管理者ガイド

Reflection for Secure IT

Server for Windows

バージョン 8.2 SP1

〔 02 版： 改訂日　2017 年 9 月 26 日 〕

#JMN-01816H-0217I

目次

1. はじめに

1.1 適用

本マニュアルは、Reflection for Secure IT　Server for Windows（以後「RSIT Windows サーバ」と省略）バージョン 8.2 SP1 について、導入やその使用方法について解説したものです。
導入後、デフォルト設定のままでもそのままお使い頂けますが、設定内容のセキュリティ上の効果をご理解頂き、お客様利用環境に適した正しい設定と運用を期待しています。
日本国内では北米ほど PKI 連携での使用が普及していない関係で、英文マニュアルにおける PKI や PKI Service Manager についての説明は割愛しました。必要時は、本社ドキュメントサイト <http://support.attachmate.com/manuals/rsit_win_server.html>上の英文マニュアルを参照下さい。

関連ファイル/フォルダ名称、プログラム表示、サーバサービス名称の中に会社名が含まれます。今回の 8.2 SP1 から Micro Focus 社(英国)に変更されました。従来より ″F-Secure″、″WRQ″、″Attachmate″ の社名が使われてきました、F-Secure 社から WRQ 社への製品移管、WRQ 社 ⇒ AttachmateWRQ 社 ⇒ Attachmate 社という社名変遷、 Micro Focus 社による Attachmate 社買収というこれまでの開発元事情によります。従来同様、一貫した開発とサポート体制により継続対応してまいりますので、ご安心してご使用下さい。

1.2 SSH の概要

telnet によるリモートログインや FTP によるファイル転送等の平文による通信では、″盗聴″、″なりすまし″、″改ざん″といった不正行為を受ける危険性が存在します。SSH (Secure Shell)は、″暗号化″、″認証″、″データの完全性保証″により、これら悪意ある行為からパスワードや通信データを確実に保護します。

SSH はクライアント機能とサーバ機能で構成されます。クライアント側は、接続の起点となり、利用者に対しユーザインターフェースや各種コマンド、オプションを提供します。サーバ側は、常に待ち受けし、デーモンにより SSH 機能を完結するサービスを提供します。またサーバ側の設定内容(Configuration)により運用環境やクライアントからのアクセス制限等を指定します。

本製品 RSIT Windows サーバ は、Windows OS 向けに SSH サーバ機能を提供します。

リモートからのターミナルログインが SSH の基本機能となります。さらに接続確立したセキュアな共通のセッションを利用し、リモートコマンド、scp(セキュアファイルコピー)、SFTP(セキュアファイル転送)、TCP ポート転送等の各種 SSH 標準機能を提供します。
リモートコマンドは、クライアント側で投入したコマンドをリモートホスト上で実行し、そのリターンコードで結果を判定します。
scp は 従来の rcp と類似のコマンド書式とオプションを用意し、rcp からの置き換えとして用意しました。

SFTP は、FTP と類似のコマンド、オプション、専用サブコマンドを用意し、FTP からの置き換えとして用意しました。
TCP ポート転送は TCP 上のアプリケーション通信をトネリングし、いわゆる VPN を実現します。

これら機能は、利用者が対話的にコマンド操作して利用するほかに、スクリプト/プログラム処理による自動実行を可能とし、お客様構築システムの組み込み部品として多く利用されています。

1.3 動作環境

(1) システム要件

(a) サポート OS

・Windows Server 2012 R2 (x86-64)
・Windows Server 2012 (x86-64)
・Windows Server 2008 R2 (x86-64)
・仮想化プラットフォーム VMware vSphere Hypervisor(ESXi)上の上記ゲスト OS

注記：

①8.2 SP1 から Windows Server 2008 と Windows 7 の正式サポートを終了しました。
②Windows Server OS の Server Core だけでは動作しません。
必ずフルインストール環境に導入下さい。
③Windows 同時使用ユーザ数/接続クライアント数等の Windows ライセンス契約は遵守下さい。
④動作条件とは別に、Windows 脆弱性対策の観点から、常に OS の最新 SP(サービスパック)ならびに アップデートを適用することを強く推奨します。

(b) 必要プログラム

・Microsoft Visual C++ 2013 Redistributable Package (x64)
・Microsoft XML 6.0 parser
インストール時に OS に存在しない場合は、セットアッププログラムが自動検知し、自動的にインストールウィザード処理へ移行し必要プログラムの追加インストールを実施します。

2. 導入

2.1 導入前の確認事項

(1) インストールプログラム

・インストールプログラムファイル名称：″rsitservwin-8.2.1.1079-wx64.exe″

今回 8.2 SP1 ですが、導入のために 8.2 を事前導入する必要はありません。

8.2 SP1 インストールプログラム単独で全機能を導入可能です。

(2) Windows OS の再起動

RSIT Windows サーバプログラムインストール直後に Windows OS の再起動が必須です。ウィザード画面の要求に従い操作再起動します。

(3) インストール操作ユーザ

ローカル管理者ユーザアカウントから必ずインストールします。

(4) バージョンアップ時の旧バージョンの処理（2.2 項 で詳述）

バージョンアップは、旧バージョンへの上書きインストール、旧バージョンの事前アンインストール、いずれも可能です。

(Windows「プログラムと機能」による旧バージョンのアンインストールの際に、プログラムファイル以外のサーバホスト鍵、設定情報、ユーザ認証用登録公開鍵 等は、削除されずに残ります。)

今回､プログラムインストール先と設定ファイル保存先が､社名変更にともない″Attachmate″フォルダから″Micro Focus″フォルダへ変更されました。

インストールの際に存在する旧設定ファイル等は、自動的に新フォルダへ移植されます。

2.2 導入上のポイント

新規インストールもバージョンアップも手順は ほぼ同一です。

RSIT Windows サーバ では、旧バージョンの設定ファイルが存在する場合、その内容を自動的に移行します。ただ 旧バージョンの移行対象は RSIT Windows サーバ 7.0 以降とし、それより前のバージョンからバージョンアップする場合は､参照用に従来の sshd2_config ファイルを事前に保存した上で、旧バージョンをアンインストール、合わせて手操作にて関連旧ファイルを削除します。設定は、新バージョンをインストール後に内容を確認しながら手操作にて再設定下さい。

手順説明の前に、製品仕様と動作上のポイントを示します。

(1) インストール先と関連ファイル保存先フォルダ（デフォルト指定時）

	Ver	
プログラム インストール先フォルダ	**8.2 SP1**	″C:¥Program Files¥**Micro Focus**¥RSecureServer¥″
	7.0～8.2	″C:¥Program Files¥**Attachmate**¥RSecureServer¥″
関連ファイル(*) 保存先フォルダ (*)・設定ファイル： ″rsshd_config.xml″ ・ホスト鍵： ″hostkey, hostkey.pub″	**8.2 SP1**	″C:¥ProgramData¥**Micro Focus**¥RSecureServer″
	7.0～8.2	1) Windows Server 2012, 2008, Windows 7 の場合 ″C:¥ProgramData¥**Attachmate**¥RSecureServer¥″ 2) Windows Server 2003 の場合 ″C:¥Documents and Settings¥All Users ¥Application Data¥**Attachmate**¥RSecureServer¥″

(2) バージョンアップ時 の処理内容

項目	処理内容
検知 旧 Ver の対処	旧 Ver プログラムは自動的にアンインストール。 旧 Ver 関連の設定ファイル、鍵ファイルは存続。
旧 Ver 検知時の 新 Ver インストール先	インストール時の指定インストール先 **[注記]**：インストール先をデフォルトから変更する場合は、前状態にかかわらずインストールの都度、明示的に指定します。
インストール直後の OS 再起動時の sshd サービス	OS 再起動後に sshd サービスを自動的に開始します。(*) (*) sshd サービス稼動状況の確認方法 a)設定画面を開き、設定画面上のステータス表示で確認 b)Windows タスクマネージャによるプロセス「rsshd.exe」確認

(3) インストール手順の概要

新規インストールも上書きインストールも、下記概要となります。

① 8.2 SP1 のインストール（詳細手順は 2.3 参照）

② Windows OS の再起動

③（設定と確認のため）手操作で sshd サービスを停止

④（必要に応じ）設定画面を通じてデフォルト設定内容から設定変更し、保存

⑤ 設定画面操作にて sshd サービスを再起動（OS の再起動は不要）

⑥ 動作確認

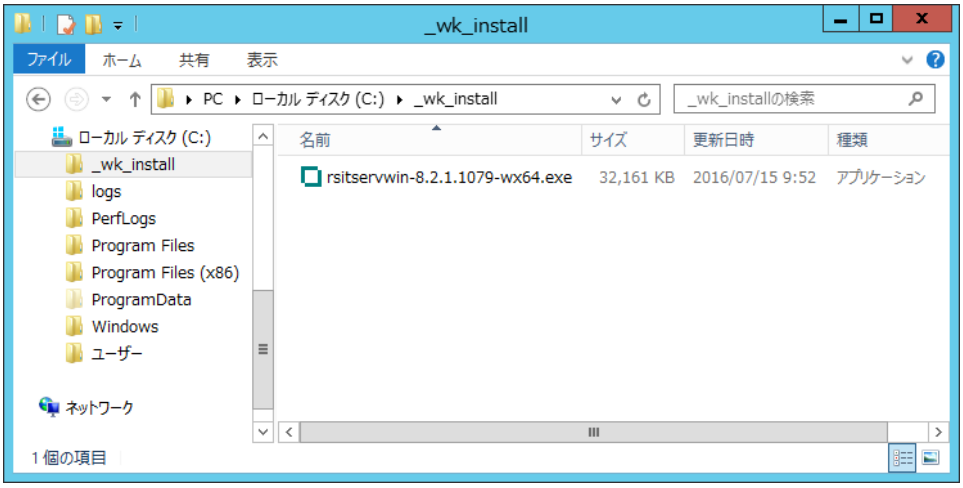
2.3 インストール操作詳細手順

以下、インストールプログラムファイル起動による操作手順について説明します。

SP(サービスパック)製品 CD、あるいは ダウンロード入手ファイルを使用し導入します。

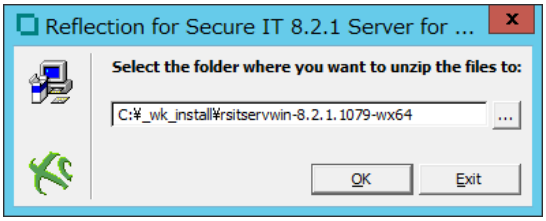
(1) インストールプログラムファイルの実行開始

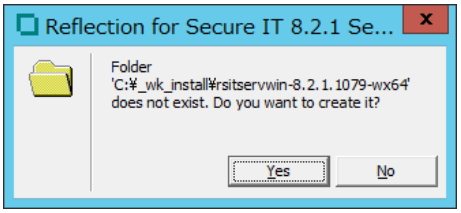
インストールプログラムファイル(例えば "rsitservwin-8.2.1.1079-wx64.exe")をローカルディスク上の任意のフォルダ下に置き、起動します。



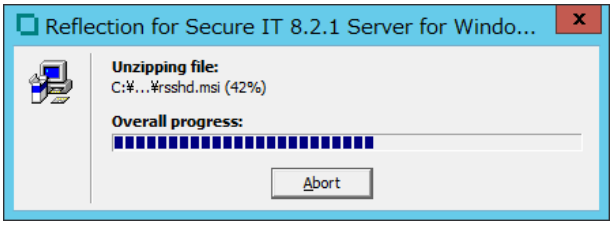
(2) インストールプログラムファイルの unzip 処理

unzip 先の確認画面を表示します。インストールプログラムファイルと同一の場所に同一名称の新規フォルダ作成の確認画面を表示しますので、そのまま[OK]ボタンをクリックし、次画面で[Yes] ボタンをクリックします。





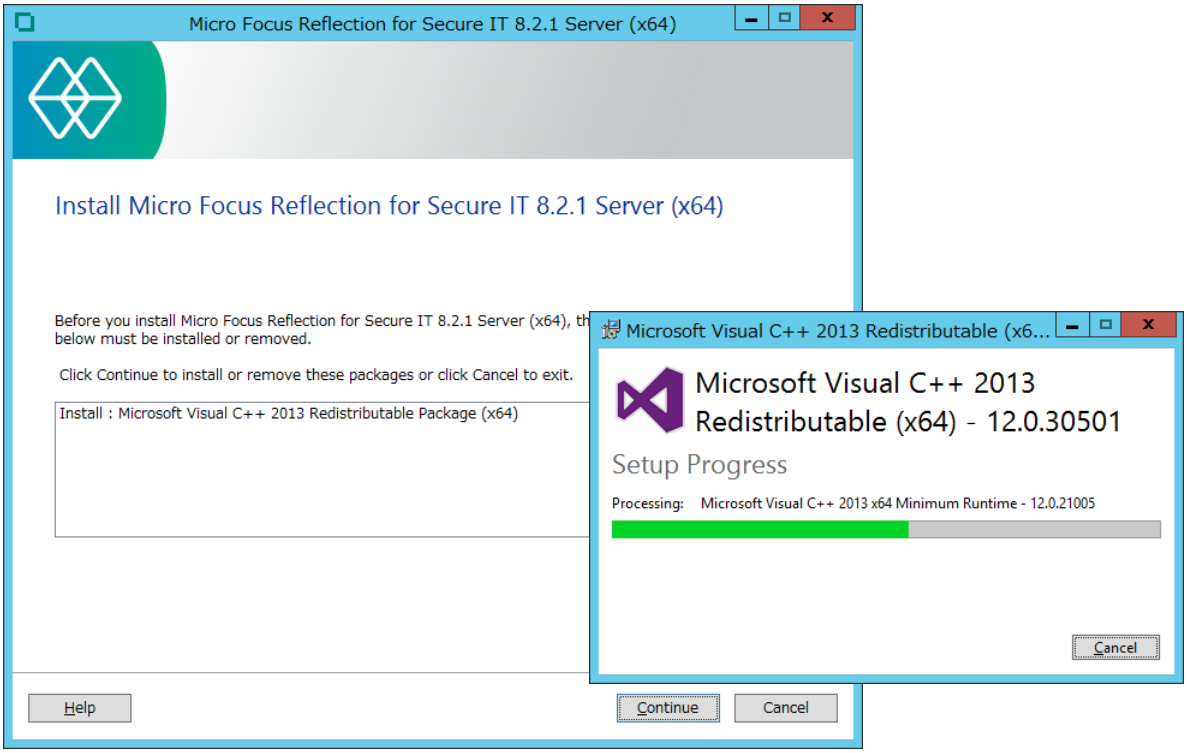
(しばらく、unzip 処理を続けます。)



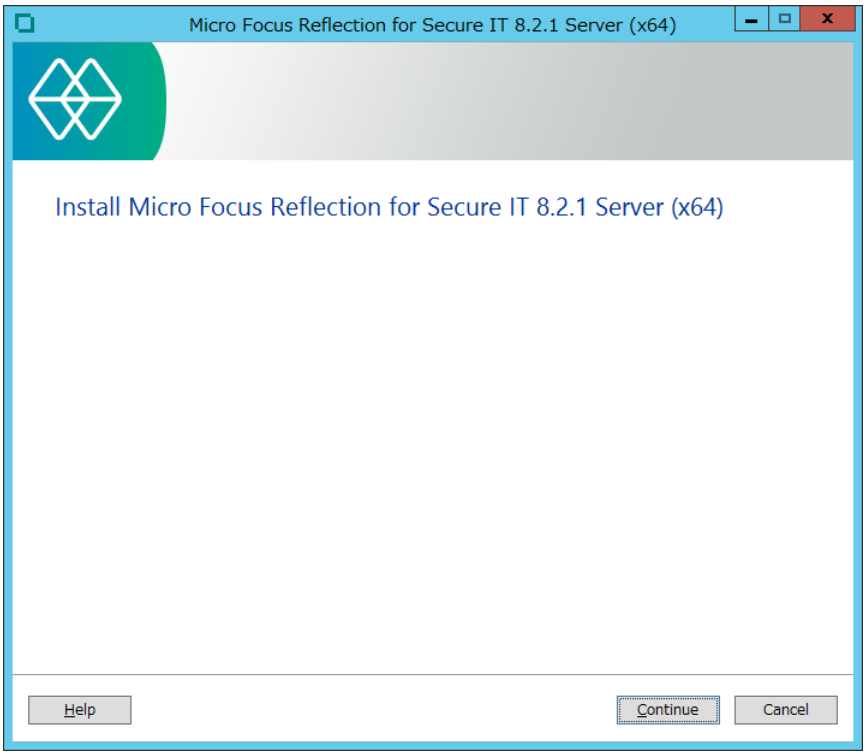
(3) 開始画面の表示

開始画面を表示します。導入マシン内に"Microsoft Visual C++ 2013 Redistributable Package (x64)"が事前に存在するかどうかで表示内容が変わりますが、指示に従い [Continue]ボタンをクリックし、処理を継続します。

