

# SteelHead CX シリーズ バックアップ&リストア ガイド

**Ver.1.5**

**2023/10/10**

丸紅情報システムズ  
技術本部  
セキュリティサービス技術部

# 目次

1	バックアップ手順 .....	4
1.1	設定ファイルのバックアップ .....	4
1.2	証明書ファイルのバックアップ .....	5
2	リストア手順 .....	7
2.1	ライセンス適用 .....	7
2.1.1	(機種が xx70 シリーズの場合) .....	8
2.1.2	(機種が xx80 シリーズの場合) .....	9
2.2	設定ファイルのリストア .....	10
2.3	時刻同期 .....	12
2.4	証明書のリストア .....	13
2.5	Peer 証明書の入替 .....	15
2.5.1	リストア機器で実施 .....	15
2.5.2	【対向機器のソフトウェアバージョン:9. x の場合】 .....	18
2.5.3	【対向機器のソフトウェアバージョン:8. x の場合】 .....	20
2.5.4	【対向機器が SMC の場合】 .....	22
2.6	ドメイン参加 .....	25
2.7	機能の正常性確認 .....	29
3	ソフトウェアのバージョンアップ .....	31
4	system dump 取得方法 .....	37
5	ハードウェア・ソフトウェア サポート終了ポリシー .....	37

## はじめに

本書は Steelhead CXA シリーズの保守サービスをご提供するにあたり、機器の復旧に必要な作業をまとめた資料となります。

現状復旧を目的とした機器交換の保守サービスでは、機器の情報として以下の情報が事前に必要となります。万が一交換時にご準備いただいていない場合、現状復旧作業を進めることはできません。機器交換作業前に、予め情報をご準備いただけますようお願い申し上げます。

該当する製品は以下になります。

【CX570、CX770、CX3070、CX5070、CX7070、CX580、CX780、CX3080、CX5080、CX7080】

## 【保守サービス – 機器交換時の事前準備リスト・注意事項】

- ☐ 復旧対象機器の 【ソフトウェアバージョン情報】
- ☐ 復旧対象機器に適応されているソフトウェアバージョンの 【設定ファイル（設定ファイルは FTP サーバから取得していること）】 ※例えば、ソフトウェアバージョン Ver. 9.6 を利用中の場合、Ver. 9.6 の設定ファイル
- ☐ 復旧対象機器の 【ログイン ID / パスワード】
- ☐ Riverbed アプライアンスの管理画面にログインできる 【端末】 【ネットワーク環境】

### 【注意-1】 SSL 通信の最適化を有効にしている場合

- ☐ SSL 証明書の保存作業

※故障機器以外の SH の証明書更新作業はお客様ご自身の実施となります。

- ☐ 【証明書のバックアップファイル（機器本体の管理画面から生成）】
- ☐ 証明書バックアップファイル生成時に設定した 【パスワード】
- ☐ Secure Peering を組んでいる対向機器の 【IP アドレス】 【機器のログイン ID / パスワード】

### 【注意-2】 SteelHead を ActiveDirectory のドメインへ参加している場合

- ☐ ドメイン参加時に設定した 【ドメイン名 / ユーザ名 / パスワード】

### 【注意-3】 SMB の最適化を有効にしている場合

☐ レプリケーションユーザ登録時に設定した 【ドメイン名 / ユーザ名 / パスワード】

## 1 バックアップ手順

復旧の際には設定ファイルが必要となります。

また、SSL 通信最適化を行っている場合には、証明書ファイルのバックアップファイルが必要となります。

下記手順に従い、バックアップを行ってください。

### 1.1 設定ファイルのバックアップ

FTP サーバまたは SCP サーバを利用し、設定ファイルをバックアップします。

※Windows クライアント OS 対応のフリーソフトの FTP サーバ/SCP サーバでも構いません。

SteelHead にアクセスするため、作業用端末に Teraterm 等のアプリケーションがインストールされていることが前提です。

- ① SteelHead に接続する端末上に FTP サーバ/SCP サーバを立てます。または、SteelHead の Primary ポートからアクセスできる FTP サーバ/SCP サーバを準備します。
- ② Teraterm 等利用し、バックアップ対象の SteelHead 本体へ SSH 接続します。接続の際、ユーザ名とパスワードが必要となります。機器本体の[ログイン ID]と[パスワード]を入力し、接続します。

- ③ 下記のようにバックアップコマンドを入力します。

・FTP サーバでのバックアップの場合

```
configuration upload active ftp://"FTP ユーザ名:パスワード"@FTP サーバ/
```

例

```
amnesiac >
```

```
amnesiac > en
```

```
amnesiac # conf t
```

```
amnesiac (config) # configuration upload initial ftp://admin:password@192.168.1.1/
```

・SCP サーバでのバックアップの場合

```
configuration upload active scp://"SCP ユーザ名:パスワード"@SCP サーバ/
```

例

```
amnesiac >
```

```
amnesiac > en
```

```
amnesiac # conf t
```

```
amnesiac (config) # configuration upload initial scp://admin:password@192.168.1.1/
```

- ④ 拡張子のないファイルが作成されますので、保存します。

例 ファイル名 initial (デフォルトの場合ファイル名は「initial」となります。)

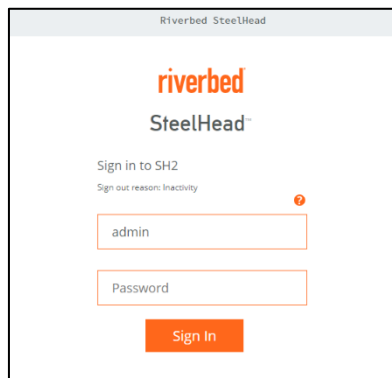
## 1.2 証明書ファイルのバックアップ

(注意) 本手順は、HTTPS(SSL 通信)の最適化の設定を有効にしている場合のみ必要です。

- ① ブラウザから管理画面を開き、ログインします。

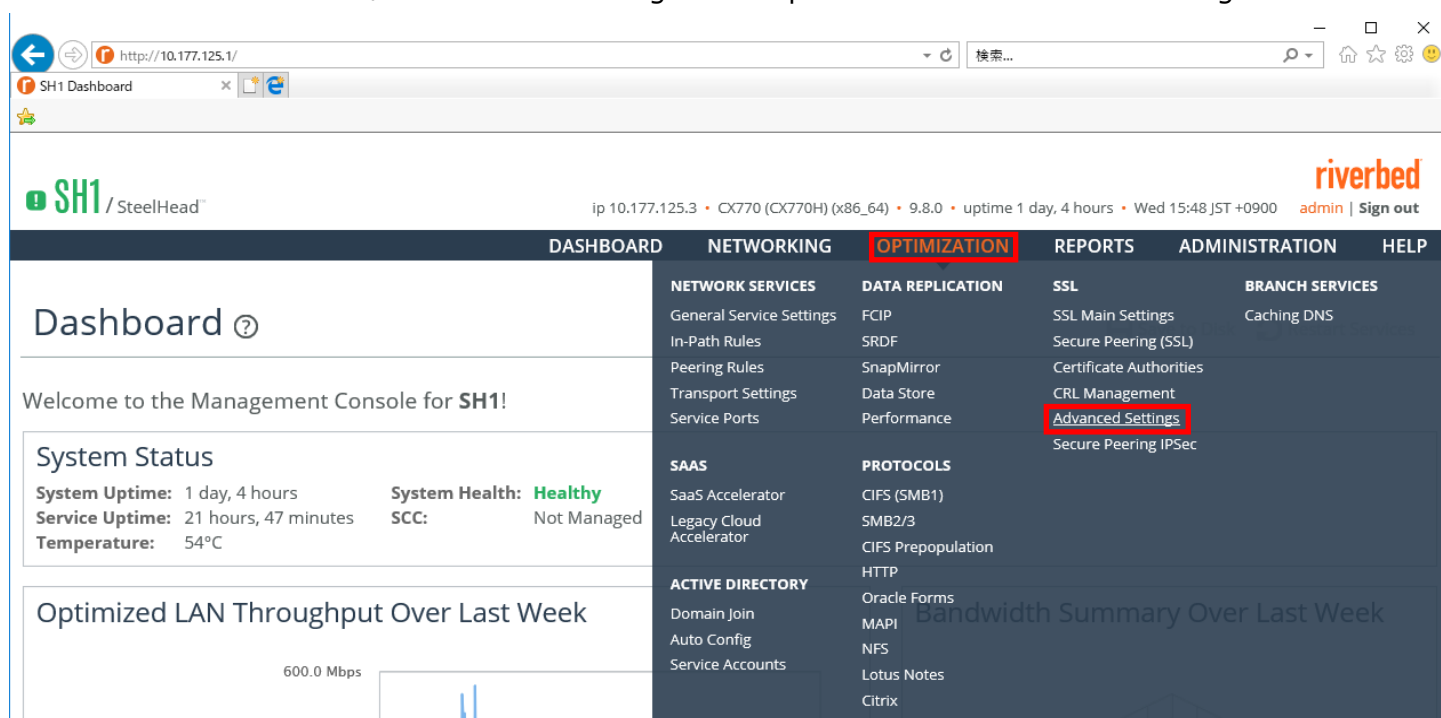
アクセス先 HTTP or HTTPS://SteelHead の IP アドレス

ユーザ名： お客様管理 パスワード： お客様管理



- ② OPTIMIZATION → Advanced Settings をクリックします。

※Software バージョン 8 系をお使いの場合、Configure → Optimization → Advanced Settings



- ③ 画面下部の「Bulk Export」で、赤枠内のチェックボックスをすべて入れ、パスワードを入力し、「Export」をクリックし、任意の場所に保存します。

例 バックアップファイル名（デフォルト） ssl\_bulk\_export.bin

（注意） 設定したパスワードは忘れないようご自身で控えておいて下さい。このパスワードを忘れた場合、リストアができません。

The screenshot shows the 'Bulk Export' section of a web application. A red rectangular box highlights the following elements:

- ☒ Include Server Certificates and Private Keys
- ☒ Include SCEP/CRL Configuration
- Password: [password field]
- Password Confirm: [password field]
- Export button

Below the highlighted area, there is a 'Bulk Import' section with an 'Upload File' field containing 'ssl\_bulk\_export.bin' and a 'Password to Decrypt' field. Above the 'Bulk Export' section, there are two 'Show Effective Overall Cipher List' buttons and a 'Server Ciphers' section with a table showing cipher strings and suite names.

