

Protecting Domain Names from Spoofing: A Guide for E-Mail Senders

Published: February 20, 2004

Microsoft's technical proposal to help deter spoofing is a suggested next step on the road to addressing the escalating problem of unwanted, unsolicited e-mail. Published in draft specification form at http://www.microsoft.com/mscorp/twc/privacy/spam_callerID.msp and open to public comment, Microsoft's approach entails publishing outbound IP addresses to create a mechanism analogous to "caller ID" for e-mail messages.

In this specification, Microsoft encourages organizations to protect their domain names from spoofing by publishing the IP addresses of their outgoing mail servers in the Domain Name System (DNS) in *e-mail policy documents*. A domain's e-mail policy document is published in a DNS text record. Text records, also known by their DNS record type, "TXT", are designed to contain free-form text. Caller-ID uses TXT records to store e-mail policy documents in eXtensible Markup Language (XML) format. (The Caller-ID Specification contains complete details about e-mail policy documents.)

This guide provides instructions and templates to help e-mail system administrators publish the IP address of outbound mail servers in e-mail policy documents. Even if a domain has no outbound e-mail servers, you can still help protect that domain name from spoofing by publishing an e-mail policy document. Follow the steps below to create and publish an e-mail policy document for each domain name your organization owns.

1. [Determine the IP addresses of the outbound e-mail servers for the domain](#)
2. [Create the e-mail policy document](#)
3. [Publish the e-mail policy document in DNS](#)

1. Determine the IP addresses of outbound e-mail servers

Identify the e-mail servers that transmit outbound e-mail and their IP addresses for all the domains and subdomains in your organization. You will need to publish an e-mail policy document for each of them.

If your organization uses any third parties to send e-mail on its behalf, such as an e-mail service provider or a hoster, you will need to know their domain names. You do not need the IP addresses of their outbound e-mail servers. (You might also advise them to publish e-mail policy documents for their own domains.)

Are there any domains in your organization that send only direct mail? In other words, are there domains that only send mail directly to the ultimate recipients and never to external mailing lists? These domains can get an extra measure of protection against spoofing through stricter checking as described in the Caller-ID specification. Caller-ID gives you a way to note this fact in the e-

mail policy document. In fact, to take advantage of these protections, you might consider creating such a domain especially for that kind of e-mail.

2. Create the e-mail policy document

Create an e-mail policy document for each domain and subdomain that sends mail from your organization. As described below, it is also possible for several domains to share the same e-mail policy document.

E-mail Policy Document Walkthrough

Before listing specific examples of e-mail policy documents, it is worth examining one of them in detail. The following example shows each element on a separate line and uses indentation to make the XML easier to read. In practice, when you create DNS TXT records, Microsoft recommends you remove most of the line breaks and all the indentation in order to make the document more compact (as shown in the templates in the next section).

```
<ep xmlns='http://ms.net/1' testing='true'>
  <out>
    <m>
      <a>192.168.0.101</a>
    </m>
  </out>
</ep>
```

The outermost **<ep>** tags indicate that this is an e-mail policy document.

The **xmlns parameter** (or *attribute*) in the opening **<ep>** tag designates an XML *namespace*. A namespace identifies a family of element and attribute names. Namespaces are a very important feature of XML because they allow different families of names to be used in the same document without naming collisions. Namespace names are often just URLs. All e-mail policy documents have the same namespace identifier, <http://ms.net/1>, regardless of the domain. The `/1` indicates that this e-mail policy document conforms to this first version of the Caller-ID specification.

The **testing attribute** indicates that this domain is currently testing its e-mail policy document and receiving systems should act as if no e-mail policy document has been published. Microsoft recommends setting the `testing` attribute on your e-mail policy documents to `true` until you are confident that you have identified all your outbound e-mail servers.

The **<out>** element is a container for elements that describe the domain's policies for outbound e-mail. There is also an **<in>** element to describe the domain's policies for inbound e-mail, but Caller-ID does not use it.

The **<m>** element is also a container, this time for information about the domain's mail servers. Since the **<m>** element is contained in, or is a *child* of, the **<out>** element, we can infer that the **<m>** element describes the domain's outbound e-mail servers.

The **<a>** element contains the IP address of a single outbound e-mail server.

E-mail Policy Document Templates

Use the following templates to create the e-mail policy document for your domain.

1. **No outbound e-mail servers.** Use this template when your domain has no outbound e-mail servers at all, but you want to protect it from being spoofed.

You can copy this template verbatim into a DNS TXT record; no changes are required.

```
<ep xmlns='http://ms.net/1'><out>
<noMailservers/>
</out></ep>
```

2. **Outbound and inbound e-mail servers are the same.** Use this template if your outbound e-mail servers are the same as your inbound e-mail servers. In effect, this template says “look at the DNS MX records for my domain, or the A records if there are no MX records present. Whatever you find there are also my outbound servers.”

You can copy this template verbatim into a DNS TXT record; no changes are required.

```
<ep xmlns='http://ms.net/1'><out><m>
<mx/>
</m></out></ep>
```

3. **Single outbound e-mail server.** Use this template (from the Walkthrough earlier in this guide) if you have just one outbound e-mail server. Simply replace the IP address below with the correct one for your server.

```
<ep xmlns='http://ms.net/1' testing='true'><out><m>
<a>192.168.0.101</a>
</m></out></ep>
```

4. **Multiple outbound e-mail servers.** Add up to about 10 `<a>` elements and enter the correct IP address in each one. If you have more than 10 outbound e-mail servers you may need to use one of the more advanced templates below.

```
<ep xmlns='http://ms.net/1' testing='true'><out><m>
<a>192.168.0.101</a>
<a>192.168.0.102</a>
<a>192.168.0.103</a>
</m></out></ep>
```

Note: DNS information is typically transmitted using a protocol called User Datagram Protocol (UDP). UDP transmits data in blocks or *packets* of at most 512 bytes. E-mail policy documents must therefore be less than 512 bytes in length, or special measures must be taken to break them up into smaller pieces. This is why we suggest an approximate (rather than exact) limit of 10 `<a>` elements in this template.

