NetBrain® Next-Gen R11+

System Security Guide

Version V2.2 for R11+ | Last Updated 2024-03-21

Version Number	Description	Date
V2.2	Additions for R11+ (10.1.15)	2024-03-21
V2	Added Secure Cryptographic Settings Section (5.3)	2022-10-08
V1	Original Version	2021-03-03

Contents

Overview

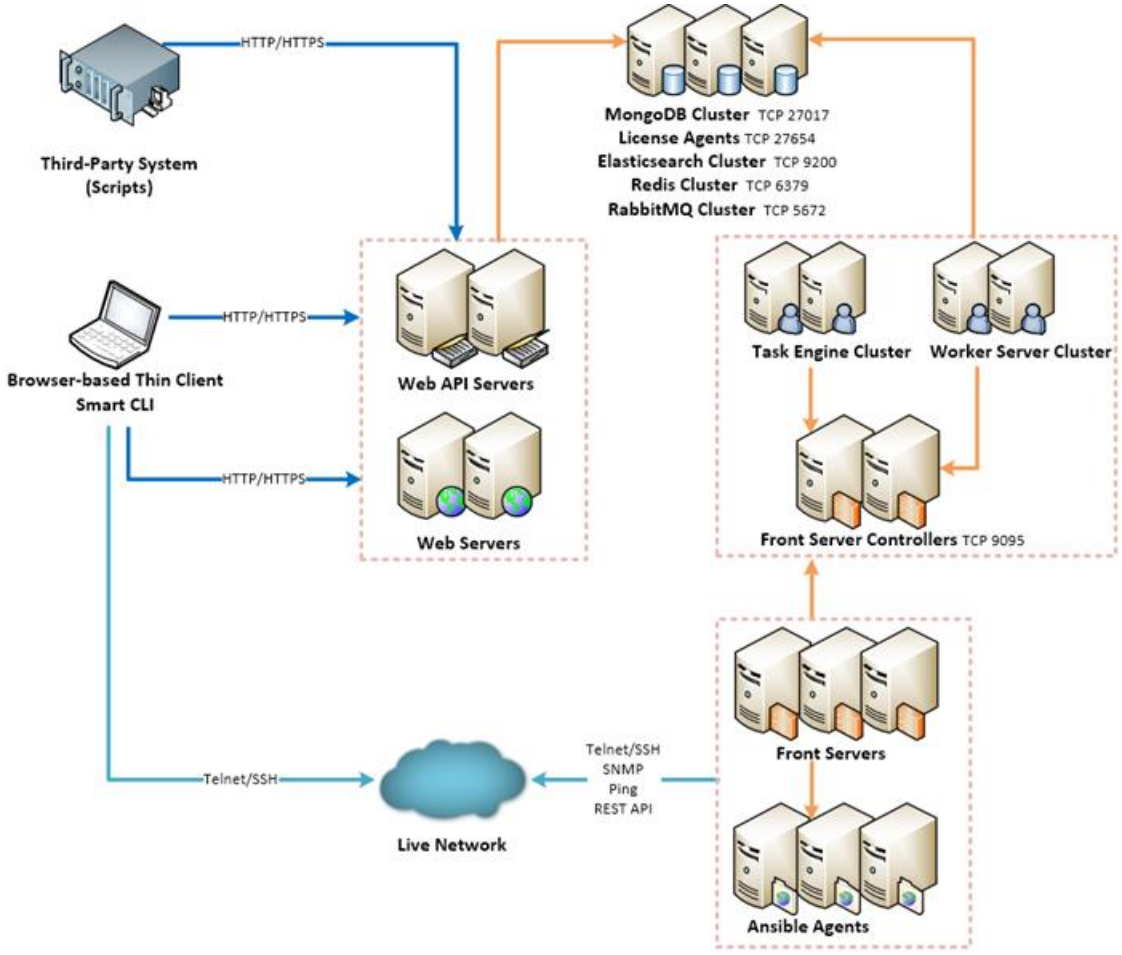
NetBrain is a browser-based interface backed by a full-stack architecture, adopting advanced distributed technologies to support large-scale networks with more expansion possibilities. Its security solution consumes industry-standard best practices, with a strong focus on outbound data isolation, communication channel encryption, and customer access management.

This document introduces the primary security features and best practices, including:

- Server Communication
- User Account Management
- Data
- APIs for Third-Party Authentication and Integration
- Best Practices

1. Server Communication

The connectivity and communications between external and system components are illustrated as follows:



Protocol and Port Number [1)]	Source	Destination
HTTP/HTTPS (80/443)	Thin Client	Web Server Web API Server
HTTP/HTTPS (80/443)	Service Monitor Agent	Web API Server
ICMP (TCP 7) SSH (TCP 22) Telnet (TCP 23) SNMP (TCP 161/162) REST API	Front Server	Live Network
TCP 4369/25672 (for HA only)	RabbitMQ	RabbitMQ

Protocol and Port Number [1)]	Source	Destination
TCP 5672	Web API Server Worker Server Task Engine Front Server Controller	RabbitMQ
TCP 6379 TCP 6380 (for HA only)	Web API Server Worker Server Front Server Controller Redis	Redis
TCP 9095	Worker Server Task Engine Front Server	Front Server Controller
TCP 9200	Web API Server Worker Server	Elasticsearch
TCP 9300 (for HA only)	Elasticsearch	Elasticsearch
TCP 27017	Web API Server Worker Server Task Engine Front Server Controller MongoDB	MongoDB
TCP 27017 (for HA only)	MongoDB	MongoDB
TCP 27654	Web API Server	License Agent
TCP 9098	Front Server	Ansible Agent
TCP 9099 (R10.1+)*	MongoDB Redis RabbitMQ Elasticsearch Web Server Worker Server Task Engine License Agent Front Server Front Server Controller	Web API Server
TCP15672*	Web API Server	RabbitMQ
TCP 5432 (listening on localhost only)	Front Server	PostgreSQL

Note: [1)] The port numbers listed are defaults only. The actual port numbers used during installation can be different.
*Ensure that ports 9099 and 15672 are open for system updates In default configuration, TLS 1.2 is utilized to secure TCP communication links. Using HTTPS to establish secure encrypted communication between the Browsers and Web Server is considered a best practice and the most secure choice.
TLS 1.3 offers several advantages over TLS 1.2. If NetBrain web server(s) is installed on Windows Server 2022 or newer, TLS 1.3 can be enabled for all incoming connections to the NetBrain web server(s). Refer to section 5.3.3.
Note: As a fallback, for configurations where TLS is not applicable, the system can also be configured to establish communications via HTTP. However, this approach lacks any inherent security.

2. User Account Management

NetBrain provides a set of policies to enable users to protect their accounts and data security. Areas addressed by these policies include Accounts, Authentication, and Authorization.

2.1. Accounts

NetBrain stores user credentials in MongoDB (Database Server). User account passwords are stored using cryptographically secure hashes. Several account control mechanisms are present in the system to allow system administrators to better secure user accounts. These mechanisms are described in detail below.

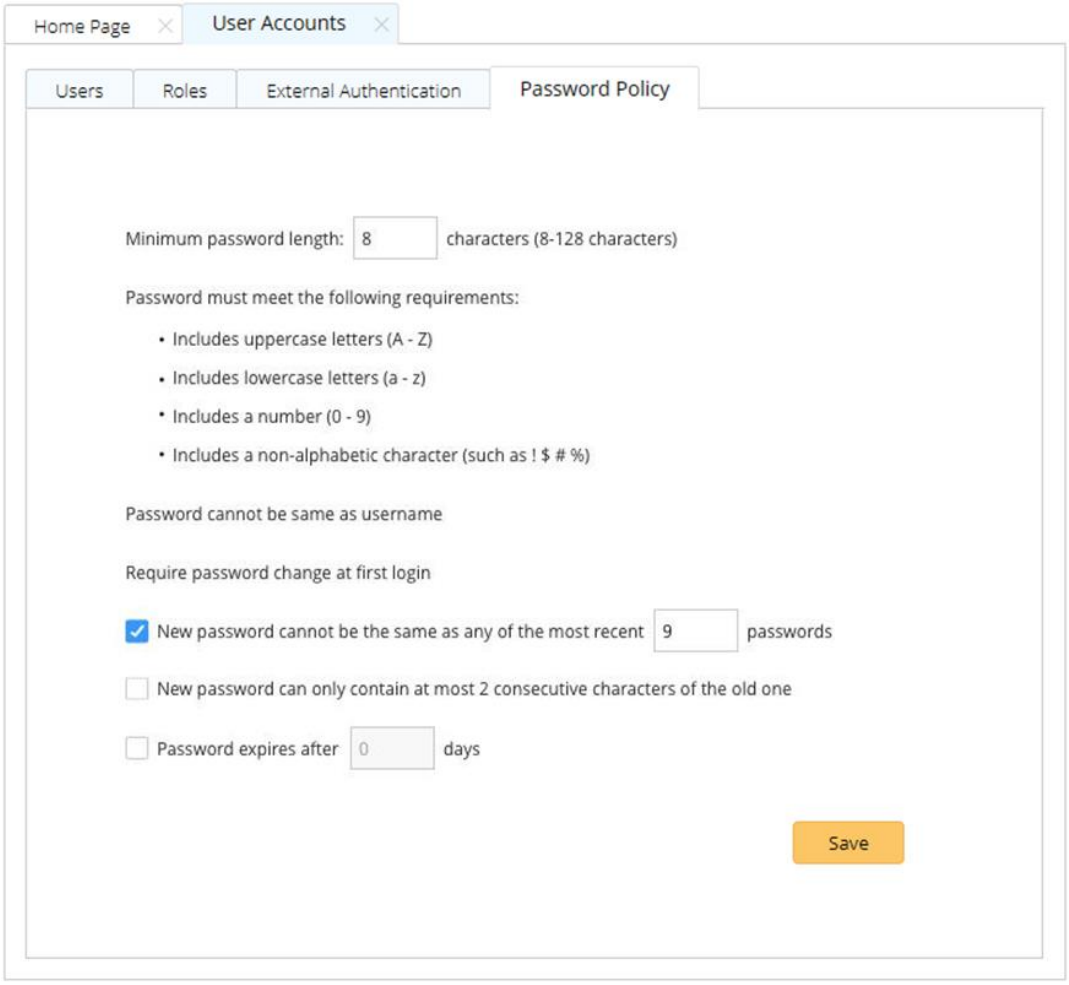
2.1.1.Password Complexity

The system allows the administrator to configure the policy governing the minimum complexity of user account passwords, including:

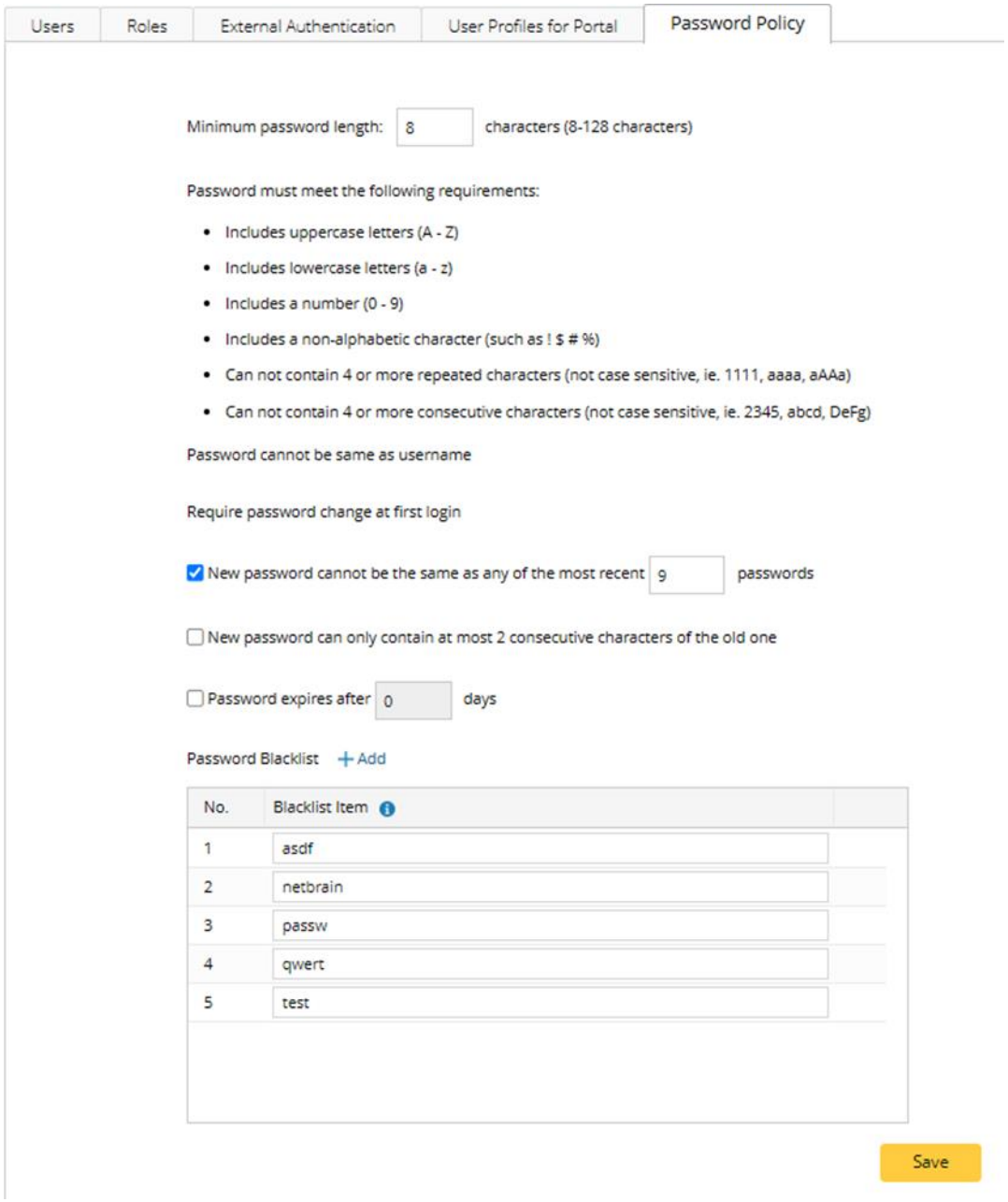
- Enforce “Require Password Change at First Login” for users whose accounts are created by admin.
- Enforce “Password cannot be the same as username”.
- Enforce Password History - “New password cannot be the same as any of the most recent N passwords”.
- Minimum password length (8 - 128 characters).
- Password Expires in days (1-9998)
- New password can only contain at most 2 consecutive characters of the old one.
  For example, if the previous password was ‘MyD0g$Gr8’, then the one ‘MyC4tRul3$’ will be invalid.
- Enforce “Password must meet the following requirements”:
  - Includes upper letters (A - Z)
  - Includes lowercase letters (a - z)
  - Includes a number (0 - 9)
  - Includes a non-alphabetic character (! @ # $ % ^ & *)
  - Does not include the strings passw, test,asdf, qwert, or netbrain (case insensitive)
  - Add password blacklist.

- Add 4 repeated and consecutive chars.

- To configure these settings, go to **System Management > User Accounts > Password Policy**.



- For Version 10.1+ To configure these settings, go to **System Management > User Accounts > Password Policy**.



2.1.2.Session

Once a user completes a successful login, a unique session for that user will be created, and a token for that session will be issued to the user account.

The default session expiry is 4 hours and configurable globally (go to **System Management > Advanced Settings**).

In IEv10.0+, if an admin session already exists, a warning notification will pop-up so the user can choose to terminate the existing session.

2.1.3.Account Lockout Policy

By default, the system automatically locks user accounts after 5 unsuccessful login attempts to protect user-information confidentiality. Locked user accounts will be available in 1 hour.

This policy also applies to the Password Reset function. When users are attempting to reset their passwords via GUI or API calls, entering incorrect passwords for too many times will lock their user accounts.

2.1.4.Audit Log

NetBrain recommends configuring to record user operations in the product audit log as a best practice.

The retention period of the log is configurable (go to **System Management > Advanced Settings**).

IEv10.1+ and R11+ add more audit logs to track users' actions more conveniently. Note that below is not a complete list of modules that have auditing available.

Module	Type	Actions
API Internet Proxy Manager	End User Operation	Apply proxy server to front server Create/Update/Delete proxy server
Webhook Management	End User Operation	Add/Edit/Remove a webhook Enable/Disable a webhook
API Server Manager	Northbound API	Add/Update/Delete an API Vendor account in API Server Manager
API Plugin Manager	Northbound API	Add/Update/Delete function template for the API Parser and API Server
API Stub Manager	Northbound API	Add/Update/Delete API Stubs
API Vendor Manager	Northbound API	Add/Update/Delete API Vendors
Cloud	End User Operation	Add/Update cloud devices
Device Access Policy	Management	Add/Update/Delete device access policies
Device Driver	End User Operation	Add/Update/Delete/Disable device drivers
Device Management	Management	Add/Remove devices from domain; Update device settings and login
Discover	End User Operation	Records when and which discover task(s) start
Domain Management	Management	Domain Management operations
Email Suffix Allow List	Management	Add/Update/Delete email suffix entries
Event Console	Northbound API	Acknowledge/Close/Delete event alerts
Execute CLI Commands	End User Operation	Records when CLI commands are executed on network devices from anywhere in the application
External Authentication	Management	Add/Update/Delete External Authentication
Front Server Controller Manager	Management	Add/Update/Delete Front Server Controllers
Global Data Clean	End User Operation	Edit global data clean settings; Trigger manual delete
Hostname Change	Management	Change in hostname of servers hosting NetBrain components
Incoming Email Server Settings	Management	Add/Update/Delete incoming email server settings
License	Management	Bind/Unbind License
Login	Management	Login attempts
Logout	Management	Logout records
Network Change	End User Operation	Add/Update/Delete/Approve network change requests
Outgoing Email Server Settings	Management	Add/Update/Delete outgoing email server settings

Password Policy	Management	Add/Update/Delete password policy
Role	Management	Add/Update/Delete user roles
Security	Management	Rotate Keystore
Share Policy	End User Operation	Update in Domain Share Policy
System Advanced Settings	Management	Update Advanced Settings
System Update	Management	System Update scheduled/running/failed/completed
System Maintenance	Management	Application Maintenance window activated or scheduled
Task Manager	End User Operation/Management	End running tasks/processes
Tenant Management	Management	Tenant Management operations
Tenant User Authorization	Management	Enable or disable the privilege of creating domains.
User Management	Management	Add/Update/Delete user accounts

2.1.5.Access Controls

The access privileges of user accounts can be managed via one or more of the following controls:

- Start services with restricted privileges – the system enforces to launch NetBrain related services with restricted privileges to reduce the risk of elevated privileges when interacting with both Windows and Linux. Startup accounts with restricted privileges will be either created or configured during the system installation, rather than using privileged accounts of operating systems.
- Management of user account authentication (if enabled).
- Domain-based user access – users can be limited to visiting specific domains and tenants.
- Role-based privileged operations – users with different roles can have different privileges to perform operations or use features in a domain.
- Starting from R11.1b, enabling debug mode for maintaining Built-in Resources requires a System Management user account on NetBrain application, and personnel from NetBrain support.

2.1.6. Built-in Admin Account

Privileged accounts may pose potential security risks if not managed. They usually have broad access to underlying customer information that resides in applications and databases. And passwords for these accounts are often embedded and stored in unencrypted text files, a vulnerability that is replicated across multiple servers to provide greater fault tolerance for applications.

To eliminate this risk, this default administrator account can be deleted.

Note: Before the deletion of the admin account, make sure there is at least one active user account with user management privilege in the system.

2.2. Authentication

The authentication aspect deals with validating user credentials and establishing the identity of the user. Users must log in to the system with their username and password. User accounts can be created by the system administrators or user managers on the System Management page.

Alternatively, the following third-party authentication methods can be used:

- LDAP/AD Authentication

  NetBrain supports integration with an LDAP/AD server to provide centralized control and management of user authentication. The Administrator can import user groups from your LDAP/AD servers and then define the corresponding roles for each group. Once configured, users can use their LDAP/AD accounts to log into the system. This solution simplifies user management for enterprise customers.

- **TACACS Authentication**

  NetBrain supports integration with a TACACS+ server as an authentication center to manage domain logins. After configuring TACACS+ settings, adding users to the TACACS+ server and finishing the corresponding configurations in the System Management page, users can use their accounts on the TACACS+ server to log into the system.

  - **SSO (Single Sign-On) Authentication**

    NetBrain supports Security Assertion Markup Language (SAML) 2.0 based SSO and integrates with federation servers or individual identity providers to share session information across different security

domains. SAML SSO works by transferring the user's identity through an exchange of digitally signed XML documents. Note that starting from R11.1.a, allowing SSO login only can be configured, and traditional end user login can be disabled.

