



United States  
Department of  
Agriculture

# **ITS Email Policy Guide**



## Table of Contents

1. Purpose.....	4
2. Acceptable Use.....	5
2.1. Abuse.....	5
2.2. Privacy.....	5
2.3. External Communications.....	6
2.4. Sensitive or Confidential Information.....	6
3. Email Best Practices.....	7
4. Email Account(s).....	8
4.1. Email Addresses.....	8
4.1.1. Primary Email Address Assignments.....	9
4.2. Display Names.....	9
4.3. Duplicate Names.....	9
4.4. Authorized Access.....	10
4.5. Employee Termination/Leave of Absence/Vacation/Transfer.....	10
4.6. Resource Mailboxes.....	10
4.6.1. Resource.....	11
4.6.1.1. Resource Account Request\Approval Process.....	11
4.6.1.2. Request Procedures.....	11
4.6.1.3. Approval Process.....	12
5. Mailbox Storage/Retention/Restores.....	13
5.1. Mailbox Size Limit.....	13
5.2. Local PST Folders.....	13
5.3. Message Size Limit.....	14
5.4. Deleted Item Retention.....	14
5.5. Forensics Investigations-Email Retrieval.....	14
6. Email Client.....	15
6.1. Supported Client(s).....	15
6.2. Outlook Access via USDA VPN or Dialup.....	15
6.3. OWA – Internal and External.....	15
7. Public Folders.....	17
8. Distribution Lists.....	18



8.1.	Distribution List Requests\Approval Process .....	18
8.1.1.	Request Procedures.....	18
8.1.2.	Approval Process .....	19
9.	Anti-Virus.....	20



## 1. Purpose

The purpose of this document is to define the decisions made by the ITS Email Team regarding the administration and use of ITS Exchange. This document hopes to ensure the proper use of the ITS's email system and inform users of acceptable email practices. The USDA reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

## 2. Acceptable Use

### 2.1. Abuse

Electronic Messaging within USDA is provided for business purposes only. USDA does recognize that some personal mail will traverse USDA's mail network, however, such correspondence should be kept to a minimum. The solicitation and/or distribution of non-USDA related materials, particularly matters of a personal nature or for personal gain, are strictly prohibited.

Misuse of Electronic Messaging is a serious problem and is considered the same as any misuse of government property, information, or equipment. Serious misuse may be considered "Gross Misconduct" and the appropriate action will be taken.

USDA employees must understand that Electronic Messaging is subject to the same rules that govern the use of other means of communication. Electronic Messaging is not removed from the legal, ethical, and social considerations that make us responsible citizens.

USDA employees must ensure they never use electronic messaging services that include, but are not limited to, the following types of email abuses:

- Represent themselves as another person.
- Transmit or store material that would be considered inappropriate, offensive or disrespectful to others.
- Harass other employees.
- Provide information about, or lists of, company employees to non-USDA employees.
- Participate in activities that interfere with their job or the jobs of other employees.
- Interfere with the operation of USDA's Messaging Systems.
- Violate any law or the rights of any person.
- Lobby, endorse, or promote affiliation with a particular political party or person.
- Originate or forward chain letters.
- Transmit or store threatening, obscene, or harassing messages.
- Generate messages for personal gain.

Employees should never knowingly generate messages that damage, disable, or disrupt electronic messaging services on USDA's messaging infrastructure.

Employees are permitted to send some personal messages, but such messages should be minimized and kept as short as possible.

It is recommended to use common sense, and Best Email Practices guidelines (see section 3) when using the ITS email system.

### 2.2. Privacy

USDA, in no way guarantees the privacy of Electronic Messaging. All electronic mail stored on USDA equipment is considered USDA property. USDA may periodically check

usage to correct network problems, and to establish proper use and security. You should not have any expectation of personal privacy for messages which you send, receive or store on these systems.

## **2.3. External Communications**

Under no circumstances should any electronic data be automatically and indiscriminately sent to a non-USDA person, mailbox, or entity. Applications which disseminate information to non-USDA employees must be tightly monitored and controlled.

Discretion should be used when communicating with non-USDA employees and should be limited to that which is necessary to conduct USDA business.

Outlook rules that automatically forward mail to an external source are prohibited.

