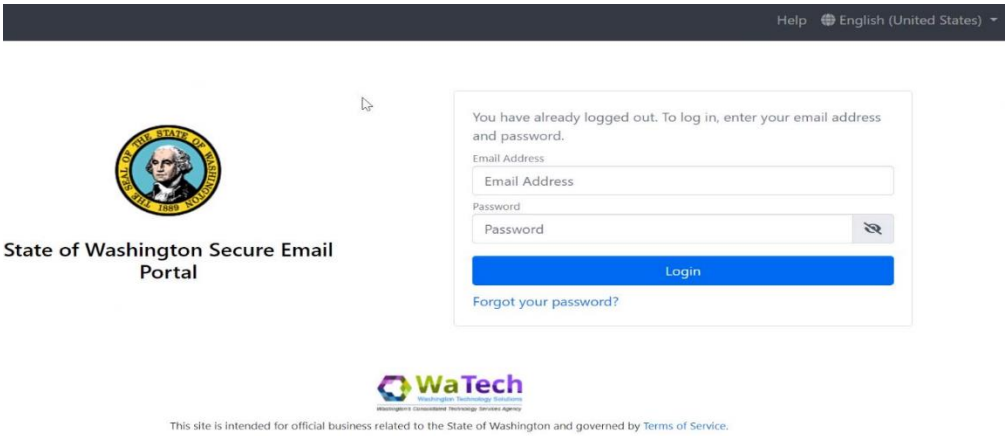
FAQ E-mail Encryption-WA State Partners

For USERS OF OFFICE 365

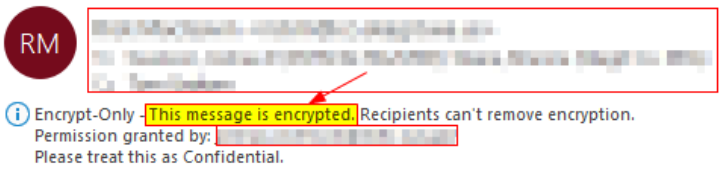
Background

The State of WA will have all email moved to Exchange Online in Microsoft Office 365 by June of 2022. As part of the contractual agreement with counties and subcontractors, transporting client records containing confidential information outside a secure area in email must be encrypted. The old email encryption service provided by WaTech in the screenshot below will be decommissioned by WaTech in Dec 2022. This solution using Trustwave and Echowrx is a third-party software as a service (SaaS) product purchased by WaTech for the State of WA and partners to interact with the state. Once all agencies in the State of Washington have been migrated to Exchange Online in the cloud, then WaTech will be decommissioning this service since the new cloud-based Microsoft email service has its own email encryption.



1. **How will we know when an e-mail is encrypted from a state partner? (DDA or DVR etc.)**

   If a state partner like DDA or DVR is sending an encrypted email, you will see a message like the screenshot below saying that "This message is encrypted." If an email is sent with [DSHS Secure] in the email subject, then it means Microsoft encryption has been removed and transport layer security (TLS) encryption in transit is forced.



2. **Is there anything we need to do, other than reply, in order to respond to an encrypted e-mail from the state?**

If you are using Office 365 and responding to someone in the State of WA in Office 365, then all you need to do it reply. Microsoft makes it easy for Microsoft to Microsoft encrypted email transfers.

3. **When will the parallel WA state secure access encrypted e-mail no longer be active?**

   WaTech is our central service email provider and they are planning on bringing down the old secure email portal in Dec 2022. DSHS is in conversations with EchoWrx/Trustwave about the possibility contracting for secure email, but there are complexities with the timeframe, contracting, support, and cost.

4. **How can I save critical e-mails which may be lost when the state secure system shuts down?**

   The old encrypted email portal saves email for 30 days before purging the email. If you need to save an email or document before the service is decommissioned, you can try saving the email to your local workstation, copying it in a word document, or printing a PDF. There are multiple methods of doing this.

