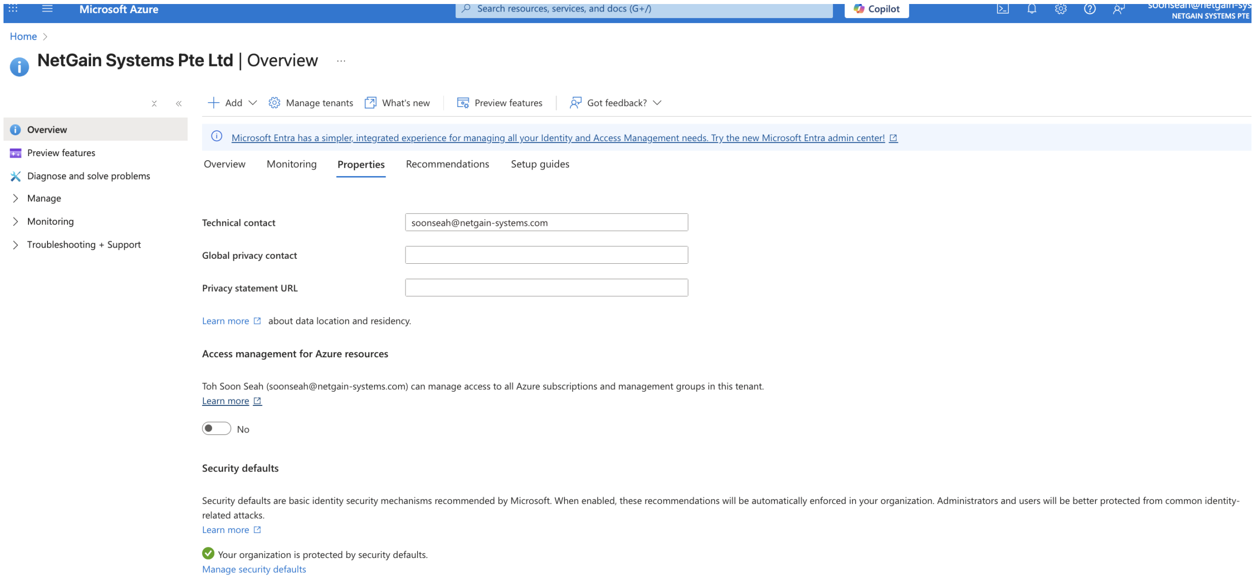
ISO 27001 — Technical Evidence Pack

This pack contains screenshot-based evidence for the requested controls.

Tech 04 — Admin Console Security (Azure)

- Security defaults enabled (MFA for admins; legacy/basic auth blocked).
- Microsoft 365 modern authentication ON; POP/IMAP/SMTP AUTH OFF.
- Per-user MFA "Enforced" for admin accounts.

Screenshots



NetGain Systems Pte Ltd | Overview

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Technical contact: soonseah@netgain-systems.com

Global privacy contact:

Privacy statement URL:

Learn more about data location and residency.

Access management for Azure resources

Toh Soon Seah (soonseah@netgain-systems.com) can manage access to all Azure subscriptions and management groups in this tenant.
Learn more

No

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.
Learn more

✓ Your organization is protected by security defaults.
Manage security defaults

Figure 1: Security defaults enabled

Tech 05 — Backup and Restoration

- Backup item shows Last backup status = Success; daily recovery points present.
- Jobs (Last 7 days) show 0 Failed; restore test record available.

Screenshots

Tech 06 — Logging and Monitoring (Cloud Vista)