## 2 リストア手順

リストアを実施する際は、下記手順に従い実施してください。

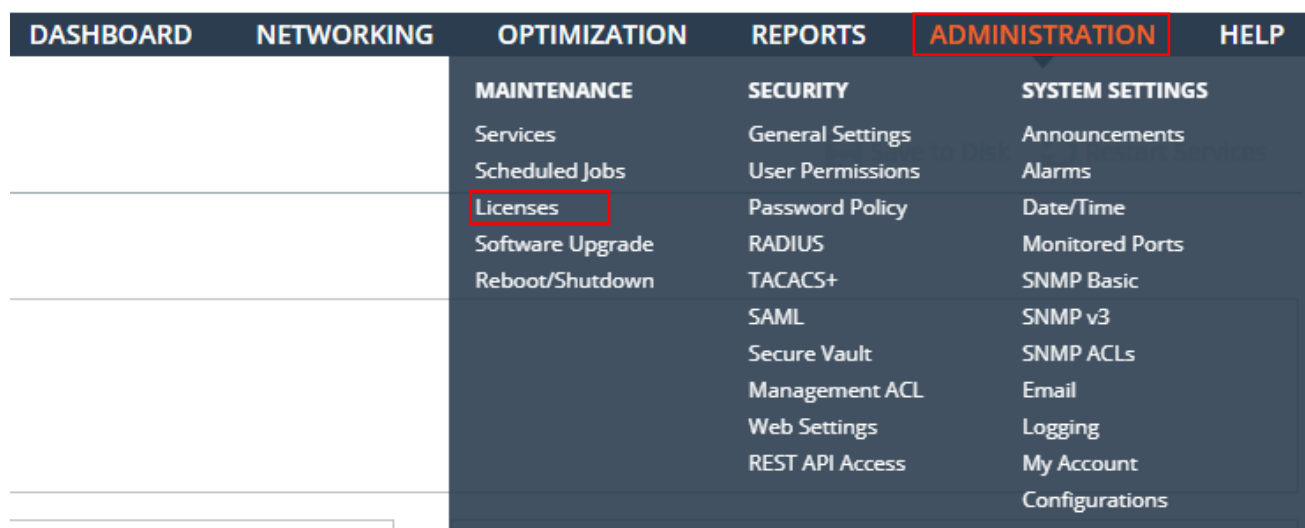
### 2.1 ライセンス適用

機器本体へライセンスを適用します。ライセンスを適用しない場合、最適化が有効になりません。

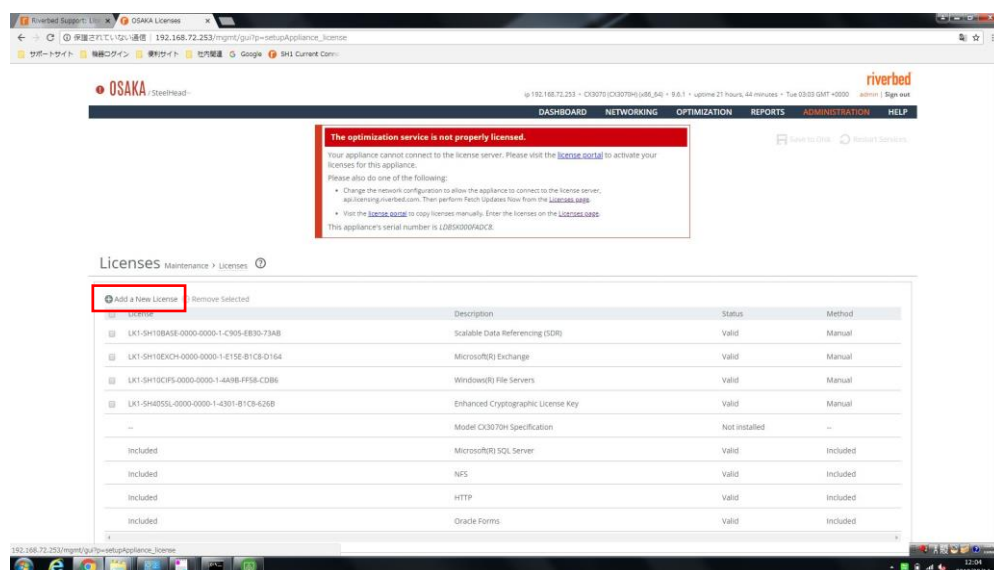
- ① ブラウザから SteelHead アプライアンスの管理画面を開き、ログインしてください。

- ・アクセス先 HTTP or HTTPS://SteelHead の IP アドレス
- ・ユーザ名 : お客様管理 パスワード : お客様管理

- ② ADMINISTRATION → Licenses をクリックします。



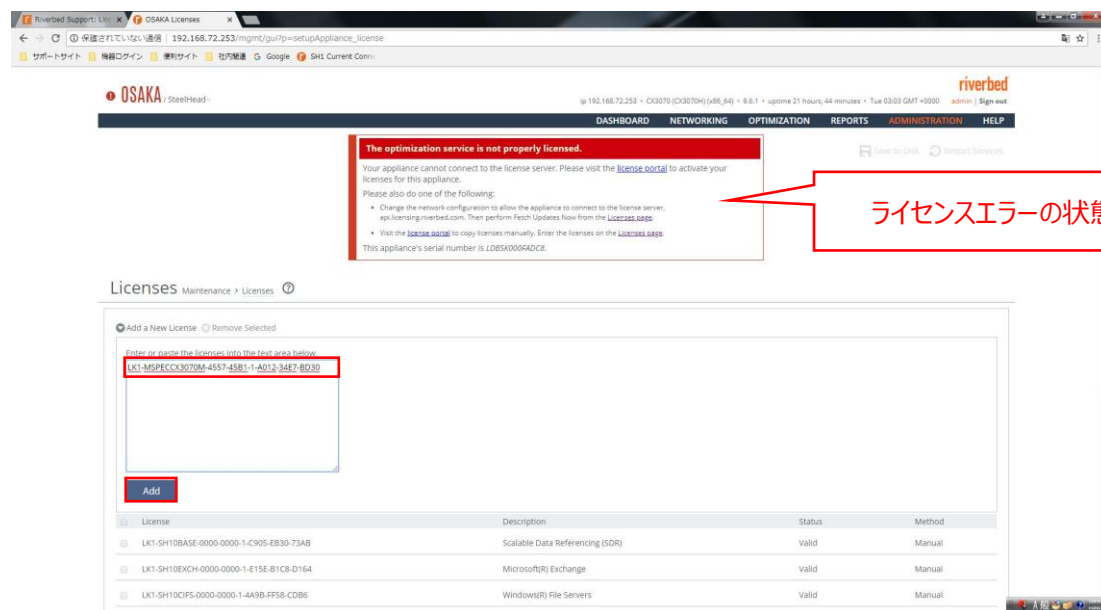
- ③ 「Add a New License」をクリックします。





④ ライセンスキーを張り付け、「Add」をクリックします。

※複数ある場合は、すべて登録します。



### 2.1.1 (機種が xx70 シリーズの場合)

追加したライセンスと同じ「Hardware Specifications」を選択して「Apply」をクリックします。

※ライセンス横の Status にある期限はライセンスの有効期限を示しています。

ライセンス期限が超過した場合、最適化機能が有効となりません。



## 2.1.2 (機種が xx80 シリーズの場合)

① ライセンスが追加されたことを確認します。

※「Specifications」を指定する必要はありません。

riverbed  
3080 / SteelHead

ip 172.19.208.31 • CXA3080B110 (CXAL3080) (x86\_64) • 9.9.1 • uptime 27 minutes, 27 seconds • Thu 10:10 GMT +0000 admin | Sign out