(a) "Microsoft Visual C++ 2013 Redistributable Package (x64)"が事前に存在しない場合：

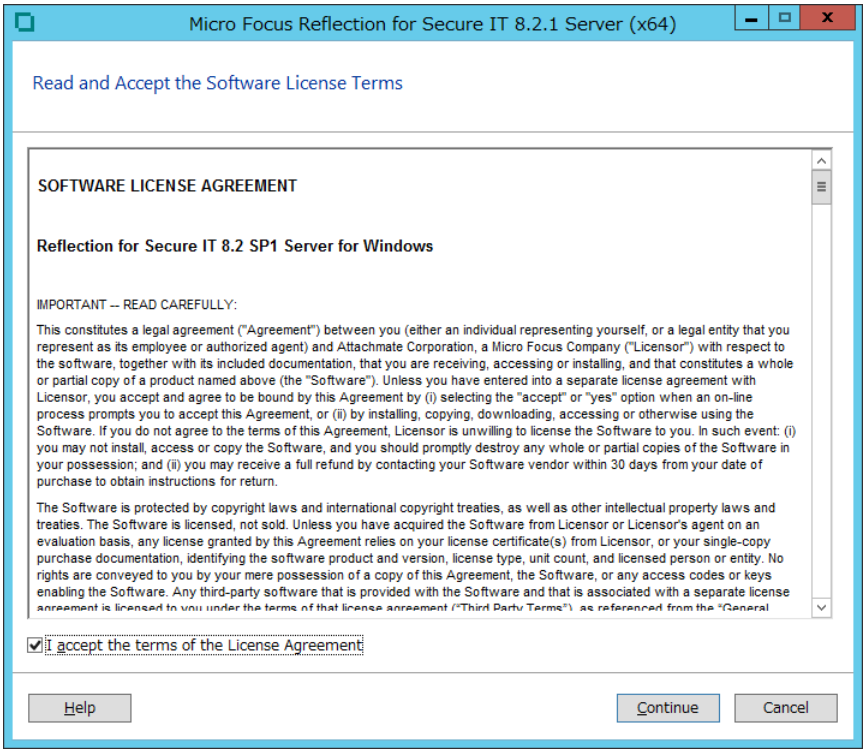


(b) "Microsoft Visual C++ 2013 Redistributable Package (x64)"が既に存在する場合：



(4) Software License Agreement（ソフトウェア使用許諾契約書)画面の表示

内容を確認し、チェックマークを入れ、 [Continue]ボタンをクリックします。



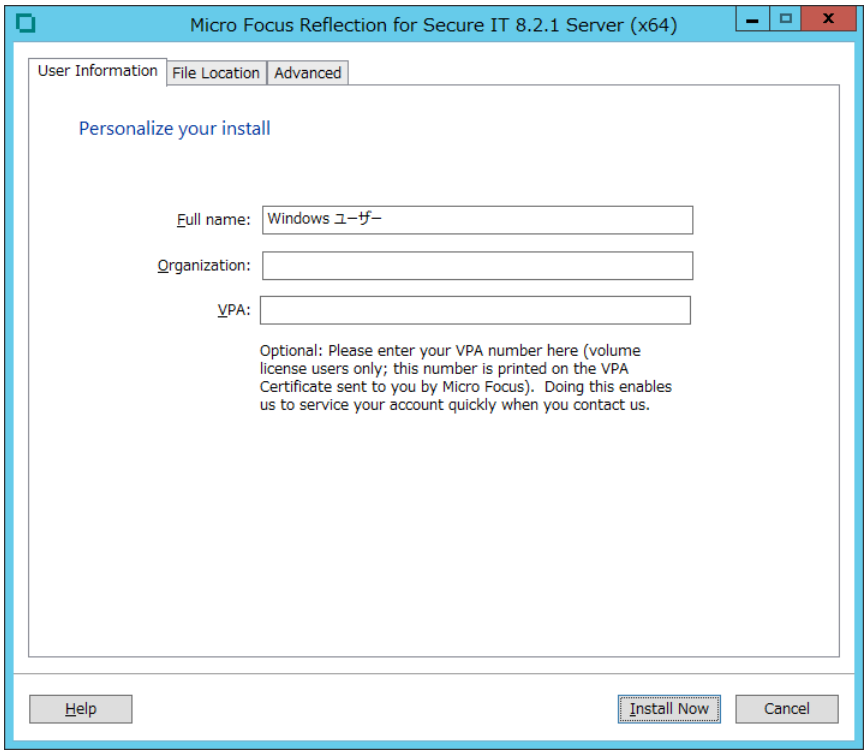
(5) インストール情報の入力

タブは３つあります。（全て未入力でも問題なく、正常に稼働します。）

確認後、[Install Now]ボタンをクリックし、先に進みます。

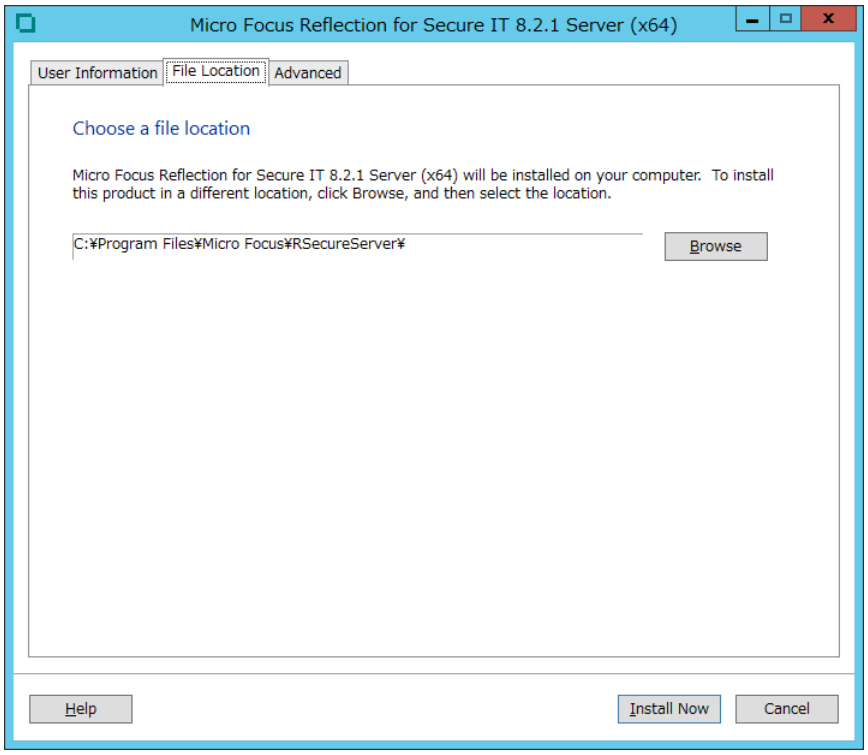
(5-1) [User Information]タブ画面からの入力

必要なお客様情報を入力します。



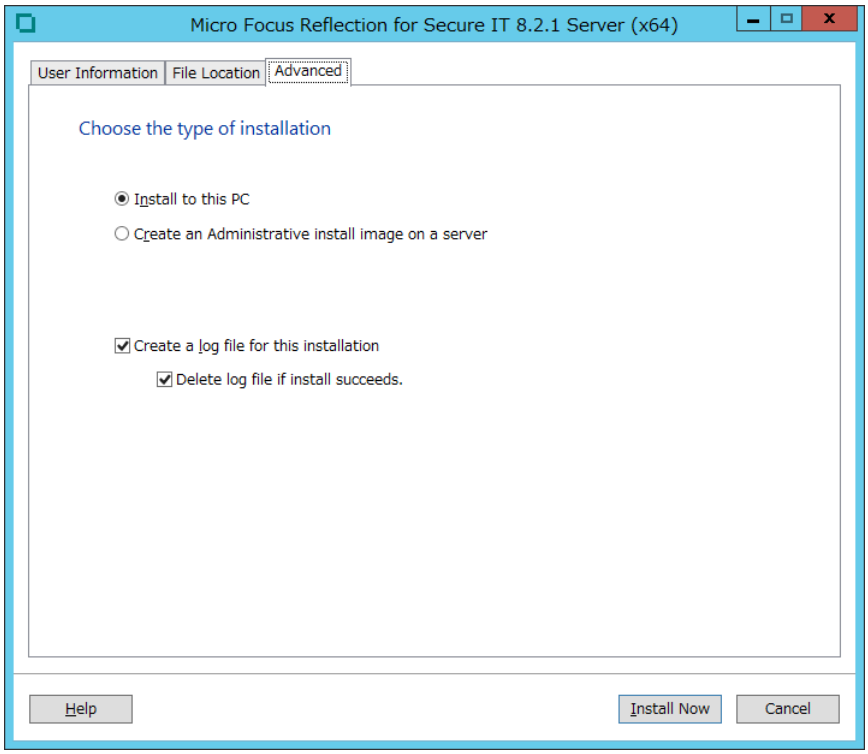
(5-2) [File Location] タブ画面からの入力

インストール先を指定します。デフォルトは、欄内に表示しているインストール先です。



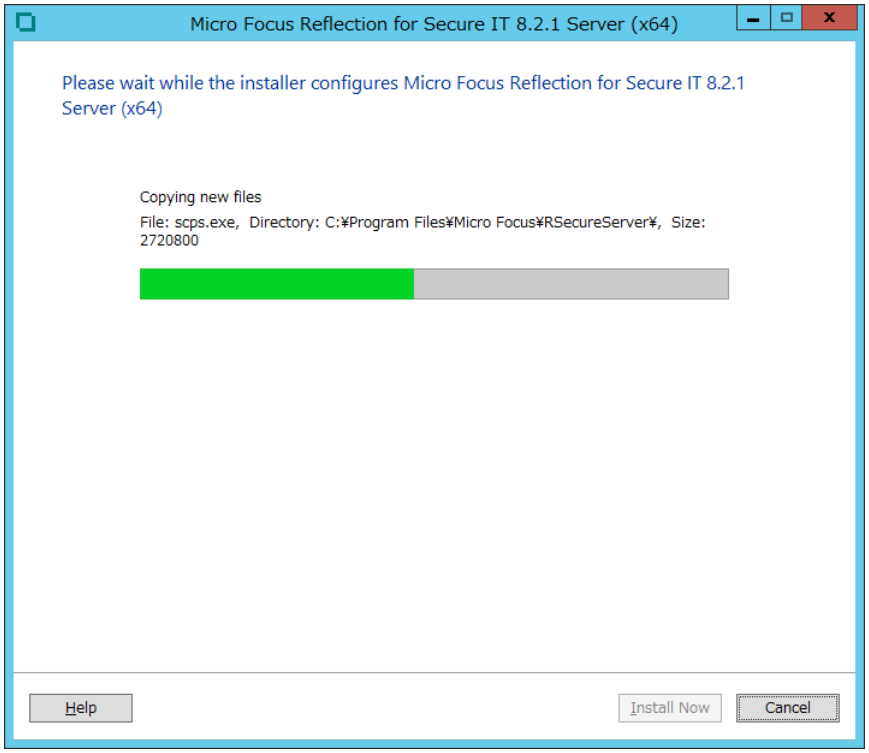
(5-3) [Advanced]タブ画面からの入力

本画面内の設定は、原則そのままとします。



(6) インストール処理の進行表示

処理中ですので、次の完了画面を表示するまで、しばらく待ちます。

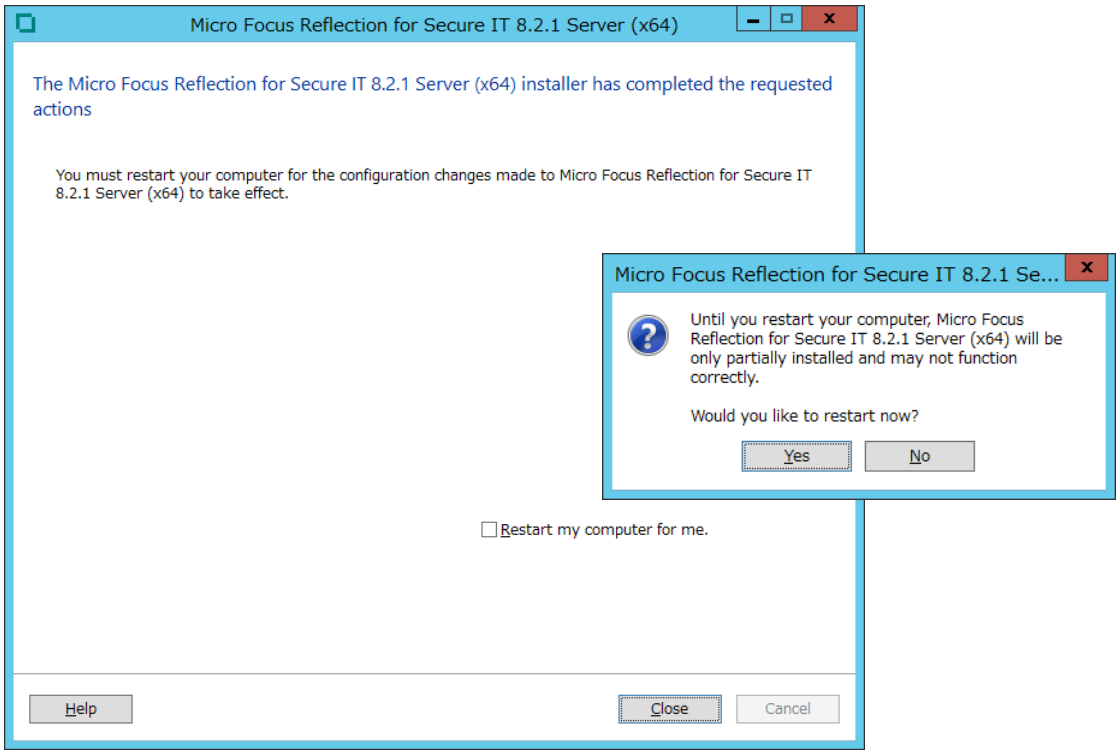


(7) インストール完了画面の表示

インストールが完了しました。Windows OS を再起動します。

"Restart my computer for me." にチェックマークを入れるか、入れずに[Close]ボタンをクリックし、OS 再起動確認画面で[Yes]ボタンをクリックすることで、OS が再起動します。

OS 再起動確認画面で[No]ボタンクリック時は、OS の再起動処理へは移行せずにインストール作業を終了しますが、その後の正常稼働のためには OS の再起動は必須となります。



(8) OS 再起動後の確認と操作

OS 再起動後、sshd サービスは自動的に開始します。

GUI 設定画面を開き、手操作にて sshd サービスを停止し(「3. 操作」参照)、GUI 設定画面から(デフォルト値からの)構成定義変更と内容確認を実施します。

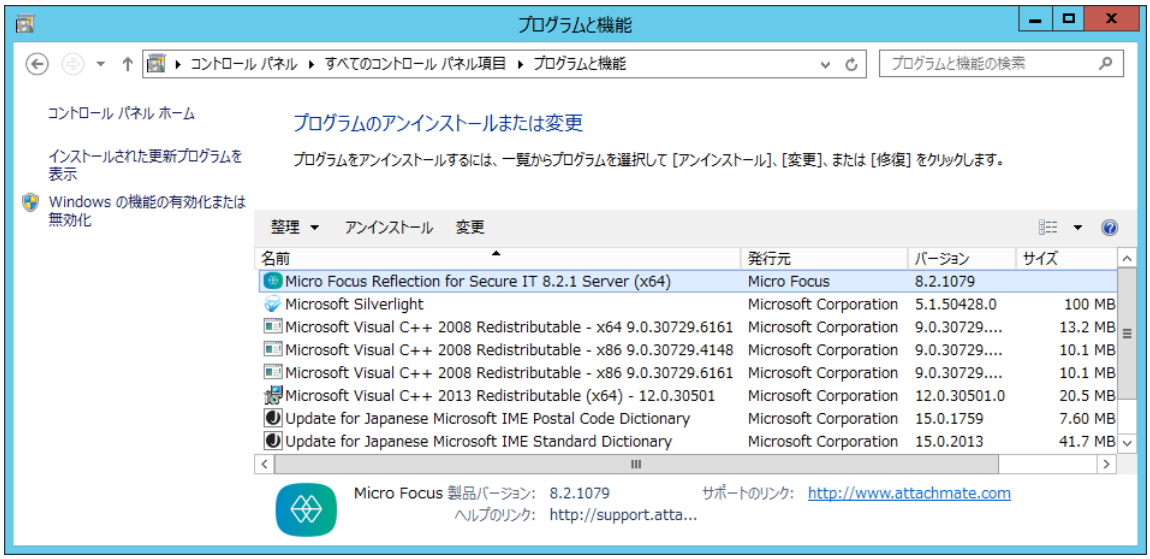
確認完了後、設定内容を保存の上、手操作にて sshd サービスを再開します。

2.4 アンインストール

(1) アンインストール操作

Windows の「プログラムと機能」からアンインストールします。

アンインストールにより、プログラムファイルは完全に削除されますが、設定ファイルとホスト鍵は削除されずに残ります。



3. 操作

3.1 設定画面からの操作設定

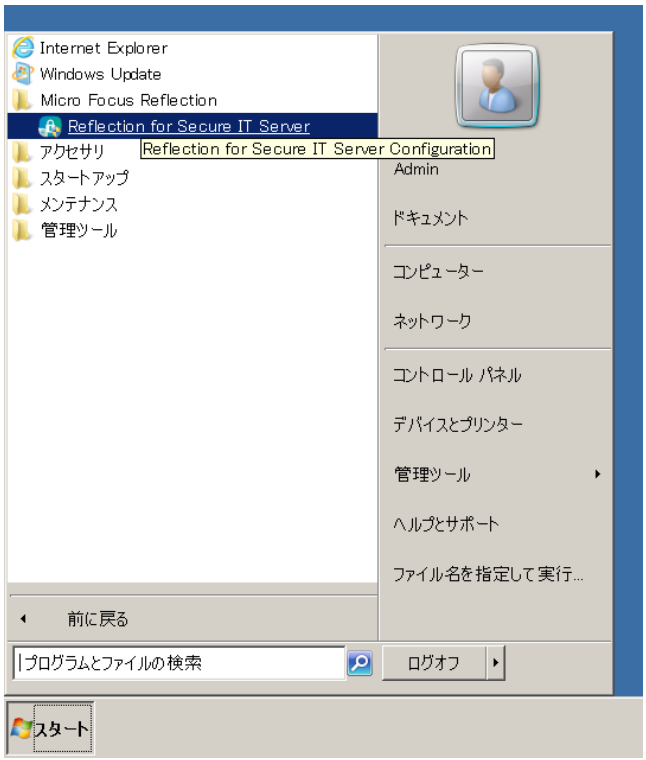
(1) 設定画面の表示

a) Windows Server 2008 R2 の場合

～ 画面左下 Windows [スタート]ボタンから順次選択。

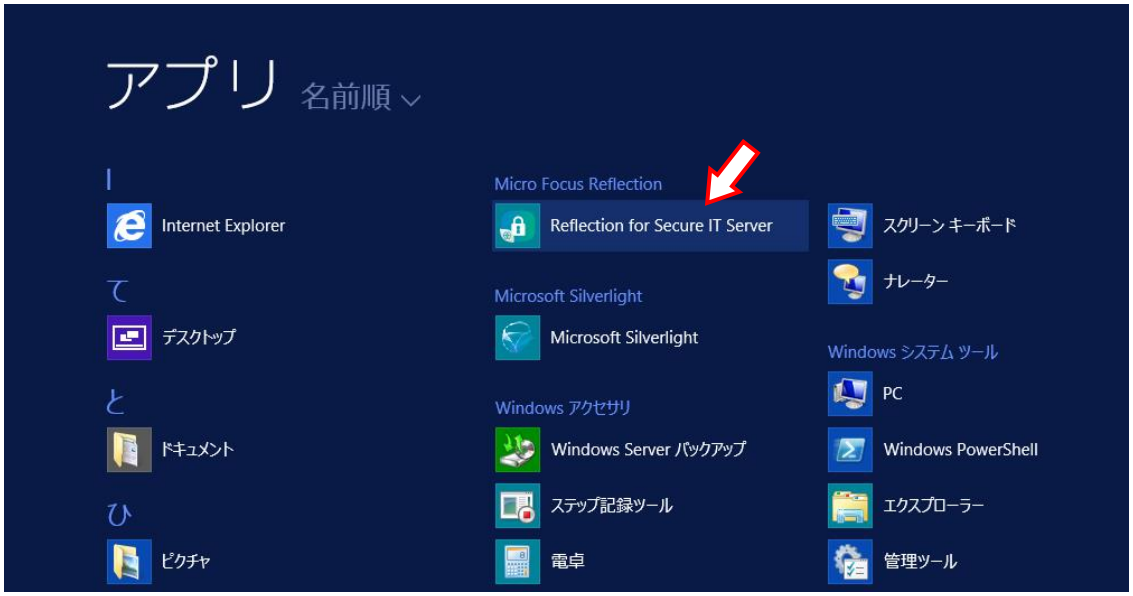
[スタート] > [すべてのプログラム] > [Micro Focus Reflection]

> [Reflection for Secure IT Server]



b) Windows Server 2012, 2012 R2 の場合

～ スタート画面下 アプリ画面内の [Reflection for Secure IT Server]を選択。



(2) 設定画面の構成

設定画面は大きく次の部位から構成されています。

部位	内容
メニュー	File、View、Action、Help の下に各種個別の指定があります。 ・File > Save Settings, Close ・View > Toolbar, Event Viewer, Latest Debug log File ・Action > Start Server, Stop Server, Restart Server, Configure Cluster, Restore All Default Settings, Restore Pane Defaults ・Help > Help Topics, Support Web, About Reflection
操作用ボタン	  ・左から [Save Settings] | [Event Viewer], [Latest debug log file], [Latest Audit log file] | [Start], [Stop], [Restart] ・右上に [Restore Pane Defaults]ボタン
[Status] タブ画面	・sshd サービスの状態を表示 ・RSIT Windows サーバの バージョン/ build とインストール先を表示
[Identity] タブ画面	・RSIT Windows サーバ ホスト鍵情報(所在, コメント, ダイジェスト)の表示 ・RSIT Windows サーバホスト証明書情報 ・Server version string (アクセス開始時にクライアントへ提示の自己情報)
[Configuration] タブ画面	・各種設定の指定/表示画面 (4. 設定 を参照)

(3) 設定画面上の基本操作

a) sshd サービスの開始と停止

設定画面上のボタン操作かメニュー選択により、sshd サービスを開始/停止/再起動します。

(*) Windows の[管理ツール] > [サービス]において、"Micro Focus Reflection for Secure IT Server" を同様に操作可能です。

b) 設定内容の保存と反映

[Configuration]タブ画面内の各種設定画面上で入力編集の後、[Save Settings] ボタン押下/メニュー選択によりその内容を"rsshd_config.xml"ファイルに上書き保存します。

設定内容により、変更保存後に直ぐに動作に反映するものと、sshd サービスの再起動後に反映するものが存在しますので、確実に設定内容を反映するためにも、変更保存後は必ず sshd サービスを再起動することを推奨します。

c) 設定内容のデフォルト値への変更

[Restore Pane Defaults]ボタン/メニューの選択 ⇒ 表示画面設定内容をデフォルトへ戻す

[Restore All Default Settings]メニューの選択 ⇒ 全画面設定内容をデフォルトへ戻す

画面内容をデフォルト値に戻した後に、[Save Settings]ボタン押下/メニュー選択により初めて、その内容が"rsshd_config.xml"ファイルに上書き保存されます。sshd サービスへの反映は上述通りです。

