Identity Management in Microsoft Environments   
Final Project

March 2020

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

This training uses various tools and utilities downloaded from the Internet for the classroom environment.   
Downloading any tools, installing and using them should only be done at your own risk security checked the tools in a test environment.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

[Identity – Final Project 1](#_Toc531612635)

[Abstract 1](#_Toc531612636)

[The Story 1](#_Toc531612637)

[Deliverables 2](#_Toc531612638)

[Evaluation Method 3](#_Toc531612639)

[Virtual environment information 4](#_Toc531612640)

[Bloodhound installation guide 5](#_Toc531612641)

# Identity – Final Project

## Abstract

In this project you will play the role of a Security Consultant hired by the Contoso company.

## The Story

Woodgrove Bank is one of the largest financial organization in Europe. They recently acquired Contoso Corporation which is the online banking leader in North America. As a part of the acquisition, the Woodgrove Bank’s CTO wants employees of both companies to share their CRM data. The security architects at Woodgrove Bank also plan to migrate users and resources from Contoso’s AD DS forest to theirs. During the migration process, both forests will be available and single-sign-on will be operational for all users.

Before starting this project, Contoso’s CISO has mandated you and your team to assess the level of security of Contoso Corporation’s AD DS and to make recommendations to secure it prior to the migration.

Miscellaneous information

To migrate the users and data, the team of architects has planned to create AD DS bi-directional trust between the two forests.

* Contoso has many legacy applications relying on LDAP for authentication.
* Sensitive files are stored on specific files servers on both companies.
* All Contoso domain controllers are virtual.
* Contoso is running only Windows 10 machines for their workstations and Windows Server 2012 R2 and Windows Server 2016 for their servers.
* Woodgrove is using a wide variety of operating systems ranging from Windows 2003 to Windows Server 2016.

Data available

To assess the security of Contoso Corporation’s AD DS forest you will be given access to:

* A privileged account for Contoso AD DS
* Access to a domain controller of Contoso’s AD DS forest (DC01) – VM named ID-Project.
* Access to the raw data collected with Sharphound to be viewed with Bloodhound (note that the clients are servers in the collected data will not be reachable during your assessment)

## Deliverables

The expected deliverables are:

1. **A Word or PowerPoint report:**
   * Review the data collected in Bloodhound and detail a possible attack path against Contoso AD DS (describe the attack step by step including the techniques and tools you would use). You must use screenshots to illustrate the different steps.
   * Identify at least two major misconfigurations on Contoso’s domain controllers and explain why they are putting the environment at risk.
   * Make at least 3 other security recommendations and order them by priority.
2. **A 12 minutes oral presentation of your proposal:**
   * Present a summary of your findings to the CTO and IT directors of Contoso and Woodgrove. This final presentation must not exceed 12 minutes. At the end of the presentation, both companies need to be aware of the security posture of Contoso. You must also present a clear summary of the recommended next steps to secure the environment.

Accepted formats for the deliverables are: Word, PowerPoint and PDF.

Each group will have exactly 12 minutes to present its work. At the end, you will leave the ppt either printed or the digital file.  
**12 minutes is a short time period. You are expected to be on time. Any late arrival will be decremented from the 12 minutes.**

The presentation will be performed in French.

## Evaluation Method

This paragraph explains how your work is going to be evaluated during the presentation session.

At all time, keep in mind that the goal of the project is to train yourself into real-life delivery of a security project. It particularly means that you must not underestimate the non-technical aspects of the project.

Important criteria which will define the success or failure of your performance:

* Ability to demonstrate relevance of any technical product or functionality. The organization won’t spend money in a solution if it does not see its value.
* Ability to demonstrate knowledge of security threats, products or features by being able to explain it in a concise and simple way to a non-expert public (CIO, CISO, …) in a very short amount of time
* Ability to understand the complexity of solutions by being able to determine a reasonable amount of effort to deploy proposed technology
* Presentation skills (you dress and present like it would be a real paying customer)

## Virtual environment information

You can connect to the machine named “**ID-Project**“ provisioned in your student environment.   
This is a virtual machine hosting a domain controller: DC01.CONTOSO.COM.

The IT team gave you the built-in administrator accounts to access the machine:

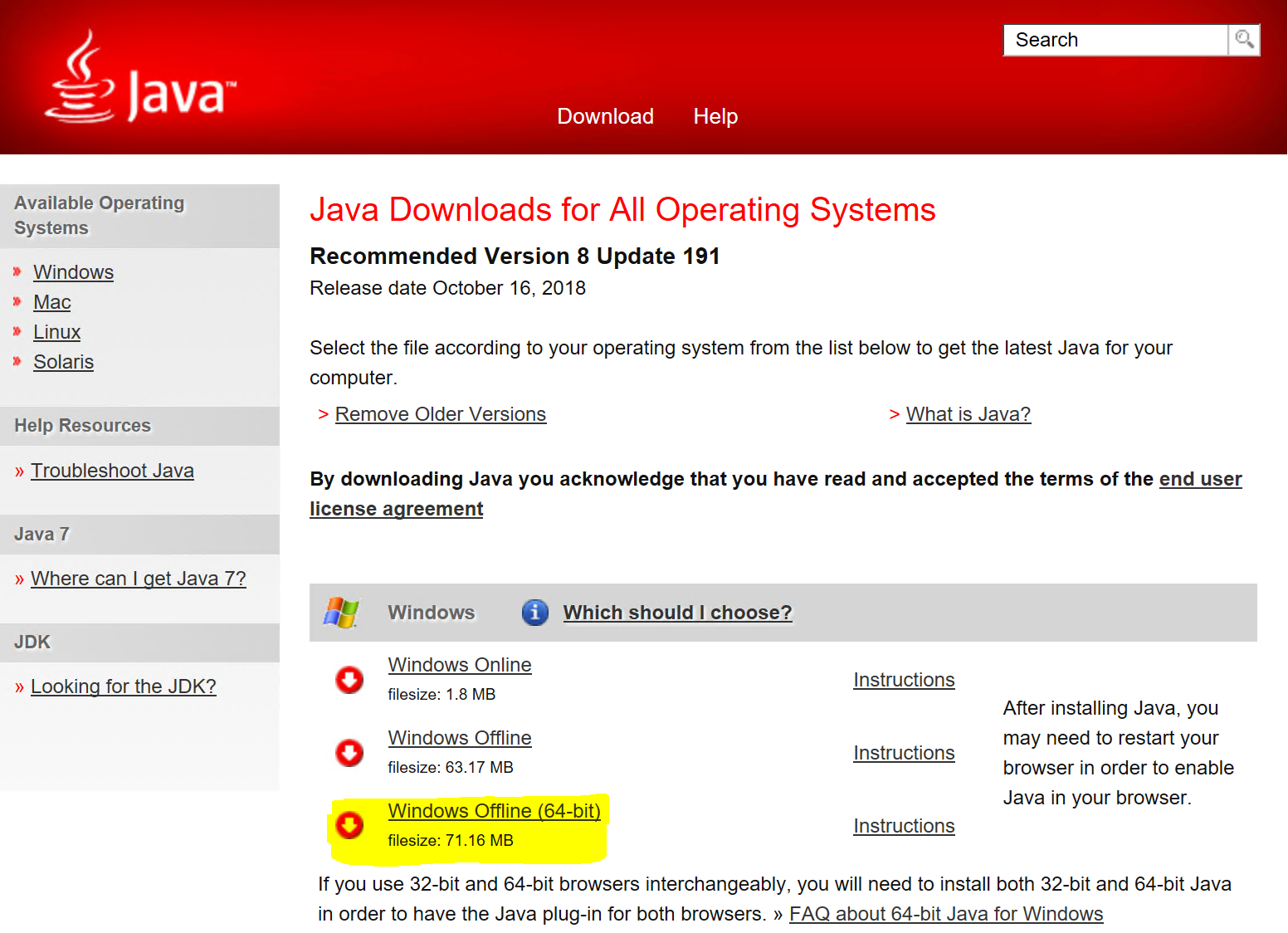
|  |  |
| --- | --- |
| Account | CONTOSO\Administrator |
| Password | PiKarAlR@AlBenMo1 |

