Synology®
White Paper

Secure Your Business Mail Service with Synology MailPlus

Based on
DSM 6.2

Table of Contents

Executive Summary

Cloud-based email services have become part of the IT landscape since Hotmail launched in 1996. Hosted email solutions have set the standard for features such as flexibility, consistency of use, integration with productivity tools, security, expandability, and administrative ease.

However, the fact remains that for business users, using a hosted service means that all the organization's email data is migrated to the cloud and gets out of your direct control[1]. Even with robust safeguards, organizations may prefer to host their own email services to maintain complete control over all their confidential data.

This white paper shows how your daily email services are protected by the software architecture of Synology MailPlus and explains the corresponding email security features, along with all the benefits associated with a self-hosted email server. Security is multi-leveled, enabling MailPlus Server to combat spam, phishing threats, viruses, and other email-borne threat vectors, while still maintaining high processing performance and allowing for high-level configurability and customization.

Synology MailPlus server and client solution offer the advantages of the cloud in terms of expandability, flexibility, integration, and ease-of-use, while still retaining the privacy and security that can only come from hosting your own data and hardware. Synology NAS architecture is an ideal combination of robust hardware, sophisticated management tools, and intuitive user interfaces, enabling organizations to enjoy the benefits of a cloud solution for email while giving them complete control over their hardware and software assets.

1. On July 2nd 2018, it was reported in a number of news outlets that Google allows some external software developers to read and analyze the inboxes of Gmail users – more **here**.

Secure your data with the self-hosted email service

In today's world, email hosting services are found everywhere and are often taken for granted. While email hosting has advantages, it also has drawbacks.

First and foremost, if you use a hosted service, your data is residing on servers outside your direct control and line of sight. Most of the time, this may not be a problem, but considering the mission-critical nature and sensitivity of today's electronic communications, "most of the time" may not be good enough.

It also impacts the requirement for **data sovereignty**, which is a legal issue for those companies and organizations that are required to store critical business and private data in the same geographical territory in which they reside – something which not all hosted services can guarantee.

These are the strong motivations for considering a self-hosted email solution.

The strongest argument for hosting your own service is **autonomy**: by running your own email server, you have exclusive control over your data, which resides wholly and solely on your infrastructure.

A self-hosted solution also offers **flexibility** – you can configure and manage the look and feel of your email system, fine-tune your own spam control and security parameters, and customize user management to meet your requirements in a way that the anonymous offerings of public cloud providers cannot achieve.

However, self-hosted email solutions also need to provide the degree of **security** which is comparable or superior to that provided by hosted solutions.

This is where Synology MailPlus comes into its own. Tightly integrated with Synology NAS platform, MailPlus provides a highly secure and configurable email solution. This white paper provides details of the in-depth security technologies that have been incorporated in Synology MailPlus.

Synology MailPlus Software Architecture

Synology MailPlus offers an expandable and fully-featured email server-client solution.

The architecture of Synology MailPlus has been specifically designed to provide all the features, functionality, security and flexibility expected from a contemporary email service. Furthermore, it is highly scalable – from small businesses comprising only five users, to large-scale applications for several thousand employees.

Incoming Mail Process

The security of Synology MailPlus has been continuously refined to provide high-level protection against spam, phishing attacks, and all the other threats and nuisances that email servers are subject to. As the vast majority of these threats originate from inbound email, this is where Synology has concentrated its efforts to provide maximum security while at the same fine-tuning processing efficiency to minimize the impact on workflow.

The following graphic provides an overview of the Synology MailPlus incoming mail process.

Postfix, the mail transfer agent, implements the first layer of defense against spambots and malware.

Postfix is integrated with other apps for spam/virus filtering, message-store access, and other SMTP-level access policies.

Dovecot LDA takes mail from Postfix and delivers it to the user mailbox.

Dovecot is the Synology MailPlus POP3/IMAP server. Dovecot also replicates mail data across the MailPlus High Availability architecture to ensure continuous availability.

The mail client may be Synology MailPlus web client or a third-party mail client such as Outlook or Thunderbird.

See Chapter 3. Email Security for further detail of Synology MailPlus incoming email security.