5. **If the case manager has not encrypted an e-mail, what are our options to respond if the content requires encryption?**

   DSHS staff should be defaulting to sending email with Microsoft email encryption using [secure] in the subject. If the recipient does not have Microsoft authentication, then DSHS staff should be using [DSHS Secure] in the subject line, which will remove Microsoft encryption and force transport layer security (TLS) encryption in transit. If DSHS staff or a case manager sends an email with no encryption at all and nothing is in the subject line, then I would assume the email is not encrypted, unless you are able to verify that your email provider is using TLS encryption. Companies like Google and Yahoo use this by default. You can respond to the email if you know that your email provider uses TLS or if you are able to utilize your own email encryption solution to initiate an email to send to DSHS.

6. **Can I add (cc) someone else to an encrypted e-mail chain initiated by a case manager?**

   If the message is being sent using Microsoft email encryption with [secure], then no, this is not possible by Microsoft design. Microsoft email encryption follows the email and attachments, so only the people in the To and CC fields will be able to read everything. The sender can CC someone, but you might have issues if you try forwarding the

encrypted email to someone not originally on the email chain. The solution is to have the sender resend the message and include all the people who need to read the message. You can also initiate a new encrypted email and copy the content, but only if it does not include an attachment since email encryption with Microsoft follows attachments. An alternative method is having the DSHS staff send an email with [DSHS Secure] in the subject line, which will remove the Microsoft email encryption and force TLS encryption in transit. In this case, the message and attachment can be forwarded as needed.

7. **How long will encrypted e-mails sent by the Case Manger be available to review?**

   At the moment, the encrypted emails will be held at Microsoft forever. There is no 30 day limit like the old email system. This is a tenant-wide setting for the State of WA, but each county or partner Office 365 tenant could be configured differently.

8. **When I respond to an encrypted e-mail from a case manager in Office 365 is it automatically encrypted?**

   If you respond to an encrypted e-mail with [secure] in the subject line, then your reply e-mail will be automatically encrypted using Microsoft e-mail encryption.
   If you respond to an encrypted e-mail with [DSHS secure] in the subject line, your reply will not be guaranteed to be encrypted. [DSHS Secure] is a custom policy that enforces TLS encryption in transit when sent FROM DSHS to an external business partner.

9. **When I forward an encrypted e-mail that I've received from a case manager, will it be automatically encrypted?**

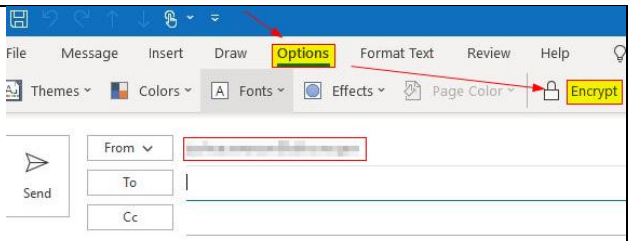
   If you forward an encrypted e-mail from DSHS with [secure] in the subject line, the e-mail will continue to be encrypted by Microsoft e-mail encryption.
   E-mails initiated by a case manager with [DSHS Secure] in the subject will only guarantee TLS encryption sent from DSHS. If you CC or forward the e-mail on, it will not guarantee encryption.

10. **Is there a way for me to save critical e-mails that exceed the 30-day settings when encrypted by the state using Office 365?**

    Is there a way for me to save critical e-mails that exceed the 30-day settings set by the state office 365 encryption system?
    Yes, critical emails that are encrypted using M365 can be saved more than 30 days. The new Microsoft email encryption will allow you to access the e-mail and it's attachments until the sender's account is disabled and unsynchronized.

11. What are my options for initiating an encrypted e-mail from office 365? (Note: Office 365 is distinct from Outlook. Encryption to/from Outlook may not be possible.)