Note: this is the only machine available in the environment, all the other machines are not reachable. You can focus your review and analysis on this one and on the contoso.com domain that it hosts.   
Since no other machines are accessible, the network configuration is irrelevant.

## Bloodhound installation guide

This section explains how to install Bloodhound on a Windows 10 (64 bits). You need to be a local administrator of your machine to perform the following operations.

1. **Download Java JRE**  
   Java JRE is required to run the Neo4j database.  
   As of the creation date of this document, the most recent version is Version 8 Update 191.  
   In your browser, go to the following site: <https://www.java.com/en/download/manual.jsp>.

Then download the **Windows Offline (64-bit)**

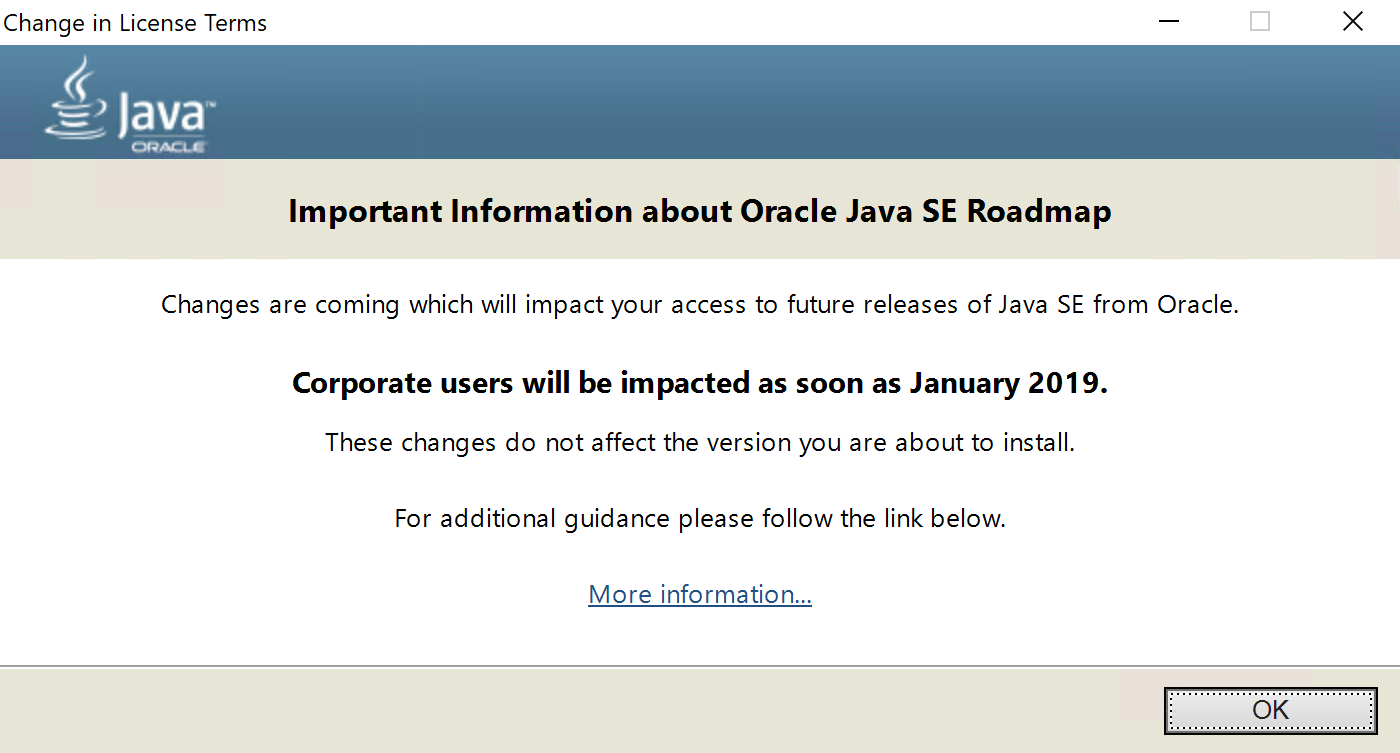
1. **Install Java JRE**

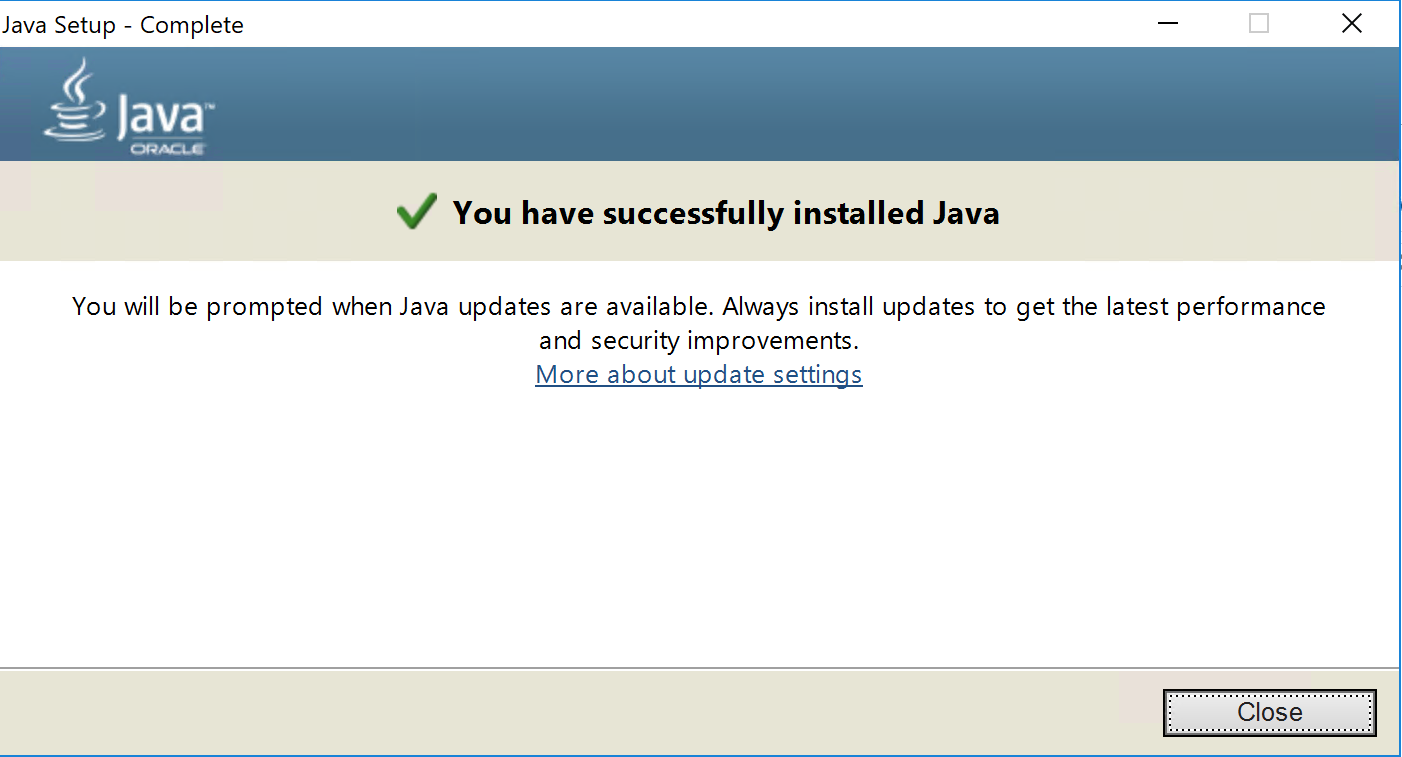
Double-click on the **jre-8u191-windows-x64.exe** executable in your download folder.