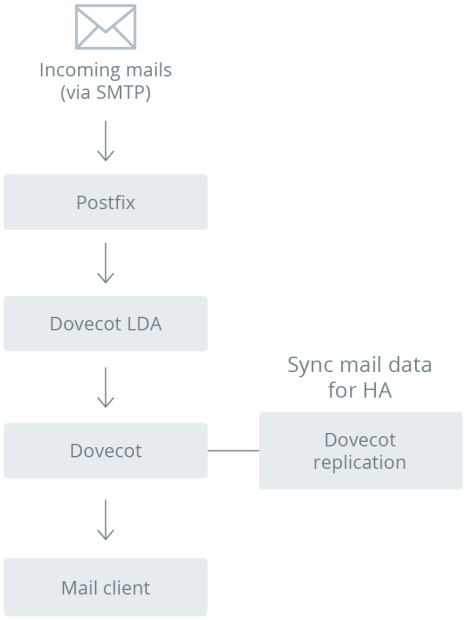

Figure 1: Incoming Mail Processing - High Level

Supported Mail Client Types

Synology MailPlus Client

Synology MailPlus client provides all the functionality you expect and need from a workstation email client, including contact management, mailbox creation, labeling, filtering, searching, and more. In addition, MailPlus offers mail utilities including priority mailbox and shared mailboxes. MailPlus is seamlessly integrated with Synology Chat and Synology Calendar, which makes MailPlus a communications and scheduling hub. With Chat and Calendar plug-ins, you can also turn email chains into real-time

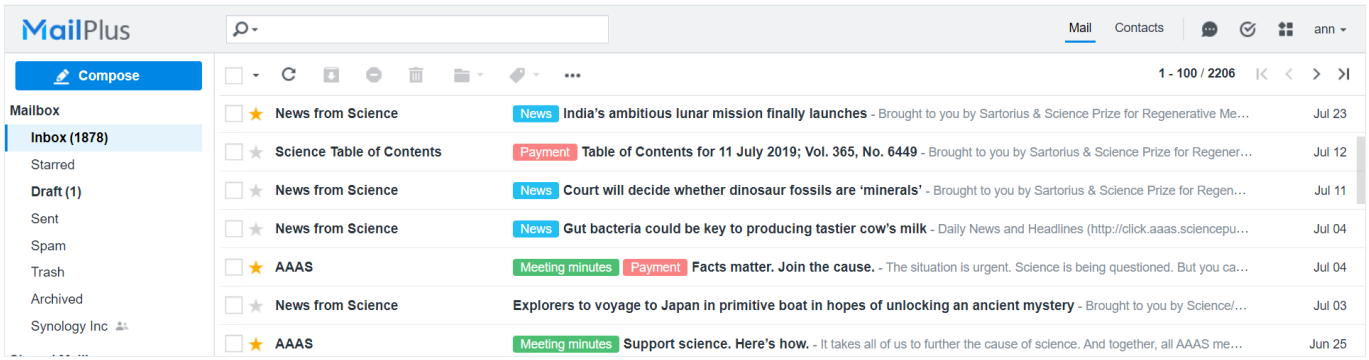

Figure 2: Synology MailPlus web client

discussions and to-do lists with a couple of clicks.

Synology MailPlus Mobile Apps

Fully-featured Synology MailPlus apps can be easily downloaded for both Android and iOS from their respective App Stores.

As noted above, Synology MailPlus Server also supports third-party mail client apps including Outlook and Thunderbird.

Email Security

"Email security" covers all of the methods required for safeguarding confidential and private information in email communication against unauthorized access, data loss, or compromise. In addition to preventing data loss, email is a prevalent threat vector for the incursion of malware, spam, and phishing attacks, that use fraudulent content to entice recipients to divulge sensitive information, open attachments, or click on hyperlinks that install malware on a target device or network.

Recently, the world has seen an explosion of large-scale computer security incidents such as WannaCry ransomware attack[2], which infected more than 230,000 computers across 150 countries in May 2017[3]. Many such attacks are initiated via email, hence the pervasiveness of threats to email highlights email security.

To address the security requirements, Synology MailPlus provides integrated security on the architecture, server and client level. Aside from incorporating a robust security infrastructure in its products, MailPlus can be easily integrated with third-party and open-source security products to provide dynamic and continuous protection against evolving spam, viruses, and malware threats.