DASHBOARD NETWORKING OPTIMIZATION REPORTS ADMINISTRATION HELP

Licenses Maintenance > Licenses

Save to Disk Restart Services

Licenses on this Appliance

Add License Remove Licenses Refresh Licenses

License	Description	Status	Method
<input type="checkbox"/> STANDARD	Base Optimization Service Scalable Data Referencing (SDR) Optimization HTTP Optimization SSL Optimization Single Ended HTTP Cache SaaS Accelerator Support Legacy Cloud Accelerator Support Microsoft(R) Exchange (MAPI) Optimization Windows(R) File Servers (SMB/CIFS) Optimization CXAL3080	Valid Mar 15 2020	Manual

Appliance Specifications

CXA3080B110: BW Limit: 235000 Kb/s Connection Limit: 14000

□印があるのが、追加ライセンス

② ライセンスエラー画面が表示されていないことを確認します。

反映まで数分程度かかりますので、適宜画面を更新します。

riverbed  
OSKA / SteelHead

ip 192.168.72.253 • CX3079 (CX3070M) (x86\_64) • 8.8.1 • uptime 21 hours, 50 minutes • Tue 03:05 GMT +0000 admin | Sign out

DASHBOARD NETWORKING OPTIMIZATION REPORTS ADMINISTRATION HELP

Licenses Maintenance > Licenses

Add a New License Remove Selected

License	Description	Status
<input type="checkbox"/> LK1-SH10BASE-0000-0000-1-C905-EB30-73A8	Scalable Data Referencing (SDR)	Valid
<input type="checkbox"/> LK1-SH10EXCH-0000-0000-1-E15E-81C8-D164	Microsoft(R) Exchange	Valid
<input type="checkbox"/> LK1-SH10CIFS-0000-0000-1-4A9B-FF58-CD86	Windows(R) File Servers	Valid
<input type="checkbox"/> LK1-MSPEC-CX3070M-4557-45B1-1-A012-34E7-8D30	Model CX3070M Specification	Valid through 2018/11/06
<input type="checkbox"/> LK1-SH40SSL-0000-0000-1-4301-81C8-62B8	Enhanced Cryptographic License Key	Valid
Included	Microsoft(R) SQL Server	Valid
Included	NFS	Valid
Included	HTTP	Valid
Included	Oracle Forms	Valid

Fetch Updates Now

Hardware Specifications

• CX3070L: BW Limit: 50000 Kb/s Connection Limit: 3000 (runnable)  
• CX3070M: BW Limit: 100000 Kb/s Connection Limit: 6000  
• CX3070H: BW Limit: 100000 Kb/s Connection Limit: 9000 (runnable)

Apply

ライセンスエラー画面が表示されていない状態

## 2.2 設定ファイルのリストア

- ① SteelHead に接続する端末上に FTP サーバ/SCP サーバを立てます。または、SteelHead の Primary ポートからアクセスできる FTP サーバ/SCP サーバを準備します。

・FTP サーバを利用する場合

例 FTP ユーザ : admin

FTP ユーザーパスワード : password

FTP ユーザーディレクトリ : C:¥Users¥xxx¥Documents¥FTPserver¥

・SCP サーバを利用する場合、環境に合わせた設定をご利用ください。

- ② 用意したリストア用 config のファイル名を変更します。

例 initial ⇒ config-msys

- ③ 用意したリストア用 config を FTP ユーザ/SCP ユーザーディレクトリ配下に配置します。

・FTP の場合

例 C:¥Users¥xxx¥Documents¥FTPserver¥config-msys

- ④ Teraterm を起動し、SteelHead にコンソール経由でログイン後、下記のコマンドを実行します。

・FTP の場合

configuration fetch ftp://“ユーザ名:パスワード”@“作業端末の IP アドレス”/設定ファイル

```
amnesiac > en
```

```
amnesiac # conf t
```

```
amnesiac (config) # configuration fetch ftp://admin:password@192.168.1.1/config-msys
```

(注意) Config のファイル名が重複する場合、設定ファイルのアップロードできません。

・SCP サーバを利用する場合、環境に合わせた設定をご利用ください。

- ⑤ 以下のコマンドを実行します。

```
amnesiac (config) # show configuration files
```

```
config-msys                2018/12/20 08:07:34
```

```
initial.bak                2018/12/20 07:59:12
```

```
initial (active)          2018/12/20 08:01:14
```

→ コマンド出力結果

⑥ 以下のコマンドを実行します。

amnesiac (config) # **configuration switch-to config-msys**

※プロンプトが応答するまでしばらく待ちます。

※この時点で設定がリストアされるため、ホスト名が変わります。

SH (config) # **show configuration files**

config-msys (active)	2018/12/20 08:07:34
initial.bak	2018/12/20 07:59:12
initial	2018/12/20 08:01:14

→ コマンド出力結果

⑦ 以下のコマンドを実行します。

SH (config) # **reload**

※機器が再起動しますので、しばらく待ちます。

※再起動が完了するまで、5 分～10 分ほどお待ちください。

## 2.3 時刻同期

- ① 作業端末の IP アドレスをリストア後 SteelHead の IP アドレスと同じセグメントにし、Primary ポートに接続します。
- ② Teraterm を起動し SteelHead に SSH 接続します。  
IP アドレス リストア後の IP アドレス  
ユーザ名 お客様管理  
パスワード お客様管理
- ③ 下記のコマンドを実行し、現在の時刻に合わせます。

```
SH > en
SH # conf t
SH (config) # clock set 'yyyy/mm/dd/ HH:MM:SS'
例 clock set '2019/01/30 19:00:00'
```

※NTP Server を利用している場合は、以下のエラーログが出力されるので、

**% NTP enabled, clock adjustment not allowed**

以下のコマンドを実行します。

```
SH (config) # ntp disable
SH (config) # clock set 'yyyy/mm/dd/ HH:MM:SS'
SH (config) # ntp enable
```

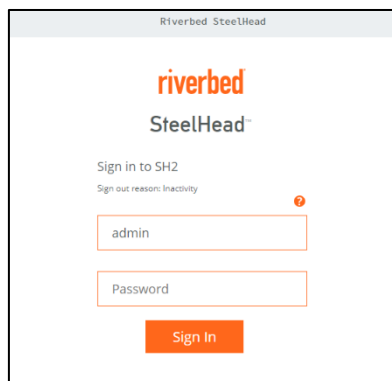
## 2.4 証明書のリストア

※SSL 最適化を利用していない場合、本作業は不要です。

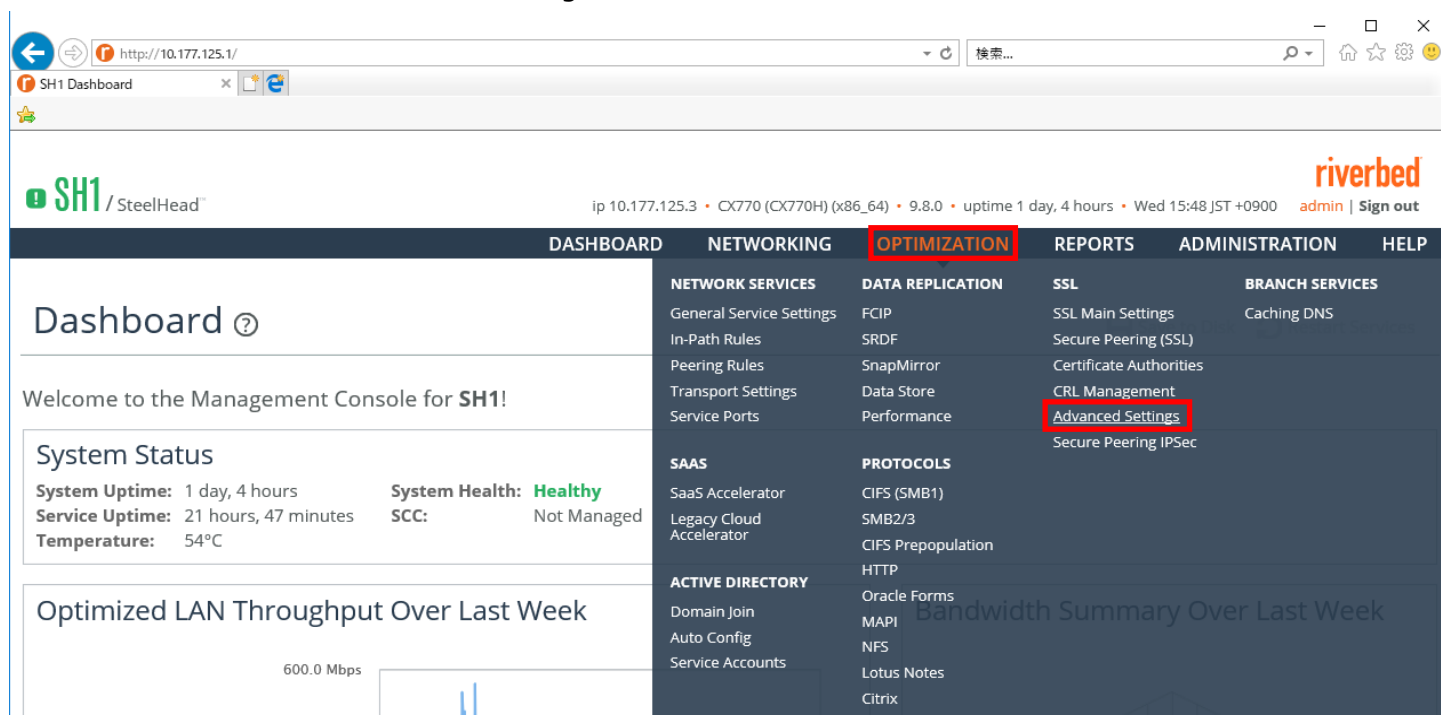
- ① ブラウザから SteelHead アプライアンスの管理画面を開き、ログインします。

