OWA/2-Factor Authentication VPN FAQ

Outlook Web Access (OWA) QUESTIONS

Q1. With OWA and ActiveSync going away, how does an employee/contractor access Outlook (email, calendar and contacts)?

A1. An employee must use their government/contractor issued equipment to access Outlook (email, calendar, and contacts) beginning July 1, 2015.

Q2. Does CMS have a help desk to assist contractors?

A2. The CMS IT help desk may be contacted at cms_it_service_desk@cms.hhs.gov or by telephone at: 1-800-562-1963.

Q3. How will contractors access Outlook or resource mailboxes?

A3. Contractors should work with their Contracting Officer Representative to discuss next steps to use their PIV cards, purchase PIV card readers or RSA tokens to access CMS' email.

Q4. Will CMS BlackBerry or GOOD users be affected by this change?

A4. No, these users will not experience any impacts as a result of these changes.

Q5. The directive states that OWA will no longer be allowed. However, If OWA is implemented with Two-factor authentication; will it be allowed for HCQIS?

A5. Access to CMS email via OWA will be generally deactivated July 1st. This will be done on a per account basis.

Q6. Will Exchange ActiveSync, a protocol that allows mobile devices to synchronize data with Exchange mailboxes, be allowed?

A6. ActiveSync will be phased out.

Q7. Does this notification today mean that CMS system users will only be able to access those systems with a PIV or RSA token or does it mean that contractors must attest that in instances in which they access the CMS system that they fully comply with the CMS Acceptable Risk Safeguards regarding authentication?

A7. The short answer is Yes. The CMS CIO and CISO are seeking confirmation that contractors are using strong authentication or that they shut down access to users that are not protected by two-factor authentication. This applies to contractors that access CMS systems or systems operated on behalf of CMS. Use of PIV, PIV-I, or RSA Tokens are preferred methods, however there are other acceptable technologies. Please contact the CMS CISO mailbox if you have questions about a particular technology.

OWA/2-Factor Authentication VPN FAQ

Q8. Is CMS "shutting off" access to these CMS systems for anyone one without multi-factor authentication?

A8. CMS is responsible for ensuring multi-factor authentication is used by contractors. It is a crucial component to an overall strategy of strong security – for example, Federal employees use PIV cards and passwords as multifactor authentication to access systems. It is our responsibility to ensure that our systems are maintained, sustained and protected and we take that seriously.

Q9. It seems to us the security issue is a CMS issue, not a contractor issue. Why do we have to make the changes to our processes?

A9. Contractors act on behalf of CMS based upon the scope of their contract. Each contract contains standard language from CMS that requires compliance with agency security and privacy requirements in order to protect the sensitive information. Component Heads need to work with both federal and contractor staff to achieve the actions in this directive.

Q10. Who should I contact with more questions?

A10. Any technical questions regarding the impact of these technical direction letters on your contract should be directed to the assigned Contracting Officer Representative (COR). If you believe that the technical guidance is not within the scope of your contract or that there are not sufficient funds available, you should not act upon the direction and should contact your Contracting Officer immediately.

OWA/2-Factor Authentication VPN FAQ

Multi-factor Authentication FAQs for CMS Information Systems

Q1. Do contractors maintaining CMS systems require multi-factor authentication?

A1. Yes. The CIO directive applies to all FISMA systems. Those having an ATO or in the process of obtaining an ATO must incorporate 2FA for all privileged and non-privileged accounts therein.

Q2. For systems hosted in external contractor operated facilities with no dependency on the CMS network, is 2FA applicable?

A2. Yes. Same as question 1.

Q3. I have a waiver, risk acceptance or other relief from using multi-factor authentication for a CMS system, how does this new policy impact my waiver?

A3. The CIO directive supersedes any existing waiver, risk acceptance memo or other exception. Appropriate processes will be followed to address these situations.

Q4. I am a contractor responsible for maintaining a CMS system residing in an external contractor operated facility and do not have a PIV card or RSA token, how do I continue to support CMS and comply with the CIO directive?

A4. The contractor should evaluate all available technical solutions for enabling 2FA for all privileged and non-privileged accounts within the system. The preferred methods are PIV and Hard Token which should be used where available. However, CMS will consider any recommended solution that we feel meets the definition of 'two factor' and integrates with existing technology, policies and standards. We encourage all of our contract partners to develop alternatives that address the resource challenges, time constraints and compliance to policy, such as 508. Some options that have been identified thus far include smart phone apps, phone back, text back, open source and others.

