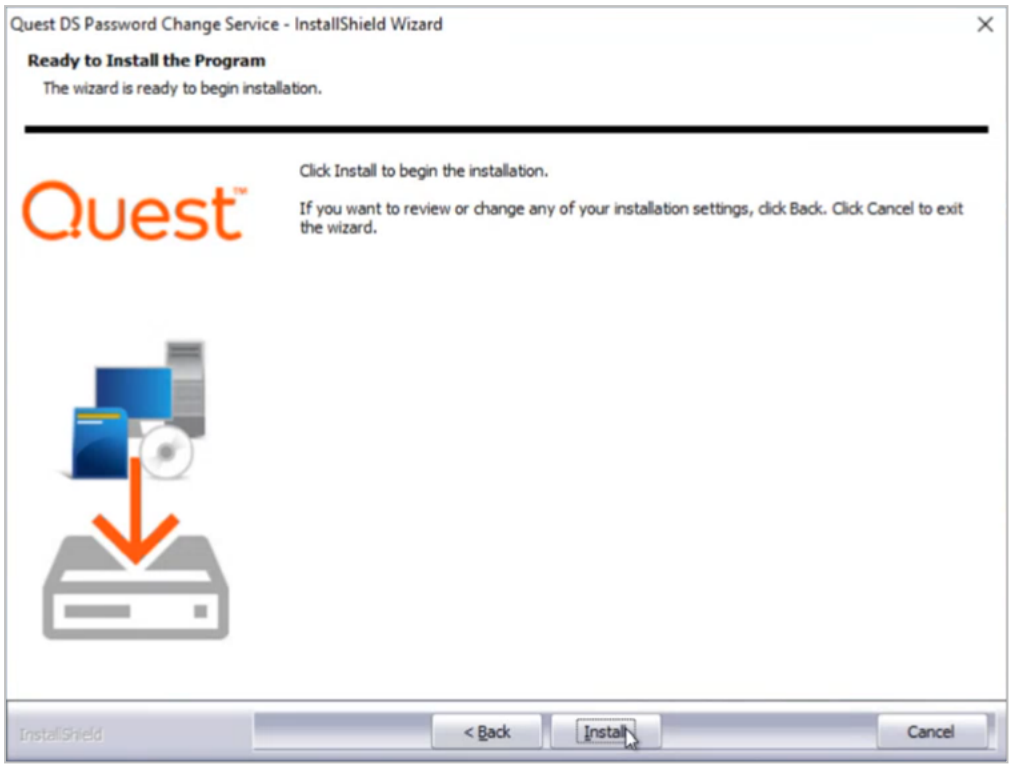


7. Select or install the SSL certificate to use to securely access the QDSPwChange site. The default port is 443 and can be changed if needed. Click **Next**.

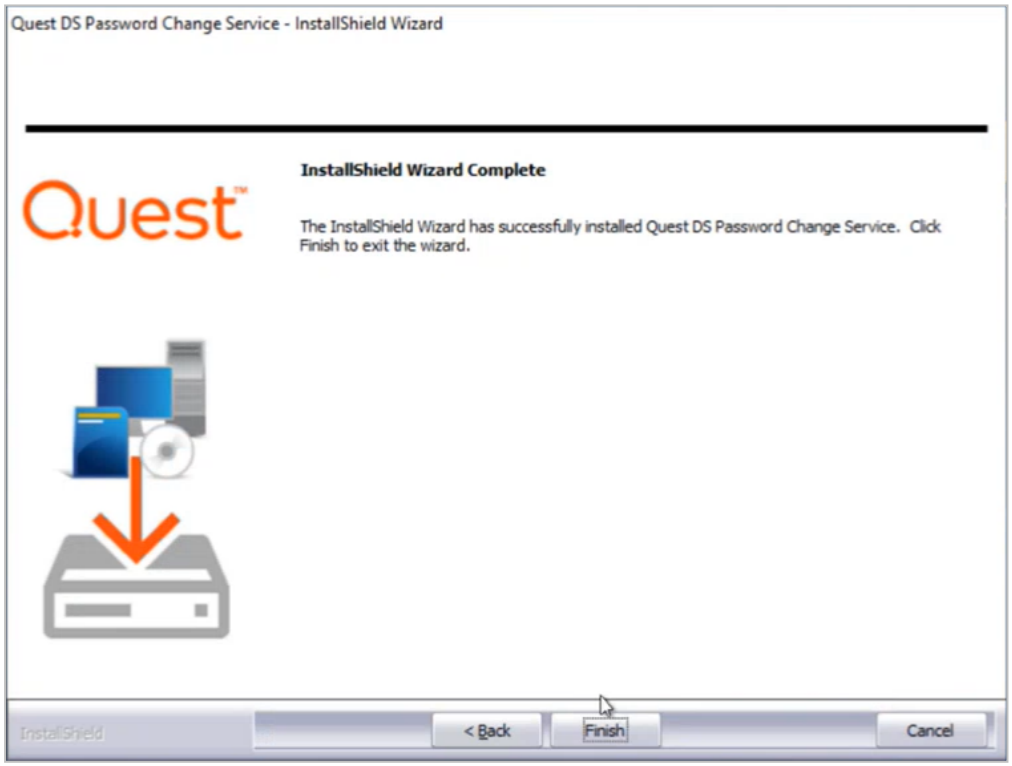
   Note: The SSL certificate can be preconfigured. See Internet Information Services (IIS) Server Certificate Installation Instructions at Microsoft for more information.