Security Control Panel

Mail security controls are accessed and managed via the **Security** page in MailPlus Server:

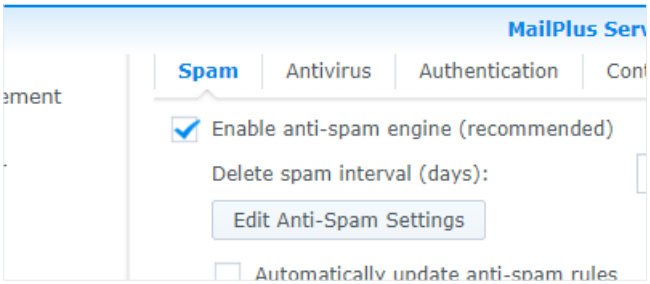

Figure 3: Synology MailPlus Server Security Controls panel

2. For illustrative purposes only, as this infection is Windows-based and doesn't affect Synology MailPlus systems.
3. https://www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware

Security Processing Workflow

As discussed in the above **Incoming Mail Process** section, Synology MailPlus applies most of its security counter-measures in the incoming mail handling process. Hereunder is a detailed description of these processes.

Postfix Security Check integrates with a number of scanning and quarantining applications which are executed in sequence for every inbound email as per the following graphic:

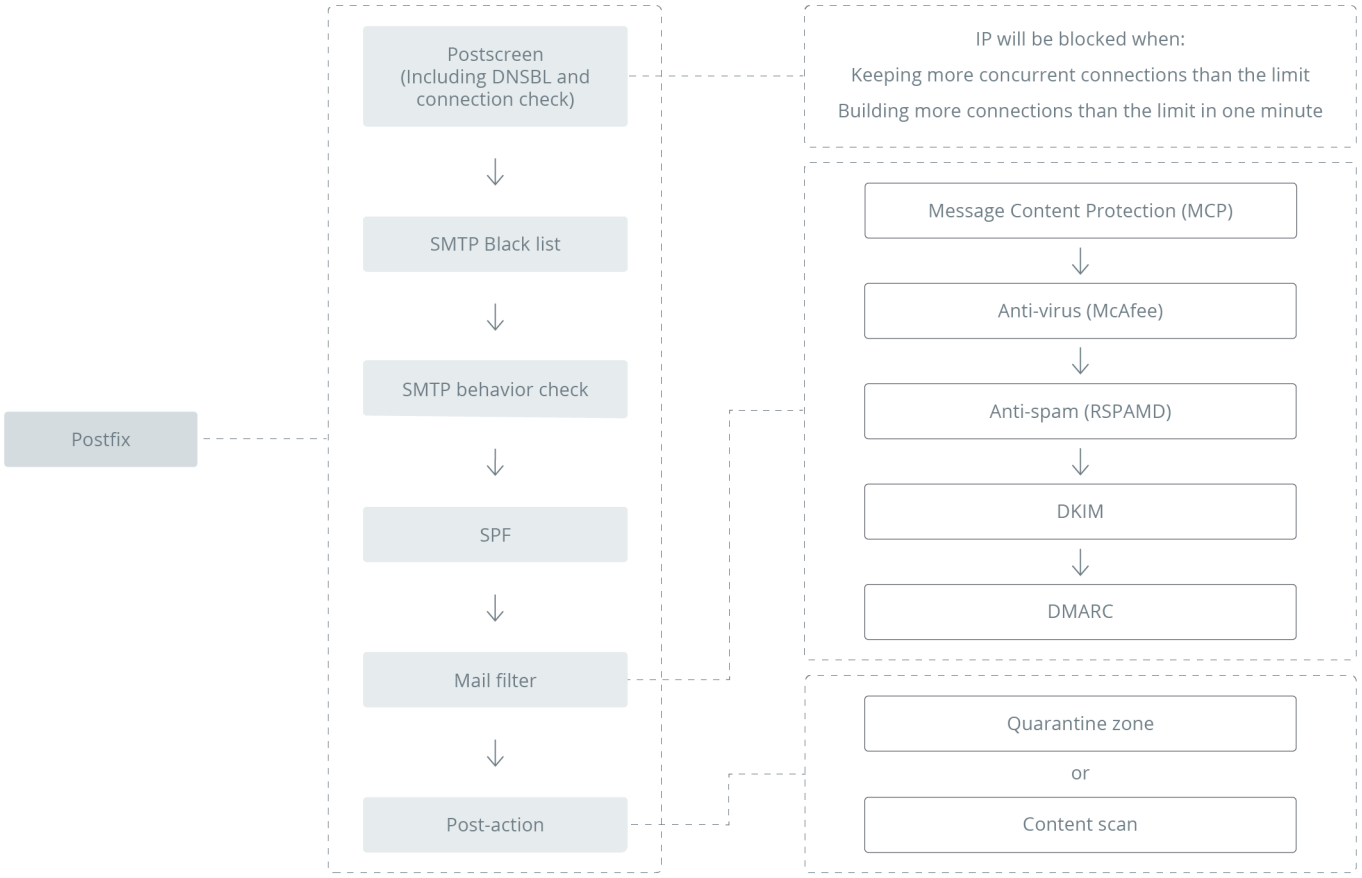

Figure 4: Postfix Process

Terminology in Security Processing Workflow

Processing Step	What it does
Postscreen (DNSBL)	Component of Postfix; acts as "bouncer" to stop unwanted spam at "front door".
SMTP Blacklist	Blacklist. All mails that match the criteria will be blocked.
SMTP Behavior Check	Executes a series of checks to reject suspect items, including poorly formed HELO hostnames, unknown client hostnames, senders without FQDN, senders from unknown domains, and more.
SPF	Sender Policy Framework - validates sending host legitimacy.
DKIM	Domain Keys Identified Mail - verifies the sender's identity using encryption methods to check if the email content has been modified.
DMARC	Domain-based Message Authentication, Reporting & Conformance - checks the sender's domain and DMARC records in DNS, and determines sender validity according to SPF/DKIM verification results and DMARC records.
Anti-Spam	Rspamd anti-spam; see further detail below.
Anti-Virus	e.g., McAfee; varies depending on user licensing arrangements. See further detail below.
Quarantine Zone	Captures suspect mail items based on detection from anti-virus and MCP rules.
MCP	Message Content Protection – applies content scanning rules (set by admin). See further details below.