4. 設定

4.1 基本事項とその設定

デフォルト設定内容の状態でも、高いセキュリティ水準でのシステム運用が可能ですが、「4.2 設定詳細」の内容を理解され、お客様セキュリティポリシー運用方針に従った適切な設定をされ運用開始されることを推奨致します。

4.2 設定詳細

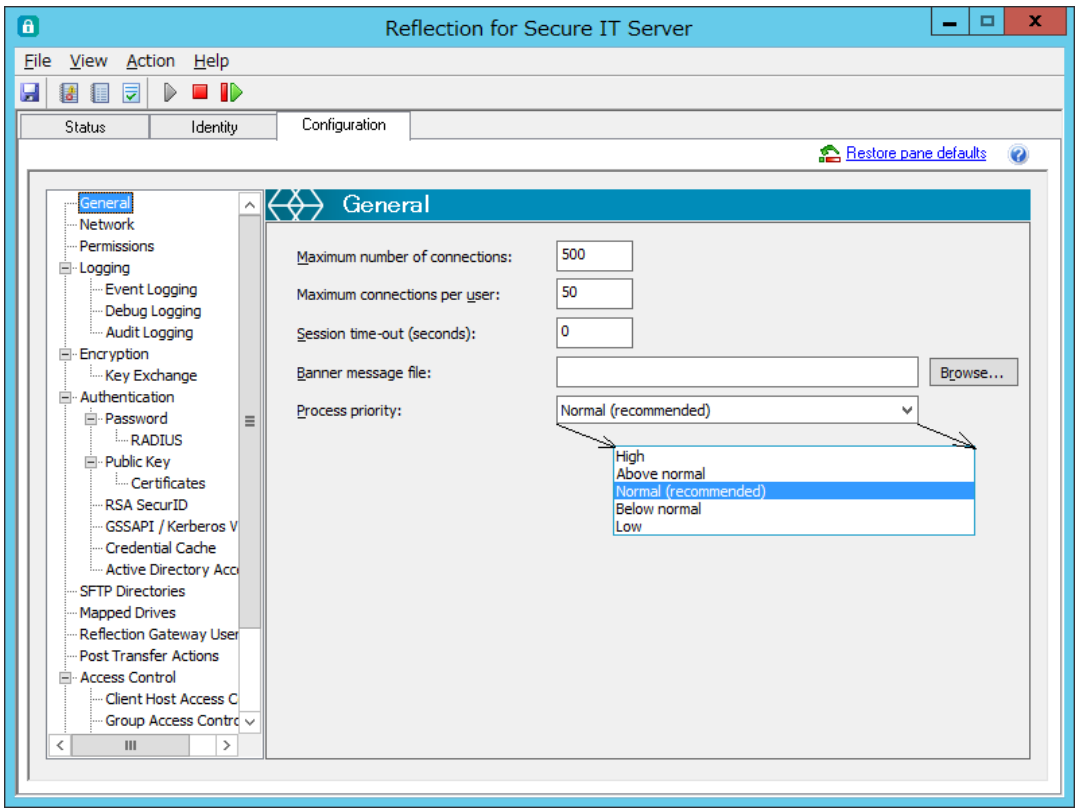
RSIT Windows サーバでは、全ての設定を GUI 設定画面を通じて指定し、"rsshd_config.xml"ファイルに保存します。
"rsshd_config.xml"ファイルは、デフォルトでは下記ディレクトリ下に保存され、メニュー操作（ Action > Set Data Folder）によりその保存先を変更可能です。

"C:¥ProgramData¥Micro Focus¥RSecureServer¥rsshd_config.xml "

注記：
直接 xml ファイルを編集することは思わぬエラーの原因ともなりますので、原則禁止です。
全て GUI 設定画面を通じて設定して下さい。

以下、各設定画面毎にその設定内容を説明します。
[Configuration] タブを選択し、画面左欄内のツリー状の選択メニューから対象設定画面名称を選択し表示します。

4.2.1 ［Genaral］設定画面



[Maximum number of connections:]

サーバに同時に接続可能な接続数の上限を設定します。

デフォルト値は ″500″。値″0″ は無制限を意味します。

connection reuse 動作時は、同一接続はチャネル多重され、connection 数 1 となります。

[Maximum connections per user:]

１ユーザ当たりの同時接続数の上限を設定します。値″0″ は無制限を意味します。

connection reuse 動作時は、同一接続はチャネル多重され、connection 数 1 となります。

[Session time-out (seconds):]

データが送受信されていないアイドル状態が継続した時に、指定時間経過後に接続を自動切断します。その指定時間を秒単位で入力します。値″0″の場合、機能無効となります。

[Banner message file:]

接続開始時にクライアント側に追加で表示するメッセージテキストファイルを指定します。

ファイルの文字コードは UTF-8 を使用し、それ以外の文字コードの時には自動変換されます。

注記：

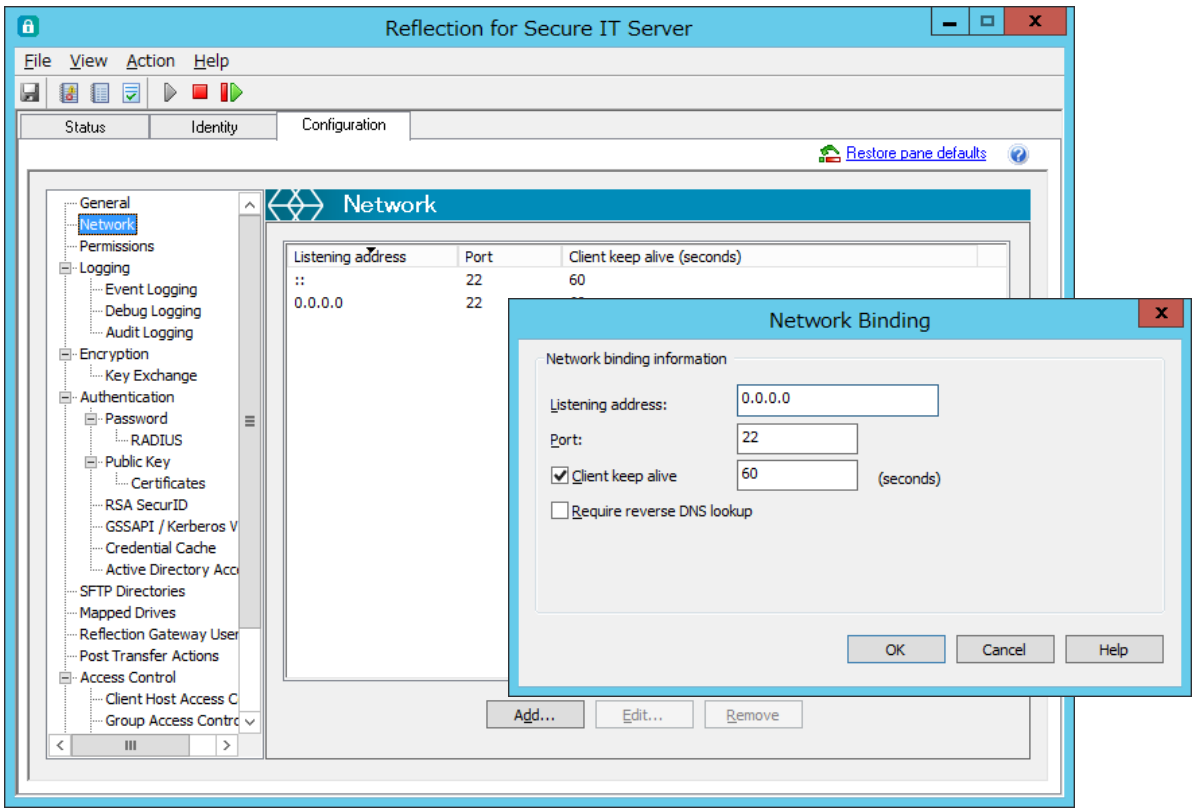
SSH クライアントによっては、バナー表示に未対応のものがあります。接続クライアントが本機能に全て対応していることを確認の上で指定下さい。

[Process priority:]

sshd サービスプロセスに対する「優先度の設定」が、Windows タスクマネージャからの指定と同様に本設定画面からも指定可能です。デフォルトは″Normal″です。

長時間ファイル転送時に他プロセスの処理低下影響を配慮した設定で、問題ない限りデフォルトのまま使用下さい。低優先の場合に、ファイル転送時間への影響も懸念され、注意が必要です。

4.2.2 [Network] 設定画面



sshd サービスが待ち受け(Listening)するアダプタとポート番号の表示と指定をします。
デフォルトは、全ての有効アダプタに対してポート 22 番を割り当てます。設定変更する場合は、[Add]/[Edit]ボタンをクリックし、[Network Binding]ダイアログボックスを通じて指定します。

[Network Binding]ダイアログボックス：

[Listening address:]

SSH クライアントからの接続を待ち受けするアダプタ(ポート)の IP アドレスを指定します。
デフォルトでは、全ての有効な IP アドレスからの受信が有効です。
全 IP アドレス指定は、IPv6 の場合 "::"とし、IPv4 の場合 "0.0.0.0" とします。

[Port:]

SSH クライアントからの接続を待ち受けする TCP ポート番号を指定します。
デフォルトは ポート 22 番です。

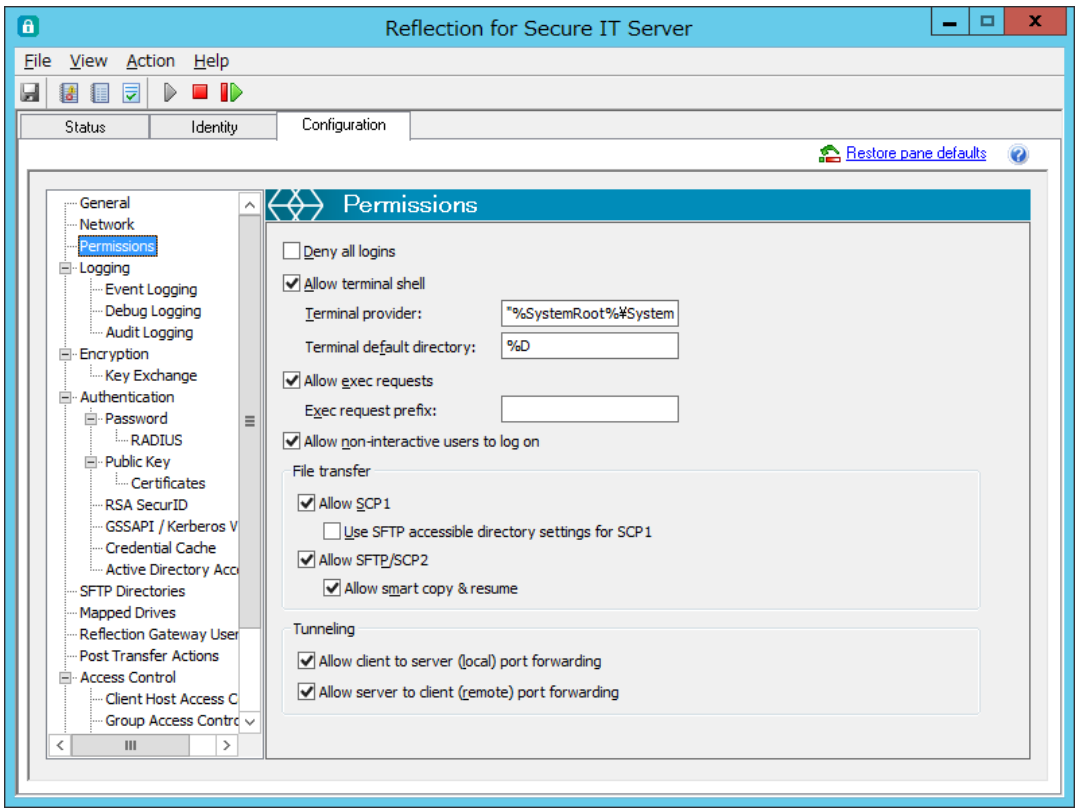
[Client keep alive]

クライアント側に対して正常性監視をします。キープアライブパケットに対して指定時間応答が無い場合に切断します。デフォルトは 60 秒 です。

[Require reverse DNS lookup]

RSIT Windows サーバは下記設定条件時に、接続要求クライアントの IP アドレスを元に DNS に対し名前の逆引き処理を実行します。その逆引き処理が失敗した時に、接続処理を即中断し切断する〔=チェック付き〕か、そのまま接続判定処理を継続する〔=チェックなし〕かの指定をします。
〈逆引き条件〉 ①[Client Host Access Control]設定にて、FQDA で Client Host 指定時
②[Client Host Configuration]設定にて、(FQDA/IP アドレスいずれかで)
Client Host 指定時

4.2.3 [Permissions] 設定画面



各種 SSH サーバサービスの提供有無をサーバ共通に設定します。

本設定の他、[Subconfiguration] 設定により、ほぼ同一内容を Client Host/Group/User 個別に指定可能です。

[Deny all logins]

(現在既に確立している接続以外の、今後の新たな)クライアントからの接続を全て拒否する指定です。[Subconfiguration]の指定に本設定はありません。

[Allow terminal shell]

クライアントからのターミナル接続を許可するかどうかの指定です。

注記：

ターミナル接続動作許可決定要因として、Windows OS のセキュリティ設定内容も影響します。

[Terminal provider:]

ターミナル接続動作に対応するサーバ側実行プログラムを指定します。

デフォルトは Windows 標準の cmd.exe です。指定変更時は、絶対パスで指定します。

注記：

指定時にパス名にスペースを含む場合は、Windows のセキュリティ上、ダブルクウォーテーション(" ")で囲って下さい。

[Terminal default directory:]

ターミナル接続開始時のカレントディレクトリとなるパス指定をします。

パス指定または、パターンストリング("%D","%H",%u","%U")を使用可能です。

デフォルトは "%D"(Windows ユーザプロファイル) 先です。

Windows ユーザプロファイルデフォルト値は以下の通りです。(管理者権限ユーザにより変更可)

C:¥Users¥username¥ (オブジェクト名"C:¥Users"、表示は"C:¥ユーザー")

〈パターンストリング〉

・%D：ユーザプロファイルフォルダ

・%H：ユーザホームフォルダ

・%u：ユーザログイン名

・%U：ドメインユーザログイン名 (domain.username の書式)

[Allow exec requests]

SSH リモートコマンドを実行可能とするかどうかを指定します。

デフォルトは実行可状態です。

[Allow non-interactive users to log on]

Windows サーバ OS の ローカルセキュリティポリシー設定にて、"ローカルログオンを許可する"

対象になっていないユーザ/グループに対して、SSH ログインを許可するかどうかを指定します。

File transfer

[Allow SCP1]

OpenSSH の scp（ここでは"SCP1"と表記）は 標準仕様に準拠しない非sftpプロトコルを使用しています。RSIT Windows サーバでは、この非 sftp プロトコルにも対応しました。

本指定は OpenSSH クライアントからの scp に対応するかどうかの指定をします。

デフォルト状態では対応します。

注記：

OpenSSH の scp はSSHセッション内の1チャネルを介したrcpコマンドにて実現しています。よって、本設定からチェックマークを外し対応不可とした場合でも、[Allow exec requests]にて実行可能の設定をしている場合は、OpenSSH からの scp が可能な状態になります。

[Use SFTP accessible directory settings for SCP1]

OpenSSH からの scp 動作に対し、[SFTP Directories]設定画面内の設定内容を適用するかどうかを指定します。

[Allow SFTP/SCP2]

クライアントからの sftp 及び（標準仕様に準拠した sftp プロトコルによる）scp（ここでは"SCP2"と表記)を許可するかどうかを指定します。デフォルトは、許可状態です。

[Allow smart copy & resume]

Smart Copy 機能(=同一ファイル存在時に転送処理をスキップする機能)と Resume 機能(=リトライ時に前回途中まで転送した分の次から再開する機能)の有効/無効を指定します。

デフォルトは有効状態です。

注記：

SSH クライアント側で Smart Copy 機能と Resume 機能に未対応の場合は、本設定に関係なく動作は無効になります。

Tunneling

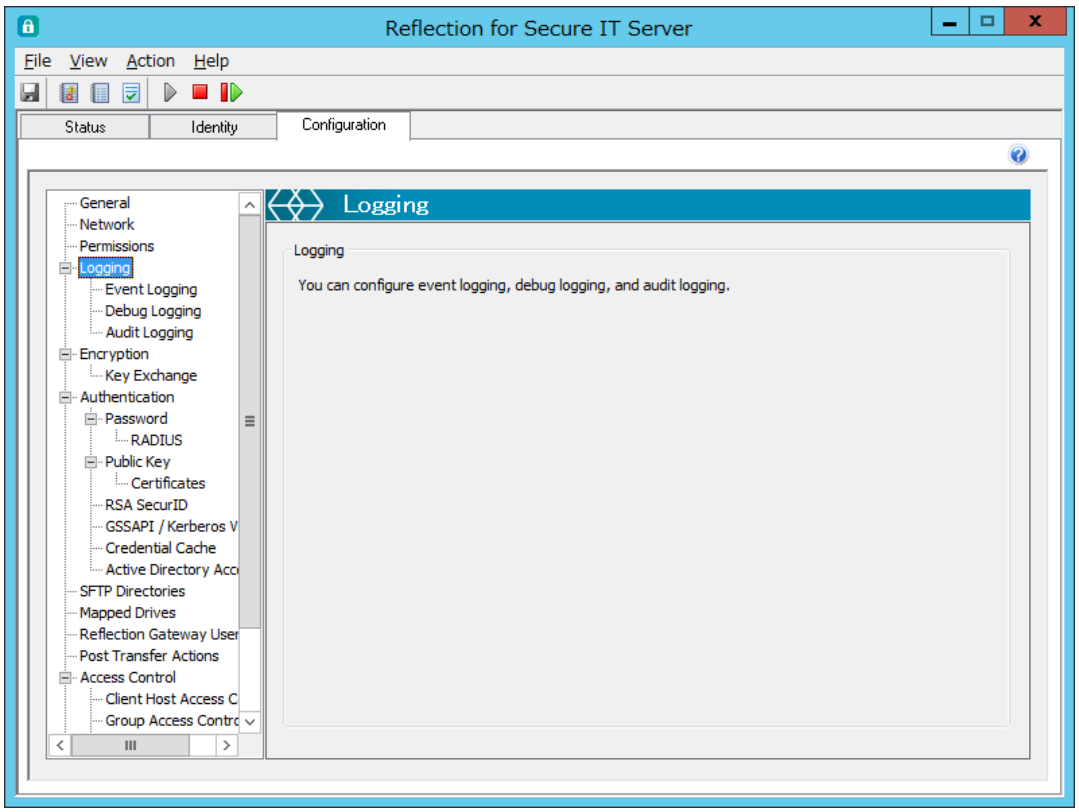
[Allow client to server (local) port forwarding]

クライアントからの "ローカル TCP ポート転送" を許可するかどうかを指定します。

[Allow server to client (remote) port forwarding]

