Getting Started: Ecrypt One hosted on Amazon Web Services (AWS)

The most up-to-date version of this document is always available here: www.ecryptone.com

Ecrypt One is a full-features email server that puts you back in control of your organization's communications. Setting it up on Amazon's Web Services (AWS) platform is easy. The steps you need to follow are all contained here.

Table of Contents

Get an AWS Account

You'll need an Amazon AWS account. You can get that here: https://aws.amazon.com

What's Your Domain?

In order to create an email server that communicates on the Internet, you need to have an email domain in-mind and eventually secured through a domain provider. To serve email for user@example.com, you need to own the example.com domain. There are many companies that can sell you a domain. Amazon's Route 53 services are one such service: https://console.aws.amazon.com/route53.

What Size of Deployment?

How many users do you need to support? You'll need computing power and storage to match your user base. This chart can be used to help you size your deployment.

Deployment Size	Number of users	Storage Required (GB)	Memory (GB)	CPU cores	AWS EC2 Instance Type	Ecrypt One AWS AMI
Extra Small	10	50	2	1	T2.small	Ecrypt One Small
Small	50	75	4	2	C4.large	Ecrypt One Small
Medium	200	150	8	4	C4.xlarge	Ecrypt One Small

More information on AWS Instance Types can be found here: https://aws.amazon.com/ec2/instance-types/

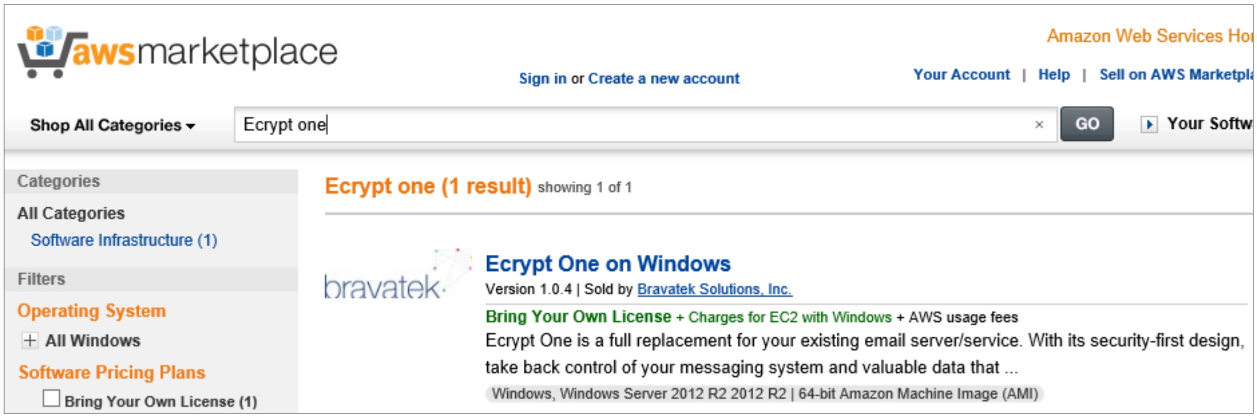
Launch your AWS Instance

When you launch your AWS instance, you need to select the Ecrypt One Amazon Image (AMI) that matches your deployment size, as determined from the table above: Ecrypt One Small or Ecrypt One Large.

Once you know what type of instance you need, you can launch your instance here: https://console.aws.amazon.com/ec2 Follow along with the notes here regarding the steps for creating an AWS instance.

Step 1: Choose and Amazon Machine Image (AMI)

In the AWS Marketplace, search for Ecrypt One and select the desired AMI.



Ecrypt one

Ecrypt one (1 result) showing 1 of 1

Ecrypt One on Windows

Version 1.0.4 | Sold by Bravatek Solutions, Inc.

Bring Your Own License + Charges for EC2 with Windows + AWS usage fees

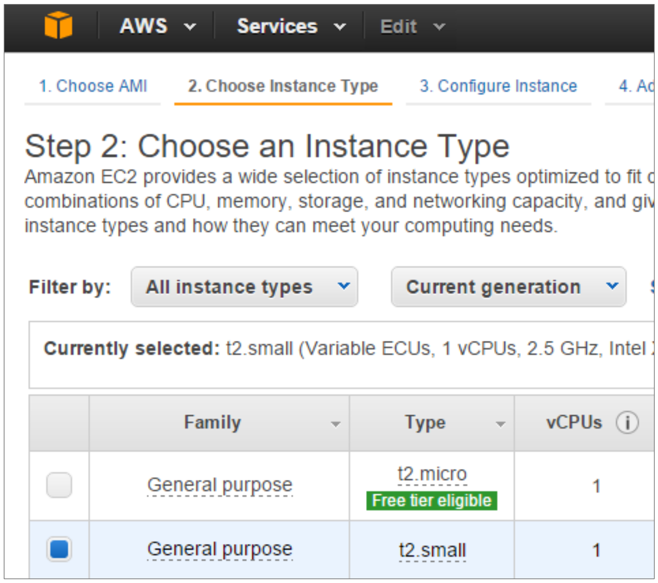
Ecrypt One is a full replacement for your existing email server/service. With its security-first design, take back control of your messaging system and valuable data that ...