In the following window, click **Install >**.



Then click **OK**.

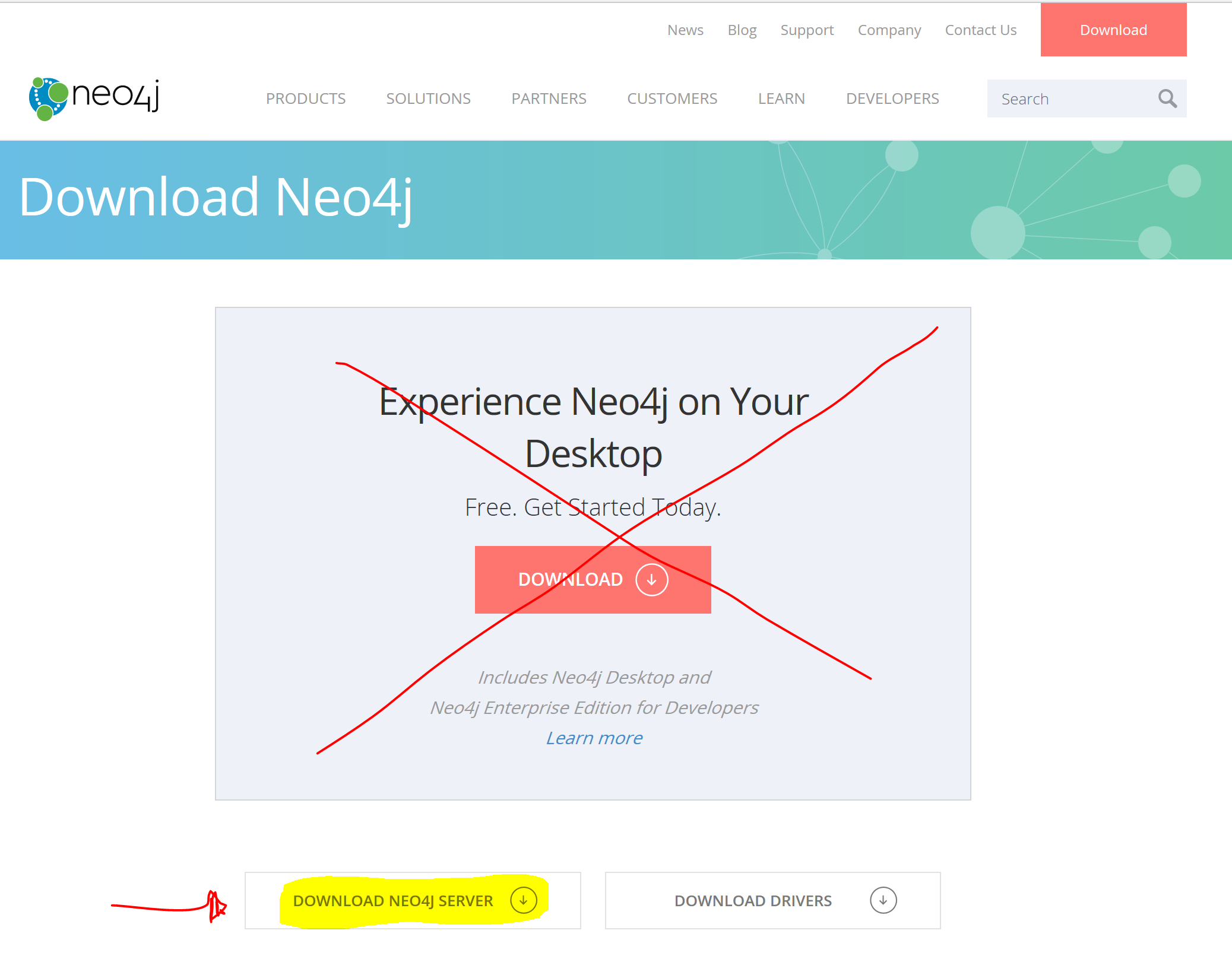
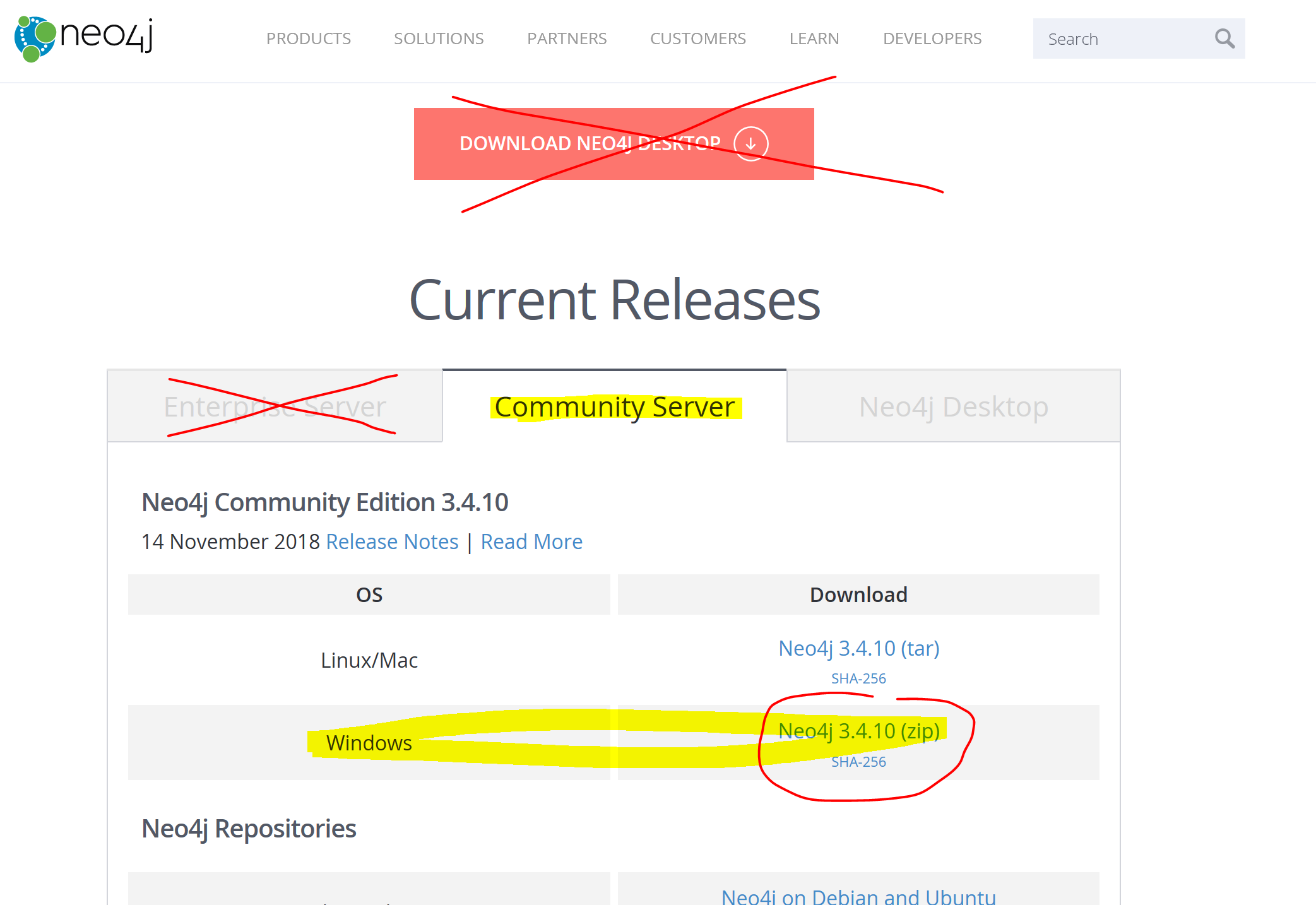