クライアントからの "リモート TCP ポート転送" を許可するかどうかを指定します。

4.2.4 [Logging] 設定画面



[Logging]機能として、下記 3 種のログを用意しました。

① [Event Logging]：Windows イベントログへの記録動作を指定

② [Debug Logging]：SSH クライアントとの接続動作解析用のログ指定

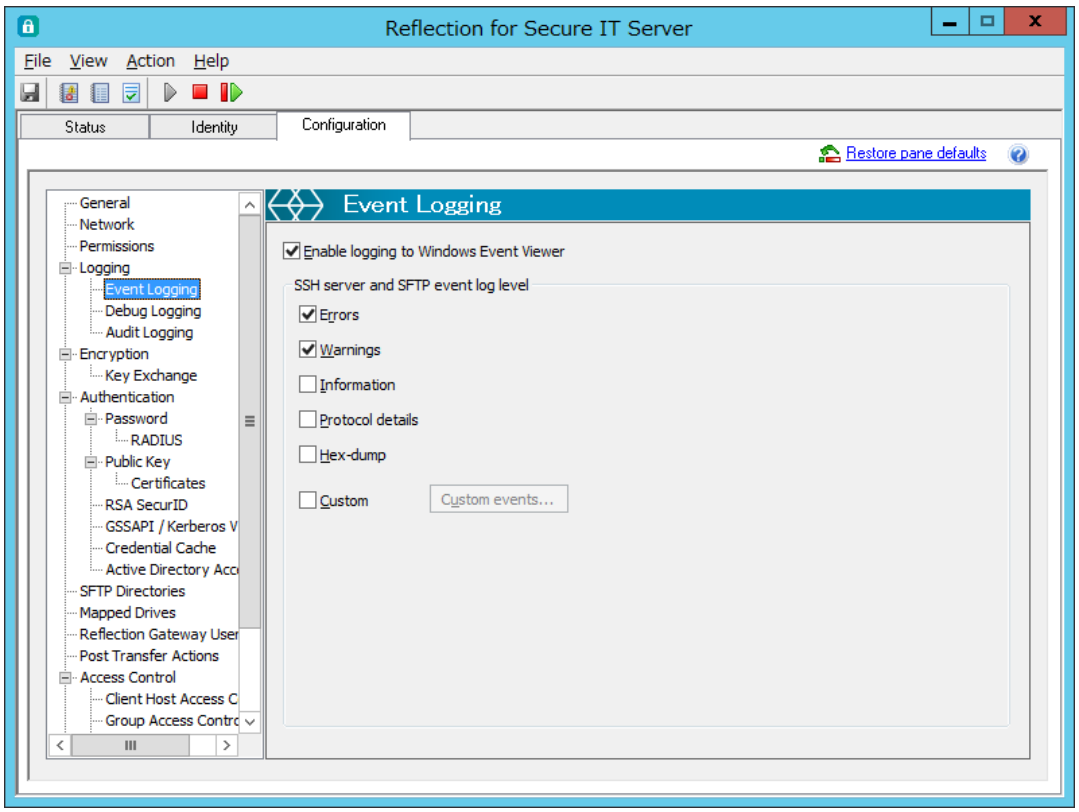
③ [Audit Logging]：ファイル転送アクセス監査ログ用として記録動作を指定

① [Event Logging]は、デフォルト有効です。必要に応じてその詳細記録レベルを指定します。

② [Debug Logging]は、本番稼働時はデフォルト状態のまま無効として下さい。
構築時や新規クライアントとの接続で問題が生じた場合に、その原因解析目的で、有効化しログを採取します。有効化時は接続処理内容を逐次ファイルに出力し、その分 動作自体に負荷がかかります。

③ [Audit Logging]は、デフォルト無効です。本サーバへのファイル転送アクセス状況を監査ログとして記録する必要がある場合に有効化します。

4.2.5 [Event Logging] 設定画面



Windows イベントログへの記録動作の指定をします。

[Enable logging to Windows Event Viewer]

イベントログへの記録を有効にします。

[Errors], [Warnings], [Information], [Protocol details], [Hex-dump]

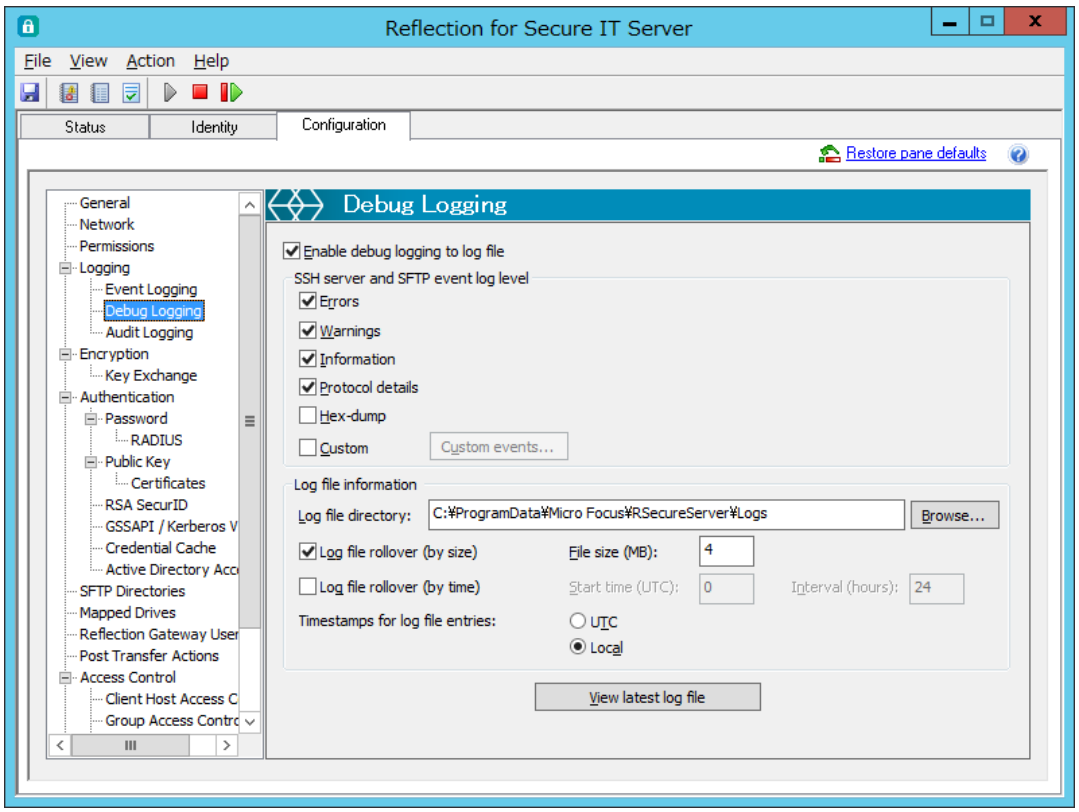
チェックマークを入れることで、どのレベルまで記録するかを指定します。

下に行くほどより詳細になります。チェックを入れた項目の上位は無条件にチェックマークが入ります。デフォルトは、"Errors", "Warnings" レベルを記録します。

[Custom]

チェックマークを入れ、[Custom events]ボタンをクリックすることで、個々の詳細イベントを個別に指定可能です。

4.2.6 [Debug Logging] 設定画面



RSIT Windows サーバ専用のデバッグログ採取の指定をします。

デバッグログは問題解析用です。特にクライアントとの接続失敗時に有効な情報を提供します。

メッセージを出力しながらプログラム処理をする関係で、RSIT Windows サーバの本来の処理の処理速度は低下します。通常運用ではチェックマークを外し無効にしてお使い下さい。

[Enable debug logging to log file]

デバッグログの記録を有効にします。

有効時、SSH サーバのサービスを起動する毎に別名の新たなデバッグログファイルを生成します。

[Errors], [Warnings], [Information], [Protocol details], [Hex-dump]

チェックマークを入れることで、どのレベルまで記録するかを指定します。

下に行くほどより詳細になります。チェックを入れた項目の上位は無条件にチェックマークが入ります。

[Custom]

チェックマークを入れ、[Custom events]ボタンをクリックすることで、個々の詳細イベントを個別に指定可能です。

Log file information

[Log file directory]

デバッグログを生成するディレクトリ先を指定します。

デバッグログは指定ディレクトリ下に、"RSSHD-YYYYMMDD-HHMMSSmmm.log"というファイル名で作成されます。ここで、"YYYYMMDD-HHMMSSmmm"は、開始時刻を示し、"YYYYMMDD" は年月日、"HHMMSSmmm" は 時分秒+マイクロ秒 です。

[Log file rollover (by size)]

上限ファイルサイズを指定し、そのサイズに達したら現デバッグログファイルを完了し、新ログファイルを新たに生成し切り替えます。

指定サイズは１ファイルのサイズ指定であり、全ログファイル容量は増え続けますので注意下さい。

[Log file rollover (by time)]

指定時間間隔で出力デバッグログファイルを新規に生成し切り替えます。

[Timestamps for log file entries]

デバッグログメッセージに付与される時間情報を指定します。

・[UTC] 選択　：UTC(国際協定時刻;Coordinated Universal Time)(グリニッジ標準時; GMT と同義) で表示。

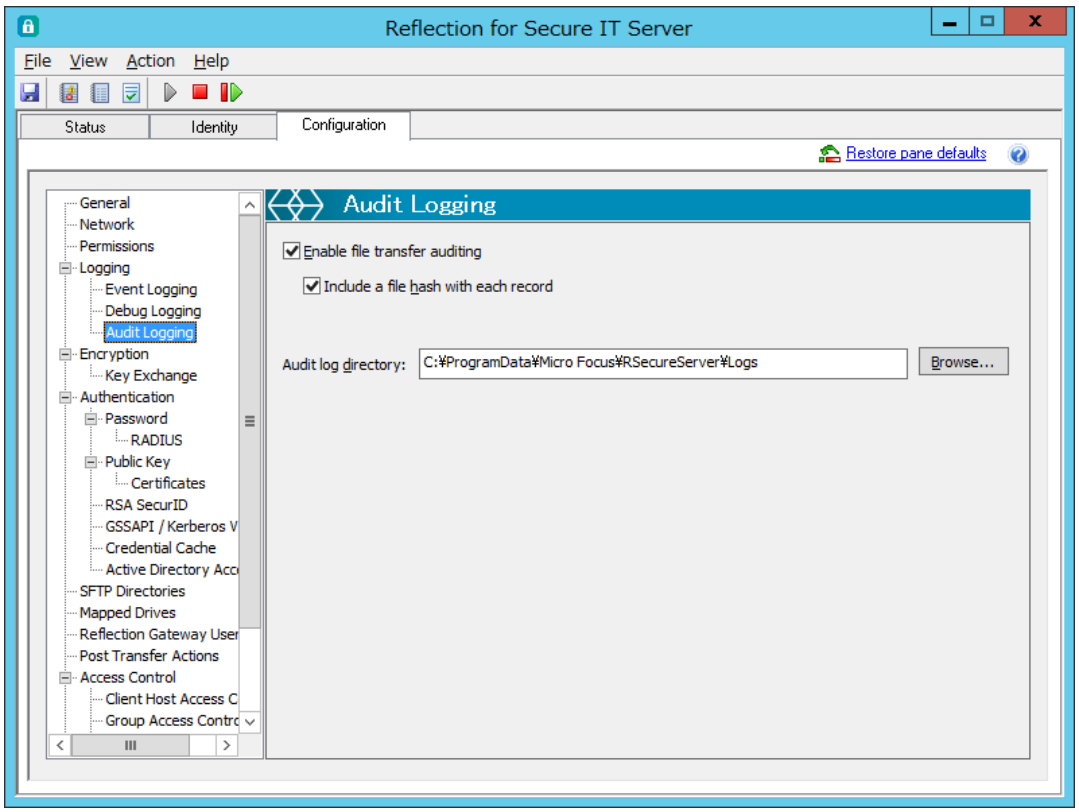
・[Local] 選択：指定タイムゾーン時刻で表示。

[View latest log file] ボタン

最新(現行)のデバッグログ内容を表示します。

尚、メニューからの選択 "View" > "Latest Debug log File" でも同様に表示します。

4.2.7 [Audit Logging] 設定画面



RSIT Windows サーバへのファイル転送アクセス状況を監査ログとして記録するよう指定をします。ログとして記録する内容は以下の通りです。日にちが変わる毎に新しいファイルを指定保存先フォルダに生成します。

ログファイル名称：RSSHD-Audit-YYYYMMDD.log　("YYYY":年、"MM":月、"DD":日)

ログ記録内容：UserID,ClientIP,Action,ServerFilename,StartTime,EndTime,
ServerFileModificationTime,ServerFileSize,BytesTransferred,Result,
Reason,ServerFileHash　　(カンマ区切り、一記録一行)

[Enable file transfer auditing]

ファイル転送アクセス状況監査ログの記録を有効にします。

有効時、SSH サーバのサービスを起動する毎に別名の新たなログファイルを生成します。

[Include a file hash with each record]

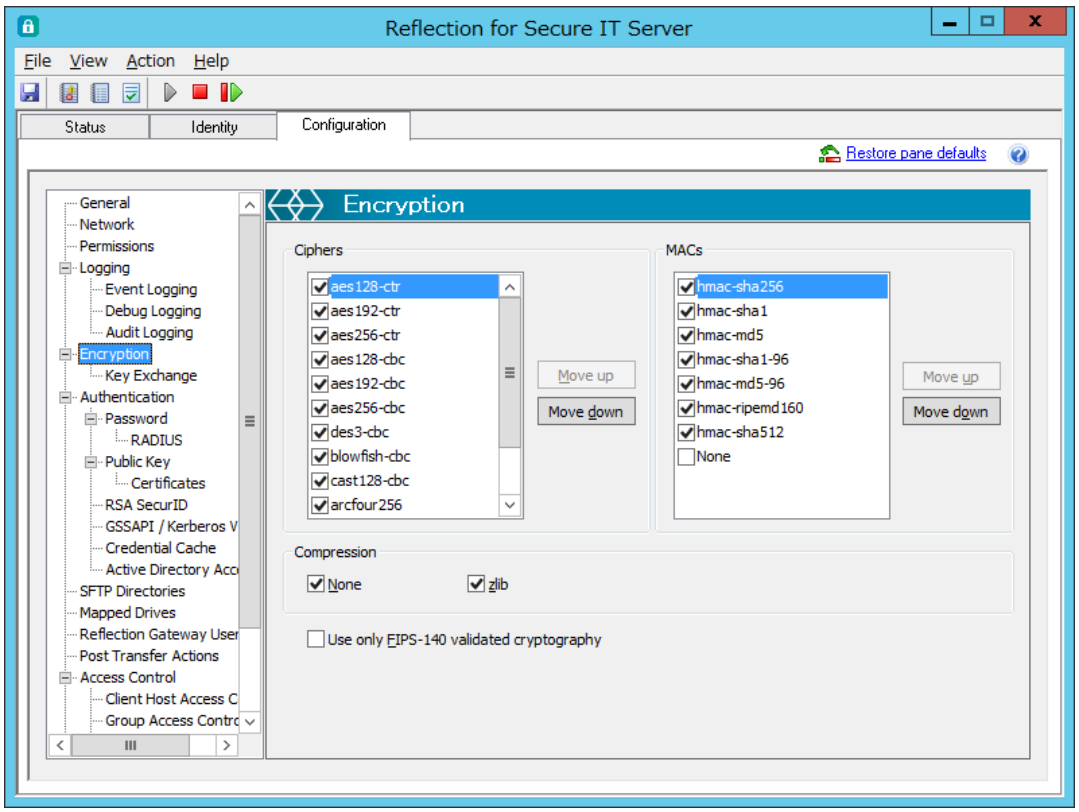
ログ内容の改ざん防止目的でログファイルに hash 値(SHA-1)を含めるかを指定します。

[Audit log directory]

ログの保存先を指定します。欄内に直接記入するか、[Browse]ボタンをクリックして指定フォルダを選択します。

デフォルト保存先フォルダの場合や事前に生成せずにプログラム動作時に自動生成された場合は、そのフォルダパーミッションは、SYSTEM と Administrators だけに付与され、そのフォルダ下のログファイルもそのパーミッションが継承されます。独自に生成したフォルダを指定する場合、そのパーミッションを SYSTEM と Administrators だけに許可し、セキュリティ上の制限をかけて下さい。

4.2.8 [Encryption] 設定画面



[Ciphers]

送受信するデータやパスワード等の情報を暗号化する共通鍵の暗号方式を指定します。

表中上位のものが、クライアントとの接続開始ネゴシエーション時に候補として優先使用されます。チェックマークの on/off と up/down により指定します。

{aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192- cbc, aes256- cbc, des3-cbc, blowfish-cbc, cast128-cbc, arcfour256, arcfour128, arcfour, none}をサポートしています。

注記：

"none"は、暗号化せずに平文のまま送信しますのでテスト解析用以外には禁止です。

[MACs]

データの完全性確認(=改ざんを検出)する MAC(Message Authentication Code)アルゴリズムを指定します。表中上位のものが、クライアントとの接続開始ネゴシエーション時に候補として優先使用されます。チェックマークの on/off と up/down により指定します。

{hmac-sha256, hmac-sha1, hmac-md5, hmac-sha1-96, hmac-md5-96, hmac-ripemd160, hmac-sha512, none}をサポートしています。

(Ver.8.0 から "hmac-sha256"が最優先になりました。)

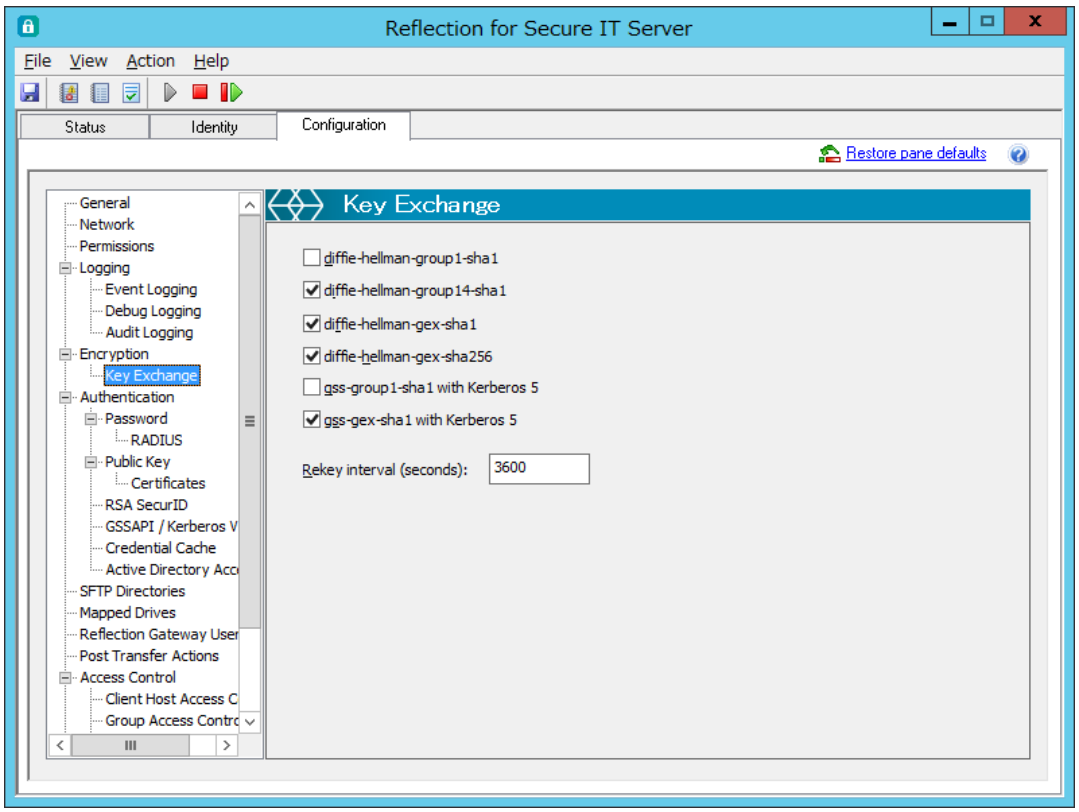
[Compression]

圧縮の指定です。

[Use only FIPS-140 validated cryptography] 02

FIPS 140-2 (米連邦政府情報処理規格 140-2) 認定の暗号モジュールのみを使用するように指定します。デフォルトは未チェック状態で、このまま使用することを推奨します。