Windows, Windows Server 2012 R2 2012 R2 | 64-bit Amazon Machine Image (AMI)

Step 2: Choose and Instance Type

In this step, select the instance type, corresponding to the deployment table above.

For example, the Extra Small deployment type above suggests a T2.small Instance Type, shown here:



Step 2: Choose an Instance Type

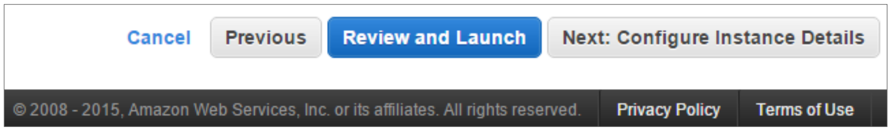
Amazon EC2 provides a wide selection of instance types optimized to fit c combinations of CPU, memory, storage, and networking capacity, and giv instance types and how they can meet your computing needs.

Filter by: All instance types Current generation

Currently selected: t2.small (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel

	Family	Type	vCPUs
□	General purpose	t2.micro Free tier eligible	1
☑	General purpose	t2.small	1

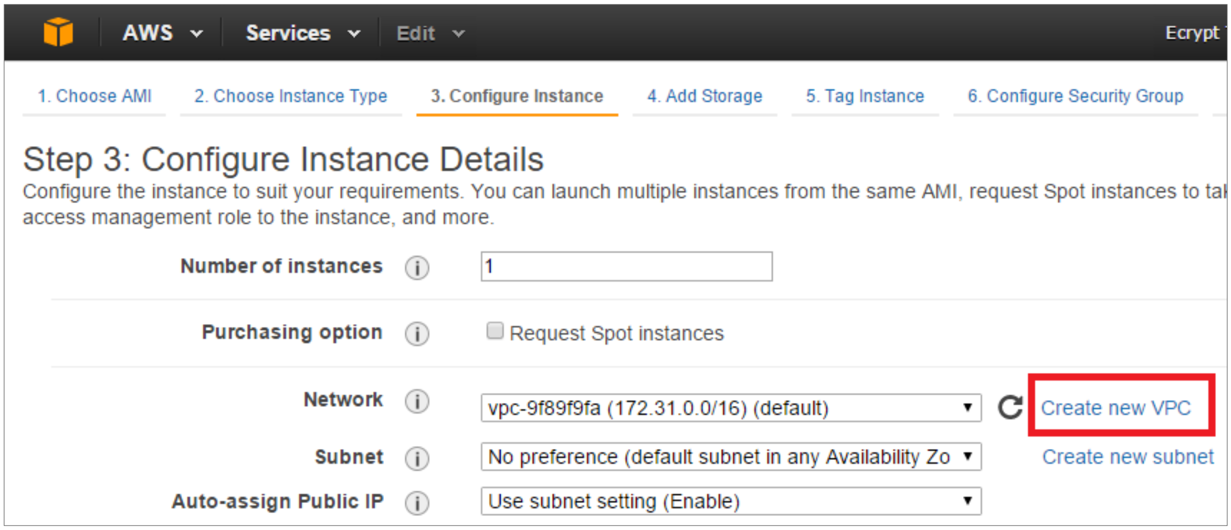
When you've selected the instance type, click the 'Next: Configure Instance Details' button


Cancel
Previous
Review and Launch
Next: Configure Instance Details
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Step 3: Configure Instance Details

In this step you configure some of the networking details for the instance.

1. Create a VPC: Virtual Private Cloud, if you don't have one already. This will make the management of the instance easier.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to tal access management role to the instance, and more.

Number of instances: 1

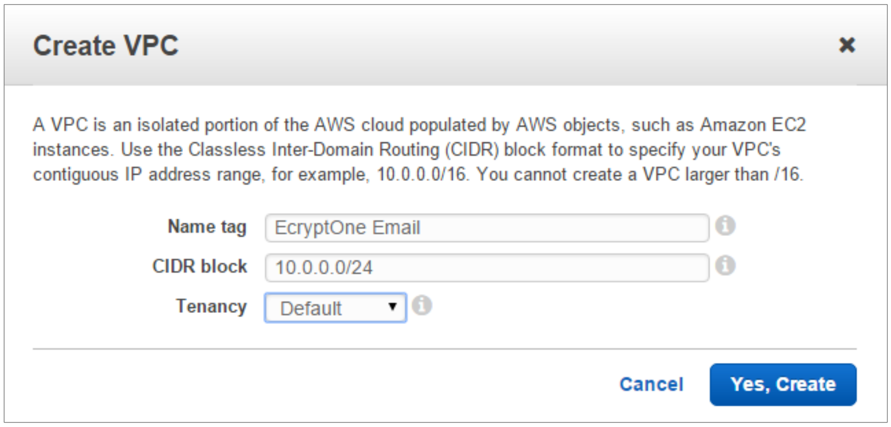
Purchasing option: □ Request Spot instances

Network: vpc-9f89f9fa (172.31.0.0/16) (default)

Subnet: No preference (default subnet in any Availability Zo

Auto-assign Public IP: Use subnet setting (Enable)

When you create a VPC, you need to specify a name and an internal IP address range. Specifying the IP range 10.0.0.0/24 is suggested.