アクセス先 HTTP or HTTPS://リストア後の IP アドレス

ユーザ名：お客様管理 パスワード：お客様管理



- ② OPTIMIZATION → Advanced Settings をクリックします。



- ③ 画面下部の「Bulk Import」の「ファイルを選択」からリストア用証明書ファイルを指定し、パスワードを入力後、「Import」をクリックします。

バックアップファイル名（デフォルト） ssl\_bulk\_export.bin

※パスワードはリストア用証明書ファイルのエクスポート時に設定された値のため、お客様ご自身でご確認ください。

The screenshot displays the SteelHead configuration interface. At the top, there are two sections for 'Server Ciphers', each with a 'Show Effective Overall Cipher List' link. Below these is the 'Bulk Import' section, which includes an 'Upload File' field with a file selection button (labeled 'ファイルを選択') and the filename 'ssl\_bulk\_export.bin'. A 'Password to Decrypt' field is also present. A red box highlights the 'Import' button. Below the 'Bulk Import' section is the 'Bulk Export' section, which has two checked options: 'Include Server Certificates and Private Keys' and 'Include SCEP/CRL Configuration'. It also has 'Password' and 'Password Confirm' fields. A red box highlights the 'Export' button.

- ④ 正常にインポートできたことを以下の画面にて確認します。



## 2.5 Peer 証明書の入替

※SSL 最適化を利用していない場合、本作業は不要です。

SSL 最適化を行っている場合、SteelHead は対向の Riverbed 製品と Peer 証明書（PEM）を用いた信頼関係の構築を行っており、これを Secure Peering と呼びます。

リストアを実施した際、リストア対象機器と Secure Peering を組んでいた対向の Riverbed 製品に対して、Peer 証明書（PEM）の更新をお客様にて行う必要があります。


### 2.5.1 リストア機器で実施

- ① ブラウザから管理画面を開き、SteelHead アプライアンスへログインします。

アクセス先 HTTP or HTTPS://リストア後の IP アドレス

ユーザ名：お客様管理 パスワード：お客様管理

- ② OPTIMIZATION → Secure Peering(SSL)をクリックします。


SH1 / SteelHead™

ip 10.177.125.3 • CX770 (CX770H) (x86\_64) • 9.8.0 • uptime 1 day, 6 hours • Wed 17:47 JST+0900
admin | Sign out

DASHBOARD

NETWORKING

OPTIMIZATION

REPORTS

ADMINISTRATION

HELP

## Dashboard ?

Welcome to the Management Console for SH1!

System Status

System Uptime: 1 day, 6 hours


Service Uptime: 13 minutes, 41 seconds

Temperature: 55°C

System Health: Healthy

SCC: Not Managed

### Optimized LAN Throughput Over Last Week



NETWORK SERVICES

General Service Settings

In-Path Rules

Peering Rules

Transport Settings

Service Ports

DATA REPLICATION

FCIP

SRDF

SnapMirror

Data Store

Performance

SAAS

SaaS Accelerator

Legacy Cloud Accelerator

ACTIVE DIRECTORY

Domain Join

Auto Config

Service Accounts

SSL

SSL Main Settings

Secure Peering (SSL)

Certificate Authorities

CRL Management

Advanced Settings

Secure Peering IPsec

BRANCH SERVICES

Caching DNS

PROTOCOLS

CIFS (SMB1)

SMB2/3

CIFS Prepopulation

HTTP

Oracle Forms

MAPI

NFS

Lotus Notes

Citrix

- ③ Certificate → PEM をクリックします。

[illegible]





④ 以下の様にドラッグしコピーします。

**Certificate:**

[illegible]

⑤ 画面下部の Peering Trust / Mobile Trust の内容確認

※Peering Trust や Mobile Trust のリストに存在する機器（対向機器）には、リストアップ前の証明書情報が登録されているため、対向機器にログインし、故障機の証明書情報削除および代替機の証明書情報登録を行います。対向機器が複数存在する場合、全ての機器に対して実施します。

Peering Trust:

+ Add a New Trusted Entity

x Remove Selected

Trusted Entity

## ●対向機器で実施

⑥ 対向機器にログインし、証明書情報の入れ替えを実施

対向機器の製品やバージョンによって操作方法が異なりますので、下記ページをご参照ください。

対向機器 : SteelHead version9 → 「2.5.2 対向機器が SteelHead version9. x の場合」

対向機器：SteelHead version8 → 「2.5.3 対向機器が SteelHead version8. x の場合」

対向機器：SMC → 「2.5.4 対向機器が SMC の場合」

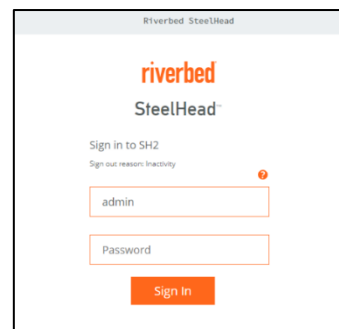
## 2.5.2 【対向機器のソフトウェアバージョン:9.xの場合】

- ① 対向の SteelHead の管理画面にログインします。

※注意：複数台ある場合は、全ての機器に同様の設定を行います。

アクセス先 HTTP or HTTPS://対向の SteelHead の IP アドレス（お客様管理）

ユーザ名：お客様管理 パスワード：お客様管理



- ② OPTIMIZATION → Secure Peering(SSL)をクリックします。

- ③ 下記赤枠の [▶] をクリックします。

- ④ 赤枠内のシリアル番号または、ホスト名が故障機と同じであることを確認します。

- ⑤ 赤枠にチェックし、「Remove Selected」をクリックし、故障機の証明書を削除します。

- ⑥ 画面下部の Peering Trust 内の「Add a New Trusted Entity」をクリックします。

SH1 Secure Peering (SSL) x +

← → ↺ 保護されていない通信 | 10.177.125.1/mgmt/gui?p=setupServiceProtocolsSSLPeering

Type: RSA  
Size: 3072

**Peering Trust:**  
Add a New Trusted Entity Remove Selected

Trusted Entity	Issued To	Expiration Date
No Trusted Entities.		

**SCEP Peering Trust:**  
Add a New SCEP Entity Remove Selected

Trusted Entity	Issued To	Expiration Date
No SCEP Entities.		

**Mobile Trust:**  
Add a New Mobile Entity Remove Selected

Trusted Entity	Issued To	Expiration Date
No Mobile Entities.		

- ⑦ 以下赤枠の[Trust New Certificate] [Cert Text] にチェックを入れます。

**Peering Trust:**  
Add a New Trusted Entity Remove Selected

☐ Trust Existing CA  
AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008  
Full CA Name: AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008  
Issuer: Chambers of Commerce Root - 2008

☒ Trust New Certificate  
Optional Local Name: (ignored if importing multiple certificates)

☐ Local File ファイルを選択 選択されていません

☒ Cert Text

Add

Trusted Entity	Issued To	Expiration Date
No Trusted Entities.		

- ⑧ 項番 2.5.1-④でコピーした内容を「Cert Text」に貼り付け、「Add」をクリックします。

※Optional Local Name は空欄にします。

**Peering Trust:**  
Add a New Trusted Entity Remove Selected

☐ Trust Existing CA  
AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008  
Full CA Name: AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008  
Issuer: Chambers of Commerce Root - 2008

☒ Trust New Certificate  
Optional Local Name: (ignored if importing multiple certificates)

☐ Local File ファイルを選択 選択されていません

☒ Cert Text

Add

Trusted Entity	Issued To	Expiration Date
<input type="checkbox"/> F80B19E7255111961F822CE218EEFADE9F4EF03A98FCC8D8BDB719A8050715C4	Steelhead EC7JX000F563F	Dec 3 15:50:45 2020 GMT

- ⑨ 以下のように「Save to Disk」と表示されている場合、クリックし Save します。  
※項番 2.5.1-⑤で、他にも機器がある場合は、項番 2.5.1-⑥に戻ります。



### 2.5.3 【対向機器のソフトウェアバージョン:8.x の場合】

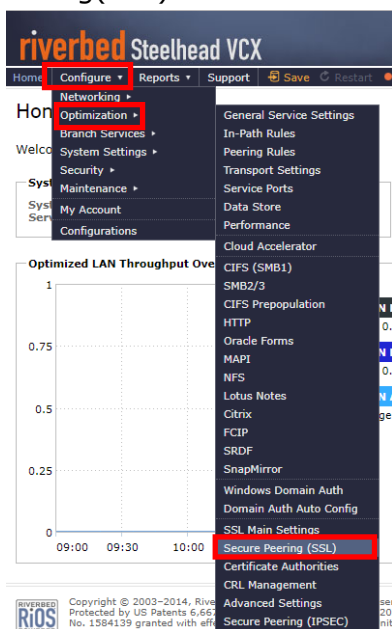
- ① ブラウザから管理画面を開き、ログインしてください。

アクセス先 HTTP or HTTPS://対向の SteelHead の IP アドレス（お客様管理）

ユーザ名：お客様管理 パスワード：お客様管理



- ② Configure>Optimization>Secure Peering(SSL)をクリックします。



- ③ 画面の Peering Trust を確認し、シリアルナンバーまたは、ホスト名が故障機と同じであることを確認します。

**Peering Trust:**

+ Add a New Trusted Entity		- Remove Selected	
<input type="checkbox"/>	Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
<input type="checkbox"/>	16587356801193D21C0132964B16A6CFF241B6AC	SH	Jan 30 03:15:52 2021 GMT

- ④ 赤枠にチェックし、「Remove Selected」をクリックし、故障期の証明書を削除します。

**Peering Trust:**

+ Add a New Trusted Entity		- Remove Selected	
<input type="checkbox"/>	Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
<input checked="" type="checkbox"/>	16587356801193D21C0132964B16A6CFF241B6AC	SH	Jan 30 03:15:52 2021 GMT

- ⑤ 画面下部の Peering Trust 内の「Add a New Trusted Entity」をクリックします。

**Peering Trust:**

+ Add a New Trusted Entity		- Remove Selected	
	Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
No Trusted Entities.			