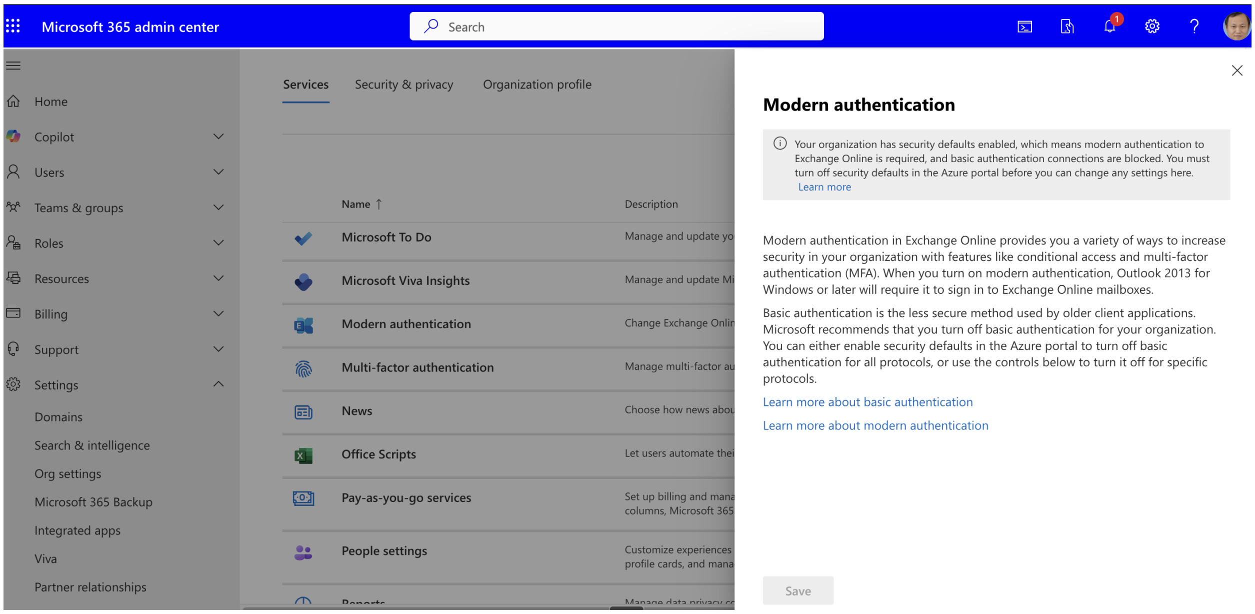
- Logs streaming and visible in SIEM (Cloud Vista Log Analytics).
- Diagnostic settings sending to Cloud Vista; alert rules configured.

Screenshots

Tech 10 — SDLC & Application Security

- TLS configured with modern protocols and ciphers; HSTS where supported.
- Server-side password hashing using strong algorithm.

Screenshots (embedded):



Name ↑	Description
Microsoft To Do	Manage and update yo
Microsoft Viva Insights	Manage and update Mi
Modern authentication	Change Exchange Onlin
Multi-factor authentication	Manage multi-factor au
News	Choose how news abou
Office Scripts	Let users automate thei
Pay-as-you-go services	Set up billing and mana columns, Microsoft 365
People settings	Customize experiences profile cards, and mana
Reports	Manage data privacy co

Modern authentication

Your organization has security defaults enabled, which means modern authentication to Exchange Online is required, and basic authentication connections are blocked. You must turn off security defaults in the Azure portal before you can change any settings here. Learn more

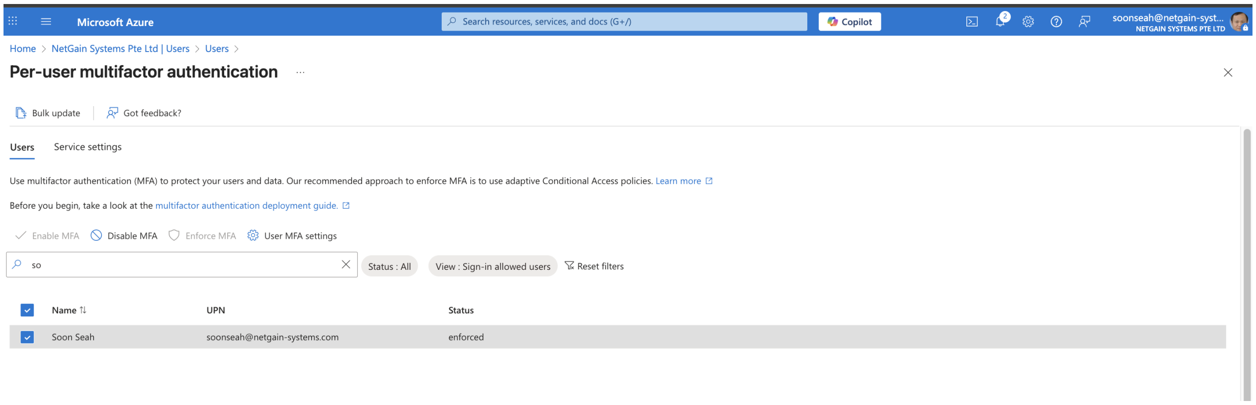
Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA). When you turn on modern authentication, Outlook 2013 for Windows or later will require it to sign in to Exchange Online mailboxes.

Basic authentication is the less secure method used by older client applications. Microsoft recommends that you turn off basic authentication for your organization. You can either enable security defaults in the Azure portal to turn off basic authentication for all protocols, or use the controls below to turn it off for specific protocols.