8. Click **Install**.



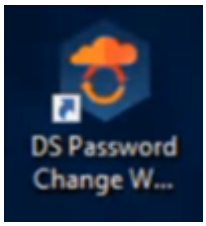
9. Click **Finish** on the Complete screen.



Configuring Password Propagation Server

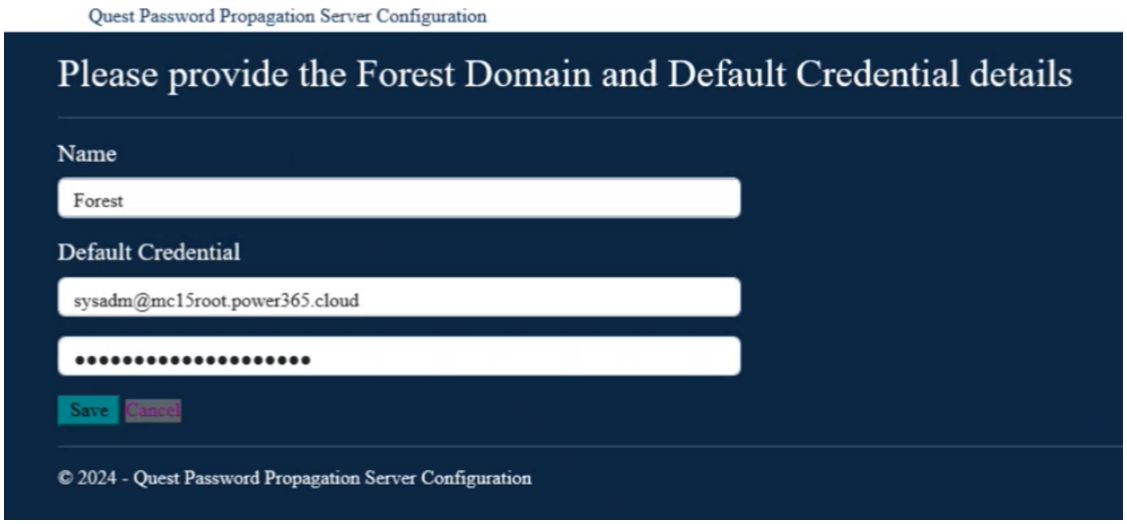
Use the Password Change WebService to configure The target environment where the passwords will be changed.

