Moat™ - User Manual

v1.0.1

Moat™ - User Manual

Table of Contents

1.0 Overview

1.1 About Us

Secure Web Apps, LLC is a provider of Cyber Security services and developer of cyber security products. We have been in business since 2007 and are located in the Raleigh, NC area.

1.2 About Moat™

Moat™ is a licensed product and a license is required for each workstation, virtual or otherwise that it is installed on. Moat™ adds the following capabilities to your Windows(R) workstations:

Workstation Hardening Via:

- Phishing Protection from 17,000+ of sites and growing
- Malware Website Protection from 67,000+ sites and growing
- Click on a bad link in a phishing email or website and you are protected from malware or ransomware.
- Phishing Protection and Malware Website Protection updated once or twice daily.

2.0 Installing Moat™

2.1 Before Installation

You should have received three items via email:

- A zip file labeled moat32 or moat64 (contains moat.exe, regdevw.exe, and mhelper.exe)
- Your customer code (keep this in a safe place)
- This manual

Make sure that the type of workstation (32 or 64 bit) matches the number 32 or 64 on the zip file you received. If they do not match, DO NOT install Moat™ and contact Secure Web Apps.

Moat™ is currently certified to run on 32bit or 64bit workstations. Supported OS's are as follows:

- Windows(R) 7 any version
- Windows(R) 8 any version
- Windows(R) 10 any version
- Windows(R) Server 2003 any version
- Windows(R) Server 2008 any version
- Windows(R) Server 2012 any version

The OS should be installed before attempting to install Moat™.

2.2 Installation - Advanced User

Extract the files from the moat zip into the directory c:\moat that you create. If you are running Norton, disable it temporarily. Start the command prompt in administrator mode. Run **regdevw** and provide the customer code in your email. Run **moat** and provide your email address for notifications.

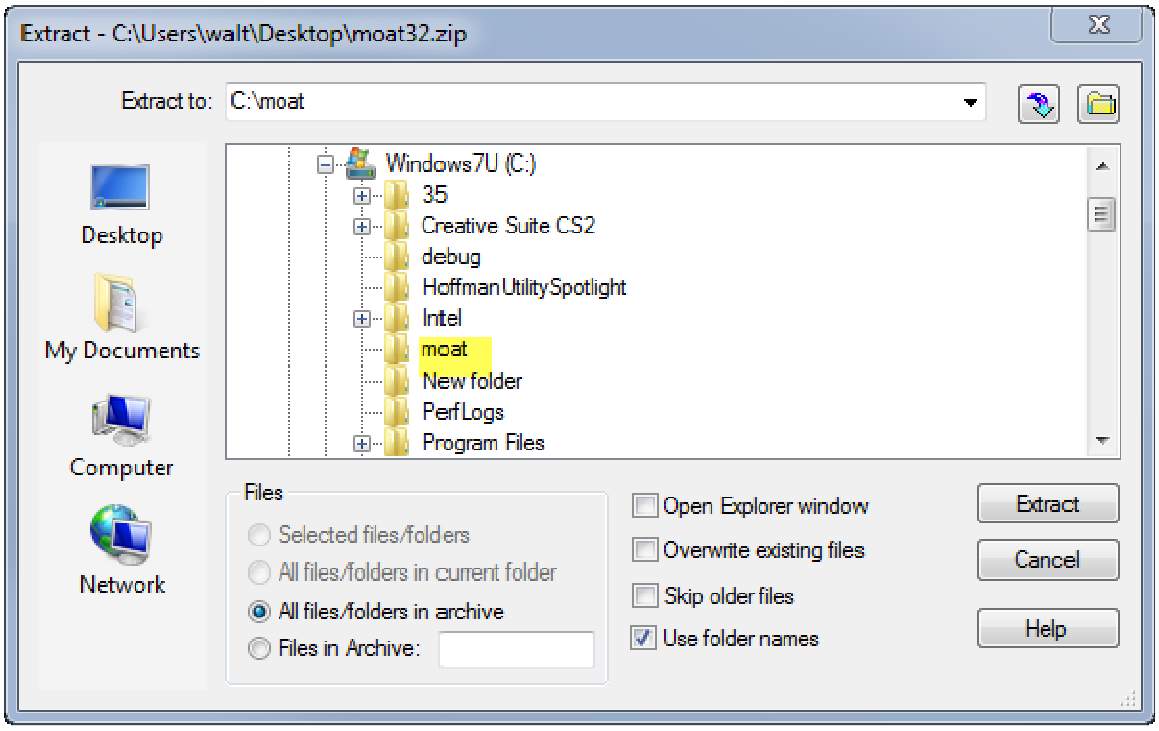
Tester Note
We are not sure whether Norton will kick moat out when the task scheduler for moat runs on day 2. All attempts to tell Norton on the local test machine that Moat is ok, fail.