- ⑥ Cert Text にチェックを入れます。

**Peering Trust:**

▼ Add a New Trusted Entity | - Remove Selected

☐ Trust Existing CA

AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Full CA Name: AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Issuer: Chambers of Commerce Root - 2008

☒ Trust New Certificate

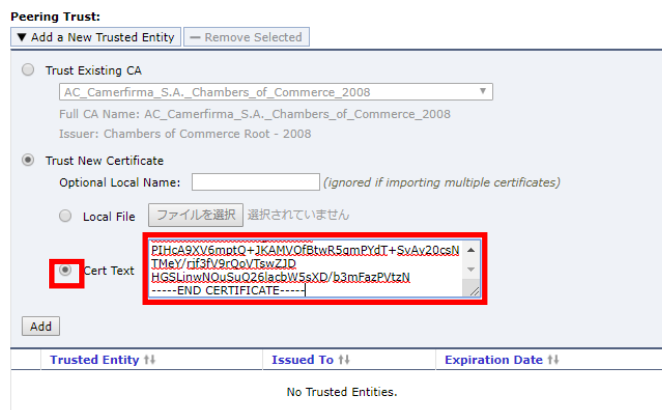
Optional Local Name:  (ignored if importing multiple certificates)

☐ Local File  選択されていません

☒ Cert Text

Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
No Trusted Entities.		

- ⑦ 項番 2.5.1-④でコピーした内容を「Cert Text」に貼り付け、「Add」をクリックします。



- ⑧ 以下のように「Save」と表示されている場合は、クリックし Save します。

※項番 2.5.1-⑤で、他にも機器がある場合は、項番 2.5.1-⑥に戻ります。



## 2.5.4 【対向機器が SMC の場合】

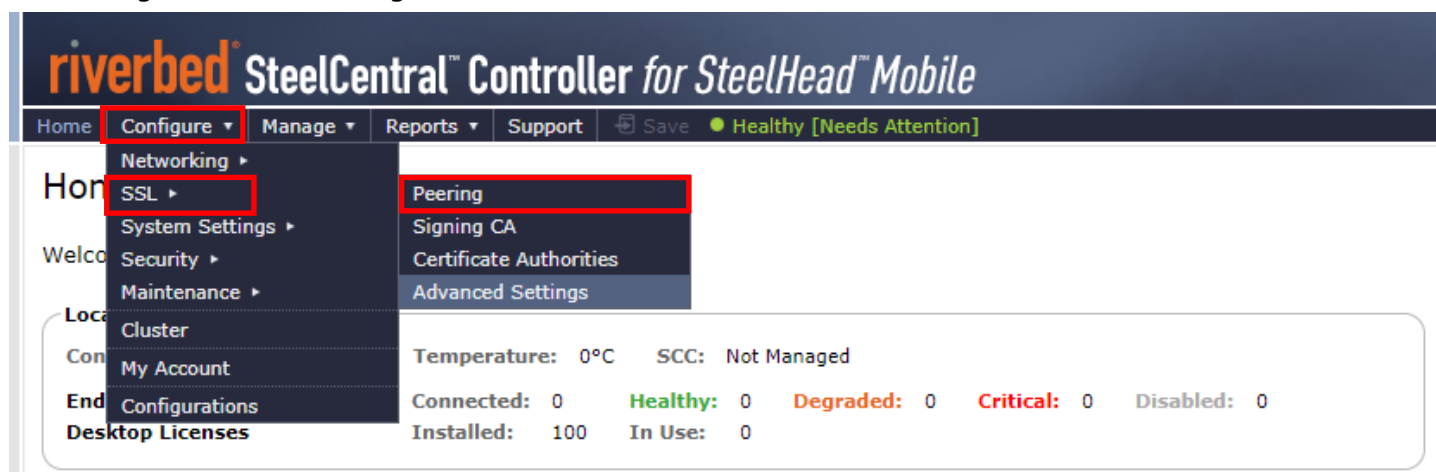
- ① ブラウザから管理画面を開き、ログインしてください。

アクセス先 HTTP or HTTPS://対向の SMC の IP アドレス（お客様管理）

ユーザ名：お客様管理 パスワード：お客様管理



- ② Configure > SSL > Peering をクリックします。



- ③ 赤枠のシリアルナンバーまたは、ホスト名が故障機器と同じであることを確認します。

## Configure > SSL > Peering ?

### Peering Trust:

+ Add a New Trusted Entity		- Remove Selected	
<input type="checkbox"/>	Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
<input type="checkbox"/>	5187FCEF64A3265C8FEB74B5CCBC1B4079F8798D	SHv8	Jan 30 16:16:30 2021 GMT

- ④ 赤枠にチェックし、「Remove Selected」をクリックし、故障期の証明書を削除します。

### Peering Trust:

+ Add a New Trusted Entity		- Remove Selected	
<input checked="" type="checkbox"/>	Trusted Entity ⇅	Issued To ⇅	Expiration Date ⇅
<input checked="" type="checkbox"/>	5187FCEF64A3265C8FEB74B5CCBC1B4079F8798D	SHv8	Jan 30 16:16:30 2021 GMT

- ⑤ 「Add a New Trusted Entity」をクリックします。





⑥ Cert Text にチェックを入れます。

riverbed SteelCentral™ Controller for SteelHead™ Mobile

Home Configure Manage Reports Support Save Degraded

Peering Signing CA Certificate Authorities Advanced Settings

Configure > SSL > Peering ?

Peering Trust:

▼ Add a New Trusted Entity — Remove Selected

☒ Trust New Certificate

Optional Local Name:  (ignored if importing multiple certificates)

☐ Local File  選択されていません

☒ Cert Text

☐ Trust Existing CA

AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Full CA Name: AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Issuer: Chambers of Commerce Root - 2008

⑦ 項番 2.5.1-④でコピーした内容を「Cert Text」に貼り付け、「Add」をクリックします。

riverbed SteelCentral™ Controller for SteelHead™ Mobile

Home Configure Manage Reports Support Save Degraded

Peering Signing CA Certificate Authorities Advanced Settings

Configure > SSL > Peering ?

Peering Trust:

▼ Add a New Trusted Entity — Remove Selected

☒ Trust New Certificate

Optional Local Name:  (ignored if importing multiple certificates)

☐ Local File  選択されていません

☒ Cert Text

☐ Trust Existing CA

AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Full CA Name: AC\_Camerfirma\_S.A.\_Chambers\_of\_Commerce\_2008