Create VPC

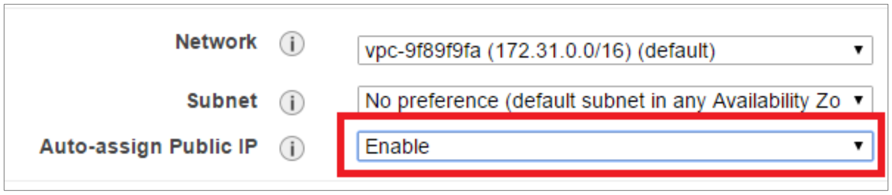
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. Use the Classless Inter-Domain Routing (CIDR) block format to specify your VPC's contiguous IP address range, for example, 10.0.0.0/16. You cannot create a VPC larger than /16.

Name tag: EcryptOne Email

CIDR block: 10.0.0.0/24

Tenancy: Default

2. Auto-assign a Public IP: make sure this is set to Enable. This will allow you to remotely log into your instance later on.

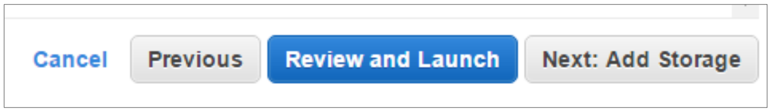


Network: vpc-9f89f9fa (172.31.0.0/16) (default)

Subnet: No preference (default subnet in any Availability Zo

Auto-assign Public IP: Enable

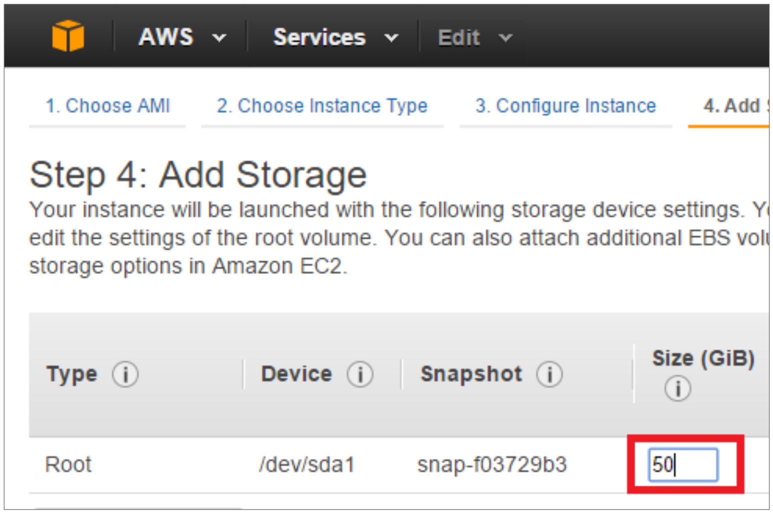
The rest of the settings' defaults are fine. Click the Next: Add Storage button.



Step 4: Add Storage

This step is where you specify how much storage you want for your server. The suggested minimums are found in the deployment table above.

For example, an Extra Small deployment has the storage suggestion of 50 GB. That would be entered as follows:

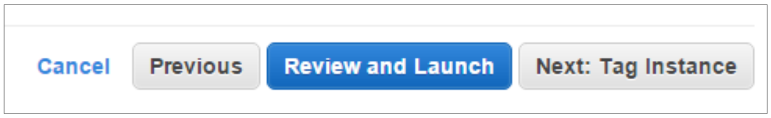


Step 4: Add Storage

Your instance will be launched with the following storage device settings. Y
edit the settings of the root volume. You can also attach additional EBS vol
storage options in Amazon EC2.

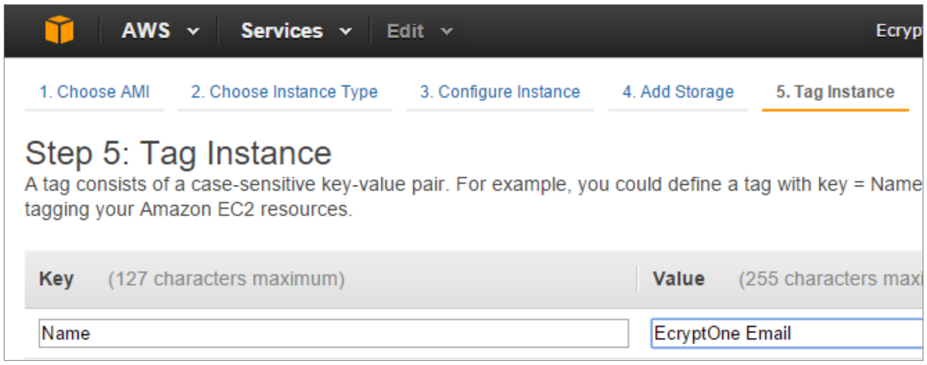
Type	Device	Snapshot	Size (GiB)
Root	/dev/sda1	snap-f03729b3	50

Click the Next: Tag Instance button.