1. Click on the DS Password Change WebService icon. The Password Propagation Server Configuration page will open.

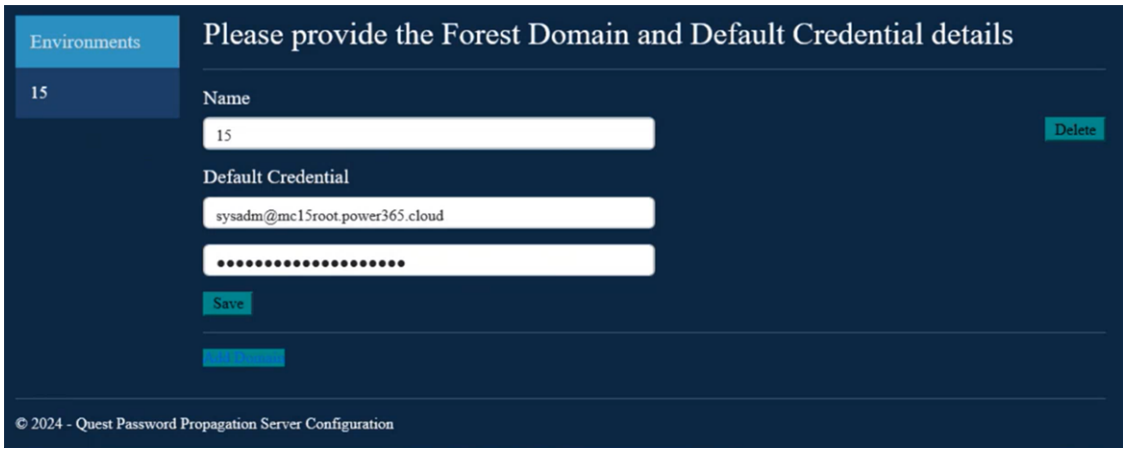


2. On the Environment Configuration page, click **Add Forest**.

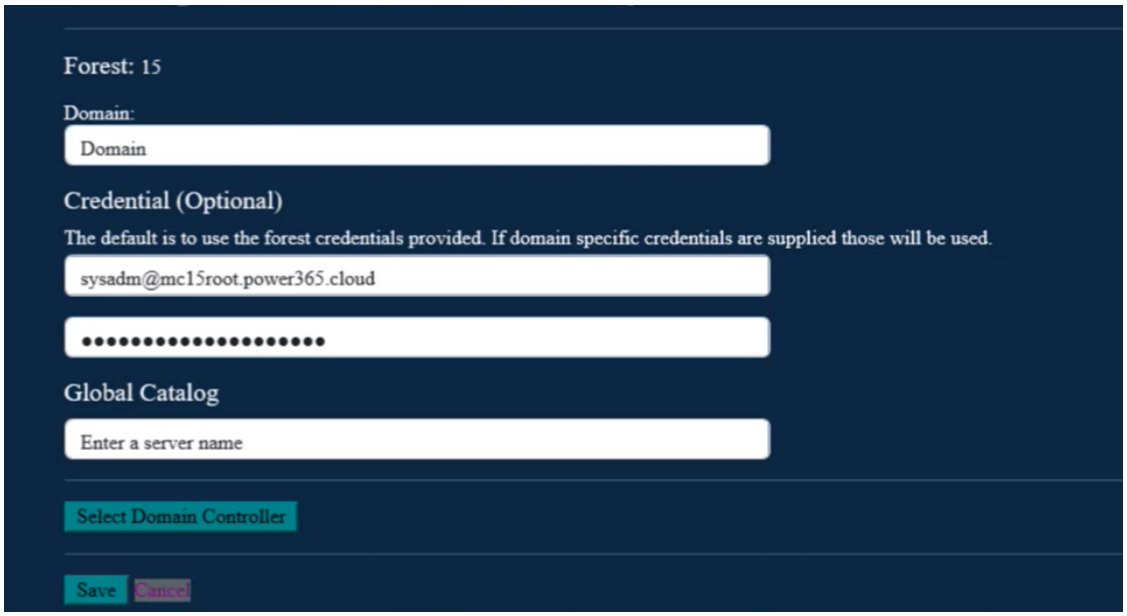
3. Enter a Forest Name and Default Credential. Click **Save**.



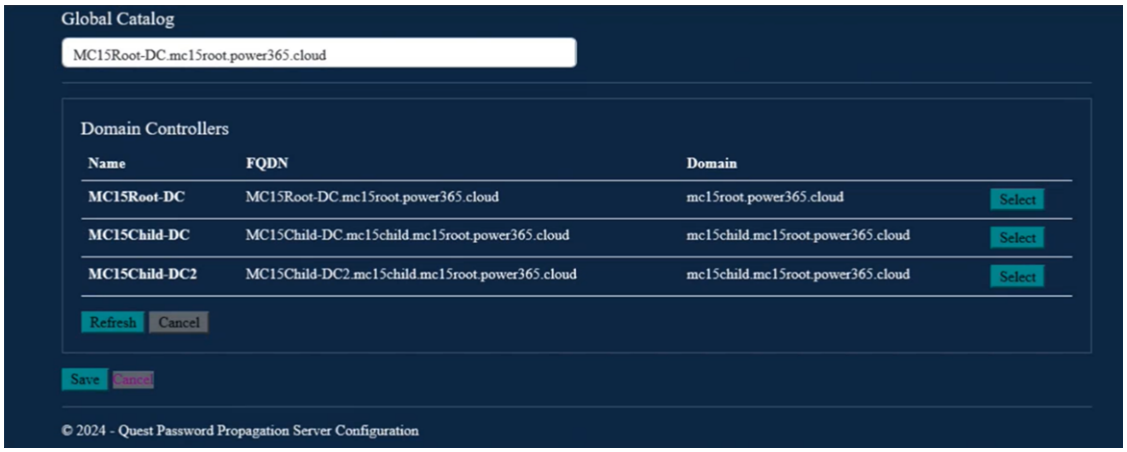
4. Click **Add Domain** to add one or more Active Directory domains to the forest.



5. Enter the Domain Name and optional Credential. If left blank, the forest credentials will be used. Enter the Global Catalog name.

