# Table of Contents

What is Azure Rights Management (RMS)? ................................................................. 1

How do I open a protected message from VA? ....................................................... 1

1. External users with an Office 365 email account ............................................. 1

2. External users with an email address that is not part of Office 365 AND not a social email address (Gmail/Yahoo/Outlook.com/Hotmail) .......................................................... 2

3. External users with a social email address (Gmail/Yahoo/Outlook.com/Hotmail) .......... 7

   3.1 Windows with Gmail: ......................................................................................... 7

   3.1.1 MacOS with Gmail: ...................................................................................... 10

   3.1.2. iOS with Gmail: .......................................................................................... 12

3.2 Windows with Yahoo: ....................................................................................... 16

   3.2.1 Mac with Yahoo: ......................................................................................... 18

   3.2.2 Android with Yahoo: .................................................................................. 19

   3.2.3. iOS with Yahoo: ..........................................................................................22

3.3 Windows with Outlook.com/Hotmail: ............................................................... 23

   3.3.1 Android with Outlook.com/Hotmail: ......................................................... 24

4. Replying to the Protected Message .................................................................. 25

Points of Contact ..................................................................................................... 25

Related Communications .......................................................................................... 26
What is Azure Rights Management (RMS)?

The U.S. Department of Veterans Affairs (VA) is committed to protecting Veteran privacy. Accordingly, VA must take a coordinated approach to identifying and managing security and privacy risks, as assuring privacy protections often depends on the presence of security safeguards and mechanisms. VA must integrate privacy and security considerations into VA processes such as training, system/information lifecycle and design, and continuous monitoring.

Azure Rights Management (RMS) is a cloud-based information protection service that uses encryption, identity, and authorization policies to help safeguard business information from unauthorized use both online and offline, inside and outside the environment. Utilizing proven security technologies—including RSA 2048-Bit encryption, certificates, modern authentication, and authorization policies—Azure RMS helps VA create reliable information protection solutions. RMS augments VA’s security strategy by providing protection of information through persistent usage policies, which remain with the information no matter where it goes. This helps VA prevent sensitive information from getting into the wrong hands, either accidentally or intentionally.

VA security and privacy practices extend to partner and third-party providers. As VA’s mission evolves to encompass flexible service delivery models, VA can reduce risk by extending the corresponding advances in VA’s security and privacy practices to its partners. VA can also educate and equip partners and third-party providers to address security and privacy challenges to improve the likelihood that Veteran information and VA data remain protected.

This User Guide for External Azure RMS Recipients communicates the process that external Azure RMS recipients can follow to achieve opening a protected Azure RMS message from VA.

How do I open a protected message from VA?

1. External users with an Office 365 email account

If you are using Microsoft’s Office 365 for your email account, you should receive an alert about the protected message’s restricted permissions in the reading pane. After opening the message, you should be able to view the message in Outlook. If for some reason this does not work, have your IT department open a case with Microsoft.

Note to IT Staff: RMS compatibility information and Office versions required: https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications

This message with restricted permission cannot be viewed in the reading pane until you verify your credentials. Open the item to read its contents and verify your credentials.
2. External users with an email address that is not part of Office 365 AND not a social email address (Gmail/Yahoo/Outlook.com/Hotmail)

If you are an external user who has an email address that is not associated with Office 365, you should receive a protected message with a prompt to verify your identity.

If you are unsure whether your email is part of Office 365 or not, please ask your IT department.

First, in the email, click the button, “Click here to read your message” to launch the portal.

One-Time Passcode:

As soon as you click on the read your message button, you can request a one-time passcode, which will be sent in a separate email.
Copy the one-time passcode from the email.

![Email with passcode]

Here is your one-time passcode

76770149

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

Don’t want to use one-time passcode every time you get a protected message? Use your email address to create a Microsoft account

Enter the one-time passcode and click “Continue” and the encrypted message will open.

![Encrypted message with passcode]

We sent a one-time passcode to [Redacted].

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode [Redacted]

This is a private computer. Keep me signed in for 12 hours.

Continue

Didn’t receive the one-time passcode? Check your spam folder or get another one-time passcode.
For users who have an email address that is not part of Office 365 and do not receive the option for a one-time passcode, the solution is RMS for individuals. You can use self-service sign up for RMS on this website: [https://aka.ms/rms-signup](https://aka.ms/rms-signup).

The website checks if your email address domain is already known in Azure Active Directory. If not, you will have to register. If the domain is unknown, you will get a one-time verification code sent in a separate email and can use it to set up the account.