2.3 Installation - Regular User

2.3.1 Create Directory for Moat and Copy Files

Use the Windows Explorer to create the directory C:\moat as shown below:

Drag the zipfile from you email to your desktop. Double click the zipfile and select extract. Select the directory c:\moat as the destination.

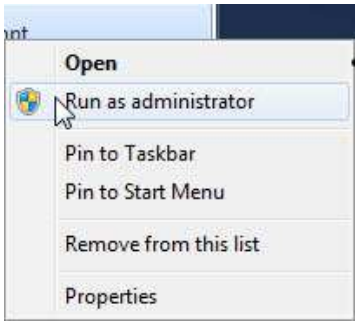


2.3.2 Installing Moat

Tester Note
We are working to make this simpler. Please let us know any other virus protections that give trouble to you so we can flag them in the manual. A screen shot of how you can work around it by approving moat would be appreciated for the manual.

Open the command window by right clicking on 'Command Prompt' on the Start Menu.

And select 'Run as Administrator' on the popup menu shown below:



You should see a command prompt window appear as shown below:

If you have done this correctly, your window should have 'Administrator' on the top left. If you do not see this, x out of this window and try again.

At the prompt type chdir c:\moat This will change the prompt so that it is working with the c:\moat directory.

At the prompt type **regdevw**. It will ask you for your customer code that you received in the email discussed in 2.1 above. This registers your device with Secure Web Apps in preparation for installing Moat™. If you are installing multiple Secure Web Apps products, you will only need to do this once per device.

If you are running Norton, it will not allow moat to install at this time. Right click on the Norton icon on your toolbar and select Disable Auto-Protect. Select 15 minutes.

Next run **moat**. Moat™ will run and will install phishing and ransomware protection. Moat™ will begin by asking you the following questions:

Moat Installation beginning
Please enter your customer code
yourcustomercode

Enter an eMail address for receiving alerts
yourname@yourcompany.com

At this point, the processing continues without any further input from you. When completed, you should see a message similar to the following (though the number of sites may vary).

Moat ended, 17764 sites have been protected (or a similar number)

When done hardening the workstation and installing monitoring software (to keep the workstation hardened), Moat™ will create the following files in the C:\moat directory:

alert-email.txt.
customer_code

If you forget your customer code, you can always refer to the contents of the customer_code file. If you need to change the email address that the alerts are sent to, edit the email address in the alert-email.txt file.

3.0 After Moat™ Installation

3.1 Monitoring/Updates

Depending upon which you selected at installation, Moat™ will be adding any reported phishing or ransomware sites.

3.2 Updates for Moat™

From time to time, Secure Web Apps will issue updates for Moat™. You will be able to run these over the top of the Moat™ that is installed and it will be updated.

3.3 Support

Support is available via email at: support@SecureWebApps.com

Response is generally fast but can be longer at peak times. Please allow up to 24 hours for a response.

4.0 Other Products

4.1 DrawBridge™ For Linux Workstations

This product does for Linux workstations what Moat™ does for workstations and more.

4.2 FortressTM for Linux Servers

Fortress protects Linux Servers against all threats. It has not been hacked in over 3 years testing outside any hardward firewall. It has survived a global challenge to hack it (ongoing) and a $10,000 bounty to hack it offered in the 2017 DefCon.