Content Scan	Scans mail content for dangerous content types, suspicious links, malicious HTML coding, etc.

Message Content Protection

Message Content Protection (MCP) applies admin-defined rules to messages being handled by the server. The MCP list is configured to filter or block emails that match the specified rules. Matches generate a score that is summed to the "total MCP score", and if the score exceeds the MCP threshold, the mail system will execute the specified action: **Save to quarantine, Deliver anyway, Delete mail, Notify sender,** or **Forward**[4].

Synology MailPlus Spam Detection

Synology has developed a new, highly configurable and efficient spam filter utilizing **Rspamd**.

Rspamd (pronounced R spam D), is a fast, open-source spam filter, written in C, which supports a variety of filtering mechanisms including regular expressions, statistical analysis and custom services like URL blacklists. Rspamd is designed to handle hundreds of messages per second simultaneously[5].

Spam Filter Performance

Implementation of Rspamd contributes to a performance boost. We carried out a test using a Synology RS3614xs+ with DSM version 6.0.2-8451, set up RAID 5, SSD cache, and ext4 file system , and enabled spam filter with rule version 1799552. Synology MailPlus client was installed and activated. The result displayed in the figure below shows an increase in the performance of Rspamd over MailScanner:

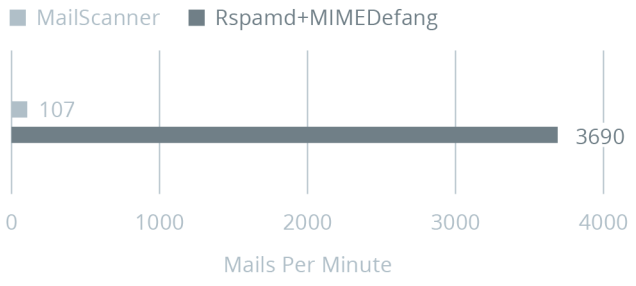

Figure 5: MailScanner Performance Test Results

Performance Summary

The integration of Rspamd with Synology MailPlus has led to a dramatic increase in the scanning speed to the order of 20x faster than in the prior version of MailScanner, and drastically reduced the resource usage:

- 30% less average CPU usage
- 20% less peak CPU usage
- 65% less loading
- 20% less memory usage

Antivirus

Synology NAS is on McAfee **SIEM** Supported Devices list[6]. McAfee Antivirus is optimized for use in Synology DiskStation. McAfee Anti-virus automatically checks for updates against McAfee's global threats database and can be configured to scan after-hours or off-peak.