## **2.4. Sensitive or Confidential Information**

USDA depends on its employees to use good judgment in discussing and transmitting sensitive issues via email. Users should consider the impact of distributing sensitive information. While it is possible to encrypt email between two parties, ITS has not identified or selected any message encryption technologies.

Employees should actively seek alternatives to Electronic Messaging in cases dealing with sensitive or confidential information.

## 3. Email Best Practices

- Emails should be well-written and use concise and descriptive subjects
- Delete any email messages that you do not need and regularly archive your older messages
- Target communications. Messages should only be sent to those people who need to receive the information
- When replying to a message, check the message header for large distribution lists. Also do not retain attachments.
- Do not send unnecessary attachments. Large attachments should be zipped (WinZip) before sending.
- Be careful when opening attachments as they might contain viruses
- Do not open email from unknown people
- Exercise good judgment in composing emails
- Out-Of-Office notifications are available but use caution when enabling. Always use generic information when configuring your out-of-office agent.
  - **Good:** I have received your email. Unfortunately, I will be unavailable until 12/6/04. I will only be checking email or voicemail periodically during this period. In the case of an emergency, please contact Jodi Watley at 202-555-1212.
  - **Bad:** I will be out of town the week of 12/15/04 in a training class. In case of emergency, please contact Jodi Watley 202-555-1212.

Please note: Messages that are sent to all users in the organization are usually sent from members of National Leadership. If you feel that a message needs to be sent to the entire organization contact your local supervisor and they will determine the business need. Before asking management for approval, think about the following questions: Is the message Business related? Do you think management would approve sending this message to the entire organization? If you know the answer to either of these questions is “NO”, then the message should not be sent. Please DO NOT send messages to all users in the Global Address list without proper authorization.

When sending email messages and selecting recipients from the Global Address Book please verify that you have selected the correct recipients before clicking on the “send” button.

Also, remember to NOT select “Reply to All” when replying to messages that are sent to all users or to a large distribution groups. Please reply only to the originator of the email message.

## 4. Email Account(s)

All email account requests, creations, deletions, and/or modifications must go through the USDA ITS centralized Exchange Operations Team. Please see section 4, 5 and 8 for Resource Account, Mailbox Size and Distribution List requests and approval processes. This standardized process eliminates the possibility of unauthorized account creation and modification, as well as, the creation of unforeseen problems in the email operation infrastructure.

### 4.1. Email Addresses

Each employee will only be allowed two email aliases. Each of the two addresses serves a specific purpose.

- [John.smith@st.usda.gov](mailto:John.smith@st.usda.gov): This is the users primary (reply) email address and will be created by an ITS administrator.
- [John.smith@one.usda.gov](mailto:John.smith@one.usda.gov): This address is for internal routing purposes only and should not be used to receive external mail. This address should match the users UPN name. **Note: this address is automatically generated**
- [John.smith@usda.gov](mailto:John.smith@usda.gov): This is an email address that will be generated automatically for all USDA employees per mandate. This functionality is currently provided elsewhere in USDA; It is not presently provided by the ITS Exchange system.

In the case of an employee name change, i.e. marriage, the employee will be given a third alias temporarily which will become the new primary. After thirty days the old primary will be removed.

## 4.1.1. Primary Email Address Assignments

Listed in the table below are the mandated domain names that must be used by each location. Every location is assigned one, and only one, email domain in addition to the @usda.gov domain assigned. Additional domains will not be accepted as part of the Exchange organization.

Location	Email Domain
States	<a href="mailto:st.usda.gov">@st.usda.gov</a>
RCD	<a href="mailto:rcdnet.net">@rcdnet.net</a>
NACD	<a href="mailto:st.nacdnet.net">@st.nacdnet.net</a>
Salt Lake	<a href="mailto:slc.usda.gov">@slc.usda.gov</a>
Portland	<a href="mailto:por.usda.gov">@por.usda.gov</a>
Greensboro	<a href="mailto:gnb.usda.gov">@gnb.usda.gov</a>
Fort Worth	<a href="mailto:ftw.usda.gov">@ftw.usda.gov</a>
Washington DC	<a href="mailto:wdc.usda.gov">@wdc.usda.gov</a>
St. Louis	<a href="mailto:stl.usda.gov">@stl.usda.gov</a>
Kansas City	<a href="mailto:kcc.usda.gov">@kcc.usda.gov</a>
Fort Collins	<a href="mailto:ftc.usda.gov">@ftc.usda.gov</a>
Lincoln	<a href="mailto:lin.usda.gov">@lin.usda.gov</a>

## 4.2. Display Names

A display name is the format in which a user's name will appear in the Global Address List (GAL). The format of the GAL display name is:

### **Last, First (City, St)**

The display name is actually created via a nightly script run by the IO Lab. The script creates the display name from the user fields in Active Directory. It is critical that users have all fields completely filled out. City must be spelled out consistently and the State field must only contain the 2 character state abbreviation.