There are two mechanisms of implementation:

- **Service Provider Initiated** — Users log into the NetBrain system by logging into other identity providers first.
- **Identity Provider Initiated** — Users who are already logged-in to other identity providers can directly view embedded NetBrain applications, such as map, path and data view.

2.3. Authorization

NetBrain uses roles and privileges to define which operations each user can perform at the domain level. Each user account can be associated with one or more roles and privileges.

- Privileges reflect individual permissions to system operations or visibility.
- Roles are based on the types of tasks that a user is expected to perform while interacting with the system and is a collection of privileges.
  - System Admin
  - User Management
  - Domain-Level Roles

2.3.1.Privileges of System Administrator

The privileges of a system administrator are separated into two types: System Management and User Management. The corresponding privileges between the two types are described in the following table:

Management Category	Featured Management Module	System Management	User Management
System Management Page	System Home Page, including Usage Report		√
	License	√	
	Tenants	√	
	User Accounts		√
	Front Server Controllers	√	
	Email Settings		√
	Advanced Settings - Global Session Timeout		√
	Advanced Settings - Others	√	
	Resource Update	√	
	Task Manager	√	
	API Adapters	√	
	Script Manager	√	
	Deployment Status	√	√
	System Update	√	
	Service Monitor	√	√
	Proxy Manager	√	
	Integrated IT Systems	√	√
Tenant Management Page	User Authorization		√
	Domain List	√	
	Multi-vendor Support	√	
	Misc Configuration	√	
	GDR Data Configuration	√	
	API Manager	√	
	Interface Type	√	
	Platform Management	√	
	Topology Link Style	√	
	Advanced Settings	√	
	Cloud Type Definition	√	

2.3.2. Privileges of Domain-Level Roles

By default, the privileges of domain-level roles are listed as follows:

Privileges	Explanation	Domain Admin	Power User	Engineer	Guest	Network Change Creator	Network Change Executor	Network Change Approver	Portal Temp User
Domain Management	Log in to the Domain Management page and do the following domain management tasks: • View, export, and delete discovery report in the Fine Tune • Add network definition • View, add, modify, delete, and disable topology links in the Topology Link Manager • Resolve duplicated IPs and subnets in the Duplicated IP and Subnet Manager • Add checkpoint OPSEC tasks in the Checkpoint OPSEC Manager • Configure network security settings and L2/L3 topology building options • Configure a desktop profile for all users under a domain	√	√			√	√	√	
Share Policy Management	Configure share policy (assign domain access and privileges to other users in this domain)	√							
Device Management	• Add, modify, and remove MPLS cloud • Remove devices from a domain	√	√			√	√	√	
Shared Resource and File Management	Only system/tenant administrator can edit built-in files in the shared folder of Device Group, Qapp, Gapp, Parser, Dashboard Widget Template, and Runbook Template	√	√	√		√	√	√	
Site Management	• Add MPLS clouds and unclassified network devices from the Fine Tune to a site • Open the Site Manager to do site management, such as creating, editing, deleting, importing, committing, and rebuilding sites	√	√			√	√	√	

Discover/Tune Network Device	• Create a do-not-scan list • Add discovery tasks from the Start Page or the Schedule Task page • Rediscover selected IPs and devices in the Fine Tune • Tune live access • Run on-demand discoveries	√	√			√	√	√	
Schedule Benchmark	Add benchmark tasks from the Start Page or the Schedule Task page	√	√			√	√	√	
Manage Network Settings	Configure and manage shared network settings	√	√			√	√	√	
Manage Device Settings	Configure and manage shared device settings for each device in a domain from the following entries: • Site pane • Map • Fine Tune • Discover • Tune Live Access	√	√	√		√	√	√	
Access to Live Network	Download the shared network settings or device settings data from the server and use these data to retrieve live device data from the network, which includes: • Run CLI commands and Qapps on a map page or in a runbook • Run monitor (Qapp-based) widgets and retrieve live data in static widgets in a dashboard • Retrieve variables once or monitor variables periodically from the live network in Instant Qapp • Calculate live paths (use the live network as the data source) • Configure SNMP, CLI timeout, SNMP hostname trim rules, management interface selection order, and live access method polling order (SNMP/Telnet/SSH/Jumpbox) • Browse live access logs in Fine Tune	√	√	√	√	√	√	√	√

Create Network Change	Create network change tasks	√	√			√			
Execute Network Change	Execute network change tasks	√	√				√		
Approve Network Change	Approve network change tasks	√	√					√	
View Network Change	View network change tasks	√	√			√	√	√	√
Delete Network Change	Delete network change tasks	√	√			√	√	√	~~√~~
Map Layout Management	Associate layout styles with site maps and shared device group maps	√	√			√	√	√	
Variable Mapping Management	View and manage variable mappings	√	√			√	√	√	
Run Qapp	Run and schedule Qapp tasks	√	√	√		√	√	√	√
Golden Baseline Manual Definition	Define golden baseline manually	√	√	√		√	√	√	
Golden Baseline Dynamic Calculation Management	Enable or disable dynamic calculation to set golden baseline	√	√						
Manage SPOG URL	View and define SPOG URL	√	√						
Portal Management	Manage function portals	√	√						
Private Resource Management	Manage private resources including: • Qapp • Gapp • Parser • Data View Template • NIC	√	√	√		√	√	√	
Primary Probe Management	Create, read, update, and delete Primary Probes	√	√						
Secondary and External Probe Management	Create, read, update, and delete Secondary and External Probes	√	√	√		√	√	√	

Adaptive Monitoring Polling Control	Manage Adaptive Monitoring Polling including: • Adjust polling frequency • Configure blocking time • Configure polling delay	√	√						
Install Automation Management	• Install Automation • Edit Decision Tree	√	√	√					
Triggered Diagnosis Management	• Create, read, update and delete incident types • Create, read, update and delete triggered automation • View diagnosis log	√	√	√					
Schedule CLI Command	**Add Schedule CLI Commands**	**√**	**√**	**√**		**√**	**√**	**√**	
Run Ansible Task	Execute Ansible Task node in Network Change (CM) and Runbook	√	√	√			√		
Guidebook Management	Create, read, update, and delete guidebooks	√	√	√					
Data Accuracy Management	Configure/manage data accuracy checks	√	√	√		√	√	√	
Run Network Intent	Execute Intents	√	√	√		√	√	√	√
Open Driver Management	Create, read, update, and delete open drivers	√	√						
Automation Bot Management	Create, read, update, and delete chat bots	√	√	√					

2.3.3. Prevention of Vertical Privilege Escalation

Vertical Privilege Escalation, also known as privilege elevation, is where a lower privilege user accesses functions or content that is reserved for higher privilege users.

The system is protected from Vertical Privilege Escalation in API calls by implementing the following measures:

- Username and user ID parameters have been removed to avoid malicious data updates.
- Enhanced inspection of the request parameter of a user ID for anonymous access.

3. Data

NetBrain provides a series of measures to protect data security.

- Data Encryption
- Data Backup
- User Data Input
- Third-Party Dependencies
- Assign Front Server to Domain
- Python Framework Security
- Rate Limiting

3.1. Data Encryption – for Data at Rest

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Securely storing and retrieving these keys as needed is a major security enhancement.

To address a significant FIPS requirement and to enhance the solution's security, IEv8.0 (and extended in 10.0, 10.1 and R11+) builds a keystore in the database, as a repository to store cryptographic keys, and also adopts enhanced hashing and encryption algorithms.

Algorithm	Adopted in IEv8.0 Extended to 10.0, 10.1, and R11+
Non-Cryptographic Hashing	SHA256 Spooky 128*
Password Hashing	PBKDF2
Encryption/Decryption	AES-256-CBC

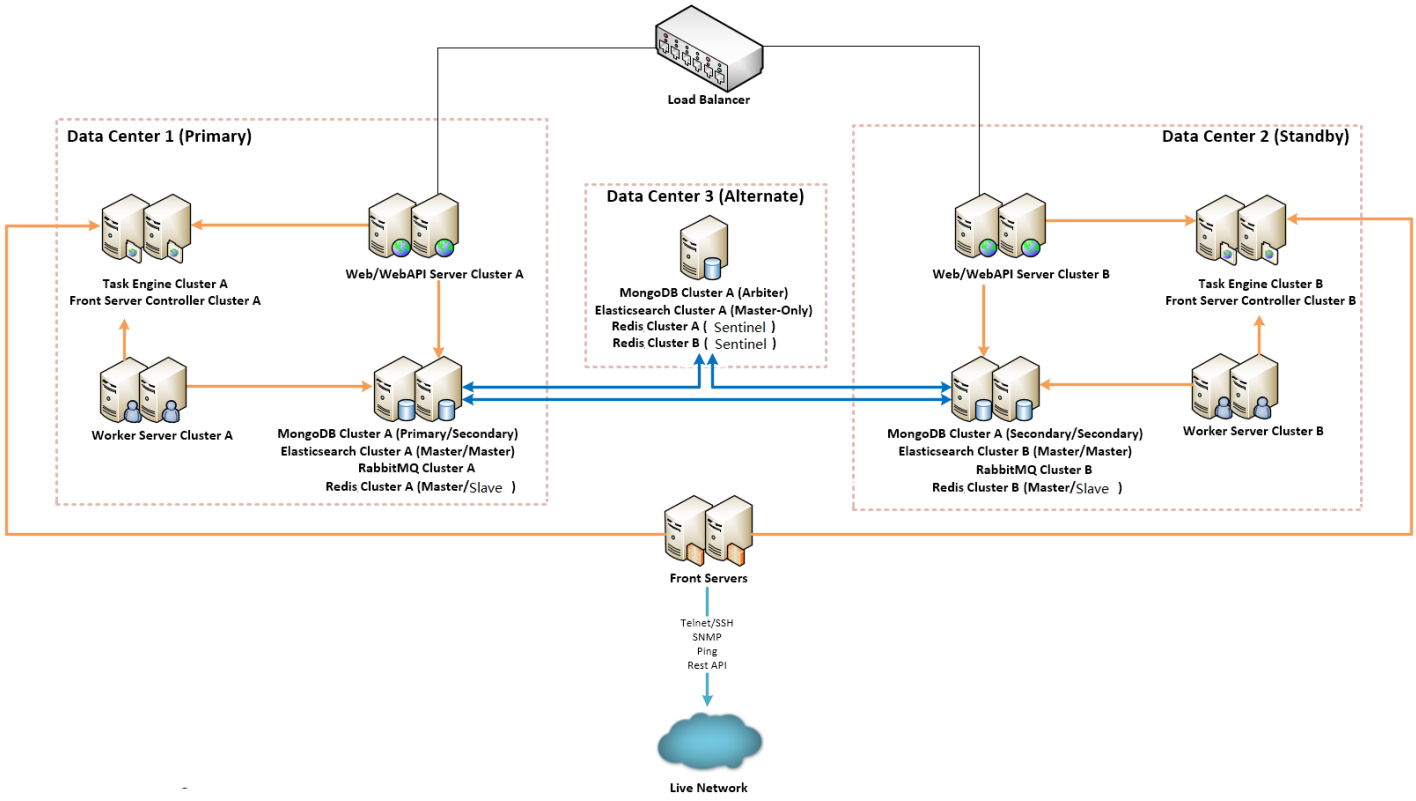
Note: This upgrade of hashing and encryption algorithms has backward compatibility with user data in IEv7.x, except for Network Settings. A convert tool can be used to adapt existing Network Settings to IEv10.0+.