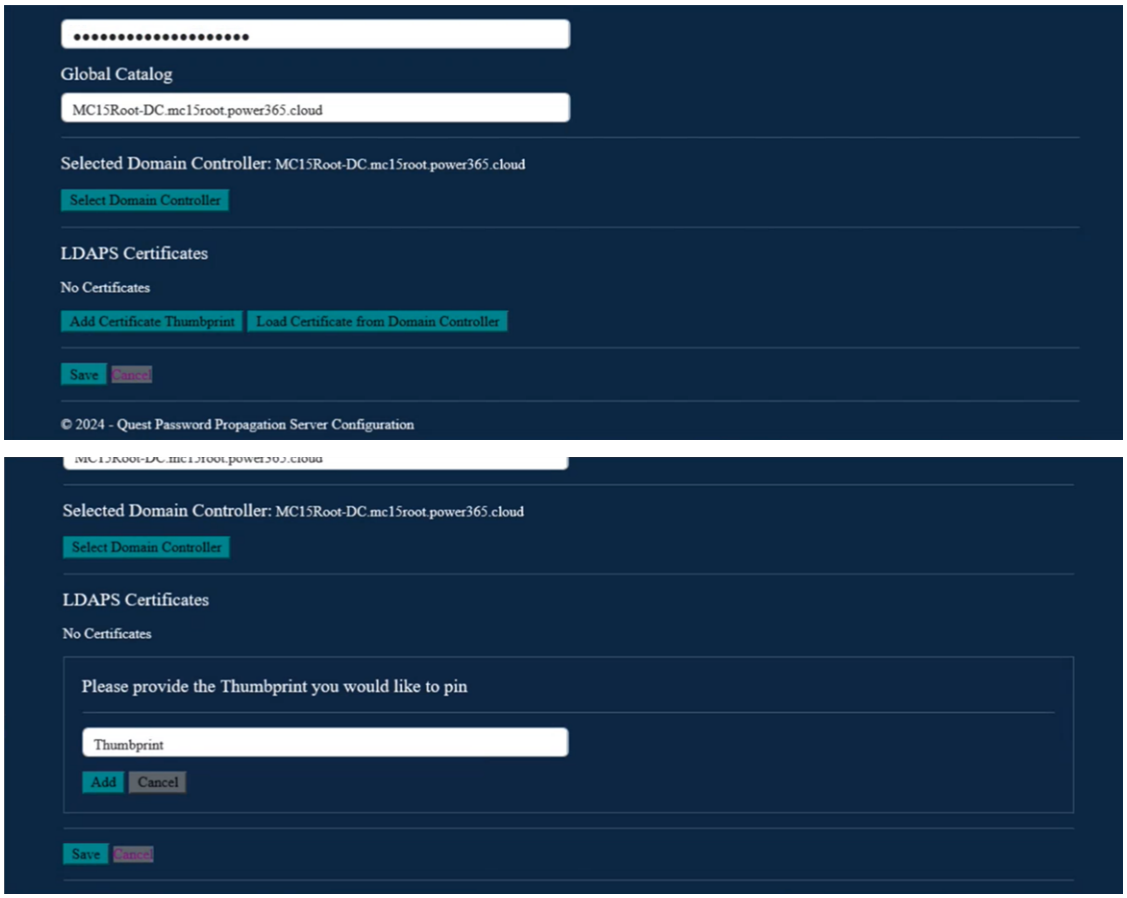


6. Click **Select Domain Controller** and then click **Select** next to the Domain Controller you wish to use.



7. To configure the LDAPS Certificates, click either **Add Certificate Thumbprint** to add the thumbprint or click **Load Certificate from Domain Controller** to retrieve the thumbprint from the Domain Controller.

   Note: See How to: Retrieve the Thumbprint of a Certificate at Microsoft for more information.



8. Click **Save**.

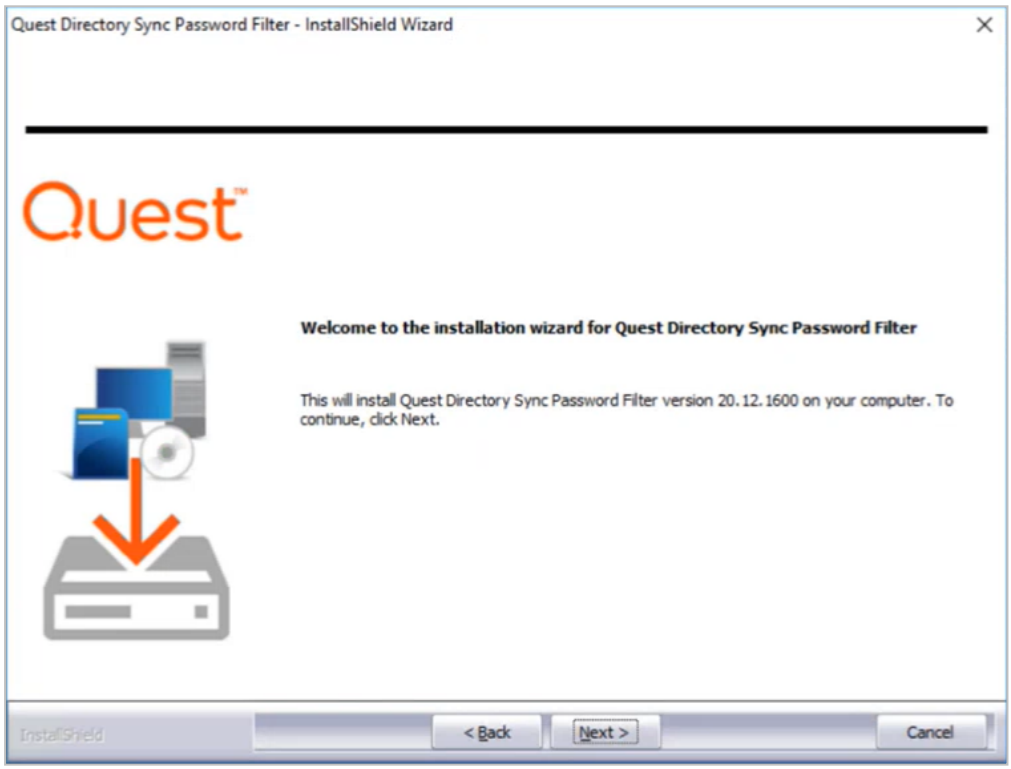
9. To add additional domains, return to the Forest page and click **Add Domain**.