Step 5: Tag Instance

This is where you give your server instance a name.

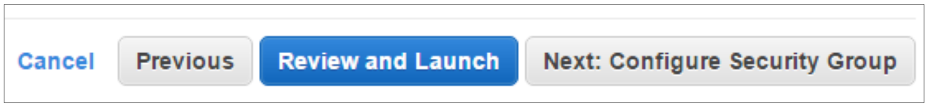


Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name
tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maxi
Name	EcryptOne Email

Click the Next: Configure Security Group button.



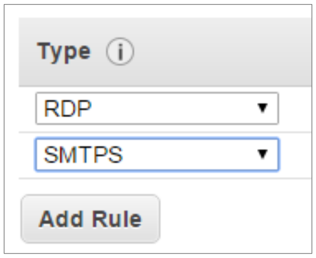
Step 6: Configure Security Group

This is the step where you configure the ports that are opened to the Internet. You'll want to leave the RDP port open in order to work with your server instance over Remote Desktop.

The following suggested ports should be opened in order to allow all the supported connectivity to the server:

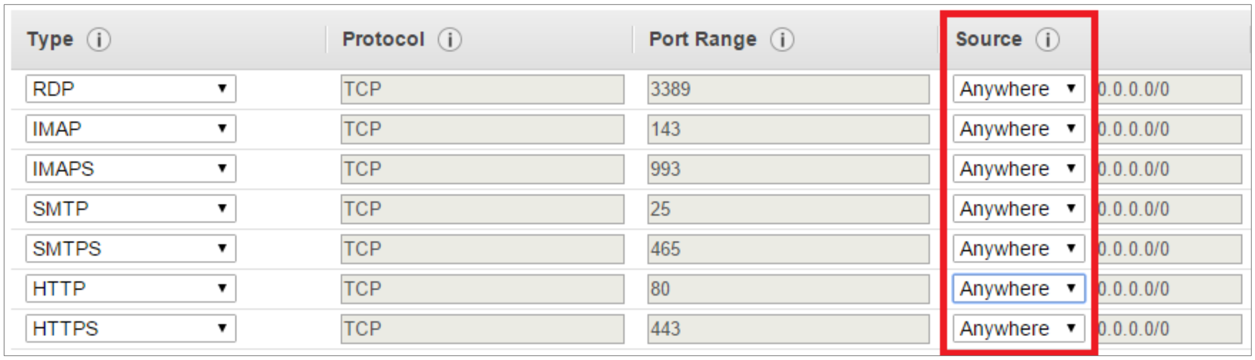
- IMAP
- IMAPS
- SMTP
- SMTPS
- HTTP
- HTTPS
- RDP

You add these port rules using the Add Rule button.



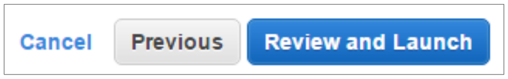
Type ⓘ
RDP ▼
SMTPS ▼

You also need to specify the Source of the connection. Typically, there is no way to know the IP range of these client addresses – it is suggested that you specify Anywhere, as shown here:



Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	
RDP ▼	TCP	3389	Anywhere ▼	0.0.0.0/0
IMAP ▼	TCP	143	Anywhere ▼	0.0.0.0/0
IMAPS ▼	TCP	993	Anywhere ▼	0.0.0.0/0
SMTP ▼	TCP	25	Anywhere ▼	0.0.0.0/0
SMTPS ▼	TCP	465	Anywhere ▼	0.0.0.0/0
HTTP ▼	TCP	80	Anywhere ▼	0.0.0.0/0
HTTPS ▼	TCP	443	Anywhere ▼	0.0.0.0/0

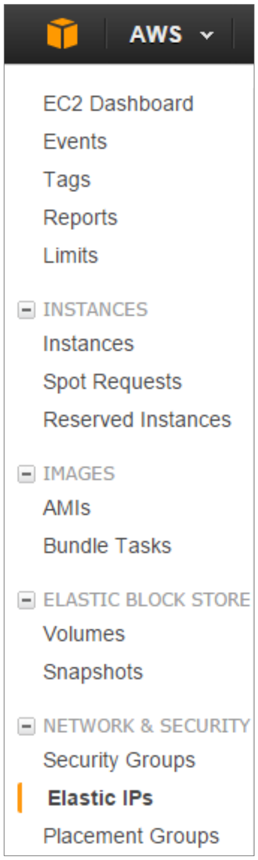
Click the Review and Launch button.