*Spooky 128 is used on non-sensitive data only and for internal processing efficiency. There is no security impact.

3.2. Data Backup

The system data is stored in MongoDB, and there are two methods to deploy MongoDB.

- A standalone MongoDB instance. For the detailed data backup procedures, see Backing Up MongoDB Data for more details.
- A MongoDB replica set to provide data availability and prevent single-point-of-failure (SPOF) or system failover, which can be even across data centers. Here is a sample figure for multi-DC deployment, with one active system and one standby system.



For multiple separate large networks managed by MSP (managed service providers), the system supports multi-tenant data storage in separate MongoDB instances, to enhance both security and performance.

3.3. User Data Input

The system performs the following checks and validations to prevent malicious attacks.

- Validation of Uploaded Files
- Prevention of Cross-Site Scripting (XSS) Injection
- Prevention of Formula Injection

3.3.1. Validation of Uploaded Files

The system validates uploaded files across four key factors, including the file extension, mime-type, size, and upload frequency. The following validations are included:

- Enforce an upper limit on file size on a case-by-case basis.
- Enforce a default whitelist or blacklist of file extensions on a case-by-case basis. For example, define forbidden file extensions for generic cases, including **exe** and **bat**; define allowed file extensions for PDF, text and Word document, including **pdf**, **txt**, and **doc**.
- Validate the frequency of file uploads in API calls, by defining the minimum interval, the maximum concurrency count, and more parameters. When the system detects a high frequency of file uploads from a single user, he or she will be prohibited from uploading. The interval for his or her next allowed attempt can be configured.
- Validate a few bytes in the header of a file, which is known as the “Magic Number” of the file format and will uniquely identify the file type. For example, all PDF files start with the byte-sequence “%PDF”.

3.3.2. Prevention of Cross-Site Scripting (XSS) Injection

The system prevents Cross-site scripting (XSS) by validating and sanitizing user input. Each character of the data is encoded using the HTML Text Element scheme, and the result string is then inserted into the generated web page. For example, the characters `<`, `>`, `"`, `'` are encoded as `&#60;`, `&#62;`, `&#34;`, `&#39;` before being inserted into an HTML Text Element.

3.3.3. Prevention of Formula Injection

A Formula Injection vulnerability refers to the exported spreadsheet files that are dynamically constructed from inadequately validated input data. Once injected, it affects application end-users that access the exported spreadsheet files. For example, if the spreadsheet contains untrusted user-supplied data, the cell-level syntax consisting of an equal sign followed by a function name or an expression could be interpreted as formulas by a recipient's spreadsheet program, such as Microsoft Excel, and execute on the recipient's system.

The system validates user input to prevent formula injection before any input is inserted into spreadsheet data fields:

- Escape all untrusted input by placing a single quote (`'`) before the content. For example, `=HYPERLINK(…)` will be processed as `'=HYPERLINK(…)`.
- Add a pair of double quotation marks (`" "`) to include an input containing a comma (`,`). For example, `a,b,c` will be processed as `"a,b,c"`.
- Avoid the use of scientific notation in CSV output. For example, `123456052535` will be processed as `="123456052535"`.

3.4. Third-Party Dependencies

To ensure the longevity of support and the most up-to-date code from a security standpoint, many components have been upgraded to the version in NetBrain R11.1b.

Component	Version in IEv10.0	Version in NB 10.1	Version in NB R11.1b installers (10.1.15)
MongoDB	4.0.19	4.0.28	6.0.2*
Elasticsearch	6.8.12	6.8.23	6.8.23
Redis	6.0.9	6.2.6	7.2.2*
RabbitMQ	3.8.9	3.8.19/3.8.30**	RedHat 8: 3.12.4* RedHat 7: 3.8.30
PostgreSQL	12.4	12.9	12.17
Java	OpenJDK 11.0.9	OpenJDK 11.0.14.1+1	OpenJDK 11.0.21+9*

* Version only available in R11.1b full NetBrain package installers. These versions will not be available when upgraded to R11.1b using auto update. Note that patches are available to upgrade Mongo, Redis and JDK in the field.

** RabbitMQ v3.8.30 was made available in minor version upgrade 10.1.7+ via Auto Update patching.

In most cases, third-party dependencies of the system have been upgraded at the time of development completion, to ensure the most up-to-date code from a security standpoint.

3.5. Assign Front Server to Domain

Starting from R11.1b, tenant managers, via the Tenant Management page, can assign front servers to a specific domain to facilitate applying more granular access policies. By default, the front server itself is configured at the tenant level, all domains under the same tenant can use these front servers.

3.6. Python Framework Security

NetBrain provides a python framework for users to write custom automations fit to achieve their goal. Starting from NetBrain R11.1, the framework is enhanced to not allow imports of unsafe python modules. Additionally,

users can configure settings to add more unsafe python modules as they see fit. This setting can be enabled from **System Management** > **Advanced Settings**.

3.7. Rate Limiting

NetBrain has applied rate limiting to appropriate functions to prevent denial of service (DoS) attacks. By limiting the number of requests, throttling helps to prevent DoS attacks. This measure is already enabled, and no further user action is needed.

4. APIs for Third-Party Authentication and Integration

NetBrain provides dozens of RESTful APIs for users to read (Get) and write (Post/Put/Delete) system data. To protect the data, NetBrain APIs use strict authentications.

Before using the APIs, users need to log in to the system with their usernames and passwords to obtain a token and then use the token for subsequent API calls. When there is no user activity until the session timeout, the token will expire.

The APIs may vary depending on different versions, including:

- IEv8.0
- IEv8.01
- IEv8.02
- IEv8.03
- IEv10.0
- IEv10.0a
- IEv10.1/R11
- R11.1
- R11.1a
- R11.1b

5. Best Practices

The following best practices are recommended to enhance system security:

- Configuring Live Network Settings
- Removing Sensitive Data from Device Configuration File

5.1. Configuring Live Network Settings

Many NetBrain features require access to live networks, such as discovery, benchmarking, path calculation and monitoring. To enable these features, go to **Domain Management > Discovery Settings > Network Settings** to complete the live-related settings, including:

- Non-privilege and privilege passwords, used to access devices via Telnet/SSH and retrieve live data by issuing CLI commands.
- SNMP RO strings, used to access devices via SNMP.
- SSH Private Key, used to log into network devices.
- Front Server settings, used to access and collect data from the live network.
- Server Jumpbox (secure administrative host), used as a hop-through system that the Front Server can access by using Telnet/SSH before accessing live devices.

5.2. Removing Sensitive Data from Device Configuration File

To remove the following sensitive data from both device configurations and user interface, go to **Domain Management > Operations > Domain Settings > Advanced Settings** and select the checkbox under the **Network Security** area.

- Line and console passwords
- Local user passwords
- Enable passwords
- Enable Secret
- SNMP community string

- TACACS and Radius keys
- VPN Keys and Certs
- SSH Private keys (these may show up on CSS devices)

5.3 Recommended Cryptographic Settings

This section will serve as a guide to configure the recommended cryptographic settings on the machines running NBIE. The recommended cryptographic settings will ensure industry standard secure communications with NBIE and among the various components that make up the product. NetBrain always recommends the latest and greatest security configurations to stay on top of vulnerabilities. We cannot include these default settings in the initial installation steps for backwards compatibility reasons. To address this, we recommend checking the installed instance of NBIE, to verify industry standard best practices are advertised.

5.3.1. Managing Cryptographic Settings on Windows by Registry Keys

Windows manages its implementation of secure settings in the Transport Layer Security (TLS) protocol and the Secure Sockets Layer (SSL) protocol through the Schannel Security Support Provider (SSP). The registry subkeys located at HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL will help you administer and troubleshoot the Schannel SSP, specifically for the TLS and SSL protocols.

A detailed document for managing cryptographic settings using registry keys can be found here (from Microsoft)

A supported (D)TLS or SSL protocol version can exist in one of the following states:

- **Enabled**: unless the SSPI caller explicitly disables this protocol version using the SCH_CREDENTIALS structure, Schannel SSP may negotiate this protocol version with a supporting peer.
- **Disabled by default**: unless the SSPI caller explicitly requests this protocol version using the deprecated SCHANNEL_CRED structure, Schannel SSP will not negotiate this protocol version.
- **Disabled**: Schannel SSP will not negotiate this protocol version regardless of the settings the SSPI caller may specify.

The system administrator can override the default (D)TLS and SSL protocol version settings by creating DWORD registry values "Enabled" and "DisabledByDefault". These registry values are configured separately for the protocol client and server roles under the registry subkeys named using the following syntax:
<SSL/TLS/DTLS> <major version number>.<minor version number><Client\Server>

These version-specific subkeys can be created under the following registry path:

HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

An example of some valid registry paths has been given here:

- HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client
- HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
- HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\DTLS 1.2\Client

The whole process mentioned above can be a bit intimidating or difficult to understand. Thus, NetBrain recommends using a simple cryptographic setting app like IISCrypto. This application has a GUI interface to configure and modify the cryptographic settings used by your machine. An example of using this application to apply NetBrain recommended settings is given in Section 5.3.3.

5.3.2. Description of SSL/ TLS Protocol and Cipher Suites

Cipher suites are bundles of rules that enable secure network communications over Secure Sockets Layer (SSL) or Transport Layer Security (TLS), These cipher suites offer the algorithms and protocols necessary to protect conversations between servers and clients in the background.

The two parties—the web server and the client—perform an SSL handshake to start an HTTPS connection. The parties involved negotiate on a shared cipher suite as part of the complex handshake phase. After that, a secure HTTPS connection is negotiated using the cipher suite.

For example:

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- *TLS* defines the protocol that this cipher suite is for; it will usually be TLS.
- *ECDHE* indicates the key exchange algorithm being used.
- *RSA* authentication mechanism during the handshake.