Installing Password Filter

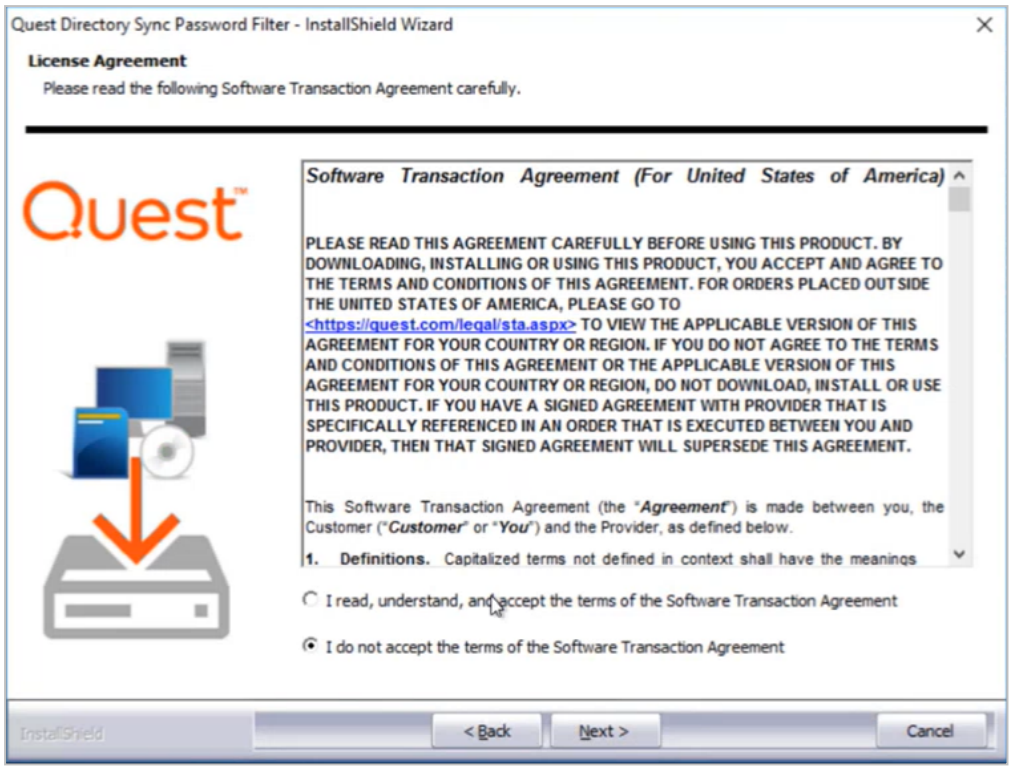
The Password Filter is installed on every Domain Controller in the source. The filter detects password changes in the source and sends the password information to the Change Service to set in the target.

1. On the Domain Controller, click the QuestDirectorySyncPasswordFilter icon. The install wizard appears.

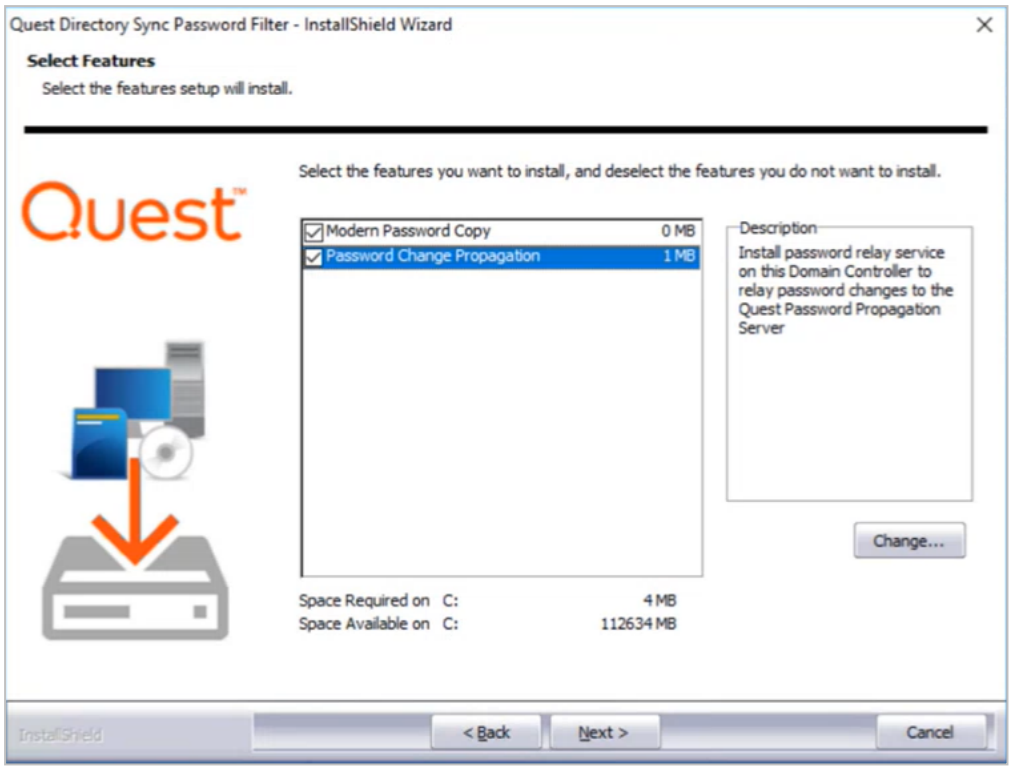
2. Click **Next** on the Welcome screen.