## 4.3. Duplicate Names

In an enterprise, such as ITS, the possibility of duplicate names will arise. Duplicate names can affect both account names and email addresses. Names are assigned on a first come first serve basis. The example below uses John Smith for an account creation. A conflict is sure to arise with such a generic name. A second John Smith will need to have a numeral or middle initial to differentiate between users. Nothing will be done to the original John Smith. Example:

## **Original**

- [John.smith@nv.usda.gov](mailto:John.smith@nv.usda.gov): Notice this is a Nevada user.
- [john.smith@one.usda.gov](mailto:john.smith@one.usda.gov)
- [John.smith@usda.gov](mailto:John.smith@usda.gov)

## **Duplicate**

- [John.smith@ca.usda.gov](mailto:John.smith@ca.usda.gov): Notice this is a California user so there is no conflict on primary email address. In the case where the users are in the same state, the email address created would be [John.Smith2@ca.usda.gov](mailto:John.Smith2@ca.usda.gov).
- [JohnR.Smith@ca.usda.gov](mailto:JohnR.Smith@ca.usda.gov): Notice this has a middle initial added to the SMTP address. This is an alternative to appending the 2 to the end of the user's name.
- [John.smith2@one.usda.gov](mailto:John.smith2@one.usda.gov): John.Smith2 will be the logon name of user
- [John.smith2@usda.gov](mailto:John.smith2@usda.gov): This is assigned outside of ITS Exchange.

## **4.4. Authorized Access**

Email Operations and Help Desk staffs do not have the authority to access an employee's mailbox without permission from either the user or senior management.

## **4.5. Employee Termination/Leave of Absence/Vacation/Transfer**

**Termination:** The employee Active Directory account and mailbox will be deleted immediately regardless of the reason for termination.

**Leave of absence:** Nothing is to be done to the employee mailbox. There shall be no forwarding rules of any kind placed on the employee mailbox during the period of absence. In the event the mailbox fills up during this period Exchange will respond to new mail with an NDR stating the mailbox is full. This is acceptable.

**Vacation:** Nothing is to be done to the employee mailbox. There shall be no forwarding rules of any kind placed on the employee mailbox during the period of absence. In the event the mailbox fills up during this period Exchange will respond to new mail with an NDR stating the mailbox is full. This is acceptable. The user should set up an out-of-office notification. See section 3 Email Best Practices for a sample of out-of-office notification.

**Transfer:** If the user will be staying in the same AD domain (i.e. Agwest), then the only thing that needs to be done to the user's mailbox is changing the primary email address. In case of a move from one domain to another (i.e. Agwest → Ageast), the administrator should contact the Centralized Helpdesk to request the mailbox move.

## **4.6. Resource Mailboxes**

ITS Exchange will house one additional type of mailbox in addition to the user mailbox. This is the resource mailbox. This mailbox will not be accessed directly via logging in. Instead the mailbox will be "accessed" via Outlook and with the user's individual logon.

## 4.6.1. Resource

A resource mailbox is a mailbox that represents physical assets, such as a conference room. The resource mailbox is primarily used for scheduling purposes. Users can access and schedule conference rooms via the resource mailbox's calendar.

Resource mailboxes are only available to large and state offices. Any other office creating such mailboxes is strictly prohibited. The Exchange Operations Team will create the resource accounts and mailboxes.

The following two types of resource mailboxes are currently being supported:

- Conference/Training Room – Scheduling of conference rooms
- Vehicle – Tracking and scheduling of government vehicles

### 4.6.1.1. Resource Account Request/Approval Process

The Exchange Operations Team has published a resource account-Distribution List request form that is located on the team services website under the Exchange folder. The file name is RA and DLs Request Form.doc. This is a combination request form to request either a new resource account or a distribution list.

Below are the procedures that must be followed when requesting a new Resource Account.

