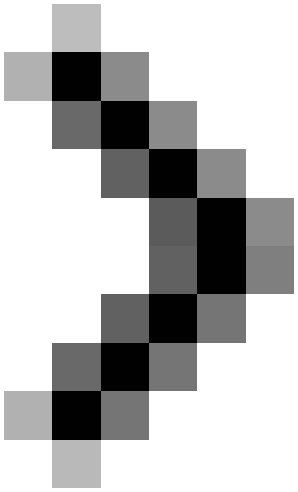
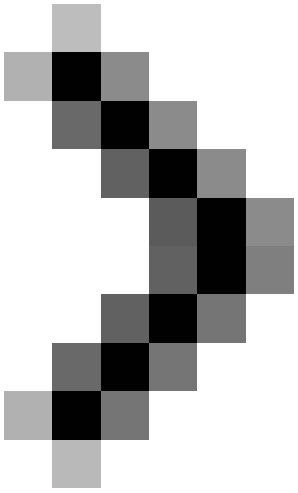
Additions for Exchange Server 2007 - Part 3: Email client access protection

This article will introduce a high-level overview of the security issues of different client email types such as POP3, IMAP4, OWA and Outlook Anywhere (also known as RPC over HTTP (S).



Part 1: Introduction steps



Part 2: Default protection

Marc Grote

Before you get started, note that this article is based on the beta version of Windows Server 2008 and Exchange Server 2007 SP1, so some of the features may be altered or removed in versions final of the product.

This article will introduce a high-level overview of the security issues of different client email types such as POP3, IMAP4, OWA and Outlook Anywhere (also known as RPC over HTTP (S).

POP3

POP3 (Post Office Protocol version 3) is a relatively old protocol that takes email from a mail server like Exchange Server. Previously, with Exchange Server 2003, Exchange supported POP3, but this protocol was disabled by default. This is similar to Exchange Server 2007, so you must change the startup type of this protocol to Automatic. One of the important changes in Exchange Server 2007 POP3 access is that it is not encrypted sessions. Exchange Server 2007 uses a certificate that assigns the same type to protect the transmission of messages. Because of this, you must configure the email client to access Exchange Server on a secure connection. You should also remove this certificate after installing Exchange with a trusted certificate from a CA certificate authentication center or with a certificate from the trusted third-party CA. To configure POP3 access, you must use the Exchange Management Shell (EMS). Starting with Exchange Server 2007 SP1, POP3 management components will be in the Exchange Management Console (EMC).

IMAP4

IMAP4 (Internet Message Access Protocol version 4) is also a relatively old protocol. IMAP4 compared to POP3 has some more advanced.

Starting with Exchange Server 2003, Exchange supports IMAP4 but this protocol is disabled by default. This is also done in Exchange Server 2007, so you must change the startup type of this protocol to Automatic. One of the important changes in Exchange Server 2007's IMAP4 access is that it is not encrypted sessions. Exchange Server 2007 uses the same assigned certificate to protect mail transmission. Therefore, you must configure the email client to access Exchange Server on a secure connection.

Ports used by POP3 and IMAP4

Default gateway protocol IMAP4 / SSL 993 (TCP) IMAP4 with or without TLS143 (TCP) POP3 / SSL995 (TCP) POP3 with or without TLS 110 (TCP)

Table 1

OWA

Outlook Web Access (OWA) is protected by default. Like any Exchange client service, Outlook Web Access is protected by an equally assigned certificate and HTTPS access is enabled by default. However, for an Administrator account, it is recommended to use its own certificate for accessing OWA from a trusted internal Certificate Authority (CA) or from a trusted third-party CA. Exchange Server 2007 Outlook Web Access has some additional security settings. Some of these security settings are part of the additional Outlook Web Access security package introduced in Exchange Server 2003. Most of this tool's settings (and some additional settings) are available. provided by default in Exchange Server 2007. Exchange Server 2007 also has some security features:

1. Split the Outlook Web Access segment
2. Full and partial client version
3. Restrict access to Outlook Web Access for certain users
4. Customize Microsoft Office Sharepoint integration
5. Control Direct Access for file server sharing issues.
6. Lock access to certain file types.

Outlook Anywhere

Outlook Anywhere, formerly known as RPC on HTTPS in Exchange Server 2003, this feature provides the most complete access to Outlook 2007 on HTTPS from outside of the network. Since securing Outlook Anywhere is similar to OWA, we won't introduce more details about this feature.

Exchange Active Sync (EAS)

Exchange Active Sync allows access to email and other issues for mobile devices such as Smartphones, PDAs (Personal Digital Assistants) and mobile phones. EAS is enabled by default and it is possible to configure its settings using Exchange Active Sync policies. With the help of these policies, you can make the following settings:

1. Password required for mobile devices
2. Request a password that has both a letter and a number
3. Allow or disallow download of attachments
4. Allow access to Windows Sharepoint services documents
5. Allows deleting lost or stolen devices
6. Activate device encryption issue

ISA Server 2006

You can use ISA Server 2006 (Internet Security and Acceleration Server) to provide an additional layer of security for Exchange Server 2007 access issues using Outlook Web Access (OWA), Outlook Anywhere and Exchange Active Sync (EAS). With the help of ISA Server 2006 you can safely publish all these Exchange Server clients. ISA Server 2006 allows additional security in HTTPS types to HTTP Bridging, Link Inspection, Content filtering, user authentication .

Patch management

You need to update the Messaging client issues and the operating system it is running regularly. You should use WSUS (Windows Server Updates Services) or some patch management software to help with this task.

Anti-SPAM

Exchange Server 2007 can integrate anti-spam features for the Hub Transport Server role and the Edge Transport Server role. You must enable anti-spam features on the Hub Transport Server through the Exchange Management Shell (EMS).

Exchange Server 2007 provides the following anti-spam features:

1. The combination of Outllook's Junk mail filter lists
2. IP Reputation service
3. Sender information
4. Sender ID
5. Filter mail through the email address sent
6. Prevent spam
7. Filter mail by content
8. SMTP Tarpitting

You can use Forefront Edge Security to provide some additional anti-spam features.

Antivirus

You should use a client-side antivirus scanner that scans access files on demand like Forefront Client Security. On the server, you should use a central antivirus solution like Microsoft Forefront Edge Security that we mentioned in the second part of this series.

Conclude

In the third part of this series, I have shown you how to secure client access via POP3, IMAP4, OWA, and Outlook Anywhere. Readers should note that this article does not focus on all the new security enhancements

and security features in Exchange Server 2007 that we will introduce in another article.