The installation should take a minute or two.  
Then click **Close**.  


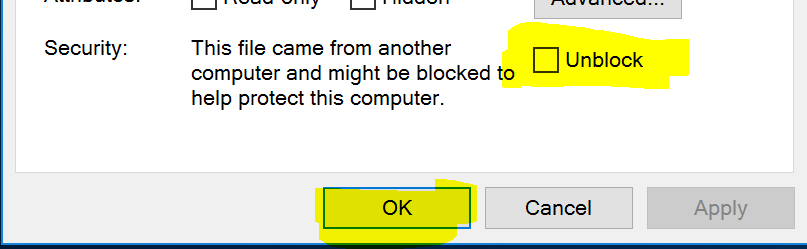
1. **Download Neo4j Community edition**A Neo4j database is required. Bloodhound is a one-page JavaScript application querying a Neo4j graph database.

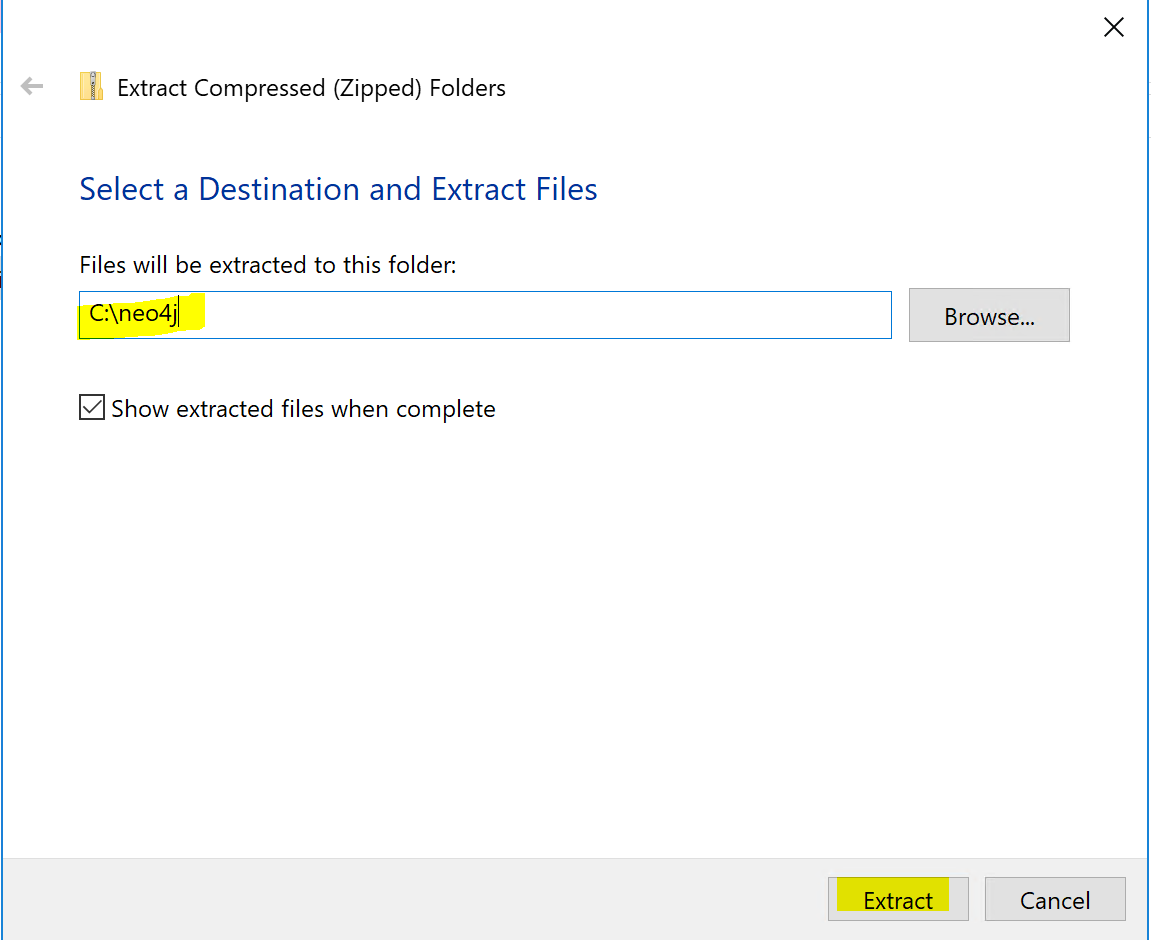
As of the creation date of this document, the most recent version of Neo4j Community is 3.4.10.  
In your browser, go to the following site: <https://neo4j.com/download/>.