- *AES* session cipher.
- *128* session encryption key size (bits) for cipher.
- *GCM* type of encryption (cipher-block dependency and additional options).
- *SHA* (SHA2) hash function. For a digest of 256 and higher. Signature mechanism. Indicates the message authentication algorithm which is used to authenticate a message.
- *256* Digest size (bits).

List of Recommended/ Secure Protocols:

- TLS 1.2
- TLS 1.3

List of Recommended/ Secure Ciphers:

- AES 128/128
- AES 256/256

List of Recommended/ Secure Hashes:

- SHA256
- SHA384
- SHA512

List of Recommended/ Secure Key Exchanges:

- PKCS
- Diffie-Hellman
- ECDH

List of Recommended/ Secure Cipher Suites:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384

Additional Cipher Suites (in case of compatibility issues) are listed here (from Microsoft).

5.3.3. Example Configurations for Secure Cryptographic Settings

In the below section we will be configuring the machine to use the protocol and cipher suites recommended in Section 5.3.2.

1) Using Windows Registry Keys

The system administrator can override the default (D)TLS and SSL protocol version settings by creating DWORD registry values "Enabled" and "DisabledByDefault". These registry values are configured separately for the protocol client and server roles under the registry subkeys named using the following format:
<SSL/TLS/DTLS> <major version number>.<minor version number><Client\Server>
These version-specific subkeys can be created under the following registry path (create if not by default):
HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\CipherSuites
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes
*HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms*Note:

- TLS 1.0 and 1.1 registry values should be 1 for DisabledbyDefault and 0 for Enabled.
- TLS 1.2 registry values should be 0 for DisabledbyDefault and 1 for Enabled.
- TLS 1.3 can be configured for NetBrain web server communications when hosted on Windows Server 2022 or newer.

Enable TLS 1.3 for NetBrain Web Server(s) communications - Registry

TLS 1.3 can be configured via the registry or via crypto tools available online that can manage this for you. NetBrain recommends IISCrypto GUI. Note to download version 3.3. or newer for TLS 1.3 support on Windows

Server 2022. Please see sub section 2 - **Using IISCrypto GUI for enabling TLS 1.3 and TLS 1.2 below the registry procedures.**

Below described procedures will only enable TLS 1.3 for web connections coming in through IIS. Currently, only Windows Server 2022 supports TLS 1.3 SERVER. This procedure will require restarting the Windows host multiple times. It is recommended to have a restore point/snapshot ready and schedule a maintenance/downtime window.

On Windows Server(s) hosting NetBrain web server(s), run below commands in Command Prompt:
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Client" /v DisabledByDefault /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Client" /v Enabled /t REG_DWORD /d 1 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server" /v DisabledByDefault /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server" /v Enabled /t REG_DWORD /d 1 /f
Go to "**Start** > **Run**". Enter: gpedit.msc

In the left pane, expand "**Computer Configuration** > A**dministrative Templates** > **Network** > **SSL Configuration Settings**", and select "Enabled".

Restart your server to apply the changes.

Note: Due to a Microsoft issue, the above step of selecting "Enabled" may not work which may cause the NetBrain Web Server to still use TLS 1.2. Change SSL Configuration Settings to "Not Configured". Restart the server, and confirm Web Server is using TLS 1.3 for client connections. It can be changed back to "Enabled" (but not required).

TLS 1.2 is to be left enabled for backwards compatibility.

Enable TLS 1.2 for NetBrain Web Server(s) communications - Registry

Below procedure will require restarting the Windows host multiple times. It is recommended to have a restore point/snapshot ready and schedule a maintenance/downtime window.

On Windows Server(s) hosting NetBrain web server(s), run below commands in Command Prompt Disable TLS 1.1 and 1.0

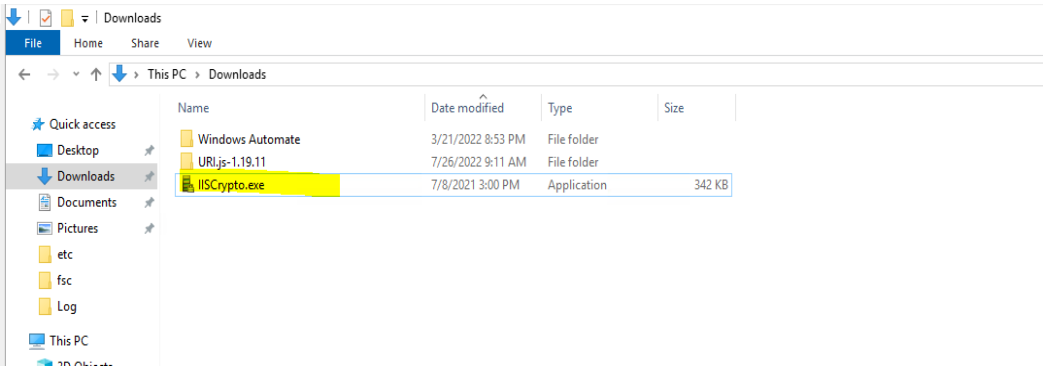
```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client" /v DisabledByDefault /t REG_DWORD /d 1 /f
```

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client" /v Enabled /t REG_DWORD /d 0 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server" /v DisabledByDefault /t REG_DWORD /d 1 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Server" /v Enabled /t REG_DWORD /d 0 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client" /v DisabledByDefault /t REG_DWORD /d 1 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client" /v Enabled /t REG_DWORD /d 0 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server" /v DisabledByDefault /t REG_DWORD /d 1 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Server" /v Enabled /t REG_DWORD /d 0 /f Enable TLS 1.2

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client" /v DisabledByDefault /t REG_DWORD /d 0 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client" /v Enabled /t REG_DWORD /d 1 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server" /v DisabledByDefault /t REG_DWORD /d 0 /f

reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server" /v Enabled /t REG_DWORD /d 1 /f
```

Restart your server to apply the changes.

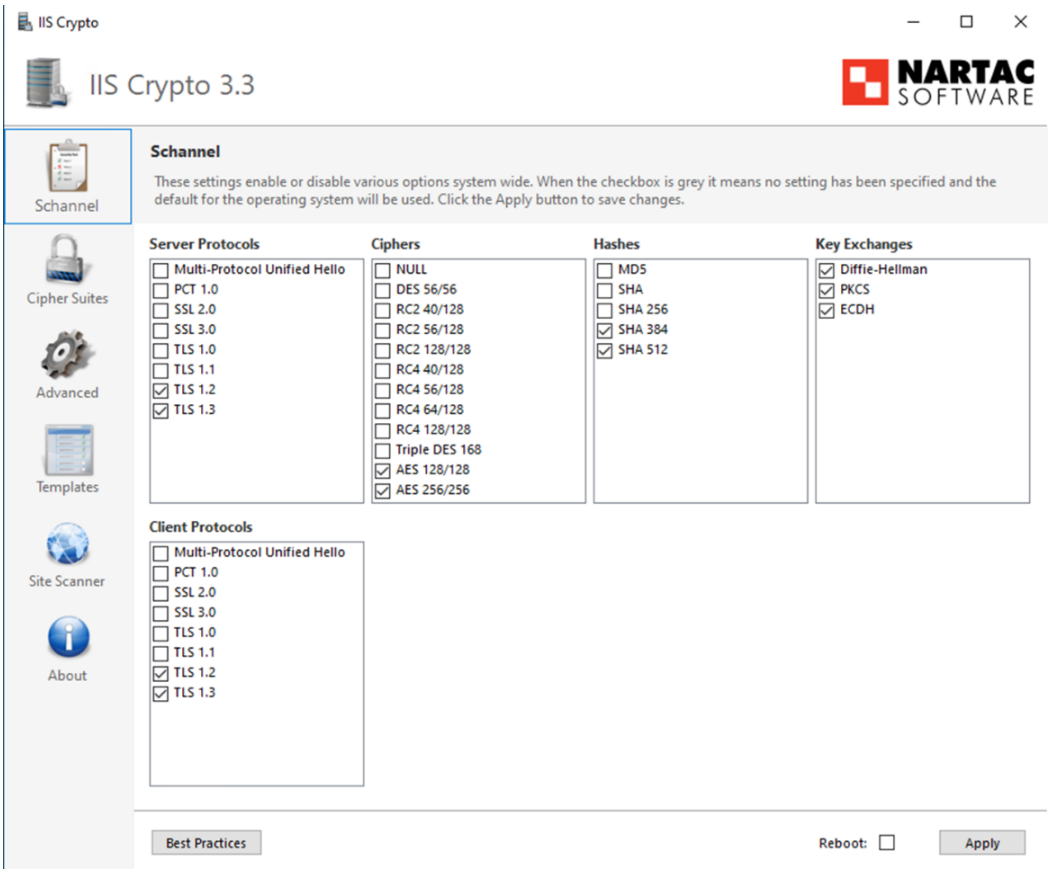
2) Using IISCrypto GUI for enabling TLS 1.3 and TLS 1.2

a) Once the NBIE is installed, download this software: IISCrypto.



b) Double-click to open the exe application. Here, we will be concerned with only 2 Tabs: **Schannel and Cipher Suites.**

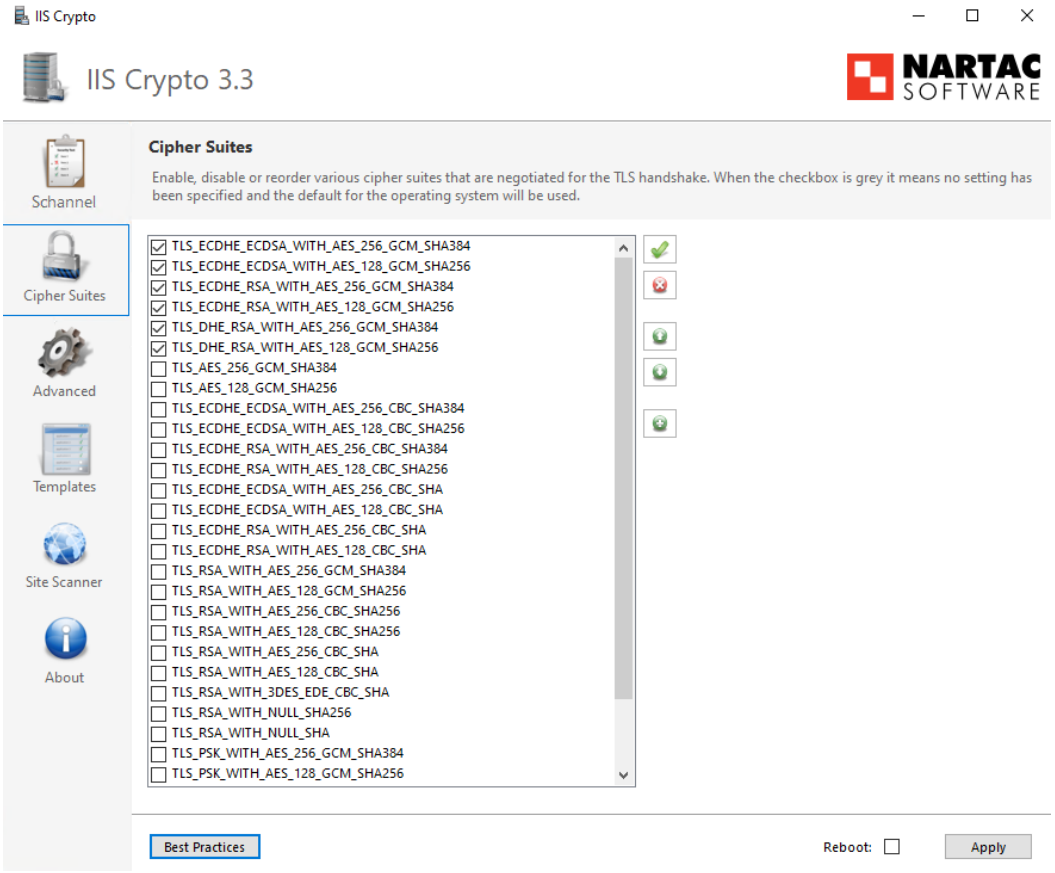
c) The recommended settings for the Schannel are given as follows:



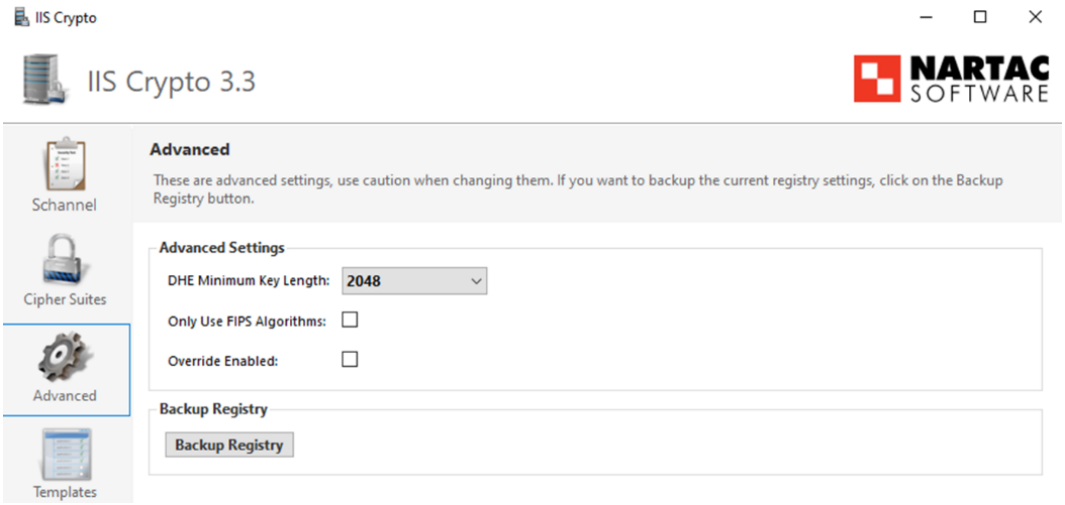
d) Go to "**Start** > **Run**", and enter: gpedit.msc

In the left pane, expand "**Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings**", then select "Enabled".

e) The recommended settings for the **Cipher Suites** are given as follows:



f) Also recheck the **Advanced Settings** Tab for this configuration:



g) Recheck all configurations, apply the settings and then **reboot** the machine. The changes will be applied.

Note: Due to a Microsoft issue, step (d) of selecting “Enabled” may not work which may cause the NetBrain Web Server to still use TLS 1.2. Change SSL Configuration Settings to "Not Configured". Restart the server, and confirm Web Server is using TLS 1.3 for client connections. It can be changed back to "Enabled" (but not required).

3) Modifications for Cryptographic Settings using Scripts

The above configuration settings can also be done using a PowerShell Script. Sample script syntax is given below:

```
# Disable SSL 3.0
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
Write-Host 'SSL 3.0 has been disabled.'
```

5.3.4. Changing Elasticsearch TLS Configuration on the Linux Machine

ElasticSearch is used in the NBIE as a full-text search and analytics engine in a distributed multi-user environment. The default port of Elasticsearch in NetBrain is 9200. The issue is that even when we have configured our Windows machine to use strong ciphers using one of the methods described earlier, Elasticsearch on Linux can still be advertising weak settings (even though they are not being used). Hence, for the fix, we need to limit the DHKey size to match with what was set earlier on the Windows machine.

Steps for the Fix:

1. Stop the Elasticsearch service using:
    - ***systemctl stop elasticsearch***
2. Open the following file: **/etc/elasticsearch/jvm.options** using vim or nano.
3. Add the following line to the file: *-Djdk.tls.ephemeralDHKeySize=matched*
    - This line is a jvm option that restricts the DHE key size to match with the public certificate advertised by ES.

```
# temporary workaround for C2 bug with JDK 10 on hardware with AVX-512
10-:-XX:UseAVX=2
-Djna.tmpdir=/usr/share/elasticsearch/temp
-XX:-UsePerfData
-Djava.net.preferIPv4Stack=true
8-13:-XX:NewRatio=3
-Xlog:gc*=warning,gc+ref=warning,gc+heap=warning,gc+age=warning:file=/var/log/netbrain/elasticsearch/gc-%p-%t.log:tags,uptime,time,level:file
-Xlog:safepoint*=warning:file=/var/log/netbrain/elasticsearch/safepoints-%p-%t.log:tags,uptime,time,level:filecount=10,filesize=5m
-Djdk.tls.ephemeralDHKeySize=matched
```

4. After adding the line to the file save the file. Restart the elasticsearch service using:
   systemctl start elasticsearch

5. Check services and verify status and working.

5.4. Setting Up an SSL-Secured NetBrain Webpage

To protect the data transfer between a client's web browser and NetBrain Web Servers, enabling HTTPS is recommended to encrypt the communication.

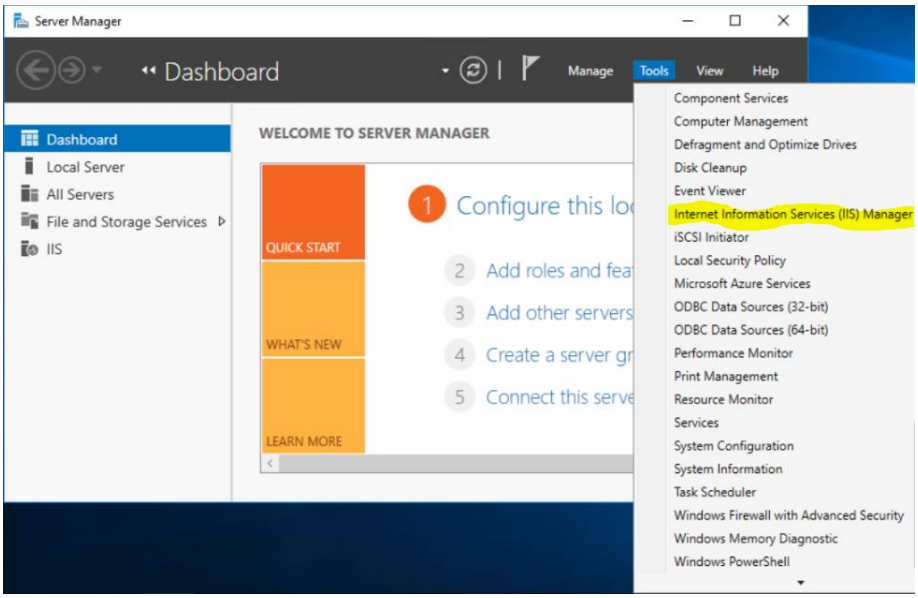
Prerequisites

- Make sure the customer has their Certificate files properly installed to enable HTTPS for the Web server. Otherwise, they can use the self-signed certificate file to enable it in IIS.
- Make sure the customer has root/administrator access to all the Linux or Windows servers deployed with NetBrain components.
- Make sure the customer has the System Admin account credential to log in to the NetBrain System Admin portal.
- NetBrain Web Server service is running normally with http(80).

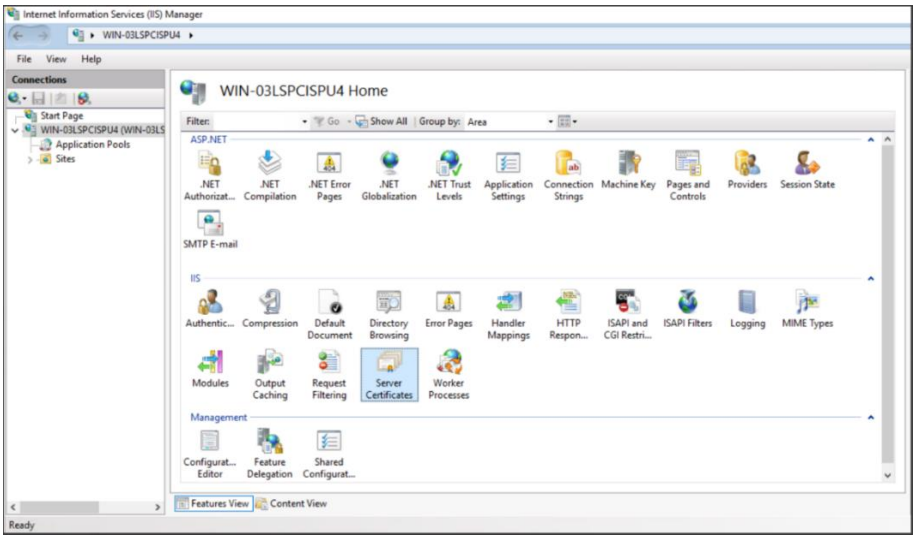
Enabling HTTPS for NetBrain Web Server

1. Log in to the Windows server, where NetBrain Web Server has been installed with an Administrator account.

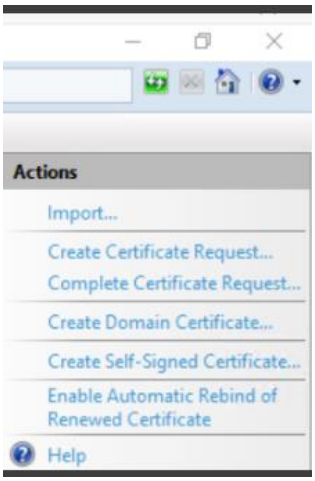
2. Open the Server Manager. Click **Tools** at the upper-right corner and select **Internet Information Services (IIS) Manager**:



3. In the IIS Manager, select **Server** from the left tab and click **Server Certificates**.

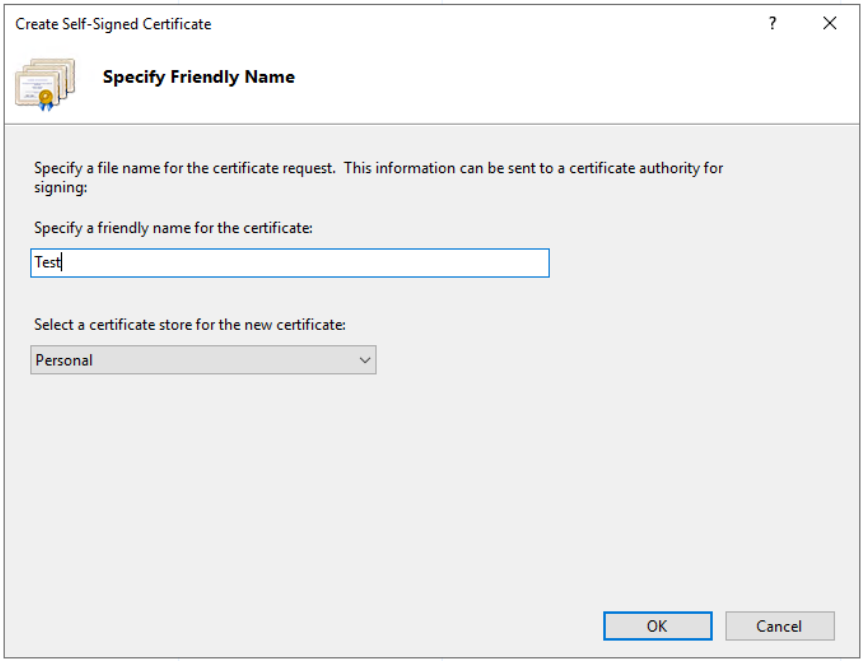


4. Select **Import** from the right **Actions** pane to import the new issued certificate file prepared by the customer.



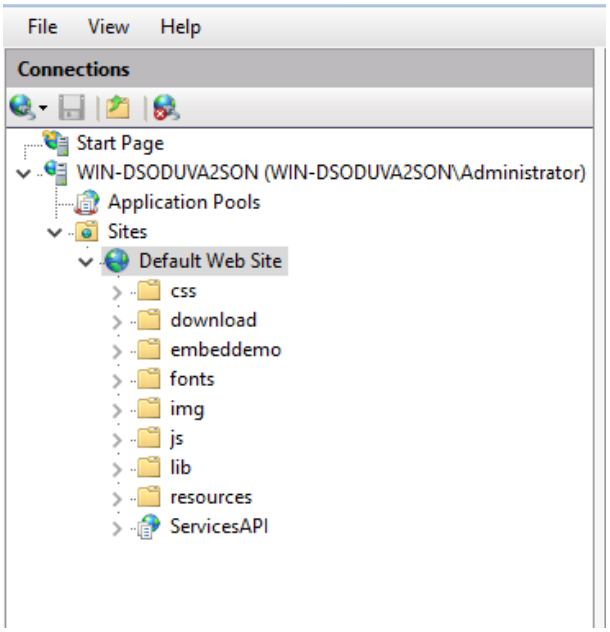
Note: It is highly recommended to use the certificate file provided by the customer.