5. **Multiple outbound e-mail servers in an address range.** If your domain groups e-mail servers in a particular address range, you can use the `<r>` element to designate an IP address range and a subnet mask. The template below identifies a group of 16 outbound e-mail servers (indicated by a 28 bit subnet mask) starting at IP address 192.168.210.0. Change this template to indicate the correct starting IP address and subnet mask length.

As with `<a>` elements, you can add up to about 10 `<r>` elements if you have outbound e-mail servers in several IP address ranges. (See the **Note** in Item 4 above for an explanation of why we suggest this limit.)

```
<ep xmlns='http://ms.net/1'><out><m>
<r>192.168.210.0/28</r>
</m></out></ep>
```

6. **Direct mail.** To indicate that mail from a domain is only sent directly to the ultimate recipients, and never to mailing lists, you can add the `directOnly` attribute to the `<out>` element of the e-mail policy document.

```
<ep xmlns='http://ms.net/1' testing='true'>
<out directOnly='true'><m>
<a>192.168.0.101</a>
</m></out></ep>
```

7. **Outsourced e-mail service provider.** Suppose your organization has outsourced some or all of its outbound e-mail to a service provider called `contoso.com`. You can designate this organization as a legitimate sender of e-mail for your domain by using an `<indirect>` element. The `<indirect>` element says, in effect, “The outbound e-mail servers of `contoso.com` are also legitimate outbound e-mail servers for my domain.”

Replace `contoso.com` with the domain name of your e-mail service provider. You can have multiple `<indirect>` elements, just like `<a>` elements.

```
<ep xmlns='http://ms.net/1'><out><m>
<indirect>contoso.com</indirect>
</m></out></ep>
```

8. **Hosted e-mail.** Many smaller organizations use the services of a “hoster” to provide e-mail and Web presence. In this case, you may need to ask your hosting service administrator to create the necessary e-mail policy documents for you.

Replace the domain name in the `<indirect>` element with the appropriate domain name for your situation.

```
<ep xmlns='http://ms.net/1'><out><m>
<indirect>contoso.com</indirect>
</m></out></ep>
```

- If you send e-mail via your hoster’s outbound e-mail servers (which is most likely the case if you read and write e-mail using a Web browser), enter the domain name of the hoster in the `<indirect>` element. This indicates that your hoster’s outbound e-mail

servers are allowed to send e-mail on behalf of your domain.

- If you send e-mail via your ISP's e-mail servers rather than your hoster's e-mail servers (this is most likely the case if you read and write e-mail using a program such as Microsoft Outlook Express, Microsoft Office Outlook, or Qualcomm Eudora), enter the domain name of the ISP in the `<indirect>` element. This indicates that your ISP's outbound e-mail servers are allowed to send e-mail on behalf of your domain.

9. **Multiple subdomains sharing the same outbound e-mail servers.** Large organizations often have many subdomains representing business units or branch offices. Often they all share the same e-mail servers run by a central IT organization.

To handle this situation, Microsoft recommends you create a dummy subdomain to hold the e-mail policy document shared by your real subdomains. You can then use DNS CNAME records to point to this dummy subdomain.

Suppose `example.com` has three subdomains, `sub1`, `sub2` and `sub3`. Shown below are the CNAME records that point to a dummy subdomain called `outbound.example.com` that holds the shared e-mail policy document. As always, this document is stored in a DNS TXT record.

```
_ep.sub1.example.com IN CNAME _ep.outbound.example.com
_ep.sub2.example.com IN CNAME _ep.outbound.example.com
_ep.sub3.example.com IN CNAME _ep.outbound.example.com
```

To customize this template for your organization, simply create the necessary CNAME and TXT records for your subdomains. Alternatively, you could create e-mail policy documents for each subdomain that use `<indirect>` elements to point to the shared e-mail policy document in the dummy domain.

10. **Mix and match.** It is perfectly permissible to mix and match `<a>`, `<r>`, `<mx/>` and `<indirect>` elements in the same e-mail policy document.
11. **Long e-mail policy documents.** Larger organizations with more complex e-mail topologies may need longer e-mail policy documents. If your organization has a large e-mail policy document, please refer to the Caller-ID specification for information on how to split it up.

3. Publish the e-mail policy document

As described at the beginning of this guide, a domain's e-mail policy document is published in a DNS text record. To ensure the e-mail policy document TXT records do not get mixed up with other TXT records a domain may publish, Caller-ID uses a special sub-domain named "`_ep`" to hold them. If your organization's domain is `example.com`, you will publish the necessary TXT records under the domain `_ep.example.com`

Once you have created the e-mail policy documents for your organization, you need to publish them in DNS TXT records. You may need the help of a DNS administrator to do this.

For each e-mail policy document, create an _ep subdomain of the appropriate domain name. Copy the e-mail policy document into a TXT record in the _ep sub-domain using your customary DNS administration tools.

Legal Notice

This is a preliminary document and may be changed substantially prior to the final commercial release of the Caller ID specification. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2004 Microsoft Corporation. All rights reserved.

Microsoft, Outlook, and Office are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

[↩ Top of document](#)