McAfee Anti-virus requires a separate license which can be downloaded from the Synology Package Center:

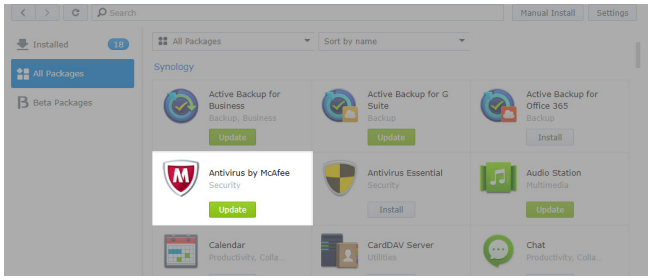

Figure 6: Synology Package Center with McAfee Antivirus highlighted

Authentication

Bullet-proof defense against spam and especially phishing scams is provided by **email authentication**. Authentication guarantees the identity of the email sender and is especially useful for establishing validated email links between businesses and important parties such as banks, suppliers, and other trusted partners (although authentication can be configured for multiple purposes).

Synology MailPlus provides checkbox controls for SPF, DKIM, and DMARC authentication:

- **SPF** is an email validation system used to validate sender ID and email address.
- **DKIM** provides validation using Public Key technology.
- **DMARC** is an email authentication, policy, and reporting protocol.

4. Also see this Knowledge Base article.
5. For detailed information and user documentation refer to https://rspamd.com/
6. https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-siem-supported-devices.pdf

Best Practice for Email Security Configuration

Synology MailPlus architecture is specifically designed to ensure maximum security and defense against incursion via email-borne threats including spam, viruses, trojan horses, and phishing. In this section, we will look at how MailPlus is able to provide high levels of security and defense for SMB users against email threats, without the need to deploy additional, expensive hardware such as dedicated security gateways. The following is a summary of the required configuration. For further details please refer to the **Synology MailPlus Server Administration Guide** (pdf).

Mail Delivery - General

- Enable SMTP authentication.
- Enable **Check if the senders' email addresses belong to the login accounts**.
- Enable **Prohibit plain text authentication over unencrypted connection** to make sure connections from Telnet are encrypted.

Security - Spam

- Enable anti-spam engine.
- Click **Edit Anti - Spam Settings**.
- At General: Set spam score to 5 (by default).
- At Auto learning:
  - Leave as default scores 12 and -1
  - Enable spam reporting: This helps users report suspicious mails to administrators and allows the system to learn for better spam identification.
- Enable postscreen protection against spam.
- DNSBL settings: The two defaulted DNSBL servers <sbl.spamhaus.org> and <xbl.spamhaus.org> are very reliable and can be trusted.

Note: Generally speaking, Synology doesn't recommend enabling grey-listing as this might adversely affect inbound mail processing times.

Security - Antivirus

- Tick the checkbox of **Enable Anti-virus Engine**.
- Anti-virus action: Choose **Save to quarantine**, so suspicious emails will be kept.

Note: Synology recommends the purchase of McAfee Anti-Virus which can be installed from the DSM Package Center. It has a higher virus detection rate than the free ClamAV which is installed by default.[7]

Security - Authentication

Enable SPF/DKIM/DMARC.

Security - Content Scan

Enable dangerous content scan:

- Reject partial messages
- Reject external message bodies
- Highlight phishing fraud

Service - Protocol

- Enable **POP3 SSL/TLS**, **IMAP SSL/TLS** and **Prohibit plain text authentication over unencrypted connection** for safe connection.

Control Panel - Security

Under the **Account** tab, enable auto block:

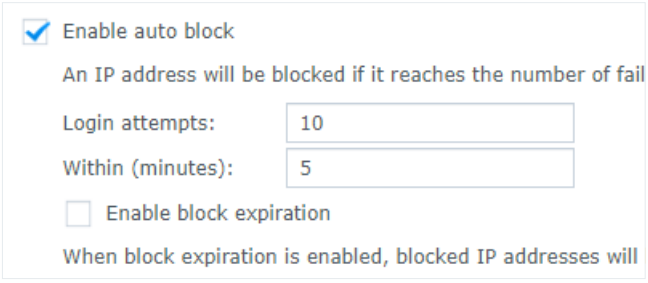

Figure 7: Enable Auto-block

Note: It is suggested that the system admin to enable auto block to defend against hackers attempting to access your system. System admin can also adjust the allowed number of failed login attempts and the time period for stricter policy.