### 4.6.1.2. Request Procedures

1. Fill out the RA and DLs Request Form and submit it to your local supervisor.
2. The local supervisor will determine if request has an acceptable business need.
3. If request is valid, the local supervisor will forward the request to the state IT representative.
4. If request is valid, the state IT representative will open a Magic ticket.
5. When opening a Magic ticket be sure to select the subject ID (Tree) and the following support subject:  
**“Exchange Email-DLs and RA Request”**.  
To find this subject you will need to drill down using the following path:  
**Software\COTS\Microsoft Applications\Email-Exchange Mail**
6. To ensure work order is properly assigned, select the following group name for assignment:  
**“ITS-IOD-HOB-EMAIL”**.
7. After creating Magic ticket, the State IT representative will attach the request form to the Magic ticket. This is accomplished by selecting the Work Order Attachments tab at the bottom of the ticket. After selecting the tab, right-mouse click and select **“Add Attachment”**.  
**Note: this can only be done after the ticket is assigned and not during the creation of the ticket.**

## 4.6.1.3. Approval Process

1. After a new request is submitted, using the approved request procedures, the Exchange Operation's Change Control Committee, will review the request within 24 hours after the Magic Work Order is received. An email will be sent to the requestor stating whether or not the request has been approved.  
**Note: To avoid delays in the approval process, please ensure that the request form is filled out in its entirety.**
2. If approved, the Resource Account will be created within 24 hours after the Exchange Operation's Change Control Committee review takes place.
3. A Communication is sent via email to the State IT representative who submitted the request.
4. It will be up to the State IT representative to configure the Resource Account according to the needs of the requestor.

## 5. Mailbox Storage/Retention/Restores

### 5.1. Mailbox Size Limit

A limit of 100MB total storage space has been imposed on each mailbox. The Exchange servers and disk arrays have been designed around these limitations. Exchange will warn users at 95MB that their mailbox is getting full, at 100MB the users will no longer be able to send messages, and at 125MB the user will no longer be able to send or receive.

If necessary, requests can be made for a larger mailbox. This must be done with management approval and via a helpdesk ticket. In addition to opening a Magic help desk ticket, the user requesting the increase must send an email to the following DL for approval:

**UG-ITS-IDD-ARCHDEF-CHIEF**

If the request is approved, the Exchange Operations Team will be notified to process the request.

Note: The following items make up the total mailbox size:

- Inbox
- Sub folders
- Calendar Entries
- Contacts
- Notes
- Journals
- Drafts
- Tasks
- Sent Items
- Deleted Items

A common mistake made by users when cleaning up their mailbox, is forgetting to delete the items in the sent items folder, as well as, the deleted items folder. After deleting email, in order to reduce the size of the mailbox, the user must close Outlook and then reopen Outlook for the Exchange server to recognize the new mailbox size.

### 5.2. Local PST Folders

There maybe a need for users to create archive folders if the user wants to retain more than 100MB of email. The location of the archive folder will depend on the user's hardware. However, all desktop and laptop users should always place the PST on their local C:\ drive. The local hard drive is the ONLY supported location for PST files. Users will have to ensure their PST is backed up on a regular basis. If you need help backing up your PST file, please see your local IT Representative.

**Warning!** Users may consider placing passwords on the PST for added security. Keep in mind that without the password the PST will not be able to be opened by anyone. Make sure the password is one that you will remember because lost passwords can not be retrieved by administrators.

**Note: There is a 2 GB limit for PST files. Multiple PST files may need to be created as the PST file approaches 2 GB of data. Also note, when copying PST files to CD, the storage capacity of a CD is only 650 MB.**

### 5.3. Message Size Limit

In order to maintain a consistent performance of the Exchange servers and the USDA networks, a message size limit has been enforced. No message will be sent or received larger than 10MB. The 10MB limit includes the combined size of the message and the attachments. This means that you will not be able to send a 10MB attachment because the size of the message or the text contained within the email message is added to the total size; making the email larger than 10MB.

### 5.4. Deleted Item Retention

Deleted emails are retained on the mail system for 14 days, and deleted mailboxes are retained for 30 days.

Deleted email restoration can be done by the users with Outlook. After an item has been deleted from the "deleted items" folder in Outlook, the user has 14 days to retrieve the message. (Reference Deleting Outlook emails document on team services web site under email team documents). Once the 14 days period has expired, the only way to retrieve the lost email is restoring the email from tape. Individual or multiple email messages will not be restored from backup beyond the user's 14 day grace period.