5. If there is no certificate file available, click **Create Self-Signed Certificate** to generate a self-signed certificate file to enable HTTPS: Enter a name (such as **Test**) and click **OK** to complete the creation of a self-signed certificate.

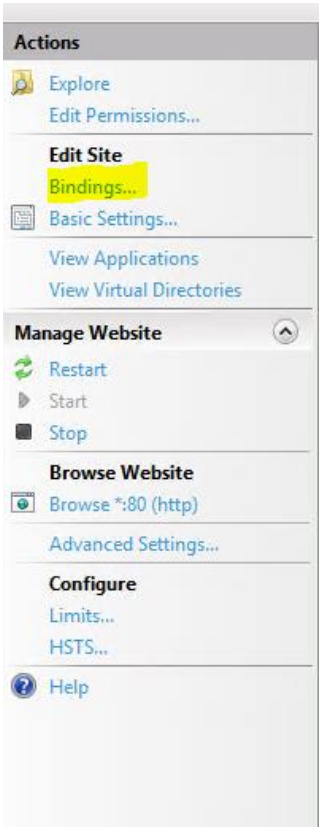


Note: By default, a self-signed certificate file will expire in 1 year.

6. Extend the **Sites** folder and select **Default Web Site**.

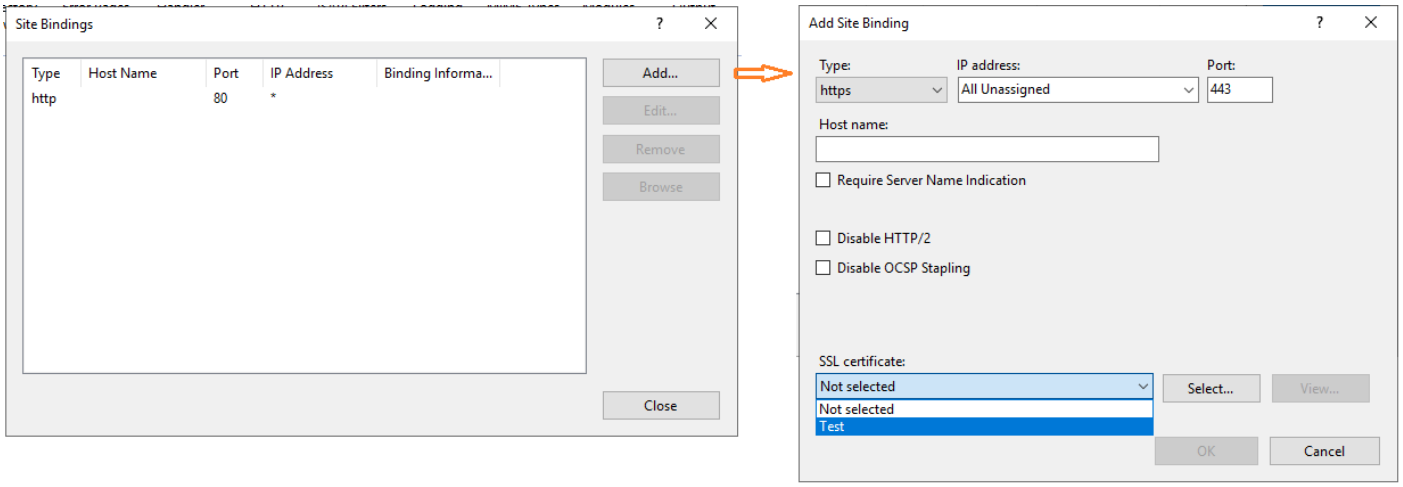


7. Click **Bindings** from the right **Actions** pane to start binding the certificate imported or created in the above step:



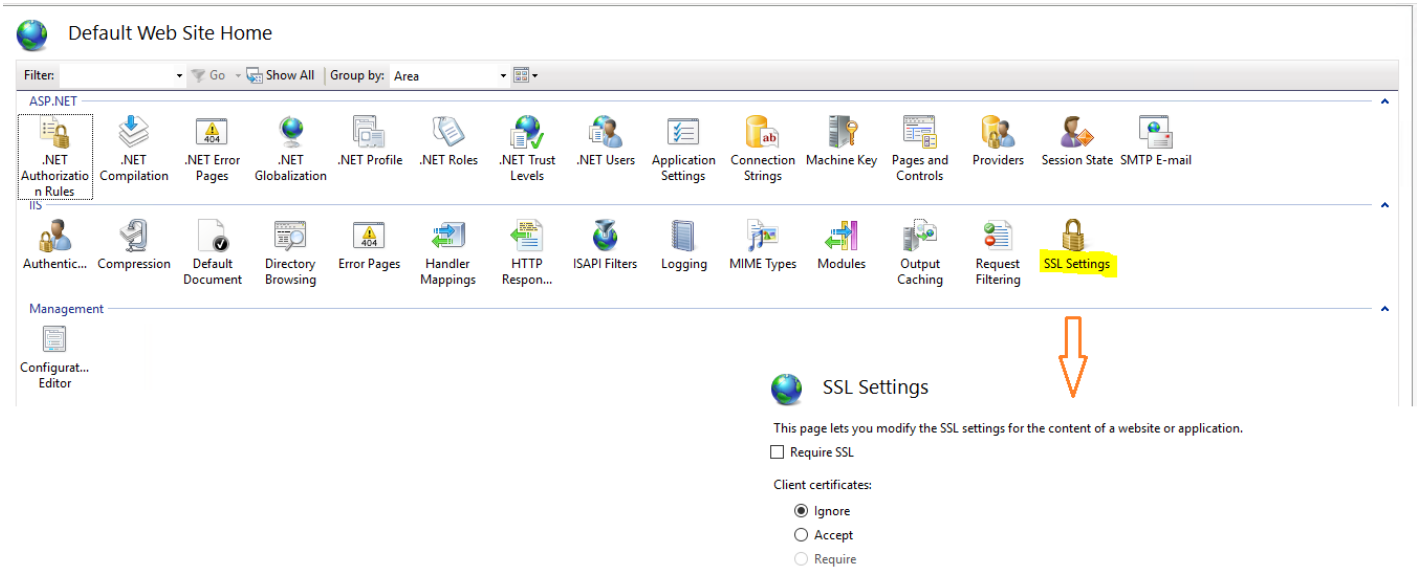
8. In the **Site Bindings** dialog, click **Add** to create a new binding. Then in the **Add Site Binding** dialog, change the type to **https**, and select **Test** in the **SSL Certificate** area. Click **OK** to save the new binding rule and close the

Site Bindings dialog.



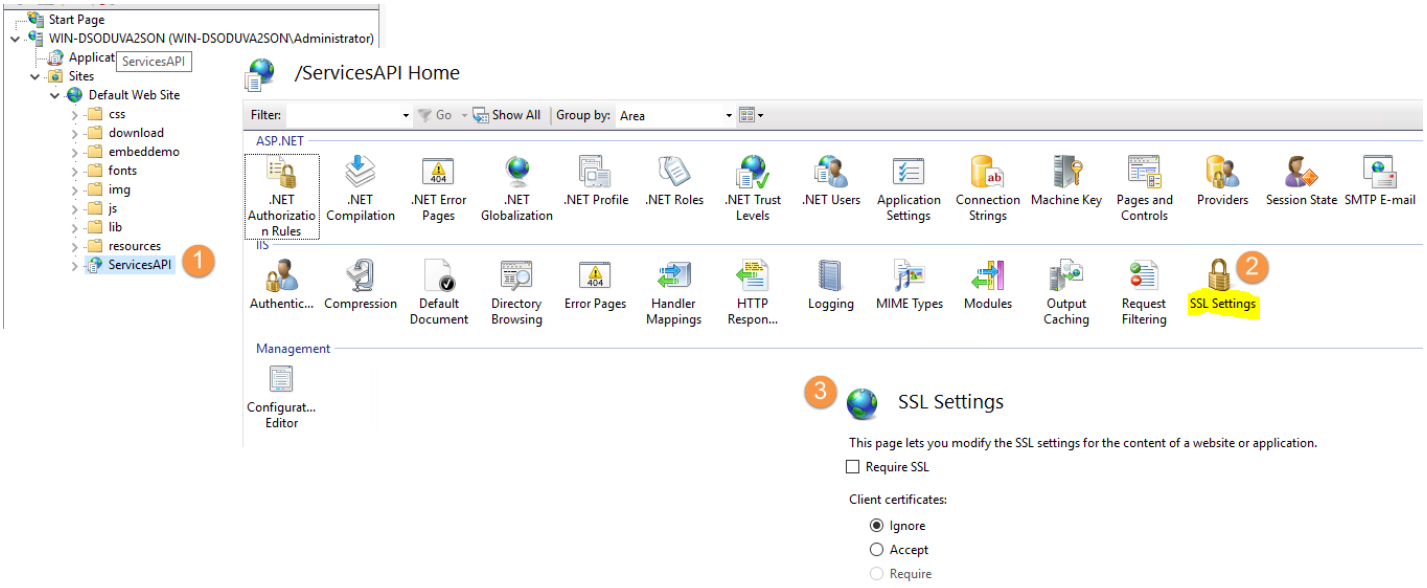
Note: If you just want to enable HTTPS for the NetBrain Web Server, remove the default existing rule accepting connections on port 80.

9. Go back to the **Default Web Site Home** page and click **SSL Settings**. Uncheck the **Require SSL** check box and change the Client certificates to **Ignore**, then click **Apply** in the right **Actions** pane to save the change.



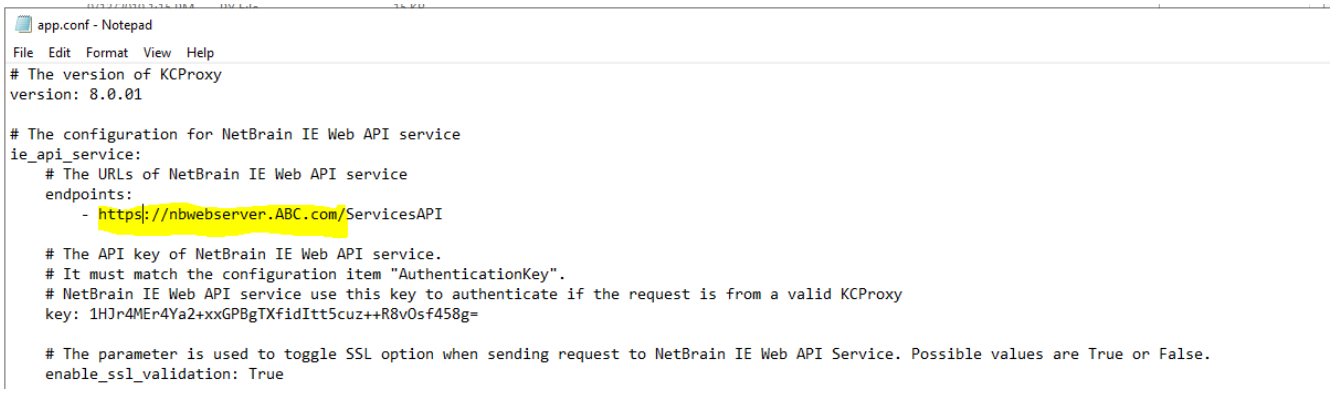
10. In the left connections panel, expand the **Default Web Site** and click **ServicesAPI**. Click **SSL Settings**, then uncheck the **Require SSL** checkbox and change the Client certificates to **Ignore**. Click **Apply** in the right

Actions pane to save the change.



Enabling HTTPS for Connection Between Web Server and KC Proxy Server

1. Log in to the Windows server, which has installed NetBrain KC Proxy server (together with Web API Server) with an Administrator account.
2. Run the `ping HOSTNAME.DOMAIN.NAME` command to ensure that the hostname with the domain name of the Web Server to which the certificate file is issued can be solved. In this case, the Fully Qualified Domain Name of the Web Server is **nbwebserver.ABC.com**, so that customers can access the Web Server using URL **https://nbwebserver.ABC.com/**, and the above command is:`ping nbwebserver.ABC.com`.
3. Go to the NetBrain installation folder and explore the KCProxy folder. By default, it is **C:\ProgramFiles\NetBrain\KCProxy\kcproxy**.
4. Open the configuration file **app.conf** and modify the URL of NetBrain IE Web API service to https://**HOSTNAME.DOMAIN.NAME**/ServicesAPI, as follows:



5. Save the file and restart the **NetBrainKCProxy** service.

Enabling HTTPS for Connection Between Web Server and Service Monitor Agent

1. Log in to the server which has installed the NetBrain Service Monitor Agent with Administrator (for Windows) or root (for Linux) user.
2. Run the `ping HOSTNAME.DOMAIN.NAME` command to ensure that the hostname with the domain name of the Web Server to which the certificate file is issued can be solved. In this example, the command is: `ping nbwebserver.ABC.com`.
3. Update all the **api_url** in the Service Monitor's configuration file **agent.conf** on all Linux and Windows servers, then save the file.
   - Linux server: **/etc/netbrain/nbagent/agent.conf**
   - Windows server: **C:\ProgramData\Netbrain\nbagent\agent.conf**