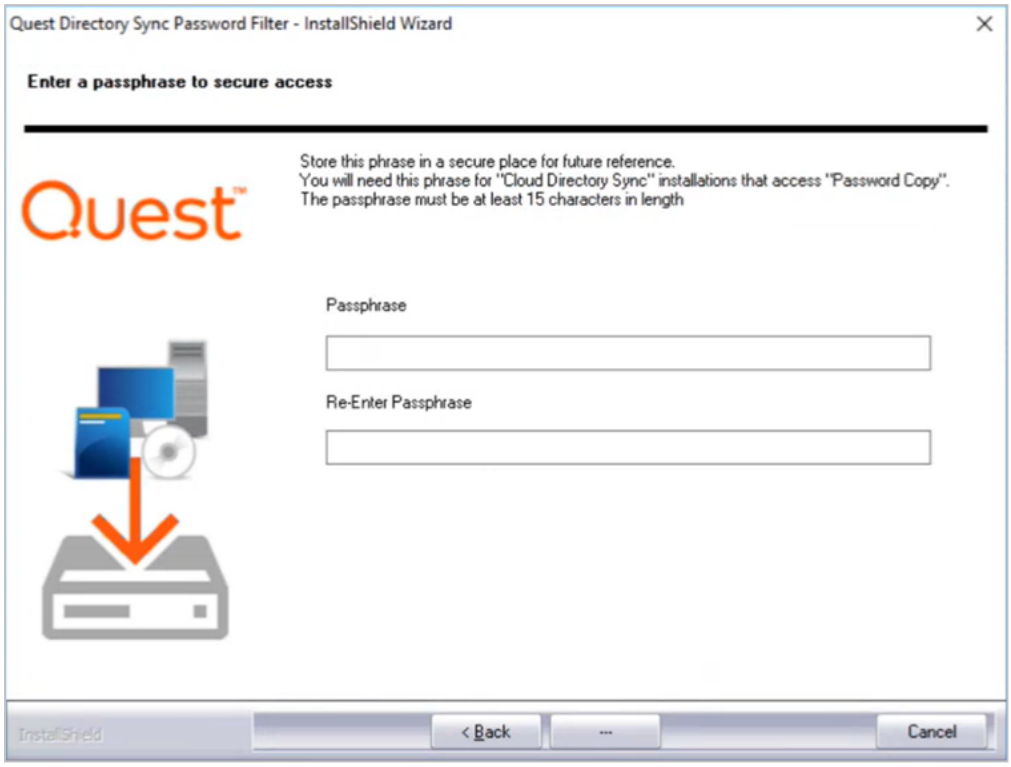
3. Read and accept the License Agreement. Click **Next**.