Learn more about basic authentication

Learn more about modern authentication

Figure 2: Modern authentication ON; legacy protocols OFF



Per-user multifactor authentication

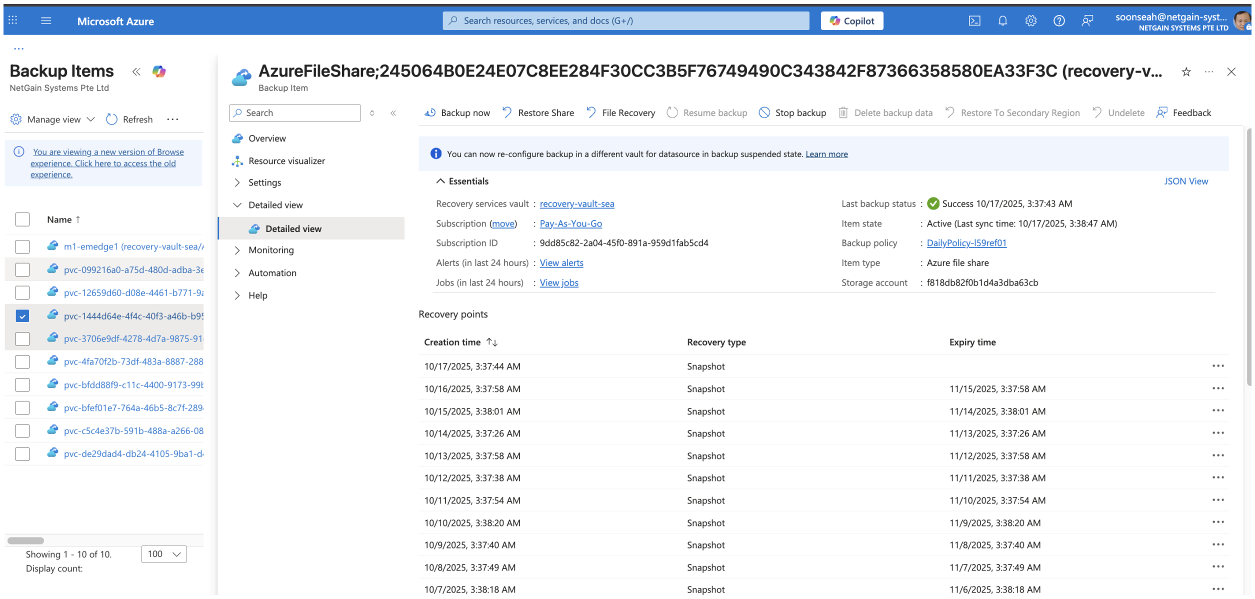
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

so

☑	Name ⇅	UPN	Status
☑	Soon Seah	soonseah@netgain-systems.com	enforced

Figure 3: Per-user MFA enforced



Backup Items

NetGain Systems Pte Ltd

You are viewing a new version of Browse experience. Click here to access the old experience.

	Name ↑
□	m1-emedge1 (recovery-vault-sea/
□	pvc-099216a0-a75d-480d-adba-3e
□	pvc-12659d60-d08e-4461-b771-9a
☑	pvc-1444d64e-4f4c-40f3-a46b-b95
□	pvc-3706e9df-4278-4d7a-9875-91
□	pvc-4fa70f2b-73df-483a-8887-288
□	pvc-bfdd88f9-c11c-4400-9173-99b
□	pvc-bfef01e7-764a-46b5-8c7f-289
□	pvc-c5c4e37b-591b-488a-a266-08
□	pvc-de29dad4-db24-4105-9ba1-d

Showing 1 - 10 of 10. Display count: 100

AzureFileShare;245064B0E24E07C8EE284F30CC3B5F76749490C343842F87366358580EA33F3C (recovery-v...

Backup Item

You can now re-configure backup in a different vault for datasource in backup suspended state. Learn more

Essentials

JSON View

Recovery services vault	: recovery-vault-sea	Last backup status	: ✓ Success 10/17/2025, 3:37:43 AM
Subscription (move)	: Pay-As-You-Go	Item state	: Active (Last sync time: 10/17/2025, 3:38:47 AM)
Subscription ID	: 9dd85c82-2a04-45f0-891a-959d1fab5cd4	Backup policy	: DailyPolicy-l59ref01
Alerts (in last 24 hours)	: View alerts	Item type	: Azure file share
Jobs (in last 24 hours)	: View jobs	Storage account	: f818db82f0b1d4a3dba63cb