Step 7: Review Instance Launch

You should review your settings in this step, then press the Launch button to create your server instance.

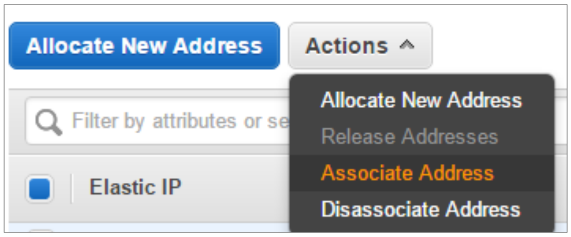
Create an Elastic IP



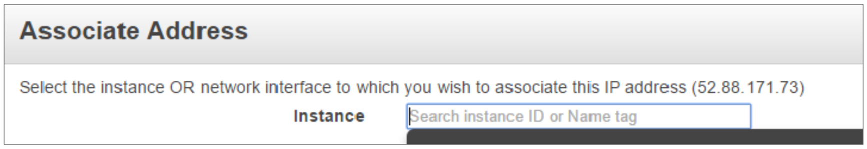
Elastic IP addresses are the AWS mechanism for creating an unchanging public IP address for your server. This is important, so that external clients and other servers can send you email, DNS servers know how to find your server, etc. The public IP address is maintained across restarts and stops/starts of the server, which is important.

In your AWS EC2 Dashboard, select Elastic IPs and press the Allocate New Address button.

Once you have an Elastic IP address, you can associate it with your new instance



Select your new address and then pop-down the Actions menu and select Associate Address.



Associate Address

Select the instance OR network interface to which you wish to associate this IP address (52.88.171.73)

Instance Search instance ID or Name tag

In this Associate Address screen, you can click in the Instance box and a menu will be shown. You can select the Tag name of the server instance you entered, then click the Associate button.

Return to the Instances area. You should see the Public IP of the instance change to the Elastic IP address.

Make note of this Public IP address: you'll need it when configuring the DNS settings for your email server.

Machine Name

You need to decide the name of your server on the Internet. This name will be used to direct email to your new server and not your Web server, typically. It will also be the name of the server used by Web Mail users and administrators. For example, internal and external users of Web Mail will navigate to mail.example.com, for example. The most common scenario, where you are serving email for a domain such as example.com, is to create a server and sub-domain named mail.*yourdomain*.com. Using a sub-domain leaves your main domain to be used for Web site traffic on your domain's main Web server, hosted elsewhere. You'll need this information when setting up your DNS configuration.

DNS Configuration

DNS is very important for email delivery, both for sending and receiving. In order to receive messages, other (SMTP) servers look at your DNS records to find out where your (SMTP) server is located on the Internet. This is the machine name mentioned above. When sending messages, other servers commonly verify email senders by checking your server for a reverse DNS entry. This is done to check to see if the sending server is the owner of traffic for the sending domain.

Typically, your domain provider is where you set up your DNS settings. You need to create the following entries with your DNS provider:

- Subdomain. E.g., mail.example.com. The IP address is the Elastic IP address noted previously
- MX record for your main domain. E.g., email sent to user@example.com. The MX record should be created for the example.com domain in this example. The host name for this record should be set to '@' and it should point to your subdomain.

Check with your domain provider for more details on setting up DNS with their service for email.

Amazon provides domain and DNS in their Route 53 services, found here:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html

Reverse DNS and Port 25

Reverse DNS allows other email servers to verify your server is the legitimate sender of email for your domain.

Related to sending email is port 25. This is the SMTP port used for sending email.

By default, Amazon's AWS prevents servers from sending mail on port 25 to avoid spamming.

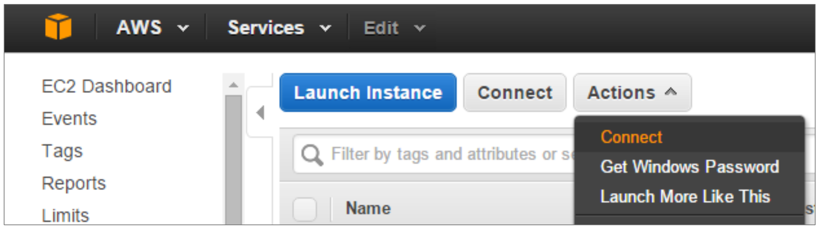
You can request a reverse DNS entry and the opening of port 25 by making a single request at the Request to Remove Email Sending Limitations page here:

http://aws.amazon.com/contact-us/ec2-email-limit-request/

You'll need to provide your Elastic IP address and machine name on that page.

Configure your Ecrypt One Server

With the above configuration arrangements made, it's time to configure your Ecrypt One email server with these settings. In the AWS EC2 Dashboard, select your instance in the Instances section, then choose Connect on the Actions menu.



Save the Remote Desktop (RDP) file that is sent to you – you'll use this often. Open the file and specify the following user ID and password:

- User: ECRYPT\Administrator
- Password: Password1!