Backup data is only kept for a one month period. In most cases, any request longer than 30 days can not be carried out.

### 5.5. Forensics Investigations-Email Retrieval

Email message retrieval or recovery from tape backup is only authorized for forensics investigations. When it is necessary to retrieve email messages for a user under investigation, a request must be sent to the following DL by senior management from the corresponding state:

**UG-ITS-IGD-FNM-CHIEF.**

If the request is approved the Exchange Operations Team will be notified with the details for the email retrieval.

## 6. Email Client

### 6.1. Supported Client(s)

In order to access any ITS mailbox the user must be connected via an ITS workstation/laptop installed with an ITS approved Operating System load. The only exception to this policy is when accessing via a web browser.

Currently there are only 2 **supported** clients for connecting to a mailbox, Outlook XP (MAPI) or Outlook Web Access (OWA).

English is the only supported language on ITS Exchange. No additional language will be supported by ITS.

### 6.2. Outlook Access via USDA VPN or Dialup

In order to access the mail through Outlook XP, remote machines must be connected to USDA network via USDA VPN or Dial Up access. Those who have broadband connections such as DSL or Cable Modem can utilize Cisco VPN to connect to the USDA network.

To apply for remote access, please see your local Telecom Representative for details.

### 6.3. OWA – Internal and External

Users can access email via Outlook Web Access (OWA), either internally (inside the USDA network) or externally (outside of the USDA network). Users using OWA externally should be cautious, especially using it in public facilities, such as libraries or cyber café. The following are some of the best practices for using OWA in public locations:

- Always close all the browsers when you are done using OWA.
- Do not open attachments on a non-trusted machine as temp files are sometimes left behind of the computer.
- Don't leave the browser up when you step away, always logoff or lock the console if the option is available.
- Pay attention to your surroundings when logging on ensuring that no one is watching you type in your password or other sensitive information.

There are 3 URL's available for OWA access. There is a separate URL for the AGEAST, AGCENTRAL, and AGWEST domains. AGLO Domain users should use the AGEAST URL for OWA. Below are the 3 URL's that should be used when not connected to the USDA network locally or through VPN:

<https://webmail-east.one.usda.gov/exchange>

<https://webmail-central.one.usda.gov/exchange>

<https://webmail-west.one.usda.gov/exchange>

When users are connected to the USDA network locally or through VPN, they should use the following URL's:

<http://webmail-east.one.usda.gov/exchange>

<http://webmail-central.one.usda.gov/exchange>

<http://webmail-west.one.usda.gov/exchange>

When users connect to one of the URL's above, they will be presented with a logon screen asking for username and password. The user must type in the domain name before the username. Example: aglo\john.smith. Note the domain name and backslash before the username. The domain name is the name of the domain the user logs into when they logon to their workstation\laptop. See example below:



Domain \user name:

Password:

Any of the three URL's mentioned above will work for users accessing OWA from the internet.

## 7. Public Folders

Public Folders are not supported by ITS. ITS acknowledges the usefulness of public folders, but has decided on Microsoft SharePoint Services as the strategic direction for document management. A limited number of public folders will be made available until SharePoint Services are fully implemented. Users that have had public folders in the past will have the data and folders migrated to Exchange. A moratorium of new folders will be enforced inside ITS Exchange.

## 8. Distribution Lists

Distribution lists are NOT to be created by any administrators other than Exchange Operations Team. Distribution list membership however will be maintained by local and state IT administrators. The creation of all distribution lists must follow the procedures listed in section 8.1 below. All administrators must carefully review each request for a distribution list. For example, a distribution group with less than five members or a DL that will only be used by a small number of people is probably not necessary. Distribution lists are visible entries in the Global Address Lists; therefore the total number of lists will affect the end user.

### 8.1. Distribution List Requests\Approval Process

The Exchange Operations Team has published a Resource Account-Distribution List request form that is located on the team services website under the Exchange folder. The file name is ra-dl-request form. This is a combination request form for new resource accounts and distribution lists.

Below are the procedures that must be followed when requesting a new distribution list.