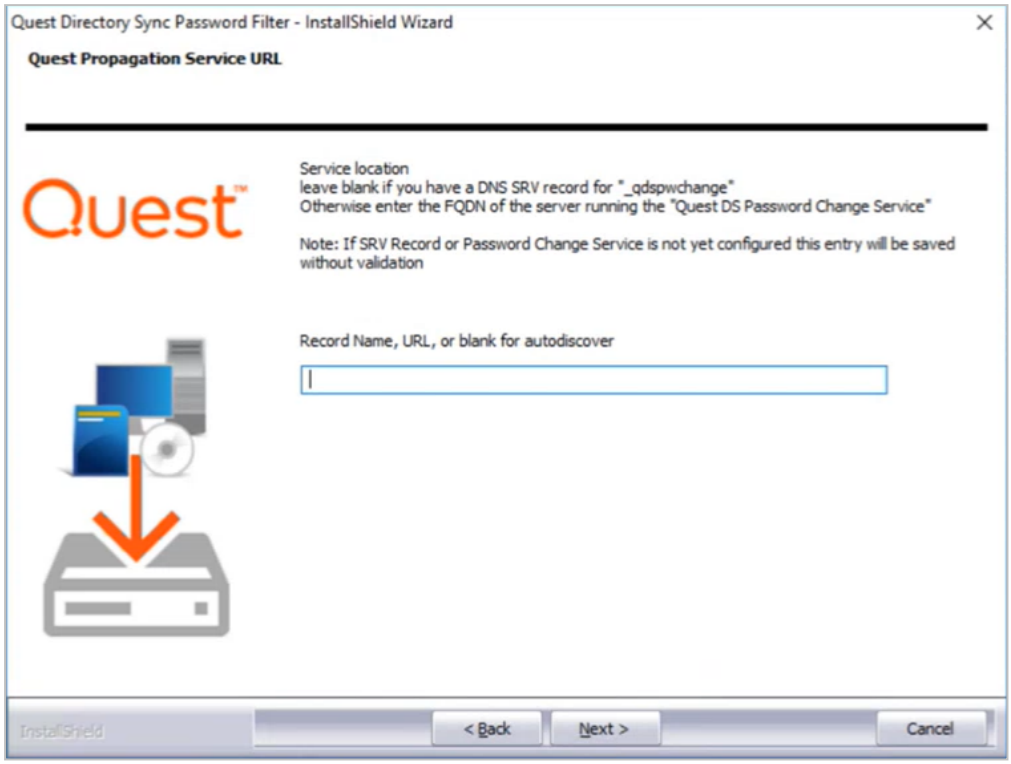
4. Check the **Password Change Propagation** feature and click **Next**. The install wizard can also install the Modern Password Copy feature if needed.



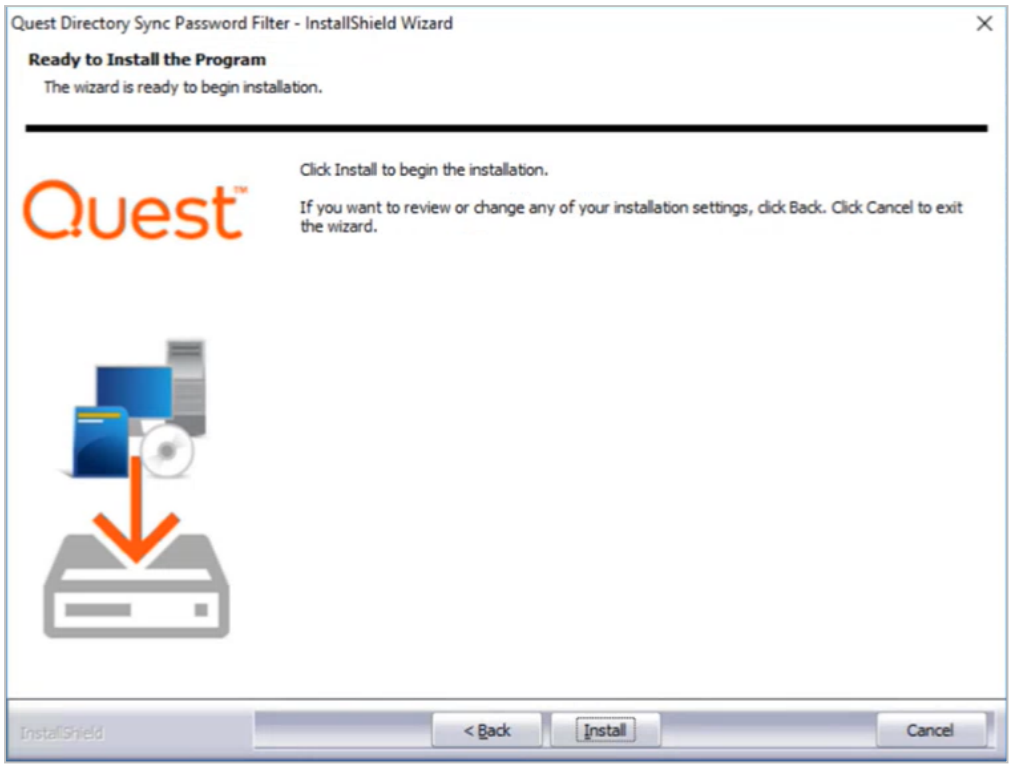
5. Enter a security passphrase for communicating with Password Propagation Services installed on other computers. This phrase must match the phrase used to install the Change Service. The passphrase must be at least 15 characters long. Click **Next**.