Then click on Download Ne4j server:

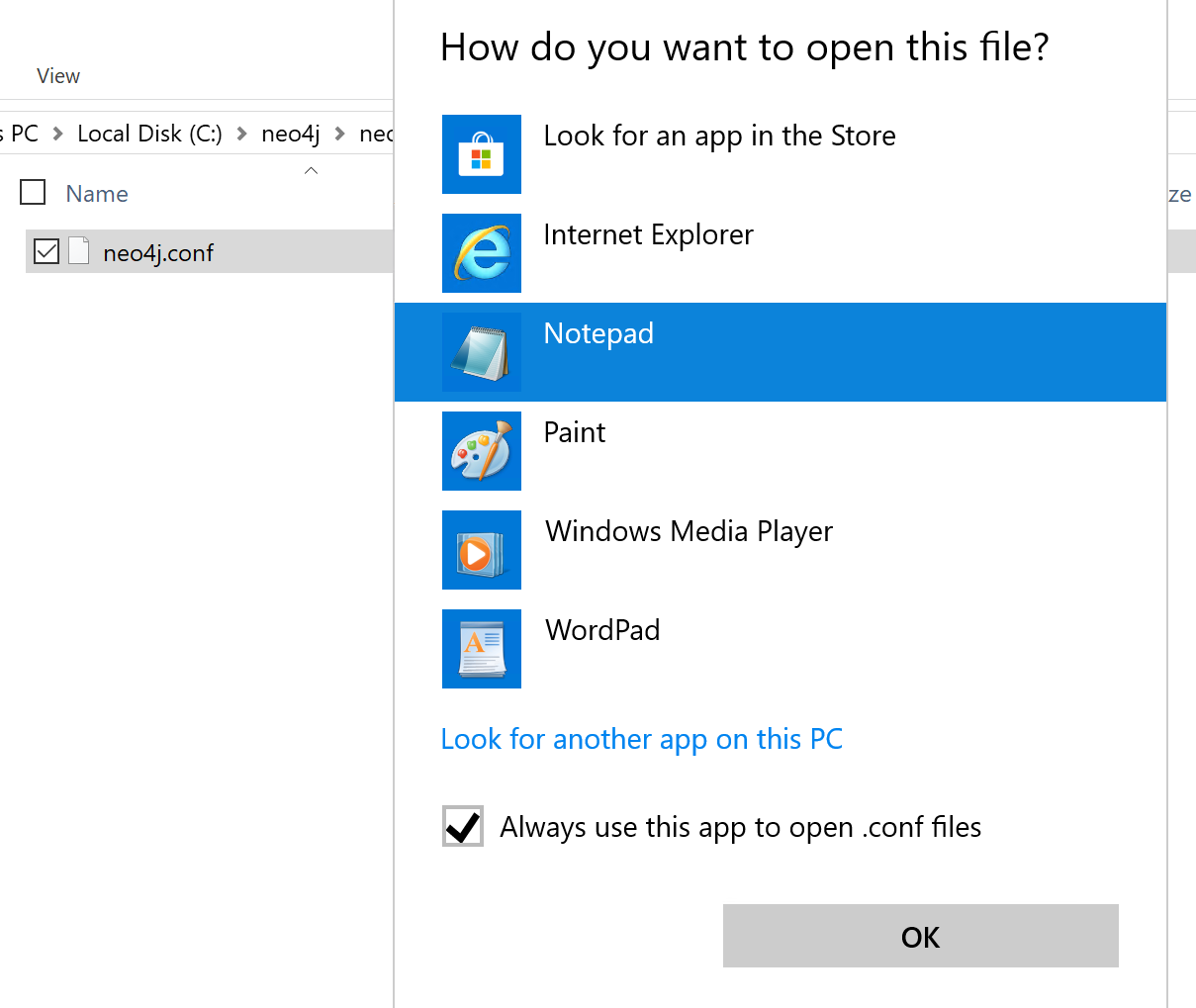
  
Do not download the Desktop version.  
Then click on **Community Server** and download **Windows Neo4j 3.4.10 (Zip)**.  


1. **Install Neo4j Community edition**Open your browser’s download folder and right-click on **neo4j-community-3.4.10-windows.zip** and click **Properties**.

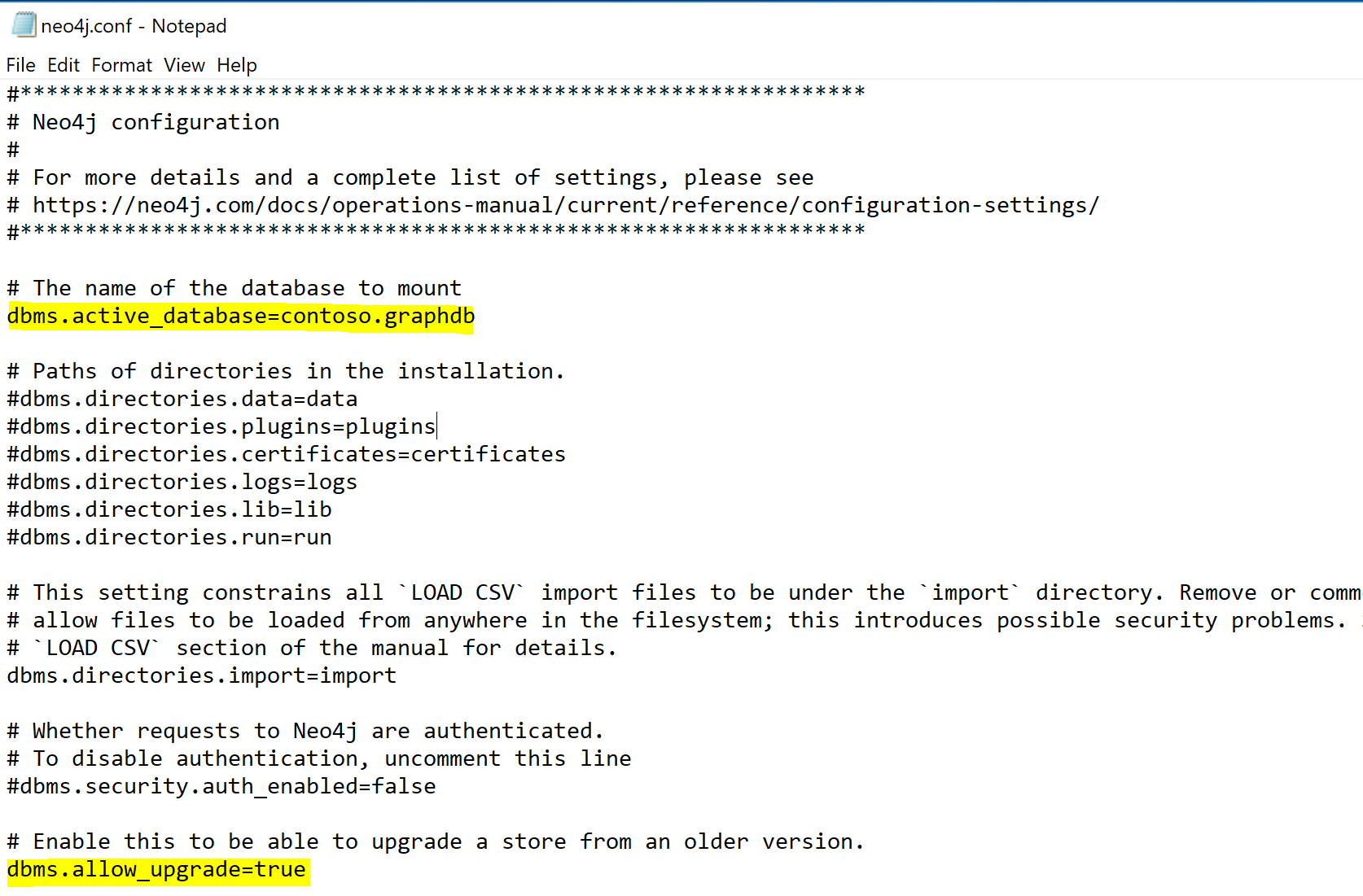
In the **General** tab, check **Unblock** and click **OK**.  