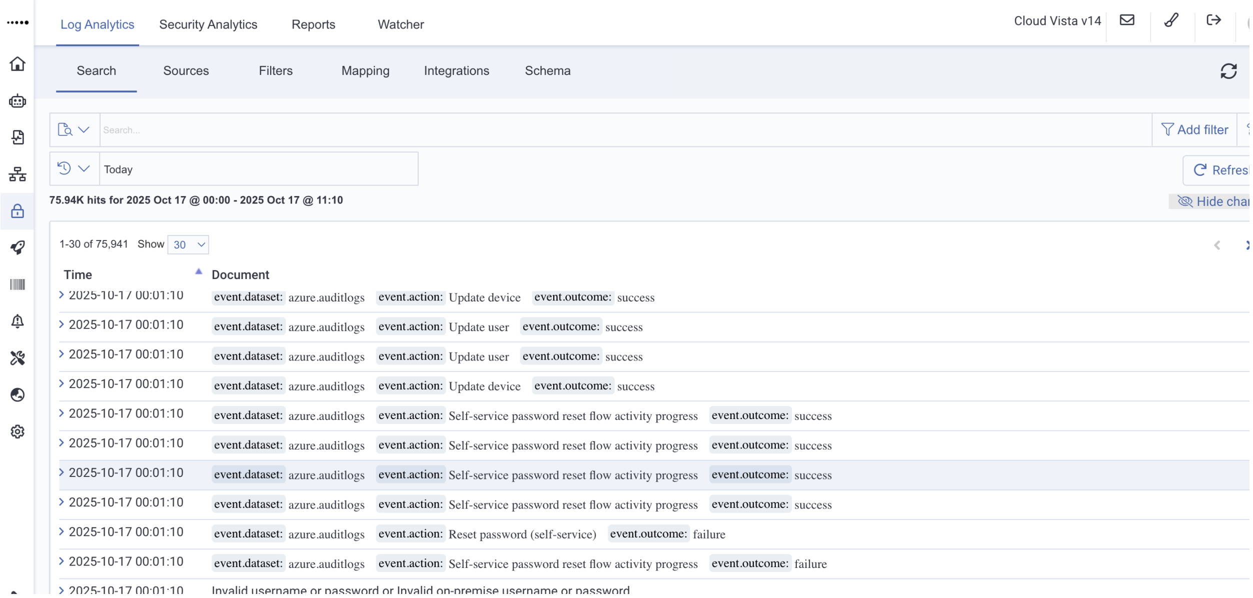
Recovery points

Creation time ↑↓	Recovery type	Expiry time	
10/17/2025, 3:37:44 AM	Snapshot		···
10/16/2025, 3:37:58 AM	Snapshot	11/15/2025, 3:37:58 AM	···
10/15/2025, 3:38:01 AM	Snapshot	11/14/2025, 3:38:01 AM	···
10/14/2025, 3:37:26 AM	Snapshot	11/13/2025, 3:37:26 AM	···
10/13/2025, 3:37:58 AM	Snapshot	11/12/2025, 3:37:58 AM	···
10/12/2025, 3:37:38 AM	Snapshot	11/11/2025, 3:37:38 AM	···
10/11/2025, 3:37:54 AM	Snapshot	11/10/2025, 3:37:54 AM	···
10/10/2025, 3:38:20 AM	Snapshot	11/9/2025, 3:38:20 AM	···
10/9/2025, 3:37:40 AM	Snapshot	11/8/2025, 3:37:40 AM	···
10/8/2025, 3:37:49 AM	Snapshot	11/7/2025, 3:37:49 AM	···
10/7/2025, 3:38:18 AM	Snapshot	11/6/2025, 3:38:18 AM	···

Figure 4: Backup item success + recovery points

Jobs last 7 days: 0 failed

Figure 5: Jobs last 7 days: 0 failed



75.94K hits for 2025 Oct 17 @ 00:00 - 2025 Oct 17 @ 11:10

1-30 of 75,941 Show 30

Time	Document
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Update device event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Update user event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Update user event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Update device event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Self-service password reset flow activity progress event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Self-service password reset flow activity progress event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Self-service password reset flow activity progress event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Self-service password reset flow activity progress event.outcome: success
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Reset password (self-service) event.outcome: failure
2025-10-17 00:01:10	event.dataset: azure.auditlogs event.action: Self-service password reset flow activity progress event.outcome: failure
2025-10-17 00:01:10	Invalid username or password or Invalid on-premise username or password