Issuer: Chambers of Commerce Root - 2008

⑧ 以下のように「Save」と表示されている場合は、クリックし Save します。

※項番 2.5.1-⑤で、他にも機器がある場合は、項番 2.5.1-⑥に戻ります。

riverbed SteelCentral™ Controller for SteelHead™ Mobile

Home Configure Manage Reports Support Save Degraded

Host Settings Network Interfaces Port Labels Host Labels

## 2.6 ドメイン参加

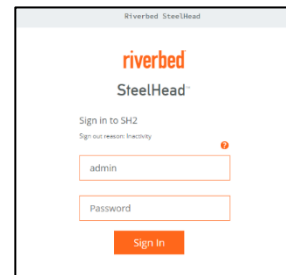
※ドメイン参加を利用していない場合は、本作業は不要です。

SMB2.1 以上の CIFS プロトコルの最適化を有効としている場合、必要な設定項目となります。

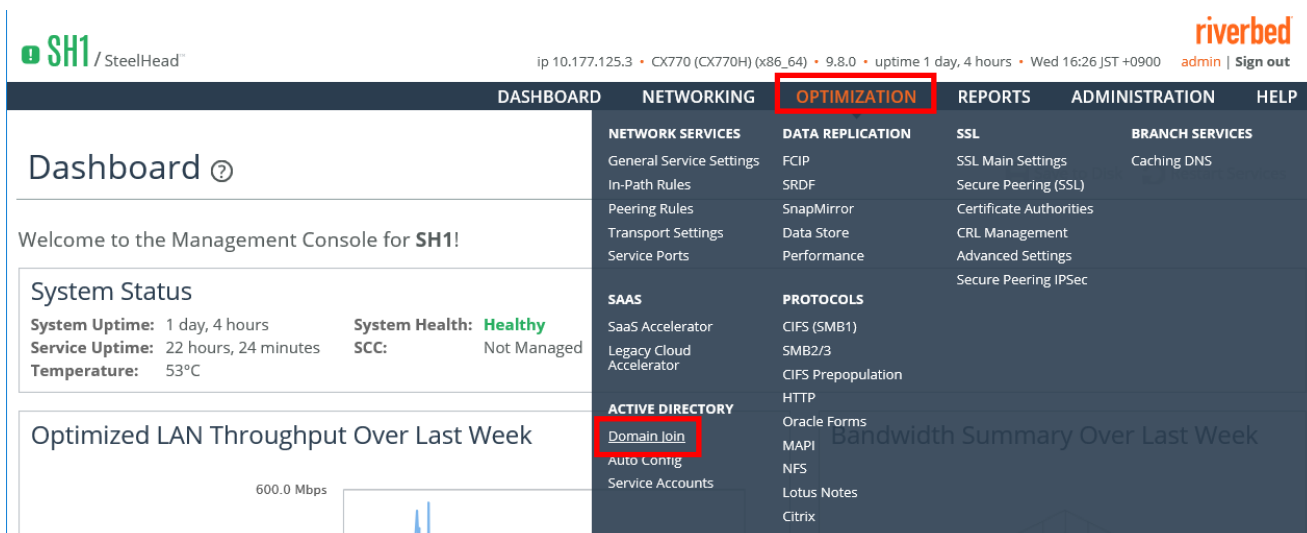
- ① ブラウザから管理画面を開き、SteelHead アプライアンスへログインします。

アクセス先 HTTP or HTTPS ://リストア後の IP アドレス

ユーザ名 : お客様管理 パスワード : お客様管理



- ② OPTIMIZATION → Domain Join をクリックします。



- ③ Domain Settings 内の赤枠に設定値を入力し、「Join」をクリックします。

Domain Join Active Directory > Domain Join ②

Domain / Local

☒ Domain Settings  
☐ Local Workgroup Settings

Select

In Domain Mode, status: Not configured

Domain Settings

Active Directory Domain Name / Realm:  (Example: eng.example.com, example.com)

Primary DNS IP Address:

Join Account Type:

Domain Login:  (must have domain join privileges)

Password:  (not stored; used only for authentication)

Domain Controller Name(s):  (comma delimited)

Short Domain Name:  (optional)

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the SteelHead and Domain Controller clocks be less than 30 seconds. The current time on this SteelHead is:

Wed 25 Jul 2018 04:00:39 UTC  
Wed 25 Jul 2018 13:00:39 JST

ドメイン名

ユーザ名

パスワード

④ 画面下の「Test Join」を実行し、「Status」が Success になることを確認します。

※Fail の場合は、前項目のドメイン名、ユーザ名、パスワードを修正します。

Domain Settings

Active Directory Domain Name / Realm:  (Example: eng.example.com, example.com)

Primary DNS IP Address:

Join Account Type:

Domain Login:  (must have domain join privileges)

Password:  (not stored; used only for this domain operation)

Domain Controller Name(s):  (comma delimited)

Short Domain Name:  (optional)

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the SteelHead and Domain Controller clocks be less than 30 seconds. The current time on this SteelHead is:

Wed 25 Jul 2018 04:02:04 UTC  
Wed 25 Jul 2018 13:02:04 JST

Diagnostics

Domain Health Check

Test DNS	S
Test Join	S
Test NTLM Authentication	--

Test domain join.

Status: **Success**

Last Run: 20 seconds ago  
2018/7/25 13:01:43 (Local web browser time)

► Show Logs (4 Lines)

⑤ OPTIMIZATION → Service Accounts をクリックします。

SH1 / SteelHead™

ip 10.177.125.3 • CX770 (CX770H) (x86\_64) • 9.8.0 • uptime 1 day, 4 hours • Wed 16:26 JST +0900 admin | Sign out

DASHBOARD NETWORKING **OPTIMIZATION** REPORTS ADMINISTRATION HELP

Dashboard ?

Welcome to the Management Console for SH1!

System Status

System Uptime: 1 day, 4 hours System Health: **Healthy**

Service Uptime: 22 hours, 24 minutes SCC: Not Managed

Temperature: 53°C

Optimized LAN Throughput Over Last Week

600.0 Mbps

Network Services

General Service Settings

In-Path Rules

Peering Rules

Transport Settings

Service Ports

SAAS

SaaS Accelerator

Legacy Cloud Accelerator

ACTIVE DIRECTORY

Domain Join

Auto Config

**Service Accounts**

DATA REPLICATION

FCIP

SRDF

SnapMirror

Data Store

Performance

PROTOCOLS

CIFS (SMB1)

SMB2/3

CIFS Prepopulation

HTTP

Oracle Forms

MAPI

NFS

Lotus Notes

Citrix

SSL

SSL Main Settings

Secure Peering (SSL)

Certificate Authorities

CRL Management

Advanced Settings

Secure Peering IPSec

BRANCH SERVICES

Caching DNS

Bandwidth Summary Over Last Week

⑥ Kerberos 欄の[Add a New User]をクリックします。

Kerberos

Replication Users:

Domain	User Domain	Username	DC Name
No replication users.			

☐ Enable Kerberos support for restricted trust environments

- ⑦ 赤枠に設定値を入力し、「Add」をクリックします。

## Kerberos

### Replication Users:

☒ Add a New User ☐ Remove Selected

Active Directory Domain Name:	RV.LOCAL
User Domain:	RV.LOCAL
Username:	rvbduser
Password:	*****
Password Confirm:	*****
<input type="checkbox"/> Enable RODC Password Replication Policy Support	
DC Name:	
<b>Add</b>	

- ⑧ Apply をクリックします。

### Kerberos

**Replication Users:**

☒ Add a New User ☐ Remove Selected

<input type="checkbox"/>	Domain	User Domain	Username	DC Name
<input type="checkbox"/>	RV.LOCAL	RV.LOCAL	rvbduser	--

☐ Enable Kerberos support for restricted trust environments

**Apply**

- ⑨ ADMINISTRATION → Services をクリックします。

SH1 / SteelHead™

ip 10.177.125.3 • CX770 (CX770H) (x86\_64) • 9.8.0 • uptime 1 day, 5 hours • Wed 16:53 JST +0900 admin | Sign out

DASHBOARDNETWORKINGOPTIMIZATIONREPORTSADMINISTRATIONHELP

Dashboard ?

Welcome to the Management Console for SH1!

System Status

System Uptime: 1 day, 5 hours

Service Uptime: 22 hours, 52 minutes

Temperature: 53°C

System Health: **Healthy**

SCC: Not Managed

MAINTENANCE

Services

Scheduled Jobs

Licenses

Software Upgrade

Reboot/Shutdown

SECURITY

General Settings

User Permissions

Password Policy

RADIUS

TACACS+

SAML

Secure Vault

Management ACL

Web Settings

REST API Access

SYSTEM SETTINGS

Announcements

Alarms

Date/Time

Monitored Ports

SNMP Basic

SNMP v3

SNMP ACLs

Email

Logging



My Account

Configurations

- ⑩ 「Restart」をクリックします。

## Services

Maintenance > Services ?

 Save to Disk  Restart Services

### Optimization Service

Restarting the optimization service will disrupt existing network connections being proxied through this appliance. Restarting may take a few seconds.

☐ Clear Data Store *(applies only to starting and restarting the service)*

Status: **running**

Stop

Start

Restart

- ⑪ 以下のように「Save to Disk」と表示されている場合、クリックし Save します。

DASHBOARD NETWORKING OPTIMIZATION REPORTS ADMINISTRATION HELP

 Save to Disk  Restart Services

## 2.7 機能の正常性確認

- ① ブラウザから管理画面を開き、SteelHead アプライアンスへログインします。

アクセス先 HTTP or HTTPS ://リストア後の IP アドレス

ユーザ名： お客様管理 パスワード： お客様管理

- ② REPORTS → Alarm Status をクリックします。

DASHBOARD		NETWORKING	OPTIMIZATION	REPORTS
NETWORKING	OPTIMIZATION	DIAGNOSTICS	BRANCH SERVICES	
Current Connections	Optimized Throughput	Alarm Status	DNS Cache Hits	
Connection History	Bandwidth Optimization	CPU Utilization	DNS Cache Utilization	
Connection Forwarding	Peers	Memory Paging	REPORT DATA	
Outbound QoS	HTTP	TCP Memory		
Inbound QoS	Live Video Stream Splitting	Disk Status	Export	
Secure Transport	NFS	System Details	RULES STATISTICS	
Top Talkers	SRDF	Network Health Check		
Traffic Summary	SnapMirror	Domain Health Check	In-Path Rule Statistics	
WAN Throughput	SSL	Benchmarks		
Application Statistics	SharePoint	User Logs		
Application Visibility	Data Store Status	User Logs Downloads		
Interface Counters	Data Store SDR-Adaptive	System Logs		
TCP Statistics	Data Store Disk Load	System Logs Downloads		
		System Dumps		
		Process Dumps		
		TCP Dumps		

③ 「Status」に異常（エラー等）がないことを確認します。

Alarm Status Diagnostics > Alarm Status ?