4.2.9 ［Key Exchange］設定画面



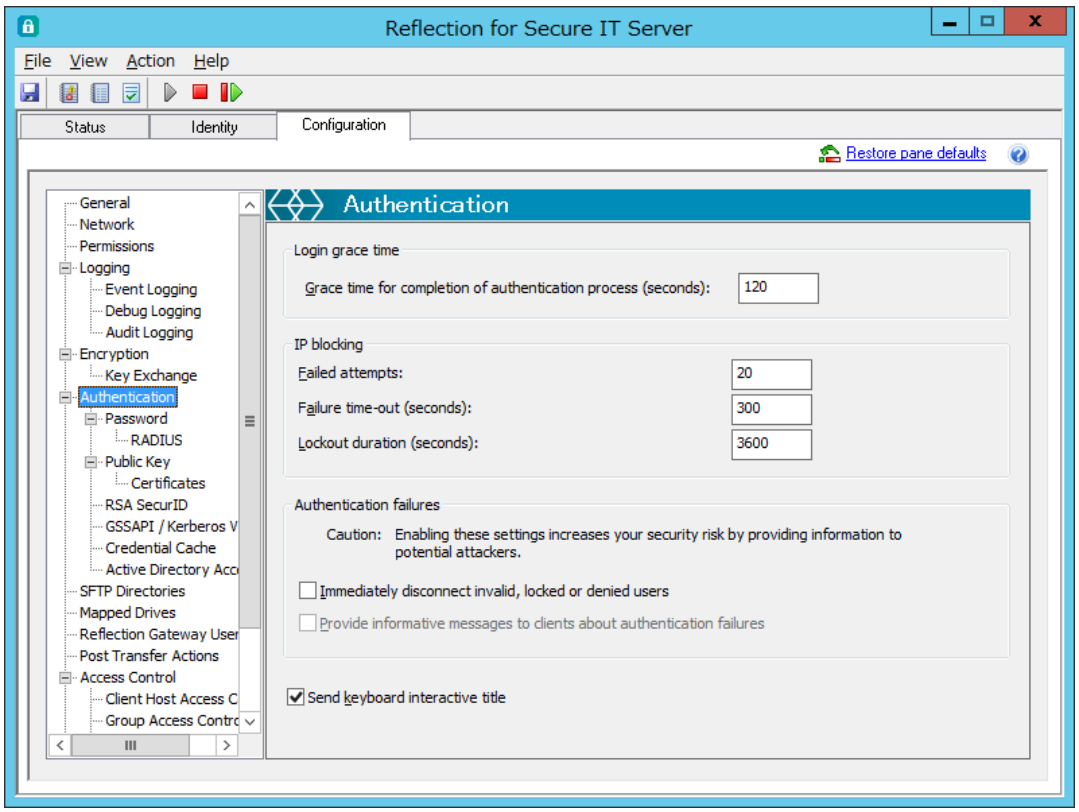
送受信データ暗号化用セッション鍵を生成するための鍵交換アルゴリズムを指定します。
デフォルトでは、8.2 SP1 から対応鍵交換アルゴリズムのうち、
"diffie-hellman-group1-sha1"と"gss-group1-sha1 with Keroberos 5"を無効化しています。
〔対応鍵交換アルゴリズム〕

{diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-gex-sha1,
diffie-hellman-gex-sha256, gss-group1-sha1 with Keroberos 5,
gss-gex-sha1 with Keroberos 5}

[Rekey interval (seconds):]

長時間 SSH 接続が継続している場合に、暗号化用セッション鍵を再生成（= Rekey）する時間間隔を指定します。デフォルトは 3600(秒)です。

4.2.10 [Authentication] 設定画面



ユーザ認証に関して全体に共通する項目を指定します。

Login grace time

[Grace time for completion of authentication process (seconds):]

ユーザ認証最大許容待ち時間(内部的なユーザ認証処理開始時点からのタイムアウト時間)を秒単位で指定します。デフォルトは 120(秒)です。

注記：

値"0" は無制限を意味しますが、保持状態継続によるシステムリソースの浪費や DoS 攻撃への配慮から、値"0" 指定は禁止とします。

IP blocking

ある特定の IP アドレスのクライアントから短時間に多くの接続失敗が繰り返された時に、その IP アドレスのクライアントに対し接続試行を一定時間ブロックすることが出来ます。

[Failed attempts:]に接続失敗回数上限値を指定し、[Failure time-out (seconds):]に基準となる監視時間を指定し、[Lockout duration (seconds):]に既定値到達後にブロックし続ける時間を指定します。

[Failed attempts:]

IP ブロッキングする失敗回数を指定します。

デフォルトは 20(回)です。値"0" は IP ブロッキング機能の無効化を意味します

[Failure time-out (seconds):]

基準となる監視時間を指定します。

デフォルトは 300(秒)です。

[Lockout duration (seconds):]

IP ブロッキングの規定値になった時点からブロックし続ける時間を指定します。

デフォルトは 3600(秒)です。

注記：

IP ブロッキング機能は、パスワード認証とキーボードインターラクティブ形式によるパスワード認証による接続試行失敗の時にのみ機能します。

IP ブロッキングに関する管理情報をメモリ上に持つため、sshd サービスを再開した場合はそれまでの情報は無効になります。

Authentication failures

[Immediately disconnect invalid, locked or denied users]

"存在しない"、"ロックされている"、"拒否設定されている"といった認証が失敗することが自明なユーザに対しての接続要求があった場合に、初回で直ぐに接続失敗とし切断する動作を指定します。

デフォルトは非チェックで、接続要求ユーザに対し試行許容回数分の認証操作を求めます。

不正なアクセス者に対しては、デフォルトの非チェック状態の方がサーバ内のユーザに関する情報を遮蔽することになりますので、より安全と言えます。

[Provide informative messages to clients for authentication failures]

上記設定にチェックマークを入れ、初回で直ぐに接続失敗とし切断する場合に、その理由をクライアントに伝えるかどうかを指定します。セキュリティ上、決して推奨出来ません。

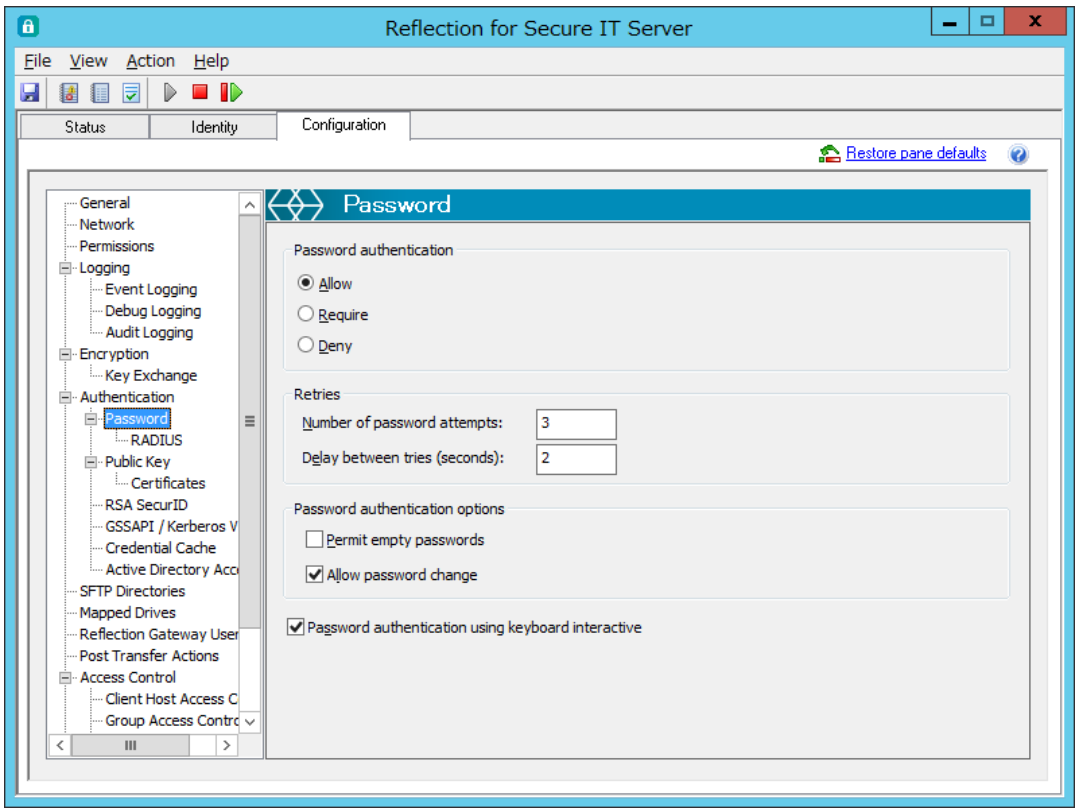
Keyboard interactive

[Send keyboard interactive title:]

キーボードインターラクティブ認証時にクライアント側画面上にタイトルテキストを表示するかどうかを指定します。

デフォルトはチェック付きで、従来通りタイトルテキストを表示します。

4.2.11 ［Password］設定画面



本設定画面を通じて、"パスワード認証"およびパスワード入力の"キーボードインターラクティブ認証"について指定します。

注記：

画面最下部［Password authentication using keyboard interactive］のチェックマーク有無が、# Password authentication 欄の｛Allow、Require、Deny｝の対象に影響します。

"Allow" と "Require" の意味について：

・"Allow" ～クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補対象として指定されます。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

・"Require" ～SSH サーバがクライアントに対してユーザ認証成功のために認証成功必須を要求する対象として指定されます。ユーザ認証成功のためには、"Require"として要求された認証方式全てが成功する必要があります。

Password authentication

(説明では、[Password authentication using keyboard interactive]を[KB int]と省略します。)

[Allow] 選択の場合：

[KB int] 選択時：パスワード認証、キーボードインターラクティブ認証両方に対して "Allow"

[KB int] 非選択時：パスワード認証に対して "Allow"

[Require] 選択の場合：

[KB int] 選択時：キーボードインターラクティブ認証に対して "Require"

[KB int] 非選択時：パスワード認証に対して "Require"

[Deny] 選択の場合：

[KB int] の選択にかかわらず、パスワード認証、キーボードインターラクティブ認証いずれもユーザ認証として使用せず。

Retries

[Number of password attempts]

一回の接続要求に対してユーザ認証失敗と見なす試行回数を指定します。

デフォルトの回数は 3 回です。

[Delay between tries (seconds)]

試行回数失敗後に再入力要求のプロンプトを表示する時間間隔を秒で指定します。

デフォルトの間隔は 2 秒です。

Password authentication options

[Permit empty passwords]

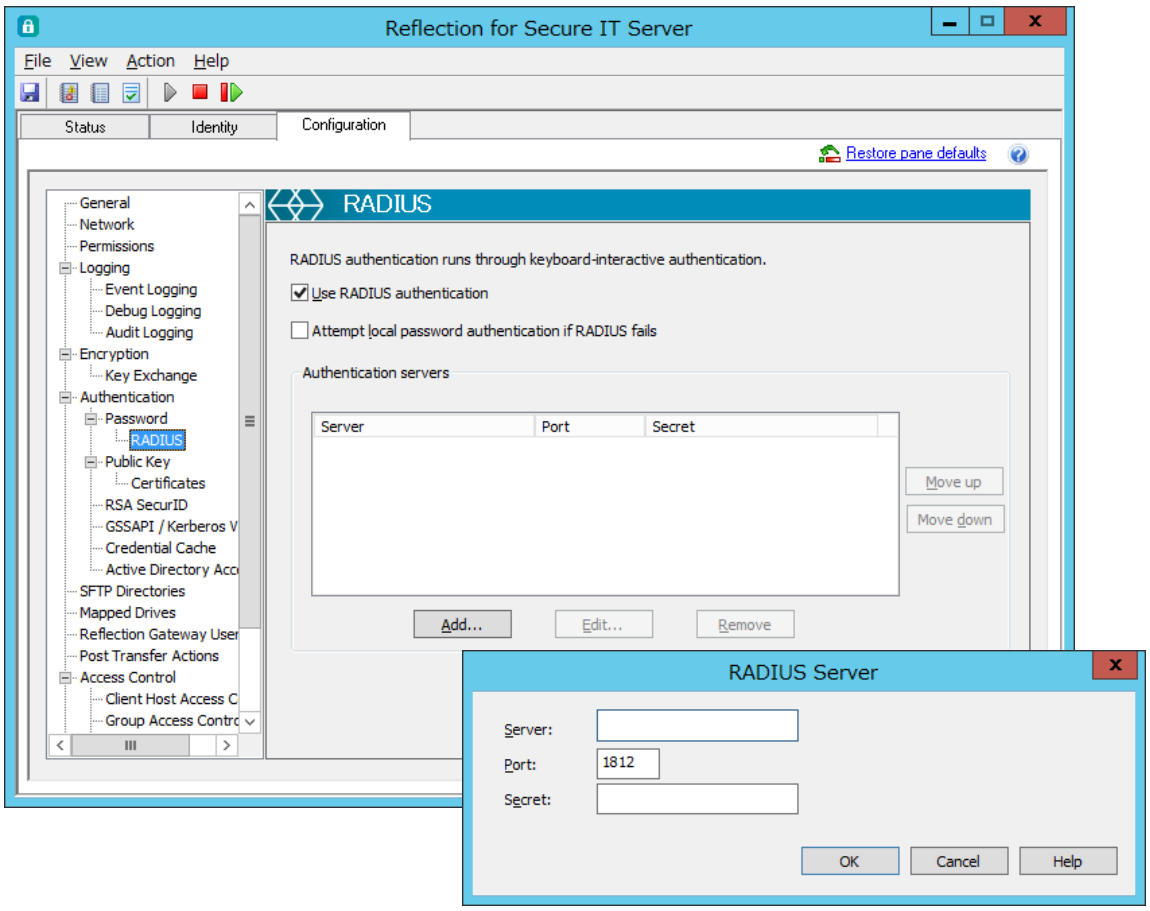
空(=空白)パスワードを許容する時、チェックを入れます。デフォルトは 禁止です。

最終的には、本設定以外に Windows OS の ポリシーの影響も受けます。

[Allow password change]

接続開始時のユーザ認証処理手順の中で OS 要求のパスワード変更処理を許すかどうかを指定します。

4.2.12 ［RADIUS］設定画面



RADIUS サーバとの連携によりユーザ認証を実現するための指定をします。

設定画面内一行目に英文で記述のように、RADIUS 認証は、キーボードインターラクティブ認証を通じて実行されます。

よって、[Password]設定画面において次の指定をした場合は、RADIUS 認証は使用出来ずに、[RADIUS]設定画面自体がグレーアウトします。

①[Password authentication]で"Deny"を選択

②[Password authentication using keyboard interactive]を非選択

注記：

ログインユーザが、サーバローカルか Windows ドメインユーザとして存在しない場合は、RADIUS サーバで認証可能でも、SSH の認証自体は失敗します。

[Use RADIUS authentication]

RADIUS サーバとの連携によるユーザ認証を有効化します。

[Password]設定画面において、①[Password authentication]で"Deny"を選択、②[Password authentication using keyboard interactive]が非選択 の時には、無効化しています。

[Attempt local password authentication if RADIUS fails.]

RADIUS サーバとの連携によりユーザ認証が失敗した時に、サーバローカルのパスワードを使用してユーザ認証をするか指定します。

Authentication servers

RADIUS Server ダイアログボックス

[Server]

RADIUS サーバの名称または IP アドレスを設定します。

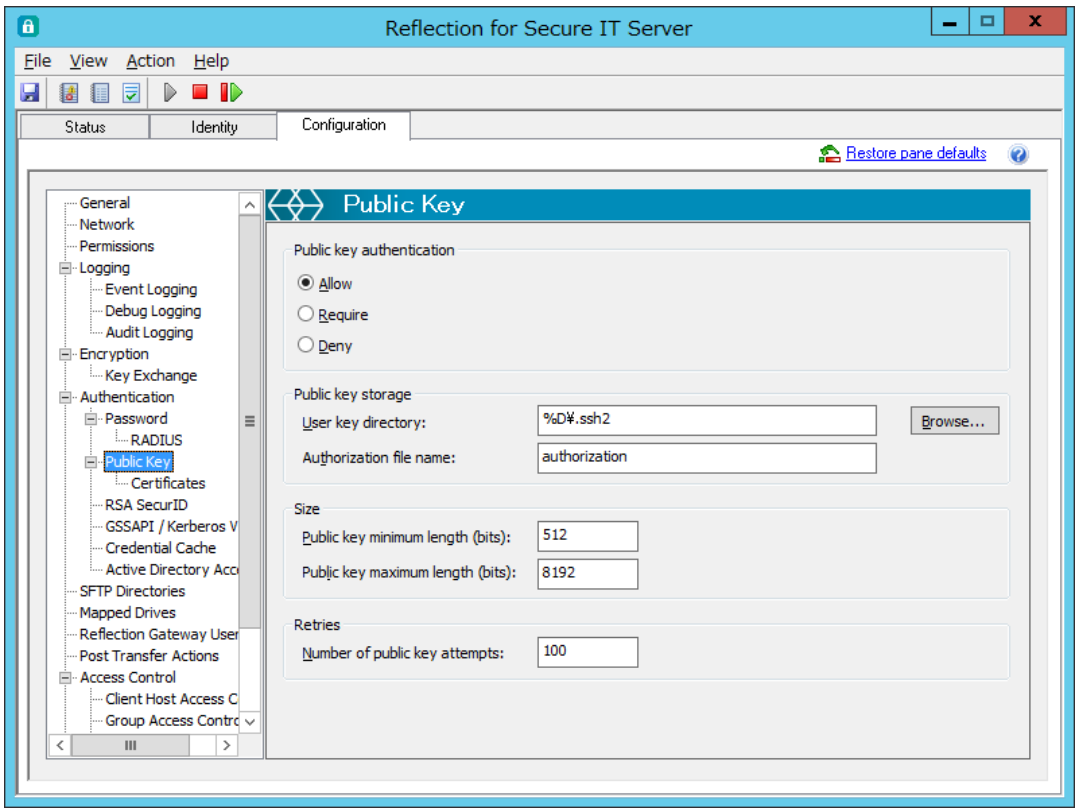
[Port]

使用するポート番号を指定します。

[Secret]

RADIUS サーバとの接続のために、RADIUS に対するホストのパスワードを設定します。

4.2.13 [Public Key] 設定画面



公開鍵認証によるユーザ認証を実現するためのサーバ側設定をします。

Public key authentication

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として公開鍵認証を指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として公開鍵認証を要求します。ユーザ認証成功のためには、"Require"として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として公開鍵認証を使用しない指定です。

Public key storage

[User key directory:]

公開鍵認証で使用するユーザの登録公開鍵の所在ディレクトリを指定します。

パスで直接指定するか、パターンストリング("%D","%H","%u","%U")を使用可能です。

デフォルトは %D¥.ssh2 (Windows ユーザプロファイル下の".ssh2"フォルダ) です。

- %D：ユーザプロファイルフォルダ
- %H：ユーザホームフォルダ
- %u：ユーザログイン名
- %U：ドメインユーザログイン名 (domain.username の書式)

[Authorization file name:]

登録公開鍵ファイル名をリストアップした管理ファイル名を指定します。

デフォルト名称は "authorization"ファイルです。

Size

[Public key minimum length (bits):]

使用可能な公開鍵の最小のビット長を規定します。

範囲は 512～8192 で、デフォルト 512 (ビット長)です。

[Public key maximum length (bits):]