Q5. I am a COR with a contractor who has not been PIV enabled or have an RSA token, what do I do?

A5. If determined that a PIV is required, the COR should have their contractor complete an HHS-745 and submit for processing. Contractors should evaluate any available option and recommend an appropriate solution. Refer to question 4.

Q6. Would the user be able to access CMS systems with her personal computer if her company purchases a PIV card reader and/or an RSA token? I'm presuming the user needs to get one or the other. As long as the computer supports the CMS VPN client needed.

A6. The CMS environment also performs compliance checks on all computers to make sure specific security criteria are met prior to allowing access. Either a PIV or RSA token will suffice, but other options may also be available depending on the specific situation.

Q7. Will CMS pay contractors for the costs to implement multi-factor authentication (e.g., the cost of getting RSA Tokens for employees)?

A7. These costs will be minimal, and CMS considers them to be general costs for doing business with the government. Multi-factor authentication is also part of what every entity should be doing to maintain high levels of security within their own business practices. Therefore, CMS expects these costs to be indirect rather than direct costs to the contract. If a contractor determines that this direction has a direct cost impact on its contract, they should explore alternative and contact their Contracting Officer.

Q8. Does each IT contractor need to take some action to shut off access to accounts that are not two factor enabled?

A8. In situations where 2FA is not possible and alternative work flows do exist, accounts should be disabled.

Q9. Please define Privileged Users:

A9. Privileged users: accounts associated with individuals who perform system administrative or other maintenance and development type actions typically not available to a standard user. Server Admins, Workstation admins, network admins, developers are a few examples. Please refer to your system security plan which includes a specific definition of privileged and non-privileged users.

(*The intent of this working definition is to assist in the initial implementation of the CIO directive. It should not be viewed as a CMS standard as it primarily covers the fundamental or traditional categories of privileged users and is not all inclusive. This definition does not cover system and service accounts, which are the accounts, used for inter-process communications and not intended for user login sessions. Password management and complexity best practice solutions are ideal to protect service/system accounts.)*

OWA/2-Factor Authentication VPN FAQ

Q10. How do I get VPN Access?

A10. Please ask your CAA to add the CTR_VPN Job code to your EUA Profile. Once the job code has been added, you may download and install the VPN software appropriate for your VPN authentication method (PIV or Token) from https://vpnext.cms.hhs.gov/download.

Q11. How do I know if I should use PIV or RSA token?

A11. Please refer to question 4 above in response to which authentication method to use.

Q12. Are there software installation instructions for the VPN software?

A12. Instructions, including screen shots, are in the **CMS VPN Contractor User Guide**.

Q13. Is there troubleshooting help for VPN access?

A13. Troubleshooting help is in **CMS VPN Contractor FAQ**.

Q14. Is there a web page containing detailed instructions for VPN access?

A14. There are two; both require a CMS User ID and password

For external access, use https://vpnext.cms.hhs.gov/download**.**

Q15. What is the process for obtaining a VPN job code for a contractor?

A15. Job codes that grant VPN access are specific to whether a token or a PIV card is used to gain access. For job code assistance, please contact your COR.

Q16. Is PIV installation software different from that used for RSA?

A16. Each type has its own set of profiles. The VPN web pages have sections for RSA and for PIV installation types.

Q 17. Why is CMS undertaking this effort?

A 17. There are several explanations for this action. First, this is not a new requirement, CMS has been working on strengthening authentication controls for many years. Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347 is the law of the land. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The NIST security controls are developed to meet the objectives of Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular

A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III. In addition, please refer to OMB M-06-16. Second, CMS is seeing an increased effort by malicious actors who are attempting to gain unauthorized access to CMS systems and data by stealing user credentials. Third, the threat against the federal government is significant; cyber-attacks against federal agencies such IRS and OPM simply reveal how devastating a data breach can be. Lastly, the Department of Health and Human Services has requested each Agency/OpDiv CIO to take immediate steps to strengthen the posture of the agency by taking immediate steps to enforce strong authentication.

Q18. What are the specifications for the PIV card reader? RSA token?

A18. The RSA Tokens are specified in the VPN document. The PIV card reader needs to be a current version from a major manufacturer.

Documentation may be obtained at https://vpnext.cms.hhs.gov/download;

OWA/2-Factor Authentication VPN FAQ