#### 8.1.1. Request Procedures

1. Fill out the RA and DLs Request Form and submit it to your local supervisor.
2. The local supervisor will determine if request has an acceptable business need.
3. If request is valid, the local supervisor will forward the request to the state IT representative.
4. If request is valid, the state IT representative will open a Magic ticket.
5. When opening a Magic ticket be sure to select the subject ID (Tree) and the following support subject:

**“Exchange Email-DLs and RA Request”.**

To find this subject you will need to drill down using the following path:

**Software\COTS\Microsoft Applications\Email-Exchange Mail**

6. To ensure work order is properly assigned, select the following group name for assignment:

**“ITS-IOD-HOB-EMAIL”.**

7. After creating Magic ticket, the State IT representative will attach the request form to the Magic ticket. This is accomplished by selecting the Work Order Attachments tab at the bottom of the ticket. After selecting the tab, right-mouse click and select

**“Add Attachment”.**

**Note: this can only be done after the ticket is assigned and not during the creation of the ticket.**

## 8.1.2. Approval Process

1. After a new request is submitted, using the approved request procedures, the Exchange Operation's Change Control Committee, will review the request within 24 hours after the Magic Work Order is received. An email will be sent to the requestor stating whether or not the request has been approved.

**Note: To avoid delays in the approval process, please ensure that the request form is filled out in its entirety.**

2. If approved, the Exchange Operation's Change Control Committee will forward the request to the IO lab where the Distribution List will be tested. Upon successful testing, the new Distribution List will be created in AD. Below is the IO lab group creation schedule. Please note, the schedule has 2 cycles:

- ✚ For inclusion in Cycle 1, a Request for Change (RFC) with the attached input file must be submitted to the Enterprise Change Management Team (CM) by Monday at Noon (GMT -5, Eastern Time US & Canada).
- ✚ Assuming a valid input file is submitted, the input file will be driven through the Interoperability Lab's (IO Lab) approved group creation process and implemented in the production ONE Active Directory forest by Wednesday of the same week at 6:00 pm (GMT -5, Eastern Time US & Canada).
- ✚ For inclusion in Cycle 2, a RFC with the attached input file must be submitted to CM by Wednesday at Noon (GMT -5, Eastern Time US & Canada).
- ✚ Assuming a valid input file is submitted, the input file will be driven through the Interoperability Lab's (IO Lab) approved group creation process and implemented in the production ONE Active Directory forest by Friday of the same week at 6:00 pm (GMT -5, Eastern Time US & Canada).
- ✚ Weeks containing holidays, alternate schedules will be followed consisting of a single cycle.
- ✚ Weeks containing a holiday on either Monday or Friday, an RFC with the attached input file must be submitted to CM by Tuesday at Noon (GMT -5, Eastern Time US & Canada).
- ✚ Assuming a valid input file is submitted, the input file will be driven through the Interoperability Lab's (IO Lab) approved group creation process and implemented in the production ONE Active Directory forest by Thursday of the same week at 6:00 pm (GMT -5, Eastern Time US & Canada).
- ✚ Weeks containing a holidays on days other than Monday or Friday, an RFC with the attached input file must be submitted to CM by Monday at Noon (GMT -5, Eastern Time US & Canada).
- ✚ Assuming a valid input file is submitted, the input file will be driven through the Interoperability Lab's (IO Lab) approved group creation process and implemented in the production ONE Active Directory forest by 6:00 pm (GMT -5, Eastern Time US & Canada) of the second business day after Monday.

## 9. Anti-Virus

The current ITS supported Anti-Virus application is GroupShield for Exchange by McAfee. GroupShield is installed on all ITS Exchange servers. GroupShield provides anti-virus scanning at the database level. GroupShield has been configured to block file extensions that have been known to contain viruses, in an effort to prevent viruses from entering the ITS Exchange infrastructure.

Below are the current file extensions that are blocked by GroupShield. If a user from outside USDA attempts to send an email with one of the extensions listed below, the attachment will be blocked and the intended USDA recipient will receive a message indicating the attachment was stripped or blocked.

File Extensions that are blocked:

ade, adp, asp, asx, bas, bat, chm, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mda, mdb, mde, mdt, mdw, mdz, msc, msi, msp, mst, ops, pcd, pif, prf, reg, scf, scr, sct, shb, shs, tmp, url, vb, vbe, vbs, vsmacro, vss, vst, vsw, ws, wsc, wsf, wsh