使用可能な公開鍵の最長のビット長を規定します。

範囲は 512～8192 で、デフォルト 8192 (ビット長)です。

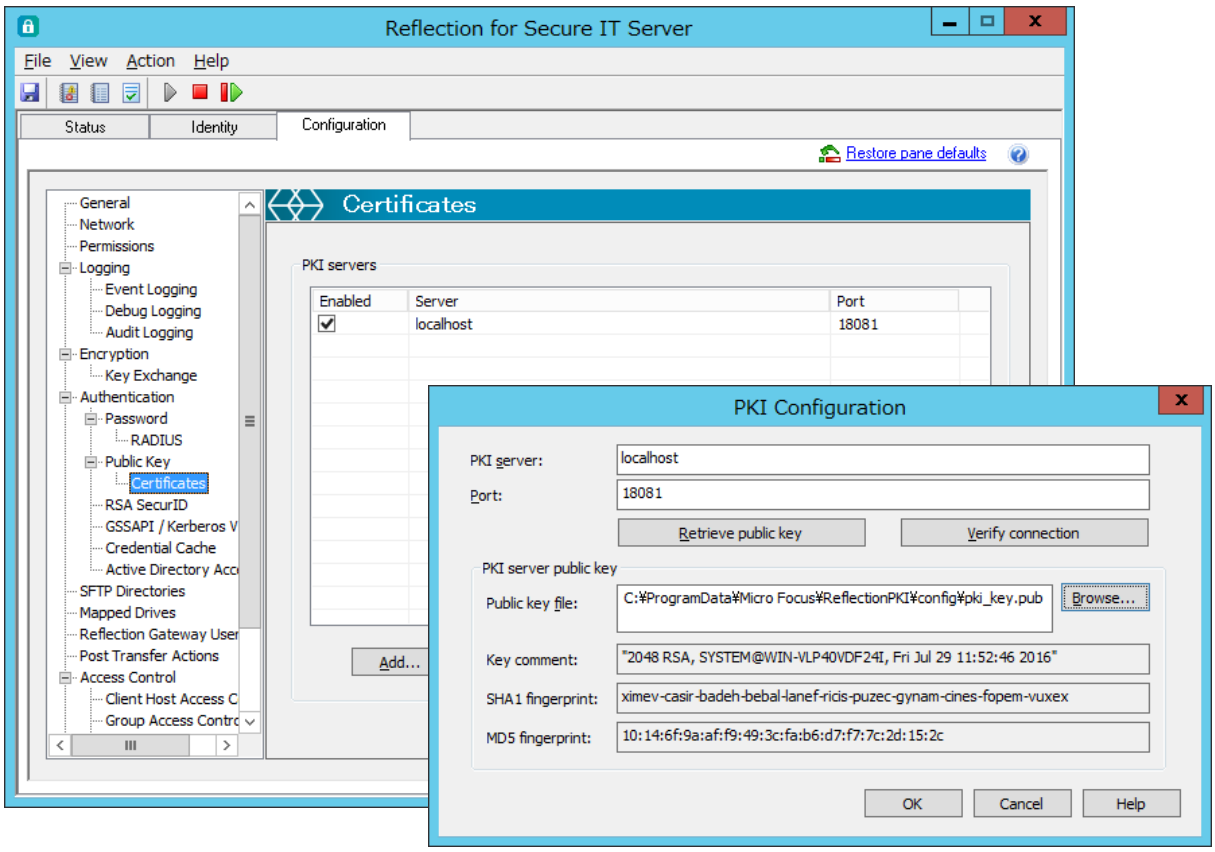
Retries

[Number of public key attempts:]

公開鍵認証を用いた接続確立処理において、クライアント内に秘密鍵が複数存在する場合は、クライアントは一つ目の秘密鍵からユーザ認証が成功するまで順次保管秘密鍵を使って認証試行を繰り返します。本設定は、サーバ側でその試行回数に制限を加えるために存在します。

デフォルトは 100 です。(…従来運用に影響ないように常識的には限りなく大きな値としました。)

4.2.14 [Certificates] 設定画面



ユーザ認証として証明書認証を使うための設定をします。

RSIT Windows サーバは、外部認証局と連携して証明書認証を実現するために、弊社オプション別製品の「Reflection PKI Services Manager」(無償)を仲介して動作します。本設定にて、その「Reflection PKI Services Manager」との連携動作のための指定をします。(「Reflection PKI Services Manager」の詳細については、英文マニュアルを参照して下さい。)

高可用性 PKI 環境実現のために複数の「Reflection PKI Services Manager」指定も可能です。

 # PKI Servers

[Server:]

対応する"Reflection PKI Services Manager" を示します。

デフォルトで "localhost" (= RSIT Windows サーバと同一サーバ内) が指定されています。

[Port:]

"Reflection PKI Services Manager" が待ち受けるポート番号を指定します。

デフォルトは 18081 番ポートです。

[Add]/ [Edit]/ [Remove]ボタン

[PKI Configuration]設定画面を"新規追加"/"編集"/"削除"する指示ボタンです。

[Launch PKI Services Manager] ボタン

同一サーバ内に"Reflection PKI Services Manager" が存在する時有効なボタンで、"Reflection PKI Services Manager" 設定画面を起動表示します。

[PKI configuration]ダイアログボックス

[PKI server:]

連携先"Reflection PKI Services Manager" を指定します。

デフォルトは "localhost" で、別サーバ指定時は、そのホスト名か IP アドレスを指定します。

[Port:]

"Reflection PKI Services Manager" 待ち受けポート番号を指定します。

[Retrieve public key] ボタン

"Reflection PKI Services Manager" 認証用ホスト鍵の取り込み操作ボタンです。

[Verify Connection] ボタン

"Reflection PKI Services Manager" との接続を確認する動作確認ボタンです。

PKI Server Public key

[Public key file:]

"Reflection PKI Services Manager" ホスト鍵のファイルを指定します。

同一マシンにインストールした場合、デフォルトファイルが表示されます。

[Key comment:]

"Reflection PKI Services Manager" ホスト鍵のコメント内容を表示します。

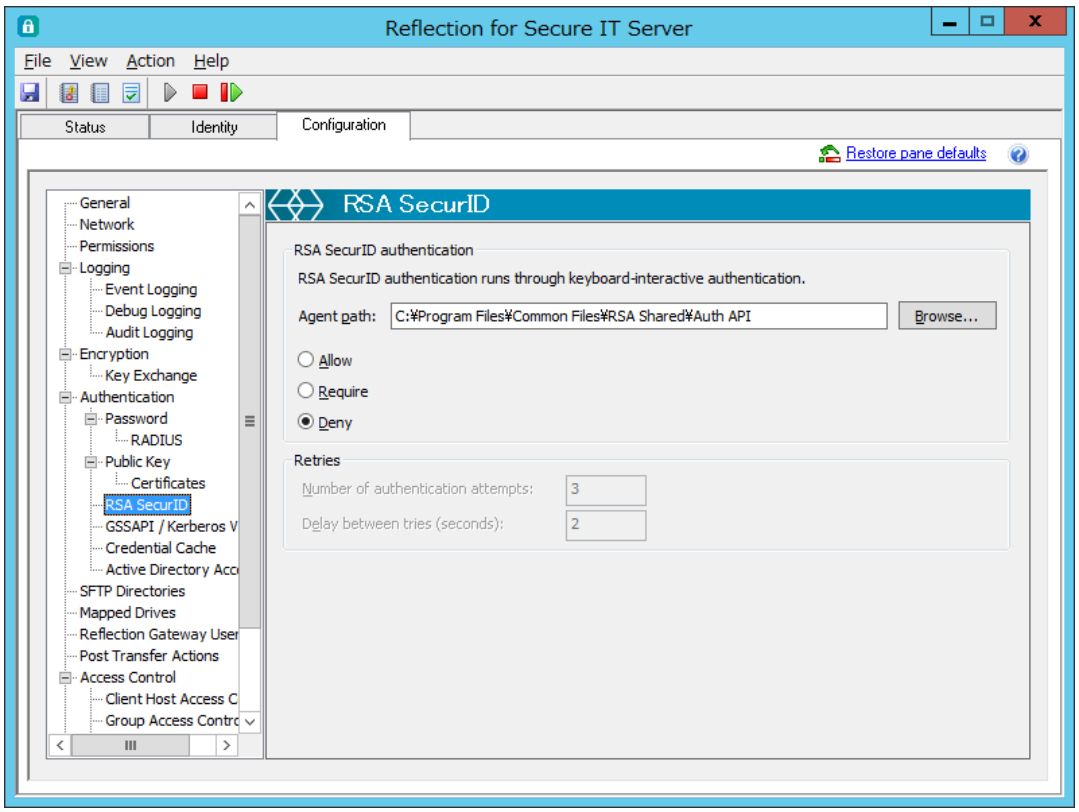
[SHA1 fingerprint:]

"Reflection PKI Services Manager" ホスト鍵の SHA1 ハッシュ関数によるメッセージダイジェスト(=fingerprint) を表示します。

[MD5 fingerprint:]

"Reflection PKI Services Manager" ホスト鍵の MD5 ハッシュ関数によるメッセージダイジェスト(=fingerprint) を表示します。

4.2.15 [RSA SecurID] 設定画面



RSA SecurID との連携によりユーザ認証を実現するための設定をします。

RSA SecurID を使用するために、同一マシン内に RSA SecurID の環境設定が正しくされている必要があります。

(設定画面上に英文で記述のように)、RSA SecurID を利用したユーザ認証は、キーボードインターラクティブ認証を通じて実行されます。(但しこの場合、[Password]設定画面における"Password authentication using keyboard interactive"の指定の影響は受けません。)

クライアント側は、ユーザ認証手段としてキーボードインターラクティブ認証を指定に含む必要があります。

注記：

ログインユーザが、ローカルユーザか Windows ドメインユーザとして存在しない場合は、認証は失敗します。

RSA SecurID authentication

[Agent path]

RSA Authentication Agent が存在するフォルダパスを指定します。

直接欄内に記入するか[Browse]ボタンをクリックして選択指定します。

{Allow、Require、Deny} から選択します。デフォルトは "Deny"です。

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として要求します。ユーザ認証成功のためには、"Require" として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として RSA SecurID 認証を使用しない指定です。

Retries

[Number of password attempts]

一回の接続要求に対してユーザ認証失敗と見なす試行回数を指定します。

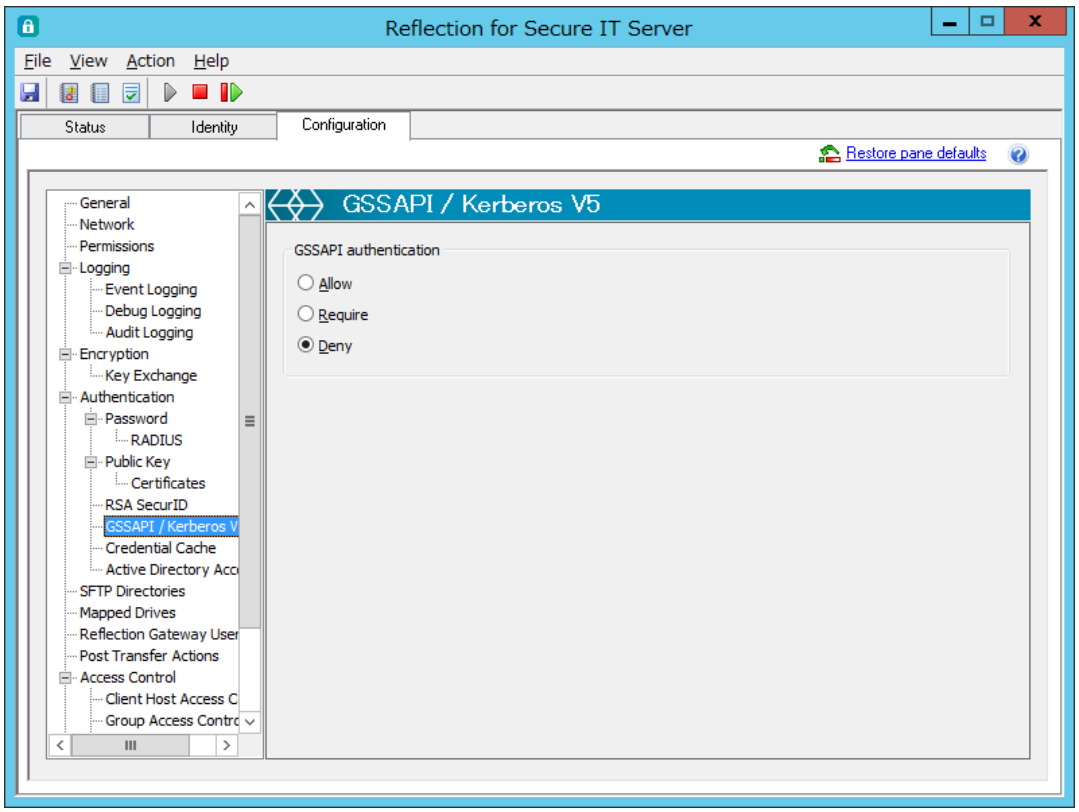
デフォルトの回数は 3 回です。

[Delay between tries (seconds)]

失敗後に再入力要求のプロンプトを表示する時間間隔を秒で指定します。

デフォルトの間隔は 2 秒です。

4.2.16 [GSSAPI/Kerberos V5] 設定画面



GSSAPI(Generic Security Service API) を用いた Kerberos V5 をユーザ認証として使用するかを指定します。

{Allow、Require、Deny} から選択します。デフォルトは "Deny"です。

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

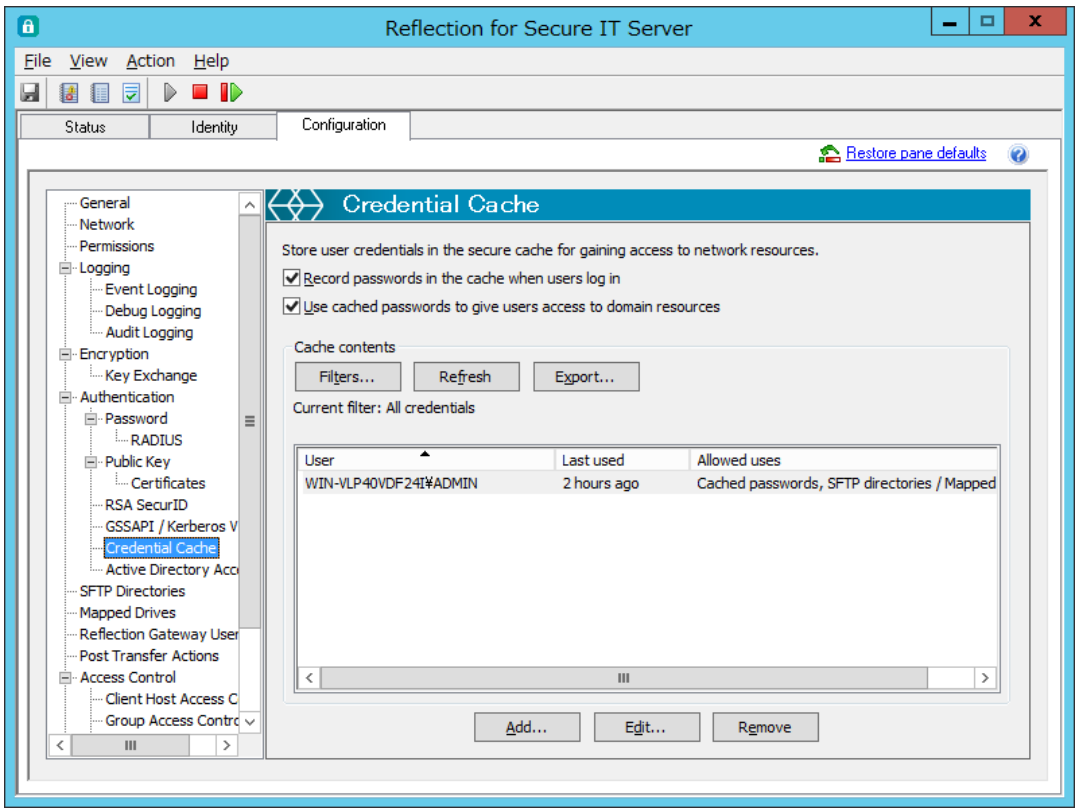
[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として要求します。ユーザ認証成功のためには、"Require" として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として Kerberos V5 認証を使用しない指定です。

4.2.17 [Credential Cashe] 設定画面



クライアントから接続する際に SSH サーバの先のネットワークリソースにアクセスするケースにおいて、ネットワークリソースへのアクセス認証に クライアントのユーザ認証情報以外の認証情報を使う場合に、本設定画面を使い指定します。定義情報は、暗号化し保存されます。

〈ネットワークリソースへのアクセスに認証情報が必要な例〉

(1)Windows ドメインユーザ認証確認時に、クライアントからのユーザ認証でパスワード情報入力が伴わない 公開鍵認証、証明書認証、SecurID 認証の場合

(2)[SFTP Directories]設定画面 "SFTP accessible directories" にネットワーク上のディレクトリを定義し、そこへのアクセスにクライアントのユーザ認証情報以外の認証情報を使う場合

(3)[Mapped Drives]設定画面にて定義したネットワークドライブへのアクセス認証として、クライアントのユーザ認証情報以外の認証情報を使う場合

[Record credentials in the cache when users log in]

選択有効時に、ネットワークリソースアクセスに必要なパスワード入力をユーザに要求し、入力された場合にそれを保存登録します。

[Use credentials in the cache for authentication]

選択有効時に、登録保存された有効なユーザ認証情報がある場合に外部ネットワークリソースへの認証に使用します。

Cache contents

[Filters] ボタン

[Filters]ダイアログボックスを表示する指示ボタンです。

[Refresh] ボタン

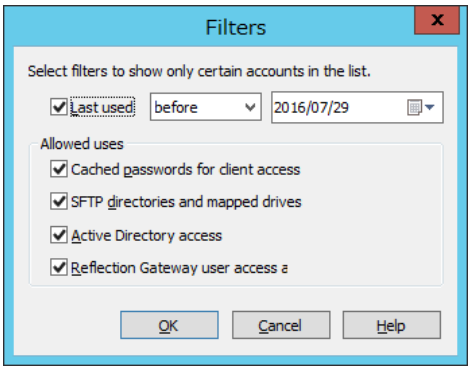
Cache contents 欄の内容を更新するボタンです。

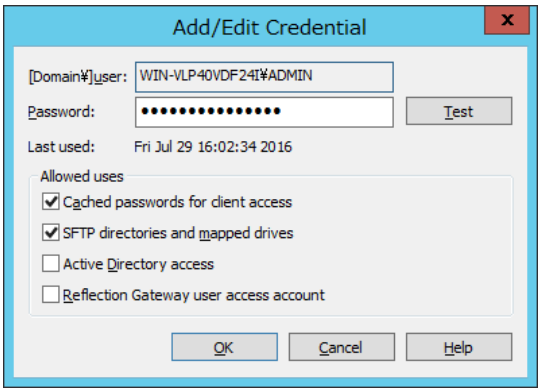
[Export] ボタン

登録保存されたユーザ認証情報を csv ファイル形式でエクスポートします。パスワードは除外。

[Current filter]

[Filters]ダイアログボックス上で設定された条件内容をリストで表示します。





 # [Filters]ダイアログボックス：

登録保存されたユーザ認証情報の使用条件/表示条件を指定します。

[Last used]

Cache contents 欄に表示するユーザ認証情報の表示条件を指定します。

 # Allowed users

[Authentication],[Drive mapping and vitual directories],[Domain accessLast used]選択

選択有効化した項目に対して、登録保存されたユーザ認証情報を使用可能とします。

 # [Add/Edit Credential]ダイアログボックス：

ユーザ認証情報を登録する指定画面です。

[Domain¥user:]

定義するユーザ情報を Domain¥user 又は Computer 名¥user の形式で指定します。

[Password:]