As soon as you finalize self-service sign up, you will be able to authenticate and properly open the protected message going forward.
For more information on RMS for individuals, refer to this Microsoft site: https://docs.microsoft.com/en-us/azure/information-protection/rms-for-individuals

**Note to IT Staff:** RMS compatibility information and Office versions required: https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications
3. External users with a social email address (Gmail/Yahoo/Outlook.com/Hotmail)

External users who have a Gmail, Yahoo or Outlook.com address can verify their identities when they receive a protected message with either their account credentials or a one-time passcode.

3.1 Windows with Gmail:

Click the “Read the message” button in the email to launch the portal.

*Pop-up blockers need to be set to allow pop-ups from this site because the site will open a new tab.*
You will have two options:

As soon as you click on the message link, you can either sign in with your Google account or request a one-time passcode, which you will receive in a separate email.
If you select **Sign in with Google**, the encrypted message will open in a browser window.
3.1.1 MacOS with Gmail:

Click the “Read the message” button in the email to launch the portal.

You will have two options:

As soon as you click on the “Read the message” button, you can either sign in with your Google account or request a one-time passcode, which you will receive in a separate email.
One-time Passcode:

If you choose the one-time passcode, there is an additional step.

Copy the one-time passcode from the email.

Enter the one-time passcode and click “Continue.” The encrypted message will open.
3.1.2. iOS with Gmail:

Click the “Read the message” button in the email to launch the portal.

Test RMS message

Patel, Rakesh (OI&T)
to me
1 minute ago Details

This message has been modified to fit your screen. Tap here to show original.

Patel, Rakesh (OI&T) (Rakesh.Patel2@va.gov) has sent you a protected message.

Learn about messages protected by Office 365 Message Encryption.
You will have two options:

As soon as you click on the “Read the message” button, you can either sign in with your Google account or request a one-time passcode, which you will receive in a separate email.
One-Time Passcode:

If you choose the one-time passcode, there is an additional step.

Copy the one-time passcode from the email.

Your one-time passcode to view the message

Here is your one-time passcode

04231034

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

Don't want to use one-time passcode every time you get a protected message? Use your email address to create a Microsoft account
Enter the one-time passcode and click “Continue.” The encrypted message will open.

We sent a one-time passcode to adrms75@gmail.com.

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode 04231034

This is a private computer. Keep me signed in for 12 hours.

Continue
3.2 Windows with Yahoo:
Click the “Read the message” button in the email to launch the portal.
OFFICE OF INFORMATION AND TECHNOLOGY

You will have two options:

If you select “Sign in with a Yahoo ID,” there is one extra step.

If you sign in with a one-time passcode, it will be the same steps as the one-time passcode steps listed above.
Click “Agree” to allow Protected Message Viewer access and your encrypted message will open.

3.2.1 Mac with Yahoo:
Click the “Read the message” button in the email to launch the portal. Then follow the same steps listed above.
3.2.2 Android with Yahoo:

Click the “Read the message” button in the email to launch the portal in a browser window. Whether you use the mobile app or a web browser, the link will open up in a new browser window.
You will have two options:

If you select “Sign in with a Yahoo ID,” there is one extra step.

If you sign in with a one-time passcode, the process will be the same as the one-time passcode steps listed above.
Click “Agree” to allow Protected Message Viewer access and your encrypted message will open.
3.2.3. iOS with Yahoo:

Click the “Read the message” button in the email to launch the portal. Then follow the same steps listed above.
3.3 Windows with Outlook.com/Hotmail:

When you receive emails as an Outlook.com or Hotmail client, pass-through authentication is used. This means there is no need for additional authentication or a one-time passcode.
3.3.1 Android with Outlook.com/Hotmail:

On Android, there is also no need for additional authentication or one-time passcode.
4. Replying to the Protected Message

When you use the options on the right side of the screen, you can reply to, reply all, or forward messages securely with the same level of encryption. To make sure your reply or forward is encrypted, you must make sure you see the banner stating that the message is encrypted.

*When replying to the encrypted email, your email address will automatically appear on the CC line so that you have a carbon copy of the email once it is sent.

Points of Contact

OIT ITOPS SD CIS RMS Team: VHARMSTeam@va.gov
Related Communications


» “RMS for individuals and Azure Information Protection” https://docs.microsoft.com/en-us/azure/information-protection/rms-for-individuals

» “Applications that support Azure Rights Management data protection” https://docs.microsoft.com/en-us/azure/information-protection/requirements-applications