Save to Disk

Restart Services

Alarm	Status
<div><div></div>Admission Control</div>	OK
Asymmetric Routing	OK
<div><div></div>Connection Forwarding</div>	OK
CPU Utilization	OK
<div><div></div>Data Store</div>	OK
<div><div></div>Disk Full</div>	OK
Domain Authentication Alert	OK
<a href="#">Domain Join Error</a>	OK
<div><div></div>Hardware</div>	OK
<a href="#">Inbound QoS WAN Bandwidth Configuration</a>	OK
<div><div></div>Licensing</div>	OK
<div><div></div>Link Duplex</div>	OK
<div><div></div>Link I/O Errors</div>	OK
<div><div></div>Link State</div>	Disabled
Memory Paging	OK
Neighbor Incompatibility	OK
Network Bypass	OK
<a href="#">NFS V2/V4 Alarm</a>	OK
<div><div></div>Optimization Service</div>	OK
<a href="#">Outbound QoS WAN Bandwidth Configuration</a>	OK
Path Selection Path Down	OK
Network Bypass	OK
<a href="#">NFS V2/V4 Alarm</a>	OK

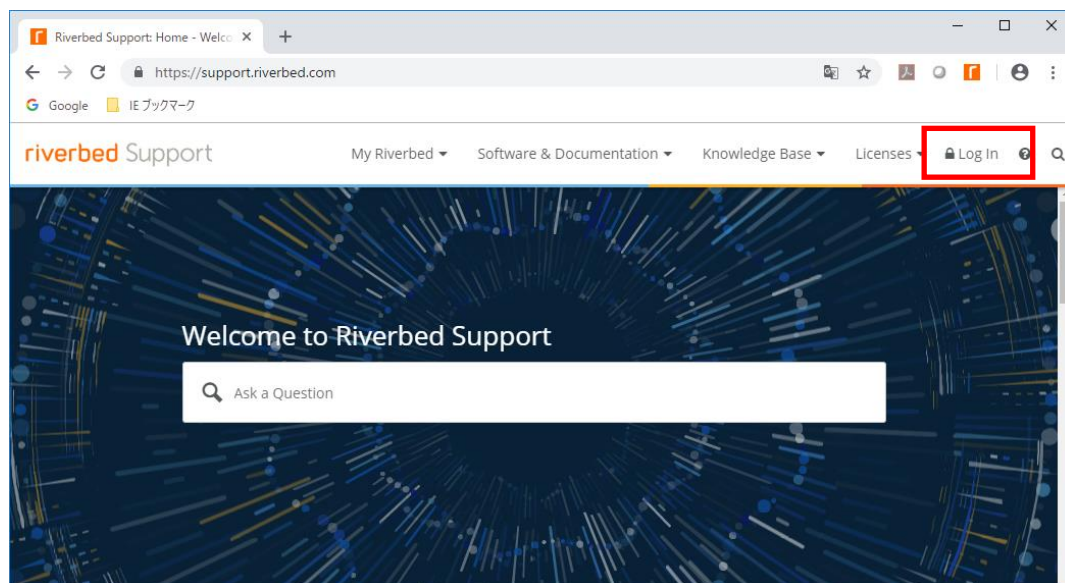
### 3 ソフトウェアのバージョンアップ

※ソフトウェアバージョンアップを実施する前に必ず以下を準備ください。

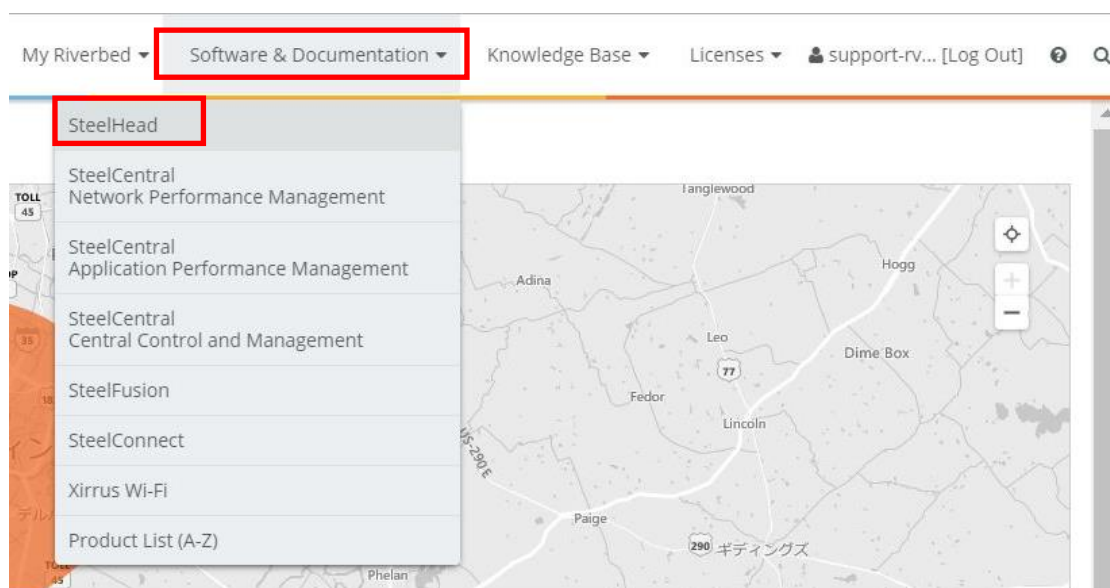
- ① [config][証明書（SSL 通信の最適化を有効にしている場合）]のバックアップを取得してください。
- ② ソフトウェア バージョンアップのステップを確認（お使いいただいておりますバージョンによっては、目的のバージョンになるまでに数回のバージョンアップを実施する必要があります。以下サイトにて確認いただけますので、バージョンアップする際、必ずご確認ください。）

<https://support.riverbed.com/content/support/software/steelhead/cx-appliance.html>

- ① サポートサイト（<https://support.riverbed.com/>）にアクセスし、「Log In」をクリックします。

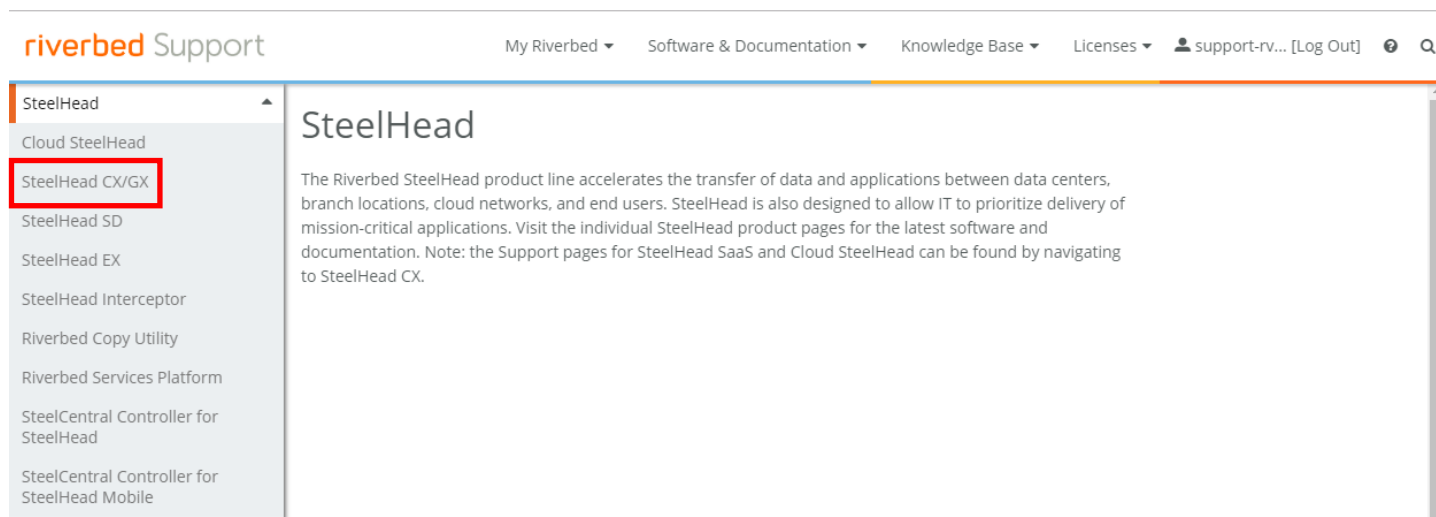


- ② Software & Documentation → SteelHead をクリックします。





③ SteelHead の場合は、以下をクリックします。



④ From Version:に現在のバージョン、To Version:にアップデートしたい Software を入力し、「Submit」をクリックします。

The screenshot shows a 'Find Software Upgrade' form. The title is 'Find Software Upgrade:' followed by the instruction 'Use the upgrade tool to find recommended upgrade paths between versions.' Below this, there are two dropdown menus labeled '\*From Version:' and '\*To Version:'. Both dropdown menus are currently set to '--Select--' and are highlighted with red rectangles. To the right of these dropdowns is an orange 'Submit' button.