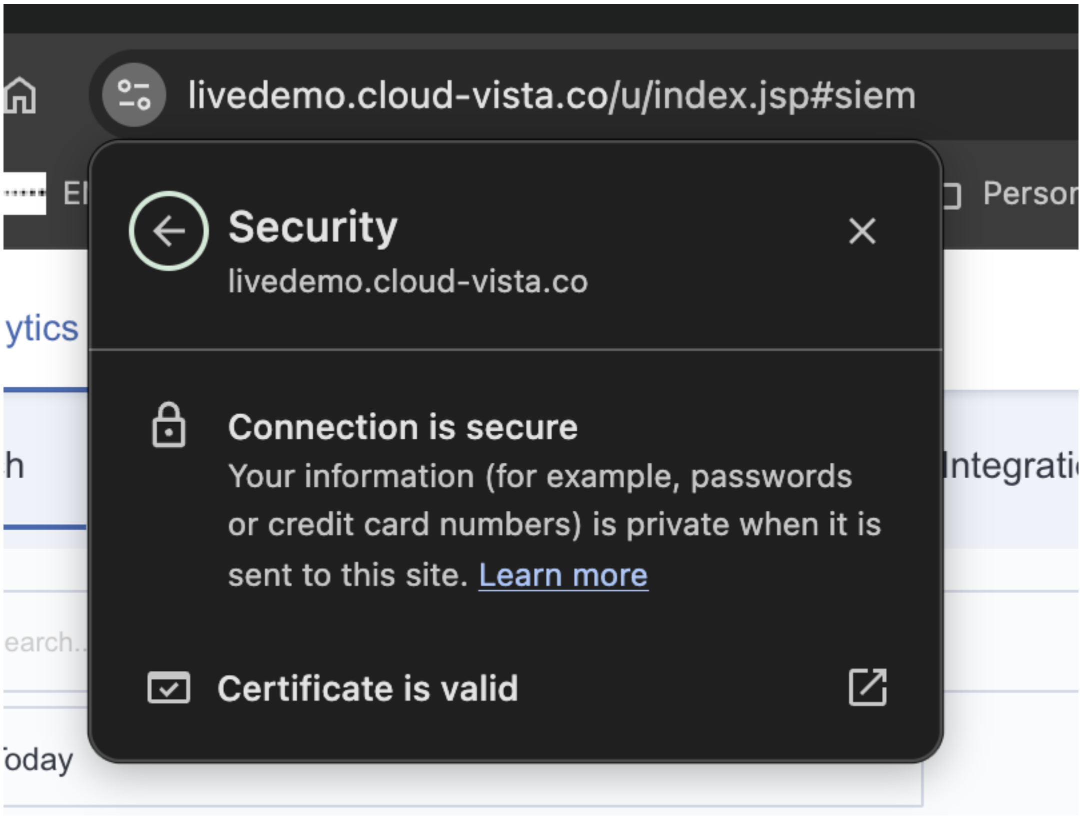
Figure 6: Cloud Vista log analytics events