Thenright-click again on **neo4j-community-3.4.10-windows.zip** and click **Extract All**.  
Enter the path **C:\neo4j** and click **Extract**.  


At the end of the extraction, it will open an explorer window in the folder **C:\neo4j**.   
Browser to **C:\neo4j\neo4j-community-3.4.10\conf** and double-click on the **neo4j.conf**. If you do not have a program associated with .conf files, pick Notepad as follow:

  
Modify as follow:  
 > dbms.active\_database=graph.db should be dbms.active\_database=contoso.db

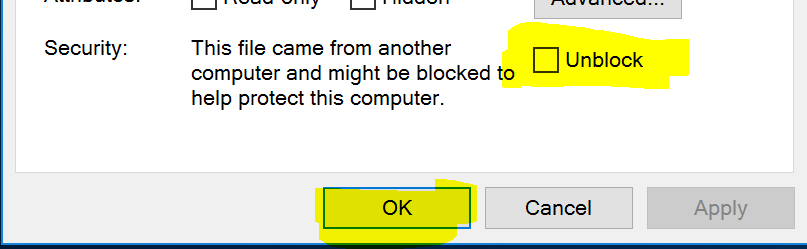
> #dbms.allow\_upgrade=true should be dbms.allow\_upgrade=true



Save and close the file.

1. **Import the contoso.graphdb**

Right-click on the **contoso.graphdb.zip** file and click **Properties**.

In the **General** tab, check **Unblock** and click **OK**.  


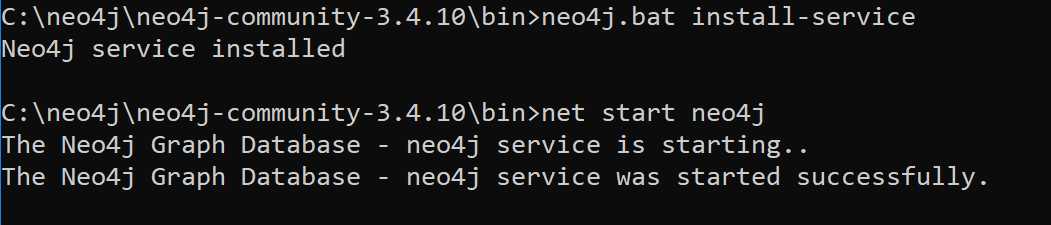
Thenright-click again on **contoso.graphdb.zip** and click **Extract all**.  
Enter the path **C:\neo4j\neo4j-community-3.4.10\data\databases** and click **Extract**.

1. **Configure Ne04J server**

Open a command prompt as an administrator and run the following commands:

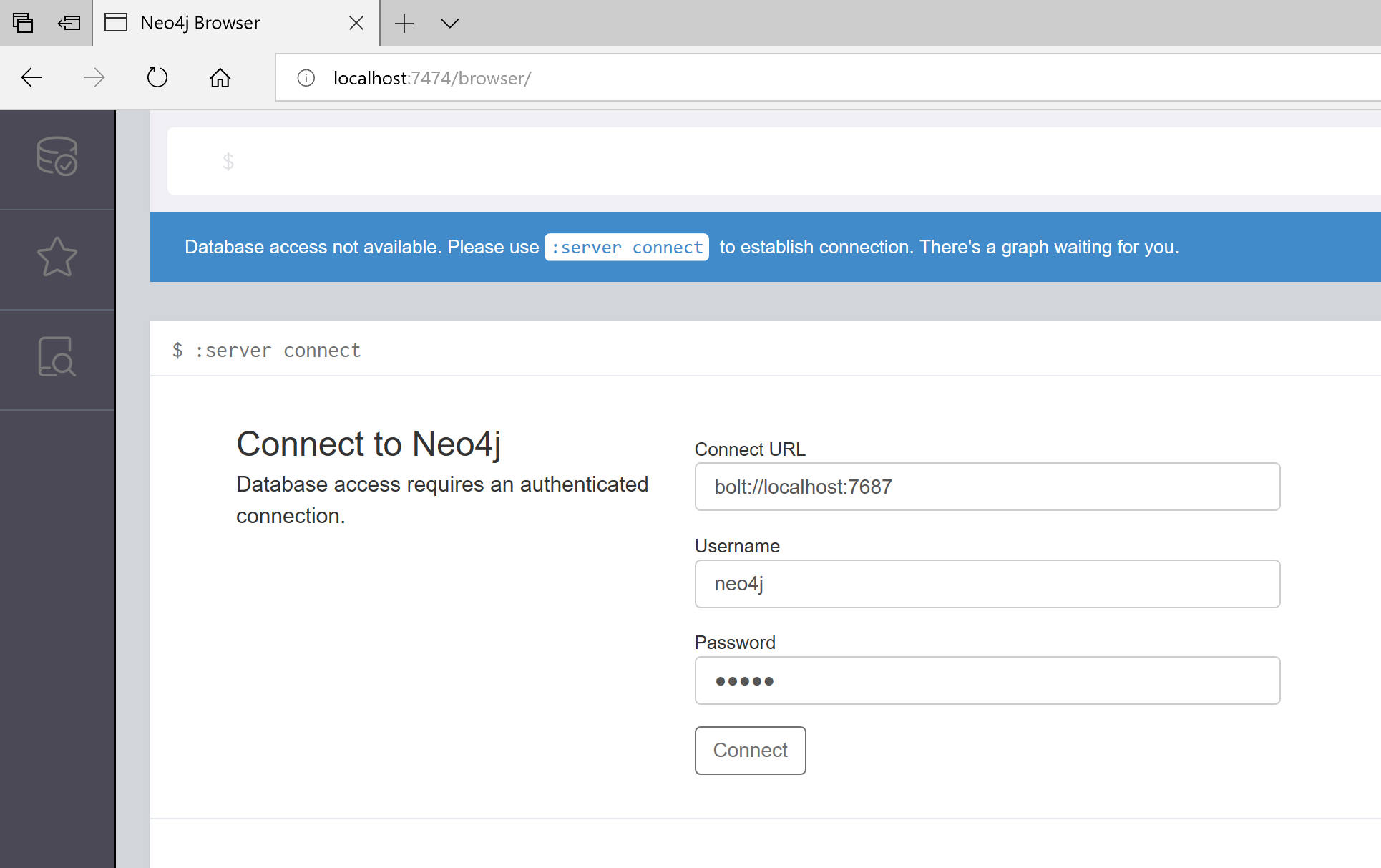
|  |
| --- |
| cd C:\neo4j\neo4j-community-3.4.10\bin  neo4j.bat install-service  net start neo4j |

You should see the service starting:

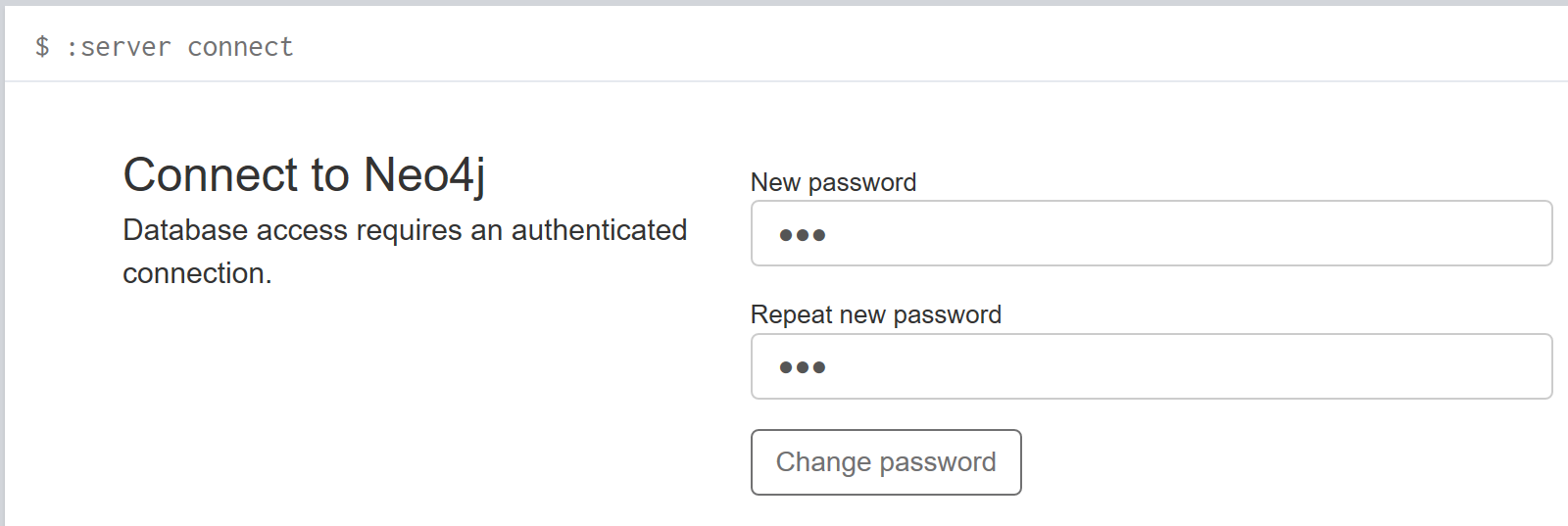


Open your browser and type the following address: <http://localhost:7474/>.

In the page, enter the password **neo4j** and click **Connect**.



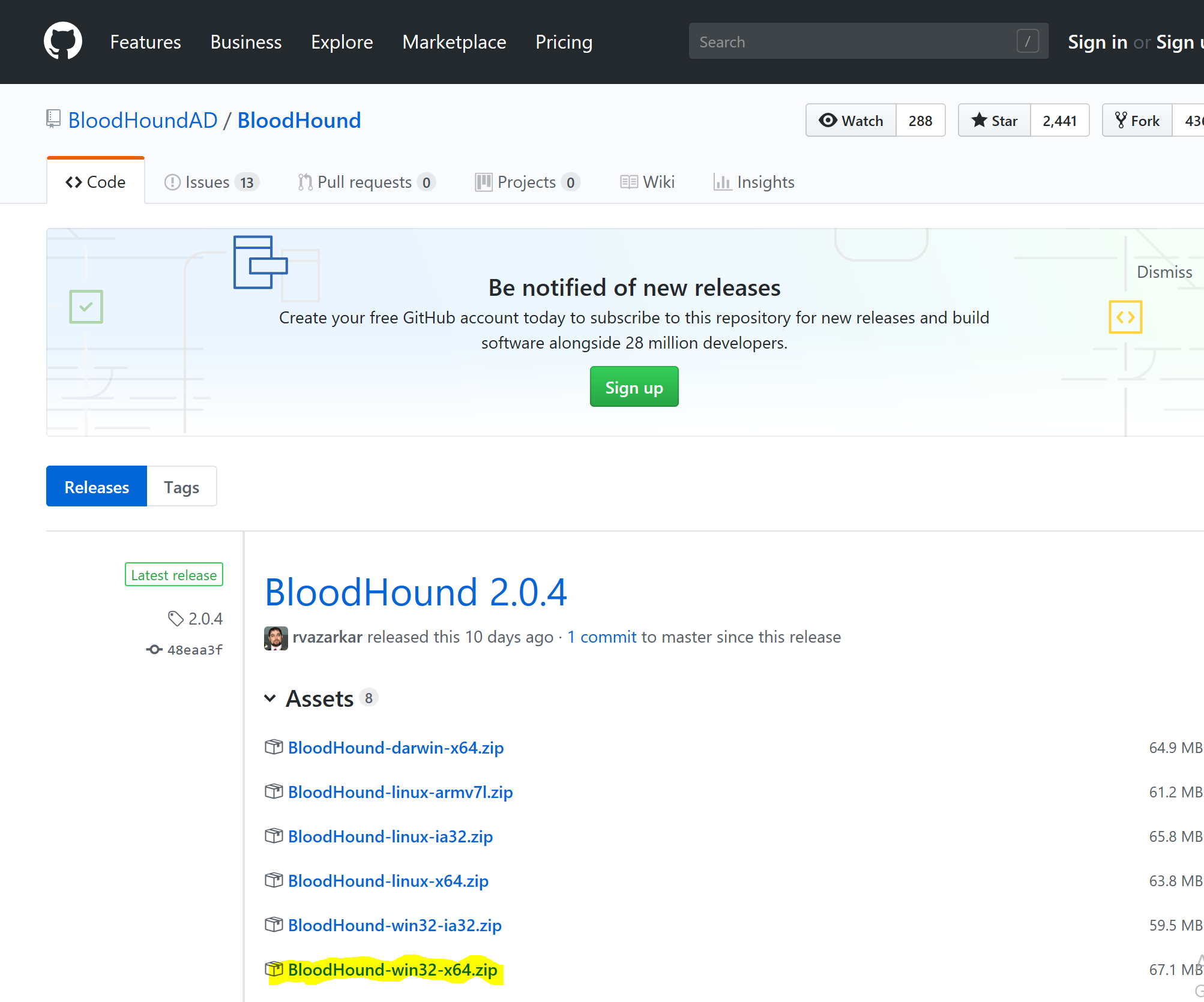
You will be asked to change your password. Enter a new password twice and click **Change password**.



Neo4j is now configured.

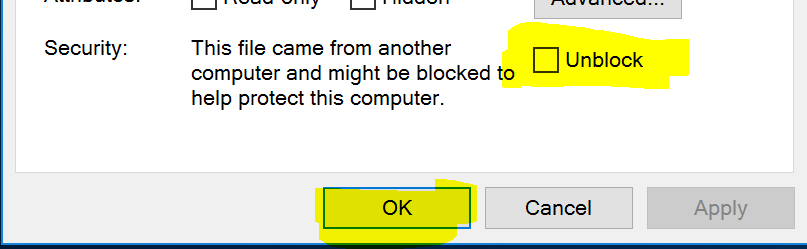
1. **Download Bloodhound**

Open your Internet browser and type the following address: <https://github.com/BloodHoundAD/BloodHound/releases>   
As of today, the current version of Bloodhound is 2.0.4. Click on **BloodHound-win32-x64.zip**.