- ⑤ 以下は、v8.6.1a から v9.8.0a にアップグレードした時の結果です。赤字にて、バージョンアップに必要な適用順序が判ります。  
例 v9.8.0a にあげるには、v9.1.3 を先に適用する必要があります。

## Find Software Upgrade:

Use the upgrade tool to find recommended upgrade paths between versions.

\*From Version: 8.6.1a ▼

\*To Version: 9.8.0a ▼

Submit

Upgrade path from 8.6.1a to 9.8.0a: 8.6.1a → 9.1.3 → 9.8.0a

Software Description	Models	Release	Downloads
SteelHead Appliance Software Image - Includes support for FIPS mode Version 9.8.0a (64-bit)	Models CX series Virtual Steelhead, next generation VCX, Steelhead CX 255, Steelhead CX 3070, Steelhead CX 5070, Steelhead CX 570, Steelhead CX 7070, Steelhead CX 770, SteelHead GX 10000	Nov 14, 2018	Software (346.9 MB) Checksum *Alert*
SteelHead Appliance Software Image - Includes support for FIPS mode Version 9.1.3 (64-bit)	Models 1050, 2050, 5050, 6050, 7050, Steelhead CX 1555, Steelhead CX 255, Steelhead CX 3070, Steelhead CX 5055, Steelhead CX 5070, Steelhead CX 570, Steelhead CX 7055, Steelhead CX 7070, Steelhead CX 770	Jun 1, 2016	Software (244.7 MB) Checksum *Alert*
Virtual SteelHead Appliance Software (Hyper-V) Version 9.1.3 (64-bit)	Models CX series Virtual Steelhead	Jun 1, 2016	Software (677.1 MB) Checksum *Alert*

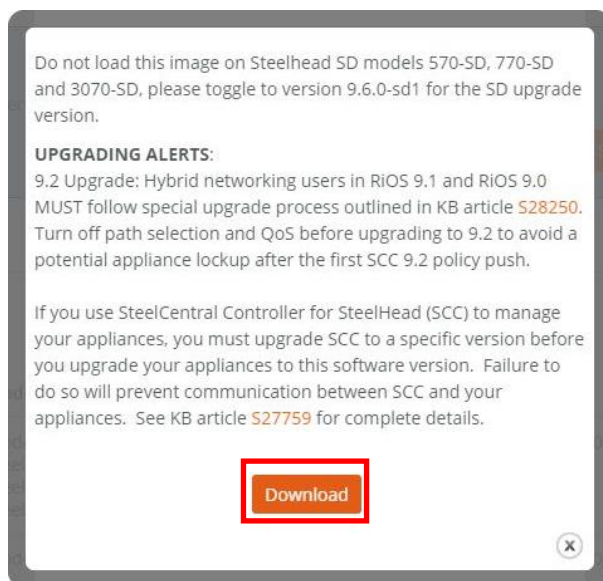
- ⑥ 製品種別やバージョン、製品型番に誤りないか確認し、「Software」をクリックします。

SteelHead Appliance Software Image - Includes support for FIPS mode Version 9.1.3 (64-bit)	Models 1050, 2050, 5050, 6050, 7050, Steelhead CX 1555, Steelhead CX 255, Steelhead CX 3070, Steelhead CX 5055, Steelhead CX 5070, Steelhead CX 570, Steelhead CX 7055, Steelhead CX 7070, Steelhead CX 770	Jun 1, 2016	Software (244.7 MB) Checksum *Alert*
---	---	-------------	--

※製品種別には Virtual SteelHead などもあります。

- ⑦ 「Download」をクリックし、ファイルを任意の場所に保存します。

※必要なバージョンをすべてダウンロードします。



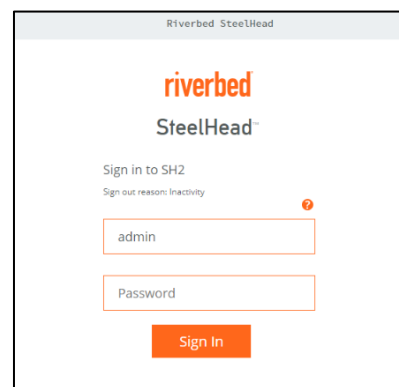
例 ファイル名 image\_rbt\_sh\_9\_1\_3\_x86\_64.img など

- ⑧ SteelHead の管理画面にログインします。

アクセス先 HTTP://SteelHead の IP アドレス

ユーザ名： お客様管理

パスワード： お客様管理



- ⑨ ADMINISTRATION → Software Upgrade をクリックします。

※Software バージョン 8 系をお使いの場合、Configure → Maintenance → Software Upgrade

DASHBOARD	NETWORKING	OPTIMIZATION	REPORTS	ADMINISTRATION	HELP
		MAINTENANCE	SECURITY	SYSTEM SETTINGS	
		Services	General Settings	Announcements	
		Scheduled Jobs	User Permissions	Alarms	
		Licenses	Password Policy	Date/Time	
		Software Upgrade	RADIUS	Monitored Ports	
		Reboot/Shutdown	TACACS+	SNMP Basic	
			SAML	SNMP v3	
			Secure Vault	SNMP ACLs	
			Management ACL	Email	
			Web Settings	Logging	
			REST API Access	My Account	
				Configurations	

- ⑩ 画面内の Form Local File に先程ダウンロードしたファイルをアップロードし、Install をクリックします。

SH1 SteelHead

ip 192.168.100.1 • CX770 (CX770H) (x86\_64) • 9.6.1 • uptime 6 days, 23 hours • Tue 18:56 JST +0900 admin | Sign out

DASHBOARD NETWORKING OPTIMIZATION REPORTS ADMINISTRATION HELP

Software Upgrade Maintenance > Software Upgrade ?

Save to Disk Restart Services

Software Upgrade

Booted Version:  
rbt\_sh 9.6.1 #88 2017-08-31 01:12:50 x86\_64

Backup Version:  
rbt\_sh 8.6.3-nic1 #3 2016-01-25 20:00:00 x86\_64

Switch to Backup Version

Install Upgrade

☐ From URL

☐ From Riverbed Support Site

Image check upgrades failed. Couldn't resolve host 'api.licensing.riverbed.com'

☒ From Local File

ファイルを選択 image\_rbt\_...86\_64.img

☐ Schedule Upgrade for Later

Date: 2018/10/23 (YYYY/MM/DD) Time: 18:56:49 (HH:MM:SS)

Install

- ⑪ 画面上部にメッセージが表示されるので、Reboot the appliance をクリックします。

Successfully installed upgrade image. Please reboot the appliance to complete the upgrade.

MAINTENANCE Services

- ⑫ Reboot をクリックし、再起します。

DASHBOARD NETWORKING

Reboot/Shutdown Maintenance > Reboot/Shutdown ?

Reboot or Shut Down

Rebooting or shutting down will disrupt existing network connections being proxied through this appliance. Reboot and shut down operations may take a few minutes.

☐ Clear Data Store

☐ Schedule for Later

Time: 2018/10/23 19:02:03

Reboot Shut Down

- ⑬ 目的のバージョンになるまで、手順[⑨～⑫]を繰り返します。

- ⑭ ADMINISTRATION → Software Upgrade をクリックし Booted Version が更新されていることを確認します

## Software Upgrade Maintenance > Software Upgrade ?

---

### Software Upgrade

**Booted Version:**  
rbt\_sh 9.8.0 #3 2018-06-29 16:32:09 x86\_64

**Backup Version:**  
rbt\_sh 9.6.1 #88 2017-08-31 01:12:50 x86\_64

[Switch to Backup Version](#)

## 4 system dump 取得方法

system dump により、機器の状態を確認します。

ブラウザから管理コンソールにログインし、下記の手順にて、System Dump の取得をお願いします。

- 
- ① Administration → System Settings → Logging へ移動します。  
※"Minimum Severity" を "info" に変更し、「Apply」を押します。
  - ② Reports → Diagnostics → System Dumps へ移動します。  
※Include Statistics と Include All Logs のどちらもチェックしてください。
  - ③ [Generate System Dump] をクリックし、生成します。
  - ④ System Dump ファイルは sysdump-"hostname"-YYYYMMDD-hhmmss.tgz のように tgz 形式で作成されます。sysdump-"hostname"-YYYYMMDD- と付いたファイル名が表示されますのでそれをクリックします。  
クリックすると下記表示されますので、～dump file: Download の Download を  
クリックするとファイルのダウンロードになります。  
ローカルの PC へ System Dump ファイルをダウンロードのうえ、弊社の担当にご連絡の上、  
共有サイトへアップロードをお願いいたします。
  - ⑤ System Dump の取得後は、手順 1 で変更した"Minimum Severity" の設定を"notice" に戻してください。
- 

## 5 ハードウェア・ソフトウェア サポート終了ポリシー

- ① Riverbed 社製品のハードウェアおよびソフトウェアのサポートポリシーは、以下 URL より確認頂けます。  
[https://support.riverbed.com/content/support/about\\_support/end\\_of\\_life\\_policy.html](https://support.riverbed.com/content/support/about_support/end_of_life_policy.html)
- ② ハードウェアおよびソフトウェアのサポート終了製品一覧  
[https://support.riverbed.com/content/support/eos\\_eoa.html](https://support.riverbed.com/content/support/eos_eoa.html)