1. Compose a new email message, click on **File**, then **Info**, and choose **Encrypt**.

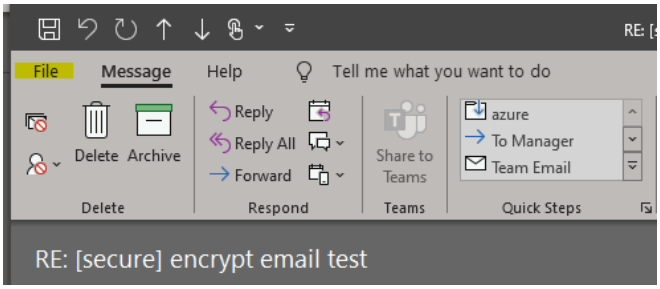


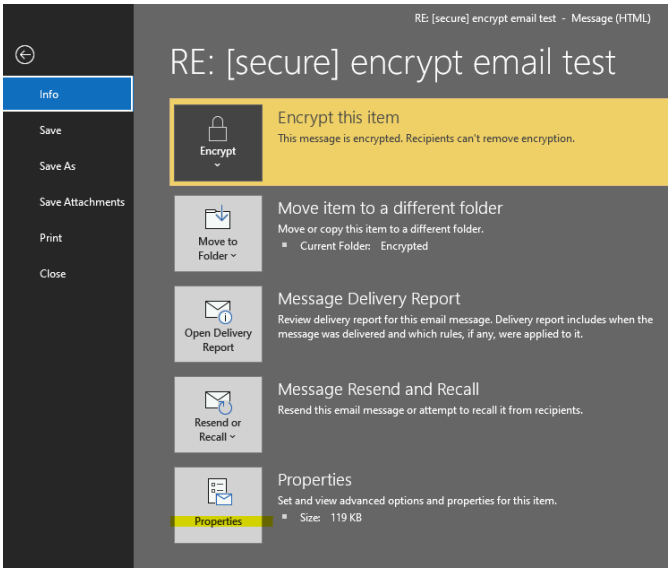
2. Compose a new email message and click on **Options** and choose **Encrypt**. (May not work with old versions.)

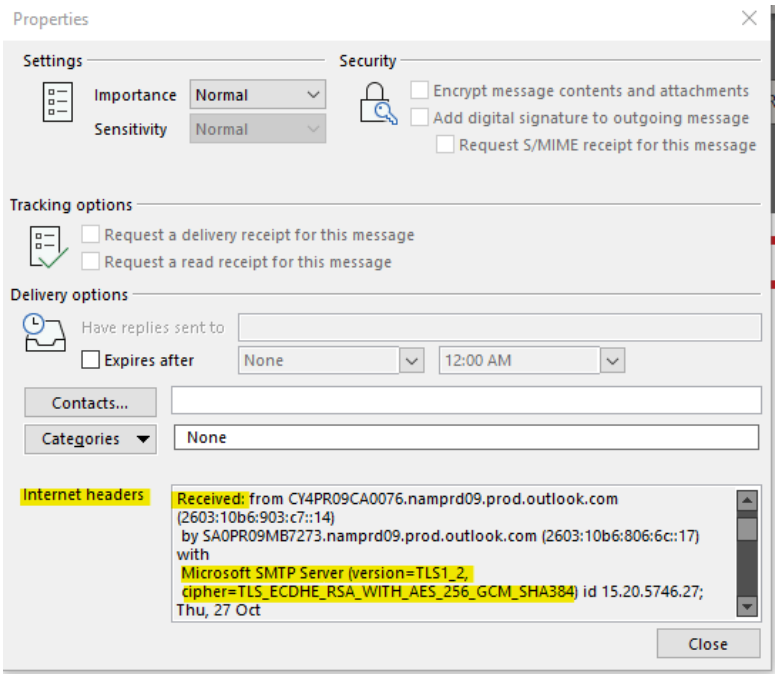
3. If you have an older version of Outlook with Office 365, you can visit the webmail link at https://outlook.office365.com, compose a new email message, and click on the **Encrypt** button to encrypt the message (*Might need to click on the 3 dots first*.)

12. How can I confirm if an email I receive meets TLS (transport layer security) encryption?

Open the e-mail in Outlook (1st screenshot below), then select file (2nd screenshot below), the select properties. Look under the 'Internet headers' property and verify that the e-mail received is TLS encrypted, should say Microsoft SMTP Server (version=TLS1_2,cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) (3rd screenshot below).







Last Updated: 10/2022