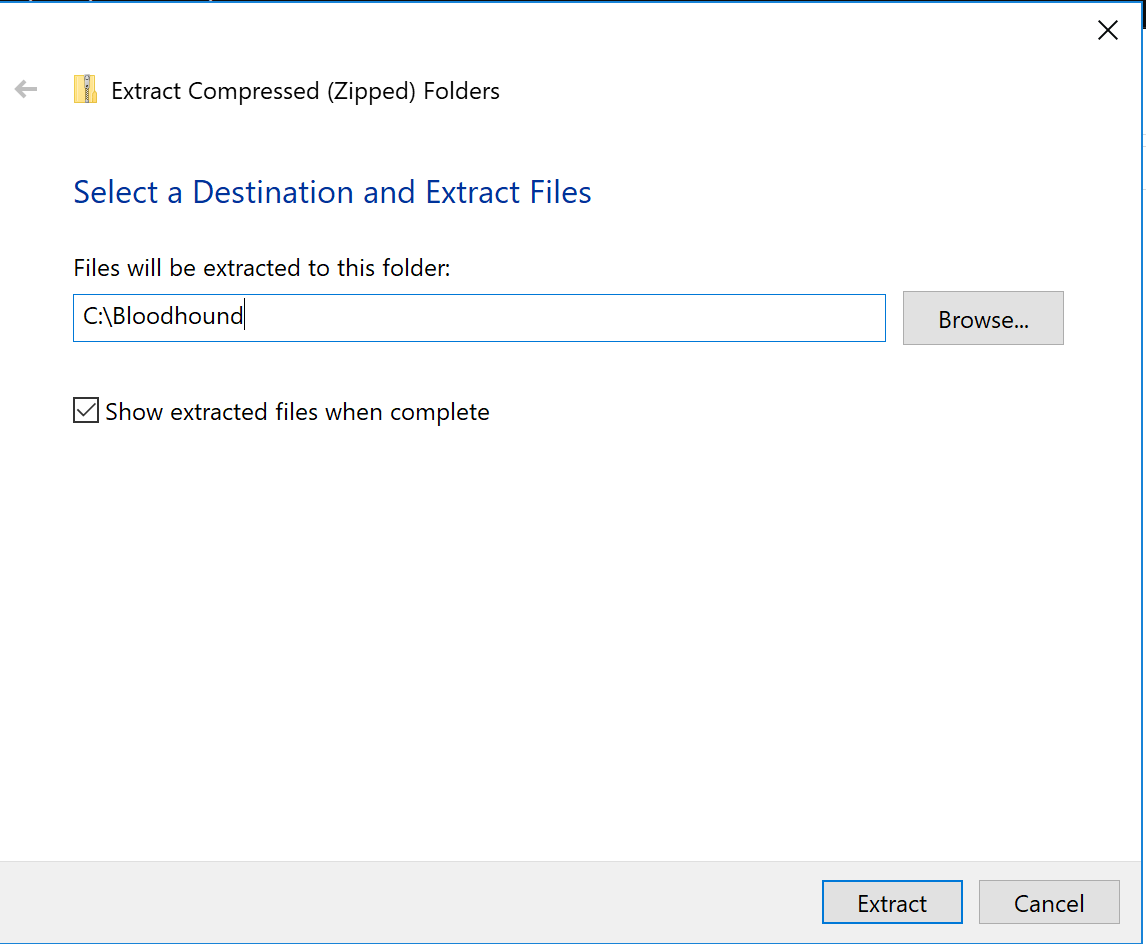
1. **Install Bloodhound**

In your downloads folder, right-click on **BloodHound-win32-x64.zip** and click **Properties**.

In the **General** tab, check **Unblock** and click **OK**.  


Thenright-click again on **BloodHound-win32-x64.zip** and click **Extract all**.

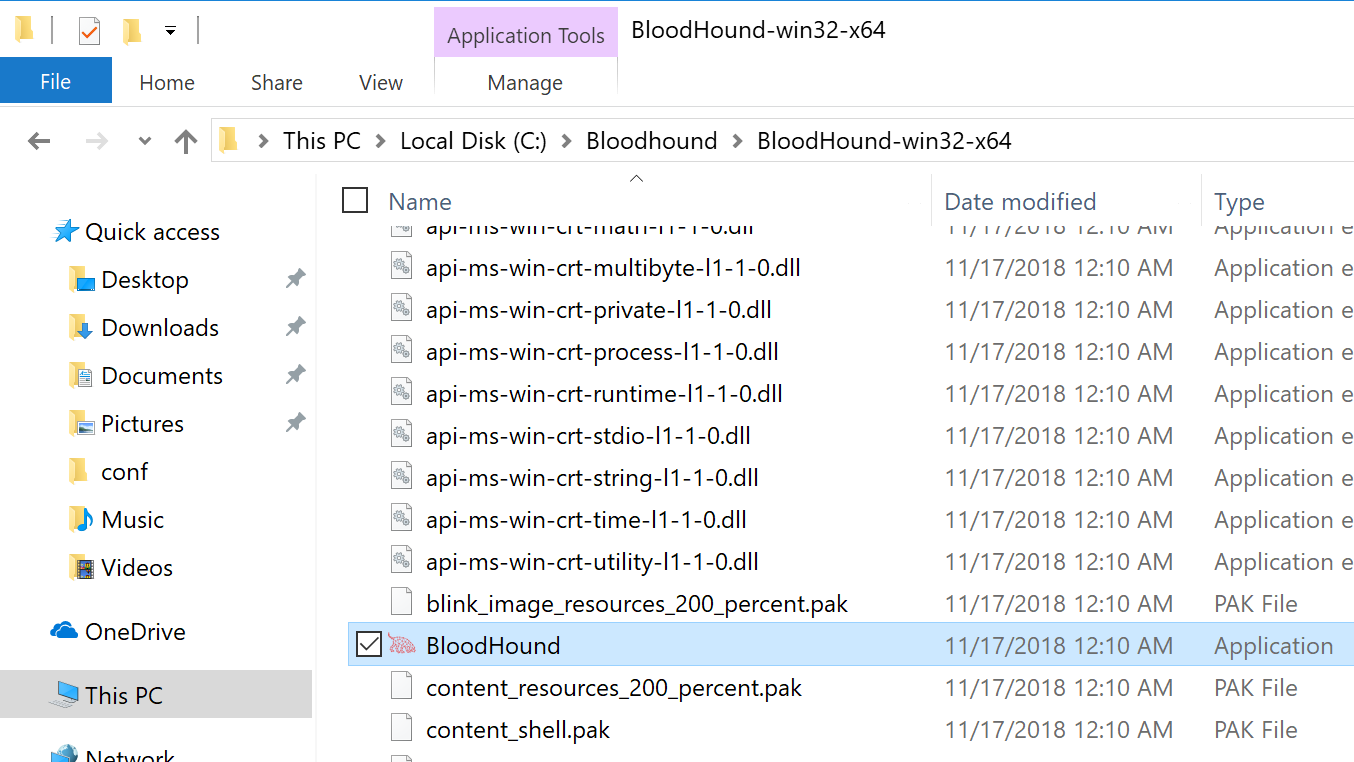
Enter the path **C:\Bloodhound** and click **Extract**.



It might take a minute or two to extract.

1. **Run Bloodhound**

Open explorer and browse to **C:\Bloodhound\BloodHound-win32-x64** and double click on **BloodHound.exe**.



Enter the username neo4j and then the password you have set in step 6.