Diagnostic settings enabled

Figure 7: Diagnostic settings enabled

Alert rules list

Figure 8: Alert rules list



livedemo.cloud-vista.co/u/index.jsp#siem

Security

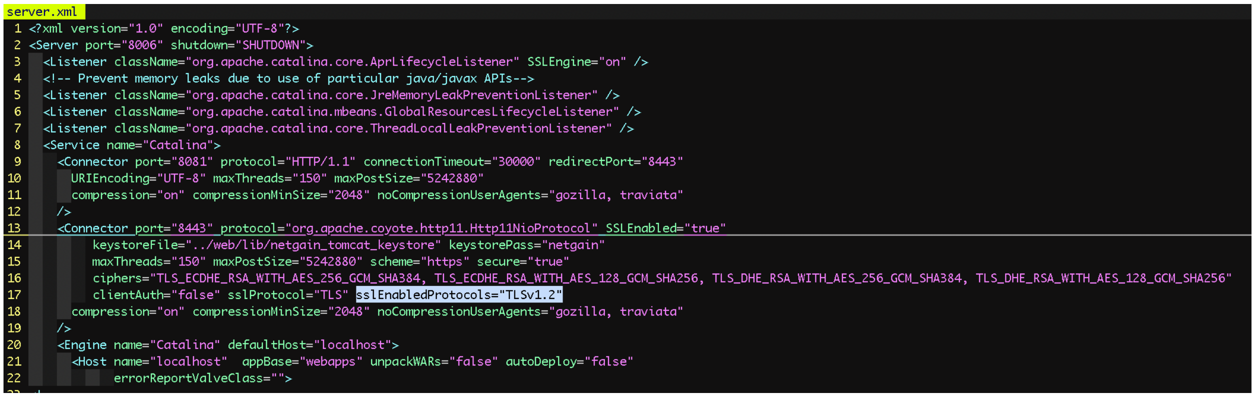
livedemo.cloud-vista.co

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

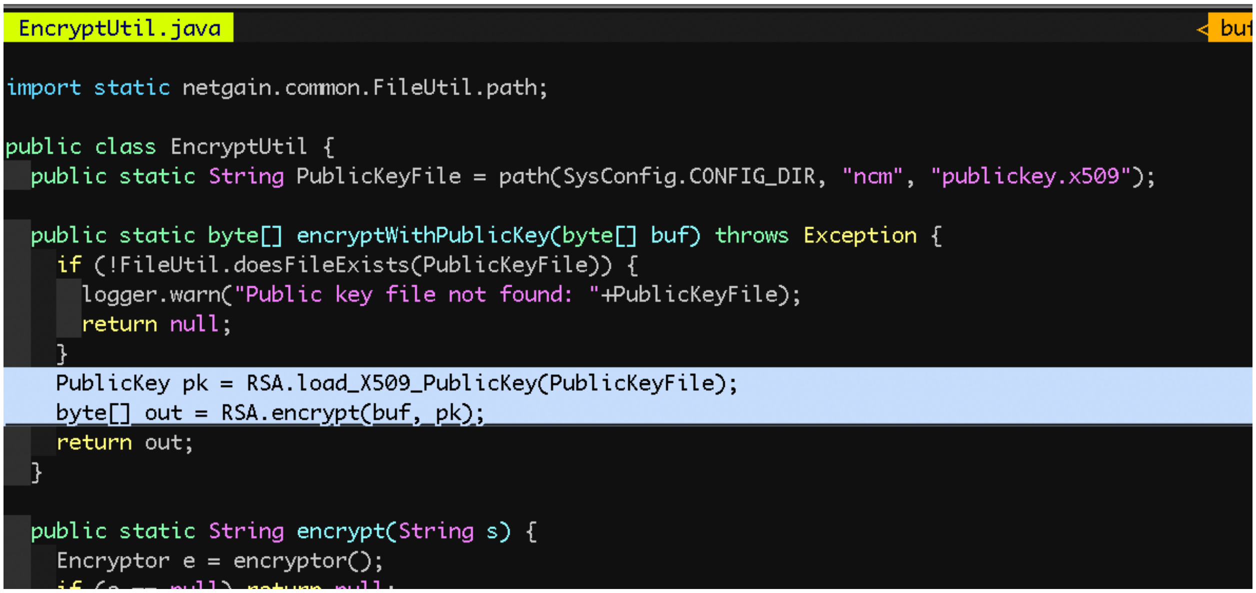
Figure 9: TLS configuration 1



server.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8006" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <!-- Prevent memory leaks due to use of particular java/javax APIs-->
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
  <Service name="Catalina">
    <Connector port="8081" protocol="HTTP/1.1" connectionTimeout="30000" redirectPort="8443"
      URIEncoding="UTF-8" maxThreads="150" maxPostSize="5242880"
      compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
    />
    <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
         keystoreFile="../web/lib/netgain_tomcat_keystore" keystorePass="netgain"
         maxThreads="150" maxPostSize="5242880" scheme="https" secure="true"
         ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256"
         clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"
      compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
    />
    <Engine name="Catalina" defaultHost="localhost">
      <Host name="localhost"  appBase="webapps" unpackWARs="false" autoDeploy="false"
            errorReportValveClass="">
```

Figure 10: TLS configuration 2



```java
import static netgain.common.FileUtil.path;

public class EncryptUtil {
  public static String PublicKeyFile = path(SysConfig.CONFIG_DIR, "ncm", "publickey.x509");

  public static byte[] encryptWithPublicKey(byte[] buf) throws Exception {
    if (!FileUtil.doesFileExists(PublicKeyFile)) {
      logger.warn("Public key file not found: "+PublicKeyFile);
      return null;
    }
    PublicKey pk = RSA.load_X509_PublicKey(PublicKeyFile);
    byte[] out = RSA.encrypt(buf, pk);
    return out;
  }

  public static String encrypt(String s) {
    Encryptor e = encryptor();
    if (e == null) return null;
```

Figure 11: Application crypto code