7. See https://www.av-test.org/en/antivirus/home-windows/, https://www.av-test.org/en/antivirus/business-windows-client/ for comparative table.

Under the **Security** tab > **General**:

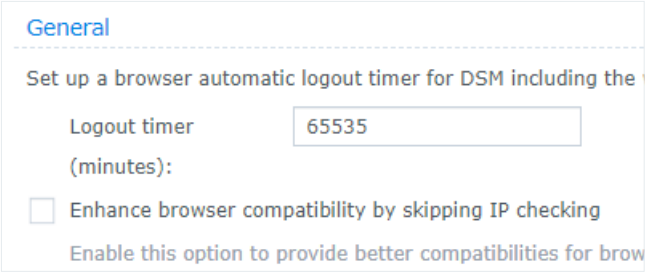

Figure 8: Security > General

Note: It is suggested that the system admin set the logout timer with a limited time period i.e. 15 mins or less so as to reduce potential exposure of the system to unauthorized access.

Summary

The architecture of Synology MailPlus has been designed specifically to provide a central managment platofrm and optimal security.

In terms of usability, Synology MailPlus offers an intuitive GUI interface along with iOS and Android apps, all of which are integrated with Synology Chat and Synology Calendar plug-ins, making it easy for users to collaborate and generate to-do lists from emails.

Synology MailPlus provides comprehensive security on the architecture, server and client level. As has been mentioned in this white paper, this is achieved through the expert integration of robust security technologies including Rspamd, SMTP authentication, message content protection, and anti-virus software. In addition to incorporating a robust security infrastructure in its products, MailPlus can be easily integrated with third-party and open-source security products to provide dynamic and continuous protection against evolving spam, viruses, and malware threats.

Synology MailPlus provides all of the features and functions you would expect of hosted, cloud-based email solutions, with the advantage of being hosted on your own premises and easily managed by your own IT administrators.

About Synology

Founded in 2000, Synology creates network-attached storage (NAS), IP surveillance solutions, and network equipment, that transform the way users manage data, conduct surveillance, and manage network in the cloud era. By taking full advantage of the latest technologies, Synology is committed to delivering products with forward-thinking features and best-in-class customer service.

References

Provisioning

Synology MailPlus Server Models

- A list of MailPlus-ready NAS solutions can be found **on this page**.
- The Synology NAS Selector is **here**.

> Note: When provisioning for Synology MailPlus Server, due to performance requirements, HDD drives + SSD cache are recommended. Additionally, enterprise-level drives are recommended for MailPlus Server. Synology NAS architecture can scale up to 180 drives and maximum raw storage of 1.4Pb.

Licensing

A single Synology MailPlus Server comes with five client licenses pre-installed. Additional licenses can be bought in lots of five or 20, both with perpetual validity. A license is bound to only one Synology Account upon activation.

High Availability Architecture units configured for Synology MailPlus includes 10 email accounts by default.

Detailed licensing information available on the **MailPlus Licensing Page**.

News Stories, Articles and Reviews

- **NHS Trusts hit by Malware** (The Guardian)
- **Google confirms external apps can scan your emails** (Australian Broadcasting Commission)
- **Review of Synology Rackstation** (Storage Review Magazine)
- **Should Your Email Live In the Cloud? A Comparative Cost Analysis** (Forrester Research)
- **AV-Test Lab tests 16 Linux antivirus products against Windows and Linux malware**
- **Best Antivirus Software for Windows Home users**
- **Best Antivirus Software for Windows Business users**

Email and Open Source Solutions Information

- **Email Security Protection 101** (Digital Guardian)
- **About DKIM**
- **Dovecot Replication with RSync**
- **MacAfee Supported Devices List** (pdf)
- **https://rspamd.com/**
- **Postfix** (Wikipedia)
- **Transport Layer Security** (Wikipedia)
- **OfflineIMAP** (Wikipedia)

SYNOLOGY INC.
9F, No. 1, Yuan Dong Rd.
Banqiao, New Taipei 22063
Taiwan
Tel: +886 2 2955 1814

SYNOLOGY AMERICA CORP.
3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

SYNOLOGY UK LTD.
Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL
United Kingdom
Tel.: +44 (0)1908 048029

SYNOLOGY FRANCE
102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

SYNOLOGY GMBH
Grafenberger Allee 125
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

SYNOLOGY SHANGHAI
200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.
4F, No. 3-1-2, Higashikanda,
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com