対象ユーザのパスワードを指定します。

[Test]ボタン

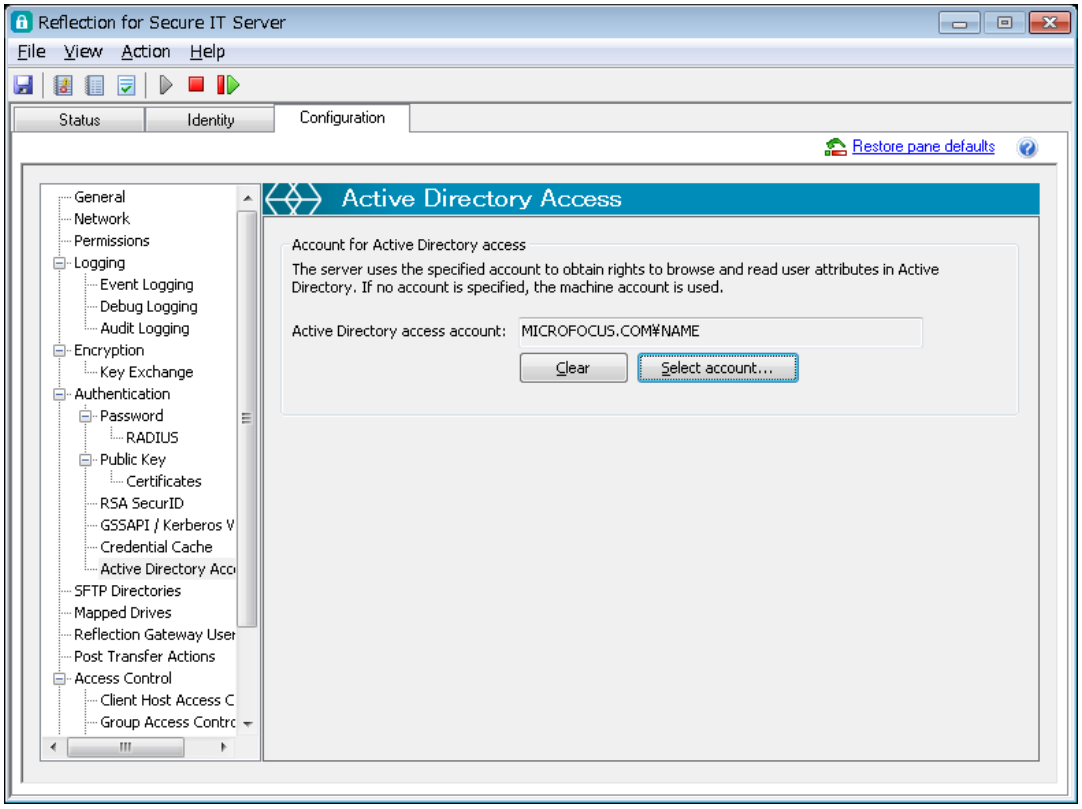
クリックすることで、指定ユーザ認証情報を使い接続試験を行います。

 # Allowed users

[Authentication],[Drive mapping and vitual directories],[Domain access]選択

選択有効化した項目に対して、登録保存されたユーザ認証情報を使用可能とします。

4.2.18 [Active Directory Access] 設定画面



RSIT Windows サーバを導入したサーバが Active Directory ドメインコントローラに対して確認要求する際のアクセス情報(credential)を設定します。

ドメインユーザでログインし、かつ下記条件のいずれかの場合に設定する必要があります。

1) ユーザ認証として、公開鍵認証、証明書認証、RSA SecurID 認証、RADIUS 認証のいずれかを使用し、かつ [Credential Cashe] 設定を通じてパスワードキャッシュを使用しない場合
2) RSIT Windows サーバの[Access Control]設定にて、Active Directory グループメンバシップの情報を使用している場合
3) RSIT Windows サーバの[Group Configuration]設定にて、Active Directory グループメンバシップの情報を使用している場合

また設定要否は、Active Directory ドメインコントローラの設定内容にも依存します。もし本設定が未設定で、かつパスワード情報を伴わない場合、RSIT Windows サーバは Local System アカウントを使いアクセスします。Active Directory ドメインコントローラ側で、本サーバの Local System アカウントにドメインユーザ属性情報リード権限を付与せず、更に匿名ユーザに許可を与えない設定をしていれば、Active Directory ドメインコントローラを使い認証判定は出来ずユーザ認証は失敗します。

[Active Directory access account]

設定された Active Directory ドメインコントローラへのアクセスアカウントを表示します。

未設定の場合、Local System アカウントが使用されます。

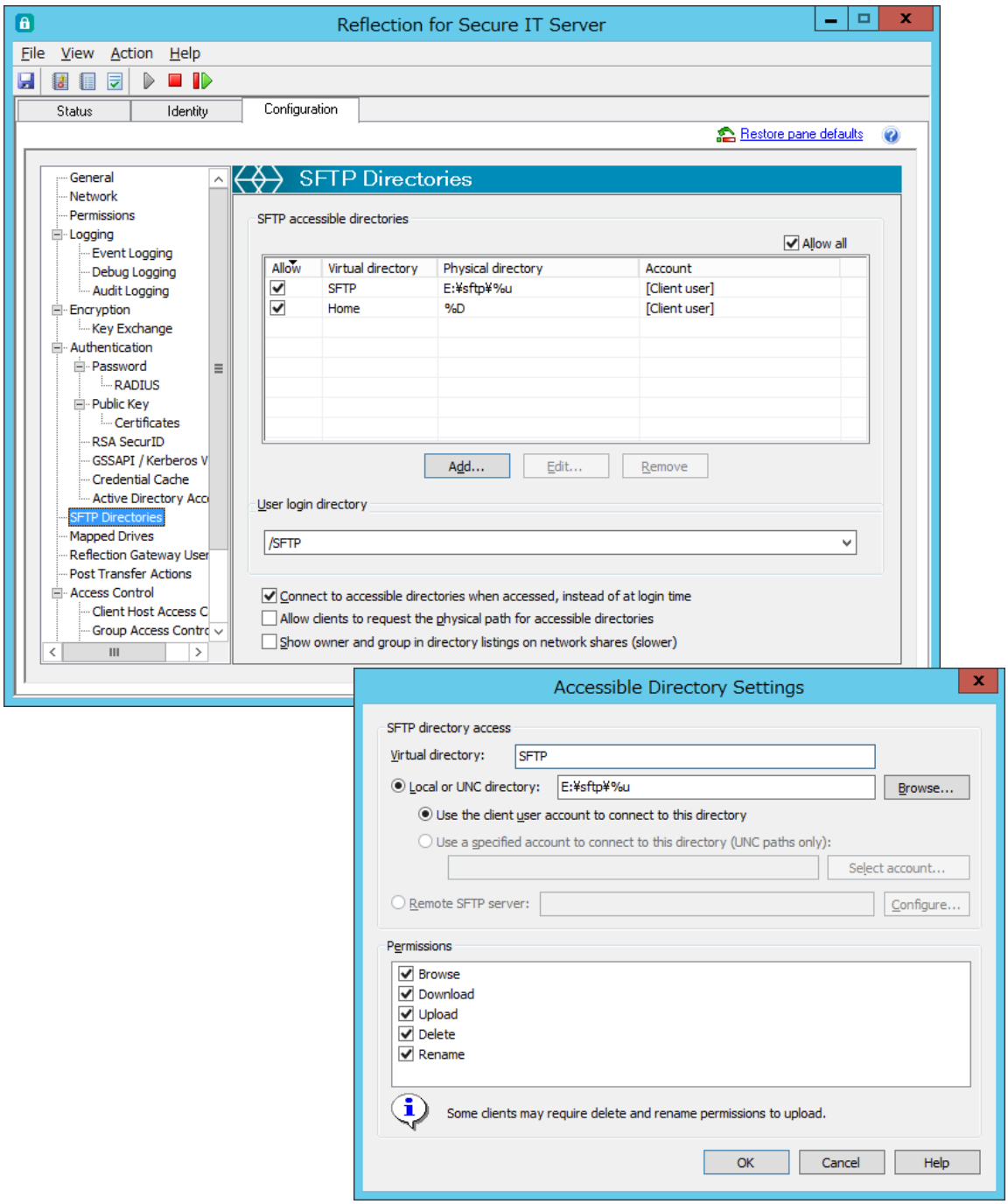
[Clear]ボタン

現設定内容をクリアします。

[Select credential]ボタン

[Select Credential]ダイアログボックスを開きます。その中で、既存ユーザ Credential キャッシュの中から選択指定するか、新規ユーザを選択指定します。

4.2.19 [SFTP Directories] 設定画面



本設定画面において、クライアントからの SFTP および scp アクセスにおけるアクセスユーザに対する ①アクセス許可範囲の指定、②ログインホームディレクトリの指定 をします。

[SFTP Accessible directories]

アクセス許可範囲をその最上位ディレクトリを記述して指定します。複数列挙可能です。

追加指定は、[Add]ボタンをクリックし、表示[Accessible Directory Settings]設定画面から所定項目を入力します。

登録済み Directory に対し、"Allow"欄 チェックマークにて有効/無効を個別指定可能です。

右上[Allow all]操作を使いチェックマークの一括操作も可能です。

[User login directory]

ログインホームディレクトリを指定します。プルダウンメニューに表示する"Virtual directory"名称から選択指定します。 デフォルトは、"/Home" です。

[Connect to accesible directories when accessed, instead of at login time]

設定した"SFTP accessible directories"先を内部接続するタイミングを規定します。

チェックオン時(有効時)(デフォルト)は、ログイン処理の時点では全登録 directory を内部接続せずに、実際に接続要求された時に接続します。

チェックオフ時(無効時)は、ログイン処理の段階で全登録 directory を内部接続します。登録 directory が極端に多い特別な使用環境の場合にログイン処理に時間要する場合があるので注意が必要です。

[Allow clients to request the physical path for accesible directories]

本設定はグレーアウト無効化されていませんが、[Reflection Gateway Users]設定画面同様、RSIT Windows サーバには関係ない設定項目です。実質 機能しませんので無視して下さい。

[Show owner and group in directory listings on network shares (slower)]

sftp クライアントへの ls -l コマンド 所有者/グループ名表示仕様を既定します。

本設定をチェックオフ(無効)(デフォルト)指定し、かつ"SFTP accessible directories"指定欄の"Physical directory"指定が UNC パス表記の場合に限り、その配下のファイル/ディレクトリの所有者/グループ名情報を取得返送しない動作仕様です。

システム構成によっては、対象となる全所有者/グループ名の情報取得に長時間を要し、コマンド返送が極端に遅くなり、結果的に sftp 処理全体が遅くなるのを回避するために設けました。

[Accessible Directory Settings]ダイアログボックス:

[SFTP directory access]

[Vitual directory]

最上位ディレクトリに仮想名称を指定します。クライアントから見た時に最上位ディレクトリ位置は本仮想名称で表示されます。

[Local or UNC directory]

ローカルの指定最上位ディレクトリを絶対パスで指定するか、共有フォルダの指定最上位ディレクトリを UNC 表記で指定します。(尚、ネットワークドライブには未対応です。)

[Browse]ボタンから選択指定することも可能です。

また指定には、パターンストリング("%D","%H","%u","%U")を使用可能です。

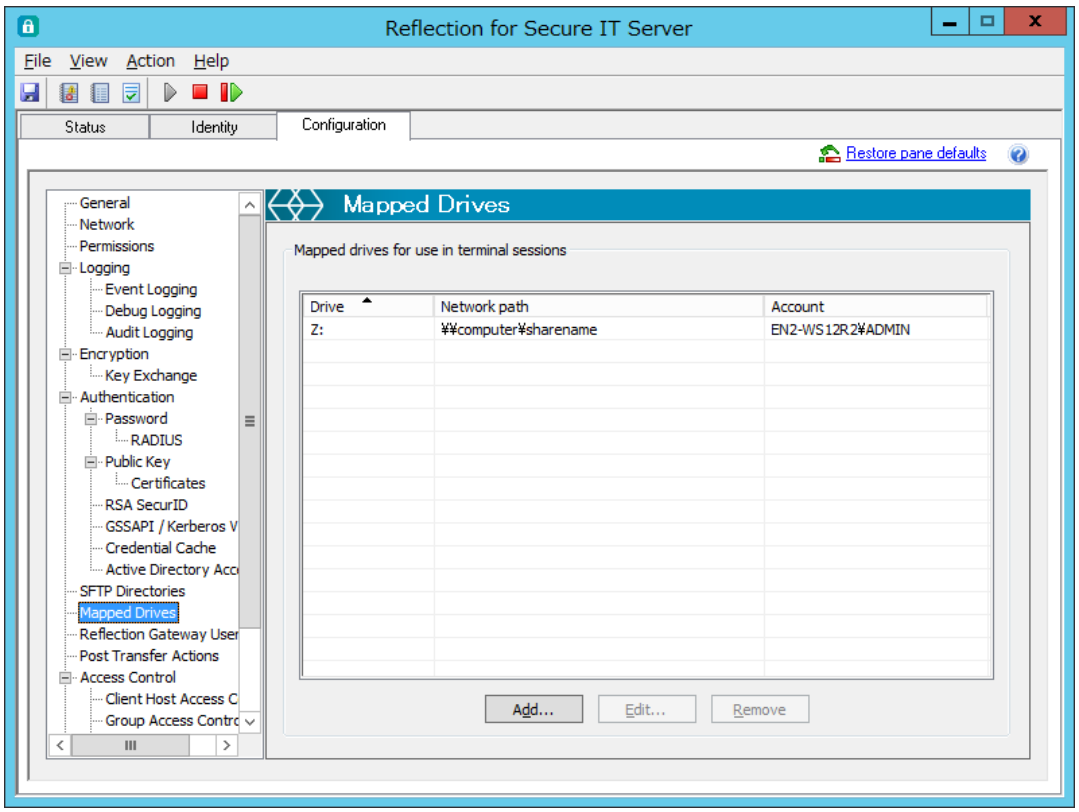
・%D：ユーザプロファイルフォルダ　　・%H：ユーザホームフォルダ

・%u：ユーザログイン名　　・%U:ドメインユーザログイン名 (domain.username の書式)

[SFTP directory access]

指定 Directory 毎に、パーミッション{Browse, Download, Upload, Delete, Rename}を個別に指定可能です。

4.2.20 ［Mapped Drives］設定画面



本設定画面において、ネットワークドライブをマッピング定義し、クライアントからのターミナル接続をアクセス可能とします。

Mapped drives for use in terminal sessinons 欄

[Drive]

マッピングされたドライブ文字を表示します。

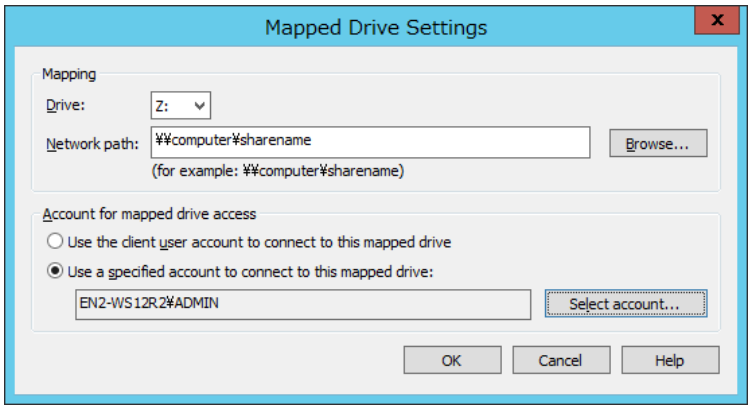
[Network path]

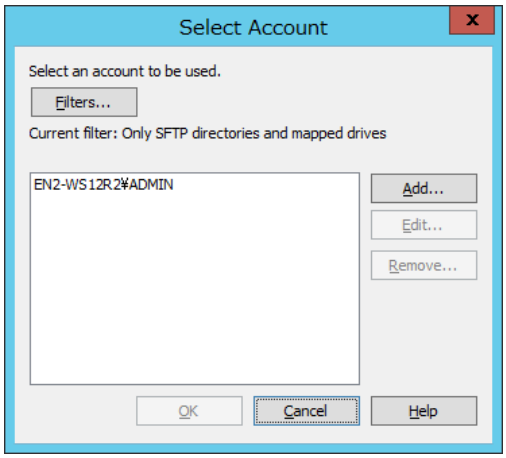
マッピングされたネットワークパスを UNC 形式で表示します。

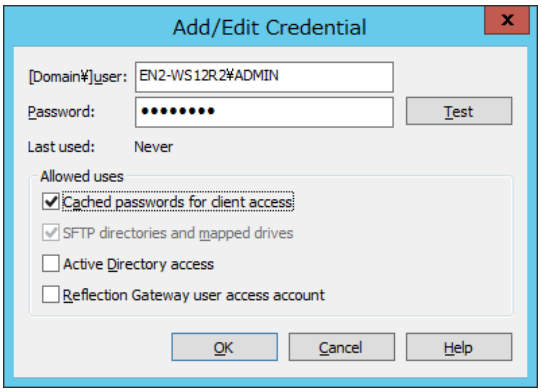
[Account]

登録した認証情報でアクセス権を得ているユーザ名を表示します。

[Client user]と表示している場合は、アクセスユーザが使用する認証情報を使います。







[Mapped Drives Settings]ダイアログボックス:

Mapping

[Drive:]

プルダウンメニューで表示する未割当のドライブ名から選択します。

[Network path:]

定義するネットワークパスを UNC 形式で指定します。〔例：¥¥computername¥path¥folder〕

直接入力するか、[Browse]ボタンクリックの上、[フォルダの参照]画面を操作して選択します。

Account for mapped drive access

[Use the client user account to connect to this mapped drive]

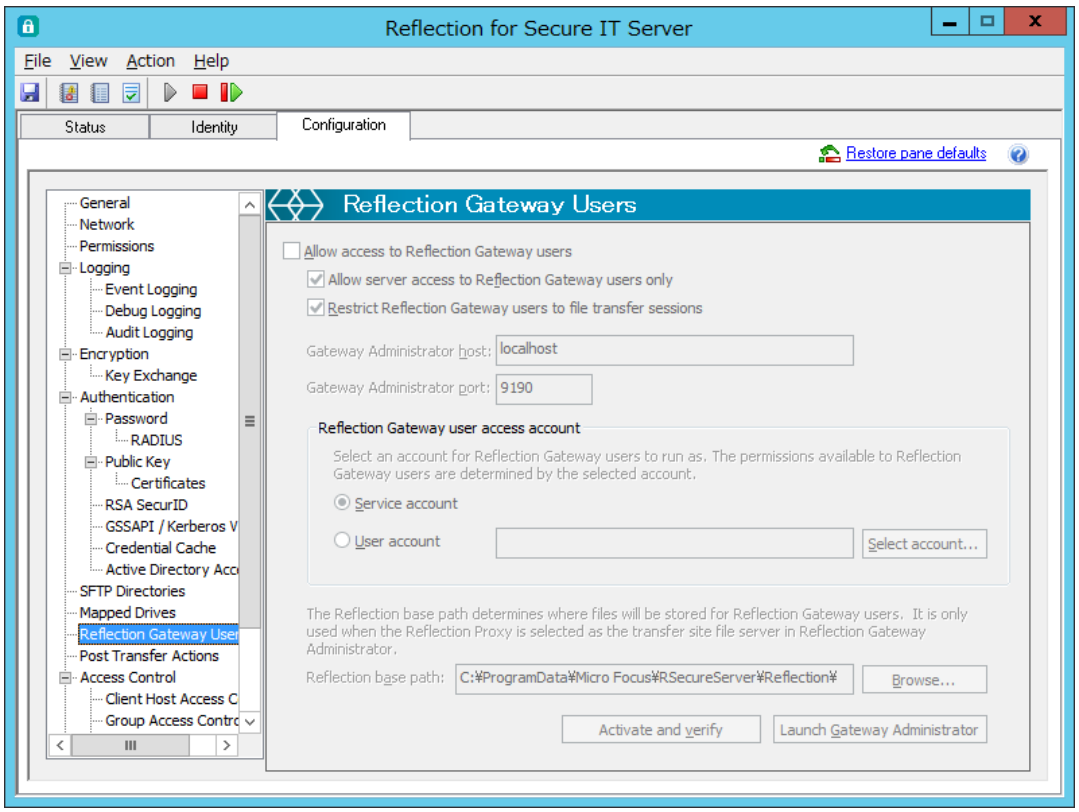
選択時(デフォルト)、クライアントユーザが持つユーザ認証情報を使いアクセス先ネットワークパスへのアクセス可否の認証を受けます。

[Use a specified account to connect to this mapped drive:]

選択時、定義ネットワークパスへは、ここで定義するユーザアカウントとパスワードを使いアクセスします。[Select account]ボタンをクリックし、[Select Account]設定画面を表示した上で、ユーザ認証情報を登録定義します。

[Select Account]設定画面上の [Add],[Edit]ボタン操作にて、更に[Add/Edit Credential]設定画面を表示し、個々のユーザ認証情報を登録定義します。