```
api_url:
    - https://nbwebserver.ABC.com/ServicesAPI

api_key: AiG6CZc58Xybg8v02K8X1nWcqAkcoLNyV3Z3FUS3iAI=


# enable ssl validation (default:False)
enable_ssl_validation: False
# cert_path: /path/to/certfile
```

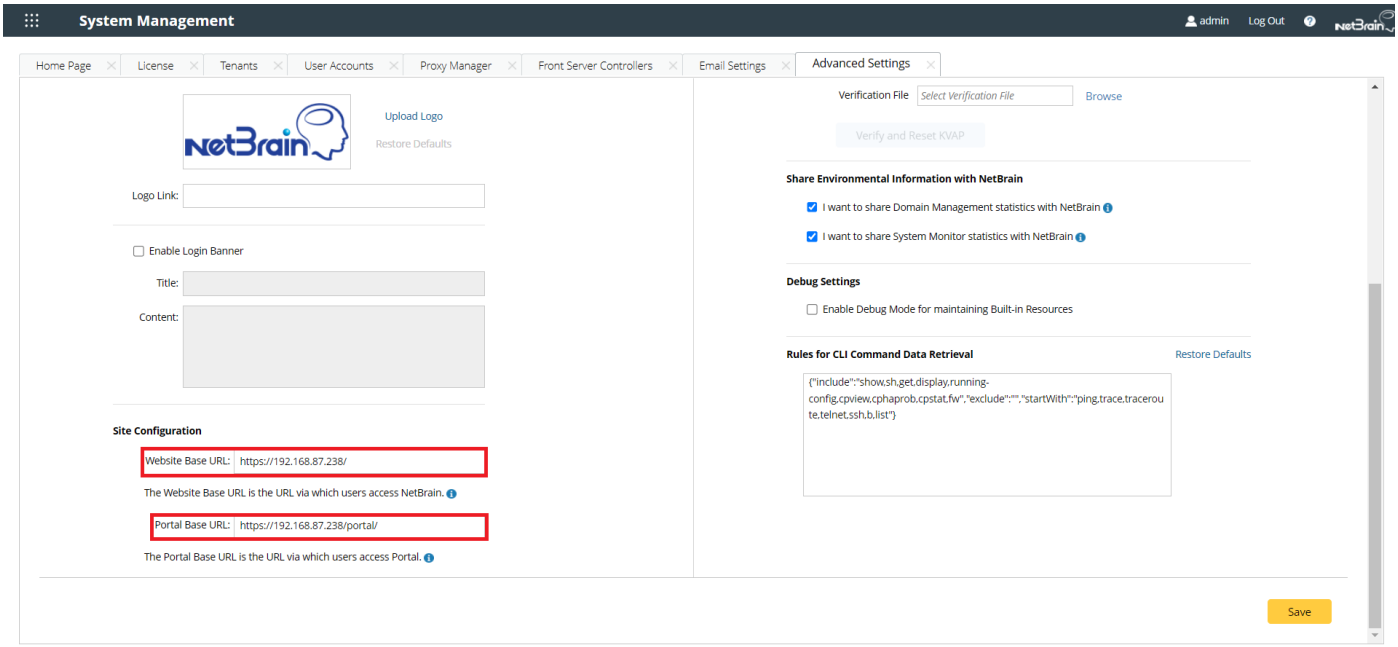
4. Restart the service of Service Monitor Agent on each server to make the change effective.
5. Log in to the Service Monitor portal to confirm the system running status and service running status are normal after restarting the service of Service Monitor Agent.

Configuring NetBrain Web API Server

Note: The following setting only applies to versions higher than IEv8.02.

1. Log in to the NetBrain System Management Page as a System Administrator.

2. On the **Advanced Settings** tab, enter **https** as the Website and Portal Base URLs as follows:



3. Click **Save**.

5.5. Hardening Data Server

HDD Encryption

While NetBrain does not configure HDD encryption by default, it is recommended to prevent outsiders from gaining easy access to data stored in the hard disk drive of any of the NetBrain servers (the number can vary based on the type of deployment), that you configure encryption of the entire hard disk drive via third-party applications or volume encryption via virtualization technologies, for example, MS BitLocker, AWS volume encryption.

Server Hardening

The systems that make up the NetBrain IE application are a part of your network environment. It is recommended to harden all servers by following your company's security policies, such as:

- Install anti-virus software
- Apply corporate security policy

- Backup VM server image if the servers are VM-based
- Patch OS and 3rd party components based on your patching policy