The first time you log in, the Ecrypt One Setup Wizard will be displayed, prompting you for required information. You can re-run the wizard if you need to quit and restart it again.

Secure you Communications

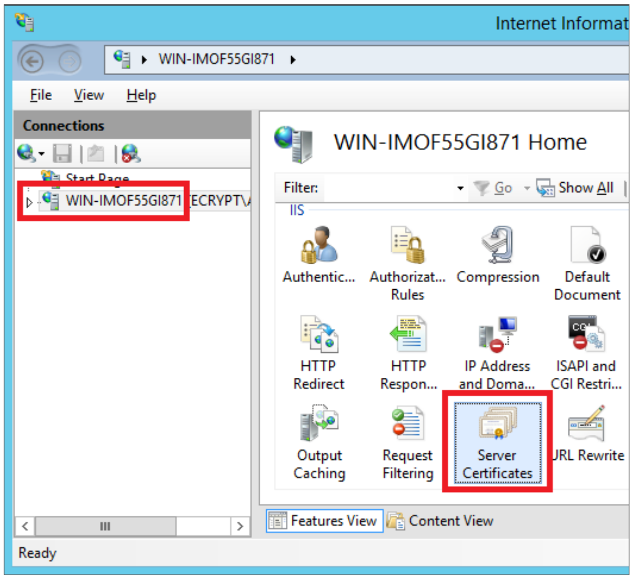
In order to communicate with your new server securely, you need to acquire an SSL/TLS certificate from a certificate authority. This step is not absolutely required, since the server setup wizard will have created a self-signed certificate and installed it. However, you'll get connection warnings when your users connect to the server (using HTTPS, IMAPS or ActiveSync). When connecting to the Web Mail portal or the Administrative portal, browsers are redirected from regular connections to secure connections, so they will always show a security warning if you do not get a trusted certificate. Companies such as Verisign, Thawte, GoDaddy and DigiCert offer standard SSL certificates for the purposes of securing Web sites, which is the kind you need.

Requesting a Certificate

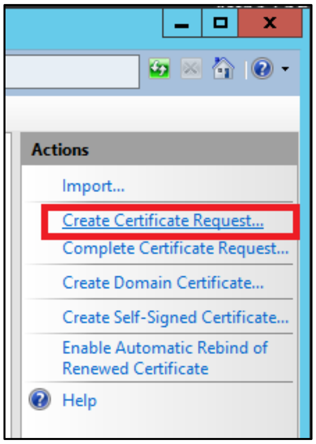
To request an SSL certificate from a Certificate Authority, you need a Certificate Signing Request from your new Ecrypt One server's Web server.

The Web server is Microsoft Internet Information Services (IIS). To requests a certificate from IIS, first open the IIS Manager.

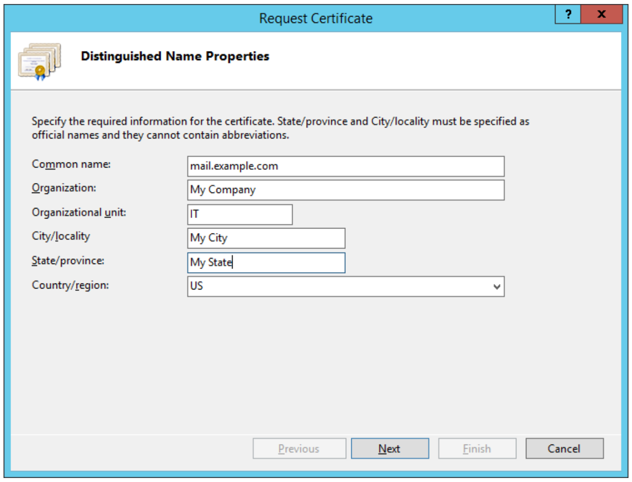
[continued on following page]



In Features View, double-click Server Certificates.


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

In the Actions pane, click Create Certificate Request.



Distinguished Name Properties

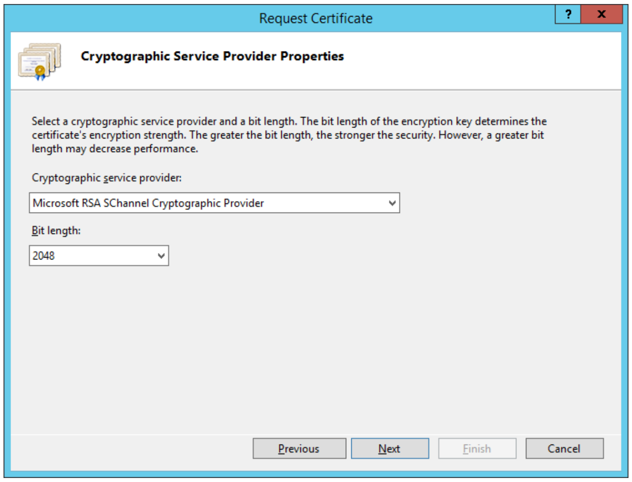
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: mail.example.com
Organization: My Company
Organizational unit: IT
City/locality My City
State/province: My State
Country/region: US

Enter the relevant information for your company similar to the following.