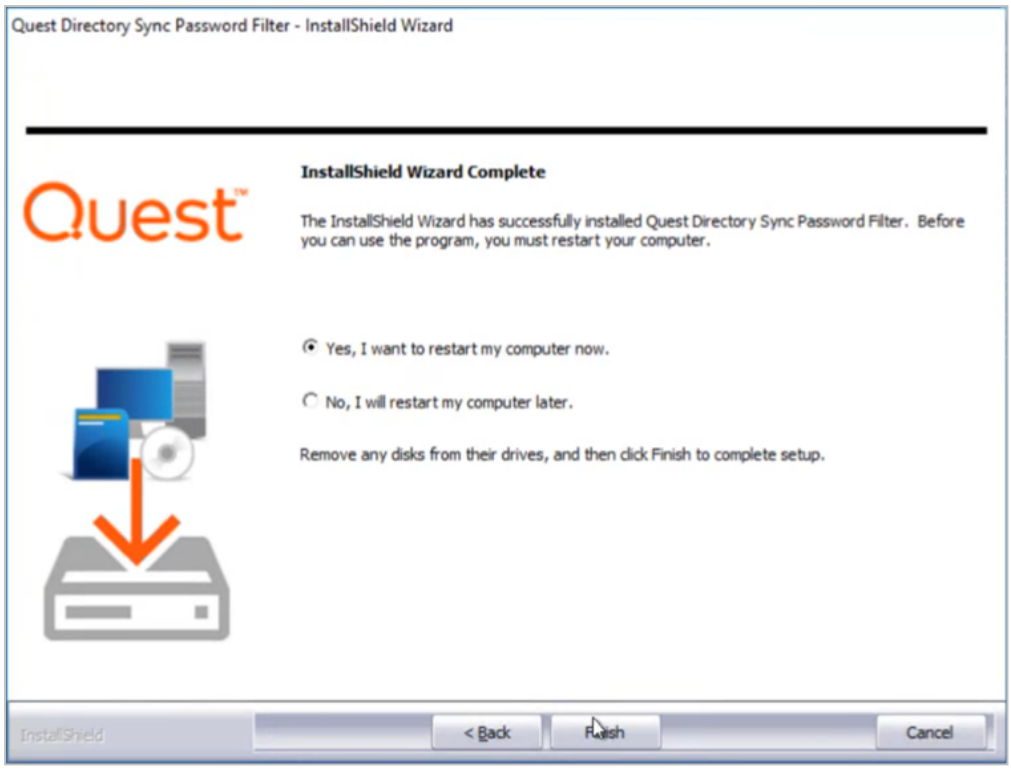
6. On the Quest Propagation Service URL page, enter the FQDN of the server running the "Quest DS Password Change Service" or leave the field blank if you have a DNS SRV record for "_qdspwchange". Click **Next**.



7. Click **Install**.



8. Click **Finish**. You must restart the computer before the program.



9. Repeat the install process on all other Domain Controllers in the source. Istallation must be configured manually on all Domain Controllers.

View Logs

Password change logs in CSV format are available in the source directory at ProgramData > Quest > DS Password Change Service > PsChangeAuditxxxxxxxx.csv.

Frequently Asked Questions

General FAQs

How do I configure an SRV record for the Password Change Service FQDN?

Please review the MS link on how to create an SRV record in General. Also, we provided the below step by step instructions for your reference.

1. Log on to the DNS server and open the DNS Manager
2. Open **DNS** and choose the zone to create the SRV record for (Current domain, forward lookup zone).
3. From the Context menu, select **Other New Records...**, navigate to **Service Location (SRV)**, and choose **Create Record**.
4. Fill in the form (shown in the following figure), specifying "_qdspwchange" to the Service: input box.
    - Enter an FQDN of the host computer (for example, Server1.contoso.com) to the **Host offering the Password Change Service**.
    - Select _http (_https) in the **Protocol:** field.
    - Select 443 in the **Port number:** input box.

How do I configure LDAPS?

Microsoft provides an article on how to enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) with a third-party certification authority: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/enable-ldap-over-ssl-3rd-certification-authority.

How do I preconfigure the SSL Certificate?

Microsoft provides instructions on how to install an IIS server certificate: https://learn.microsoft.com/en-us/dotnet/framework/wcf/samples/iis-server-certificate-installation-instructions.

How do I find a certificate's thumbprint?

Microsoft provides a how-to article on how to retrieve the thumbprint of a certificate: https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate.

Do Passwords pass through On Demand Migration servers? (only applicable when working with On Demand Migration Active Directory)

Password Propagation Service syncs directly from the source Active Directory to the target Active Directory without transmitting passwords to On Demand Migration. User mapping data captured by the On Demand Migration Directory Sync Service is used solely to map the source and target user objects and Active Directory to facilitate the synchronization of passwords.

Can I enable Legacy/Modern Password Copy while using Password Propagation Service?

Password Propagation Service provides password synchronization functions for environments that have RC4 encryption disabled. Legacy and Modern Password can copy passwords, but it can only copy NTLM or RC4 Password Hash. For this reason, if the environment has RC4 disabled, we cannot enable both Password Copy and

Password Propagation Service at the same time. Password copy can be enabled to copy the NTLM/RC4 passwords, but once RC4 is disabled in the environment, Password Propagation Service should be used instead.

How can I trigger passwords to be synced to the target user when using Password Propagation Service?

Unlike Password Copy (Legacy and Modern) which will copy the Password Hash to the target user object, Password Propagation will set the password to the target object when the password is changed in the source. Therefore, passwords can only be synced/set in the target if the source user password was changed by either the end user or the administrator.

Do I need to add all domain controllers from my target Active Directory in the Password Change Service Environment setting on my local server?

No, you do not need to add all domain controllers in your target Active Directory. Only one domain controller per domain is needed.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product