The common name is typically your server name.

Click Next after entering your information.



Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

On the next page, the Bit length defaults to 1024 but it is suggested that you choose 2048.

Click Next.

On the final page, provide a file name for the certificate request.

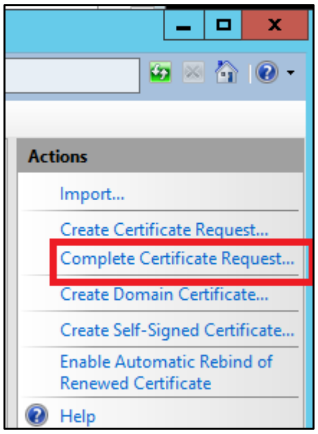
Click Finish to save the file.

This file can now be uploaded to your certificate authority of choice.

Installing your Certificate

When you get your certificate, it needs to be installed in the Web server for securing HTTP traffic. It then needs to be installed in the Ecrypt One server for securing SMTP and IMAP traffic.

Complete the Certificate Request


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

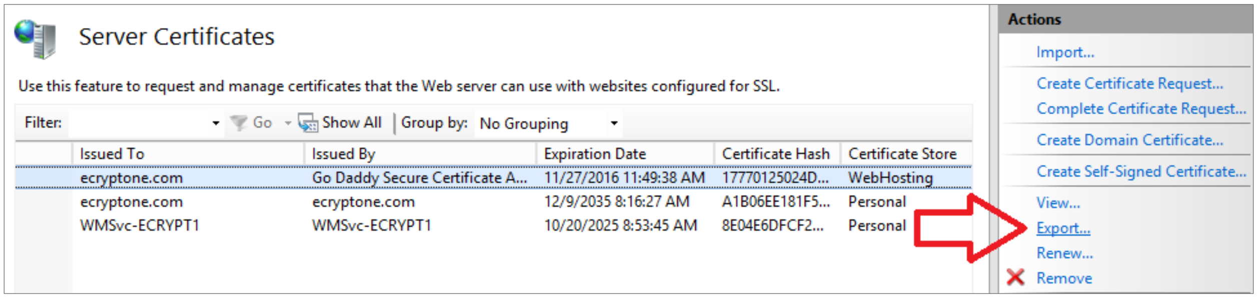
With the IIS Manager Service Certificates panel open, choose Complete Certificate Request and supply the file that was provided to you by the certificate authority.

Note: depending on the certificate authority, you may have to install intermediate CA certificates in order to provide a full chain of authority. This is done in Windows using the Internet Options commonly accessed via Internet Explorer.

Install the Certificate in Ecrypt One

Ecrypt One requires the same SSL/TLS certificate to be installed in order to support secure SMTP, IMAP and Start TLS (secure email transit from server to server). This needs to be done with the full private-public key pair. Now that the certificate request has been completed within IIS, the key pair can be exported to a file for import by Ecrypt One.

In IIS, find your newly imported certificate, such as shown below:



Server Certificates

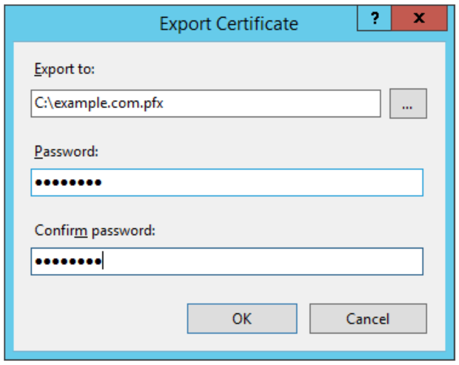
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
ecryptone.com	Go Daddy Secure Certificate A...	11/27/2016 11:49:38 AM	17770125024D...	WebHosting
ecryptone.com	ecryptone.com	12/9/2035 8:16:27 AM	A1B06EE181F5...	Personal
WMSvc-ECRYPT1	WMSvc-ECRYPT1	10/20/2025 8:53:45 AM	8E04E6DFCF2...	Personal

Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove

With the correct certificate selected, choose the Export action at the right.



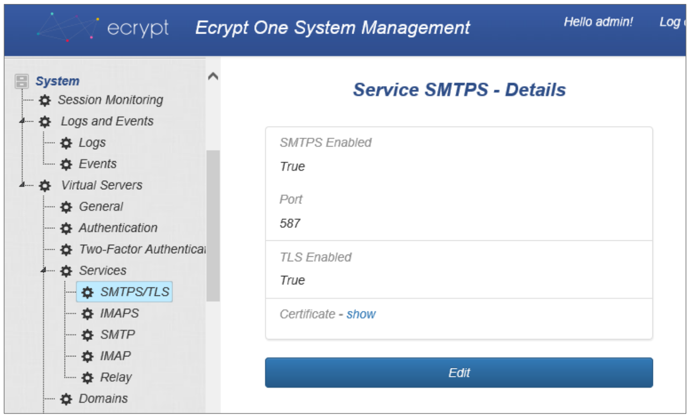
Export Certificate

Export to: C:\example.com.pfx

Password: ••••••••

Confirm password: ••••••••

Enter a file name and password to secure the file.



Ecrypt One System Management

Service SMTPS - Details

SMTPS Enabled: True

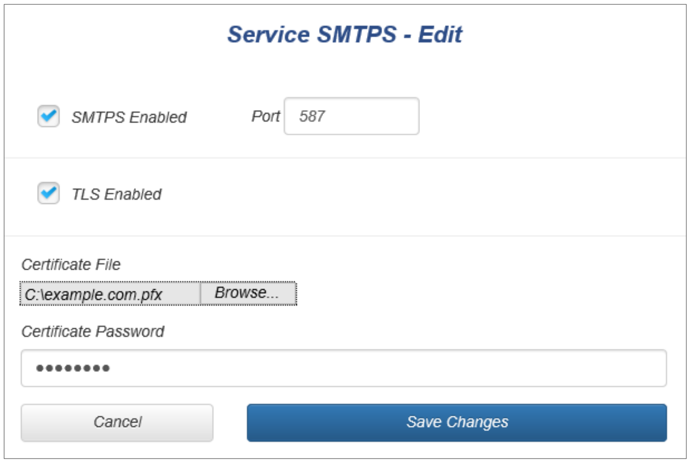
Port: 587

TLS Enabled: True

Certificate - show

Log into the Admin portal of the Ecrypt One server by navigating to https://localhost/admin then select SMTPS/TLS and click the Edit button.

Tip: now that the server has a trusted certificate, you can navigate to https://yourdomain/admin and avoid the warning about an untrusted server.



Service SMTPS - Edit

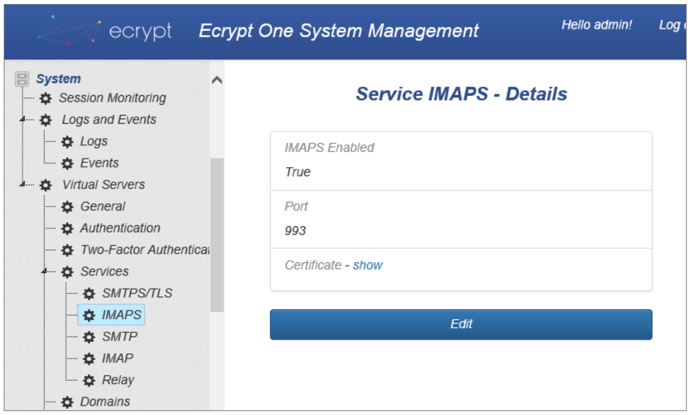
☑ SMTPS Enabled Port: 587

☑ TLS Enabled

Certificate File: C:\example.com.pfx

Certificate Password: ••••••••

Enter the path to the certificate file you saved and select Save. Ensure the SMTPS Enabled and TLS Enabled check boxes are checked, as shown here.



Service IMAPS - Details

IMAPS Enabled
True

Port
993

Certificate - show

Repeat the procedure for IMAPS.

You’re Done!

Your server is now fully configured. You can now create some user accounts and try sending some messages. Remember that Ecrypt One blacklists the Internet by default, so if you want to send or receive messages from outside your server, you need to enable the external users or domains that you want to trust. See the help on the External Address Book feature of Ecrypt One for details on this configuration procedure.

Verification

A great tool for verifying your email server installation is the Web site MX Toolbox, located at http://mxtoolbox.com Running the test, “Test Email Server” provides a good check of the server’s availability and configuration on the Internet.

Troubleshooting

Installing SSL/TLS Certificates

In some cases, when submitting a Certificate Service Request (CSR) request some certificate authorities only have the option to select the server as “IIS” or "IIS 5+". The actual version we run is IIS 8. When IIS 5+ is selected the certificate is issued as a “.CRT” file. If this is the case, here are directions to convert your .CRT to a .CER file.

1) Double-click on the yourwebsite.CRT file to open it in the Certificate display.
2) Select the Details tab, and then click the "Copy to File"
3) Press Next on the Certificate Export Wizard, then select Base-64 encoded X.509 (.CER) and click Next.
4) Select Browse, choose where to save the exported file, and assign a filename of "yourwebsite" (don't specify an extension of ".cer").
5) Click Next, then click Finished.

This completes the export process for yourwebsite.CER

Confirming Certification Installation in IIS

DigiCert makes a great tool that can verify the installation of your SSL/TLS certificate. This important since the export/import of the certificate into Ecrypt One depends on the correct installation of the certificate.

You find DigiCert’s helpful troubleshooting pages here:

https://www.digicert.com/ssl-certificate-installation-microsoft-iis-8.htm

DigiCert’s SSL Utility can be downloaded here:

https://www.digicert.com/util/

This tool makes the exporting of your certificate to .PFX file format very easy too, for subsequent import into Ecrypt One.