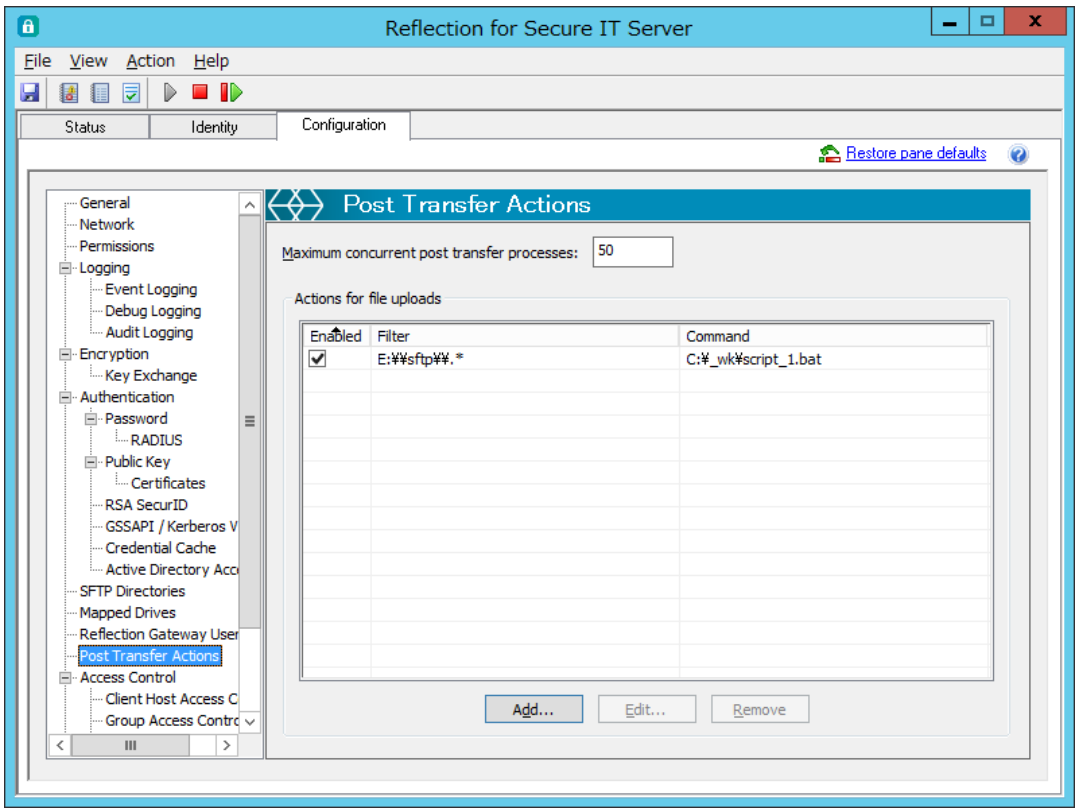
4.2.21 ［Reflection Gateway Users］設定画面



本設定画面は、RSIT Windows サーバの場合、画面全体がグレーアウトし無効化されています。

本設定画面は、Micro Focus 社 別製品 Reflection Gateway に含まれる SSH サーバ機能設定用に使われます。
Reflection Gateway SSH サーバ機能と RSIT Windows サーバとを共通化しているために本画面が見えています。

4.2.22 [Post Transfer Actions] 設定画面



"Post Transfer Actions" は、ファイルを正常受信時にその条件を判定し、条件合致時に指定コマンドを起動する機能です。本設定画面から、その起動条件とコマンドを指定します。

[Maximum concurrent post transfer processes]

起動可能なコマンドの同時動作上限値を指定します。デフォルト"50"、値"0"は無制限の意。

Action for file uploads

[Enabled]

登録済み Filter,Command 指定内容に対し、チェックマークにより有効/無効を指定します。

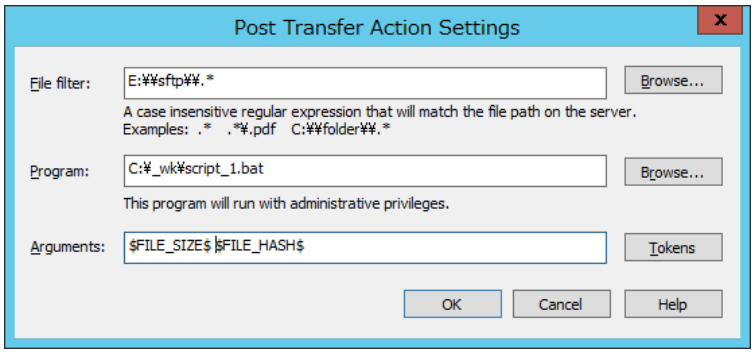
[Filter]

ファイル受信時のコマンド起動条件です。

[Command]

コマンド実行ファイルやバッチファイルを絶対パスで指定します。

[Post Transfer Action Settings]ダイアログボックスから入力,編集します。



[Post Transfer Action Settings]ダイアログボックス:

[Add], [Edit]ボタンの押下により、本設定画面を表示し新規作成、編集します。

[File filter]

ファイル受信時のコマンド起動条件を正規表現を使い指定します。

〔条件例：指定フォルダに受信、指定名称のファイルを受信、受信時無条件に起動 等〕

フォルダ位置を指定する場合、[Browse]ボタンから選択指定可能です。その場合は、指定先フォルダパスとその配下全ファイル(¥¥.*)が正規表現により自動的に入力されます。

パスやファイル名を手入力する場合､区切り記号"¥"や拡張子"."は正規表現のメタキャラクタですので、エスケープ文字"¥"を追加し、"¥¥"、"¥."と記述します。

[Program]

コマンド実行ファイルやバッチファイルを絶対パスで指定します｡[Browse]ボタンから選択指定可能です。

コマンドプログラムの実行権限は、RSIT サーバサービスと同一のアカウント権限です。

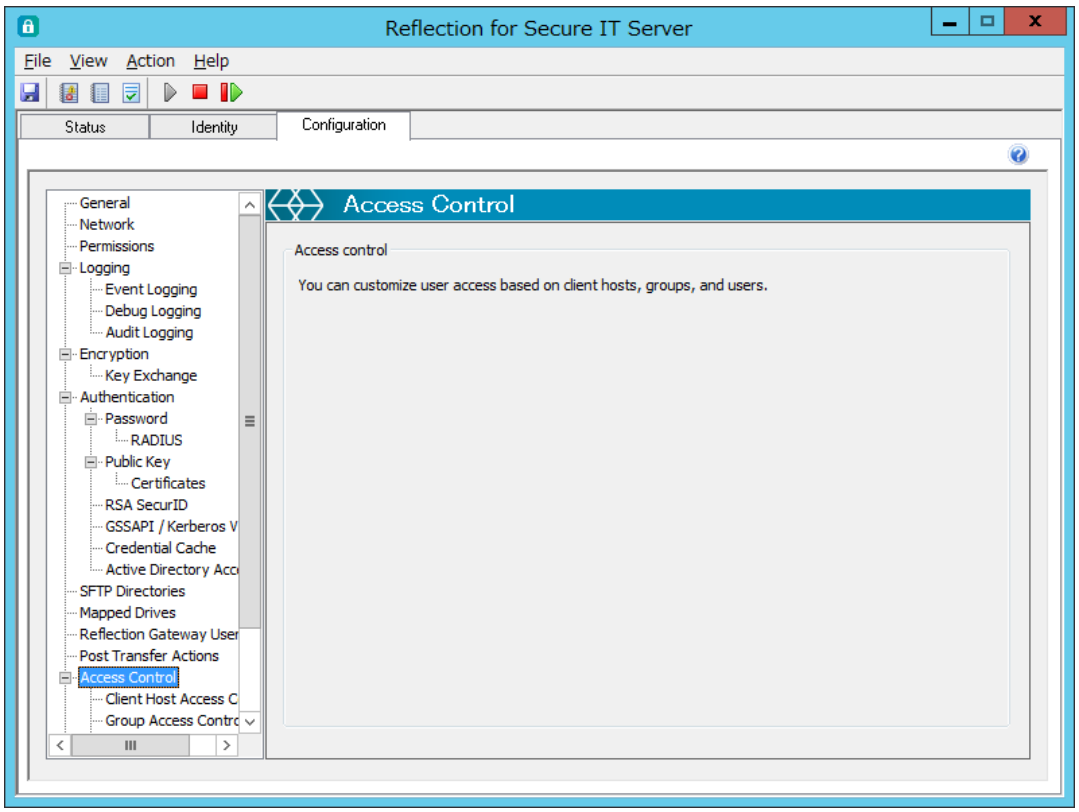
[Arguments]

トークン指定により バッチファイルスクリプトへ引数を渡すことができます。

[Tokens]ボタンを押下し、プルダウンメニューから選択します。

トークン	内容	例
CLIENT_IP	接続クライアント IP アドレス	192.168.2.123
DATE	ファイル受信の日付	2014/11/07
FILENAME	受信ファイル名称	myfile.txt
FILE_HASH	受信ファイルの SHA-1 ハッシュ値	8439cbbf04f2b10acd32844ee0983bd1bc3175d3
FILE_PATH	受信フォルダのパス	E:¥sftp¥ichiro
FILE_SIZE	受信ファイルの容量(Byte)	7326
FULL_PATH	受信ファイル名称含むパス	E:¥sftp¥ichiro¥myfile.txt
INITIATOR_USERID	ユーザ名	mydomain¥ichiro
TIME	ファイル受信の時刻	14:26:59
TIMEZONE	サーバのタイムゾーン	+0900

4.2.23 [Access Control] 設定画面



[Access Control] 設定として、３つの観点からアクセス制御(許可/拒否指定)を指定可能です。

① [Client Host Access Control]：クライアント単位で指定

② [Group Access Control]：グループ単位で指定

③ [User Access Control]：ユーザ単位で指定

各設定とも[Add]、[Edit] ボタンからダイアログボックスを表示し、入力編集します。

クライアント/グループ/ユーザの指定内容との一致判定は正規表現規則に従い判定します。

指定内容は次の規則に従い適用されます。

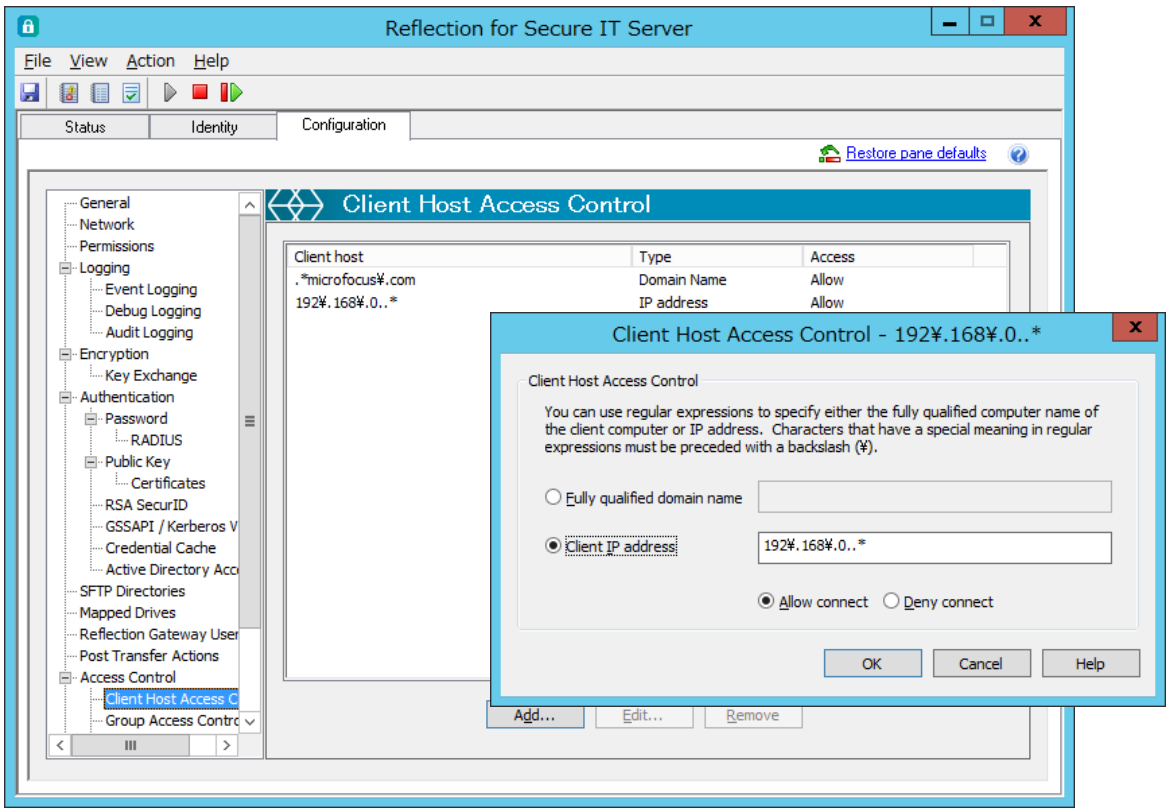
1) クライアント単位の"拒否"に該当する場合は、グループ単位/ユーザ単位の指定内容にかかわらずアクセスは拒否されます。

2) クライアント単位の"拒否"に該当しない場合、次にいずれかの設定画面に個別の"許可"指定が存在するかどうかを確認します。

2a) 個別の"許可"指定が全く存在しない場合は、アクセスは許可されます。

2b) いずれかの設定画面で個別の"許可"指定が存在する場合は、その"許可"指定条件に合致しない限り、アクセスは拒否されます。

4.2.24 [Client Host Access Control] 設定画面



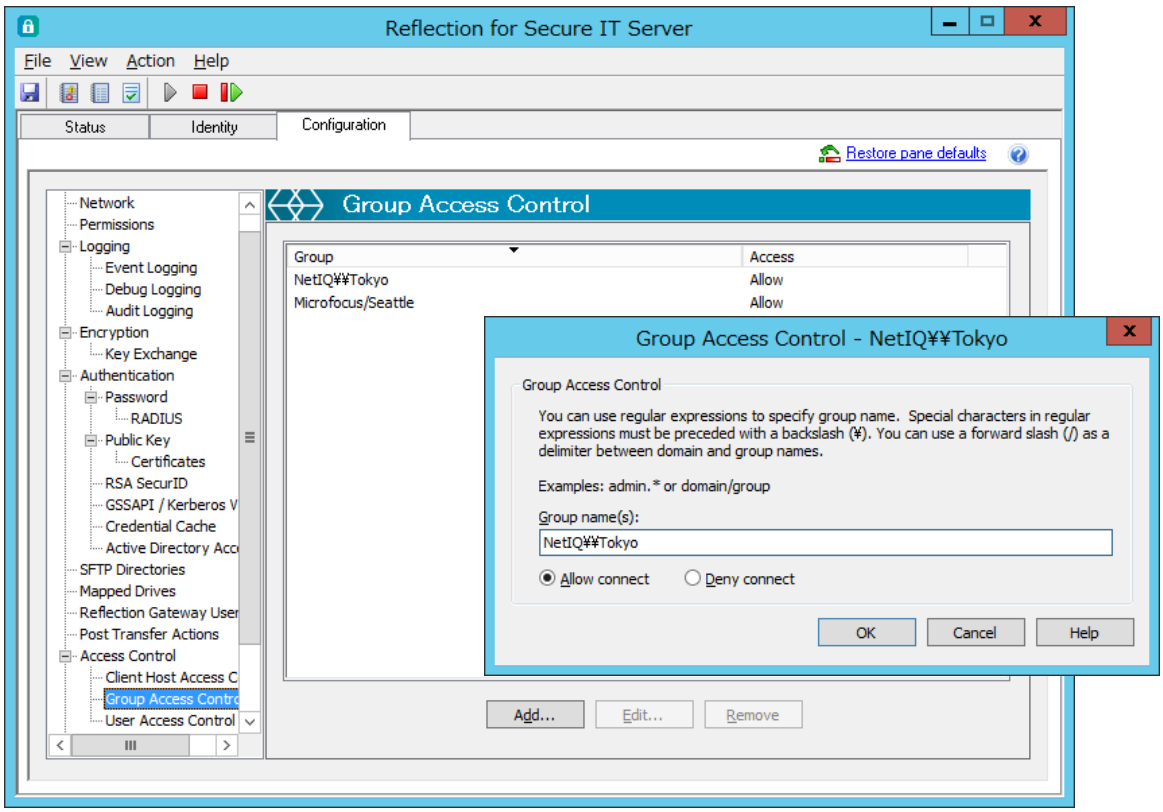
クライアント単位でのアクセス制御(許可/拒否指定)を指定します。

[Add]、[Edit] ボタンをクリックし、ダイアログボックスから入力編集します。

指定は、ドメイン名か IP アドレスにて指定します。

記述内容の一致判定は正規表現規則に従います。区切り記号"."(ドット)は正規表現のメタキャラクタですので、エスケープ文字"¥"を追加し、"¥."と記述します。

4.2.25 ［Group Access Control］設定画面



グループ名指定によりアクセス制御(許可/拒否指定)を指定します。

[Add]、[Edit] ボタンをクリックし、ダイアログボックスから入力編集します。

Windows Active Directory ドメインのグループ名指定の書式は、以下の通りです。

1) ①ドメイン名/グループ名 ②ドメイン名¥¥グループ名 のいずれも可能です。

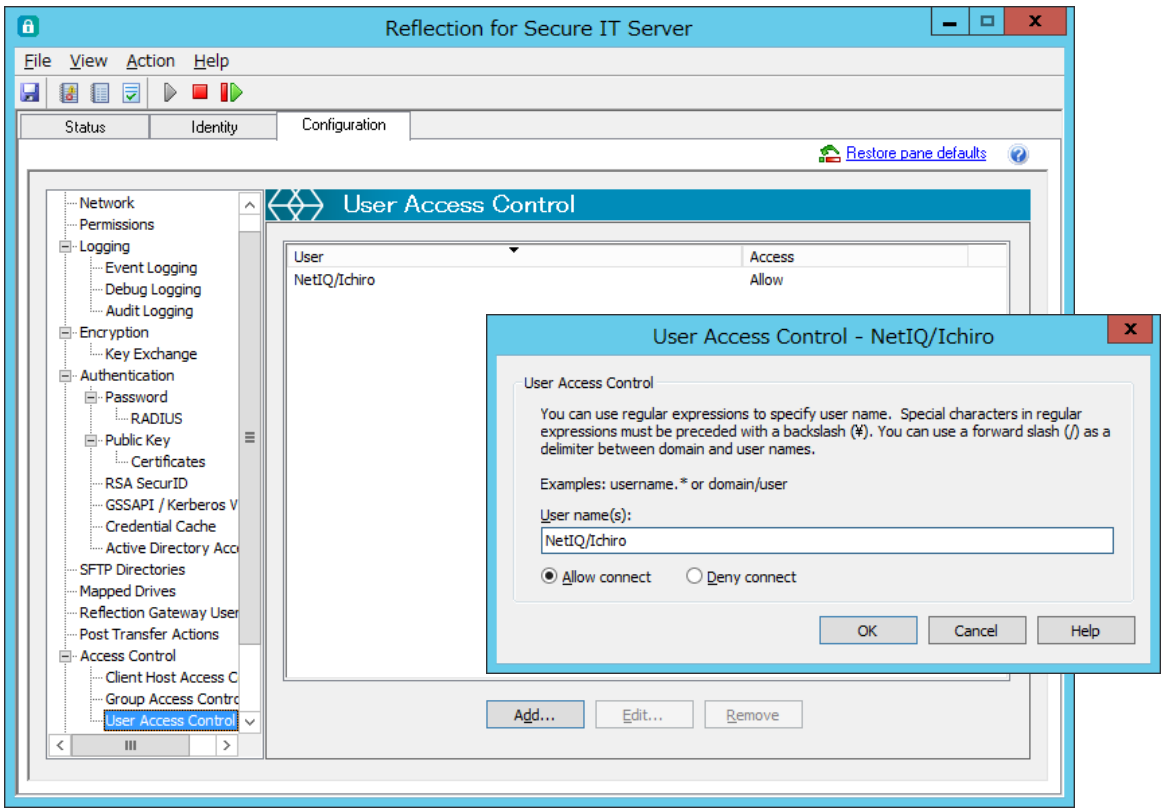
2) グループ名にスペースを含む場合は、"[ ]"(大かっこ)で囲みます。

注記：

記述内容の一致判定は正規表現規則に従います。

ドメイン名.グループ名 の書式でも一見動作する場合が多いのですが、メタキャラクタ ".(ドット)" と解釈され、改行を除く任意の一文字扱いになります。よって、".(ドット)"の位置を別な文字に置き換えた内容とも合致することになります。

4.2.26 [User Access Control] 設定画面



ユーザ名指定によりアクセス制御(許可/拒否指定)を指定します。

[Add]、[Edit] ボタンをクリックし、ダイアログボックスから入力編集します。

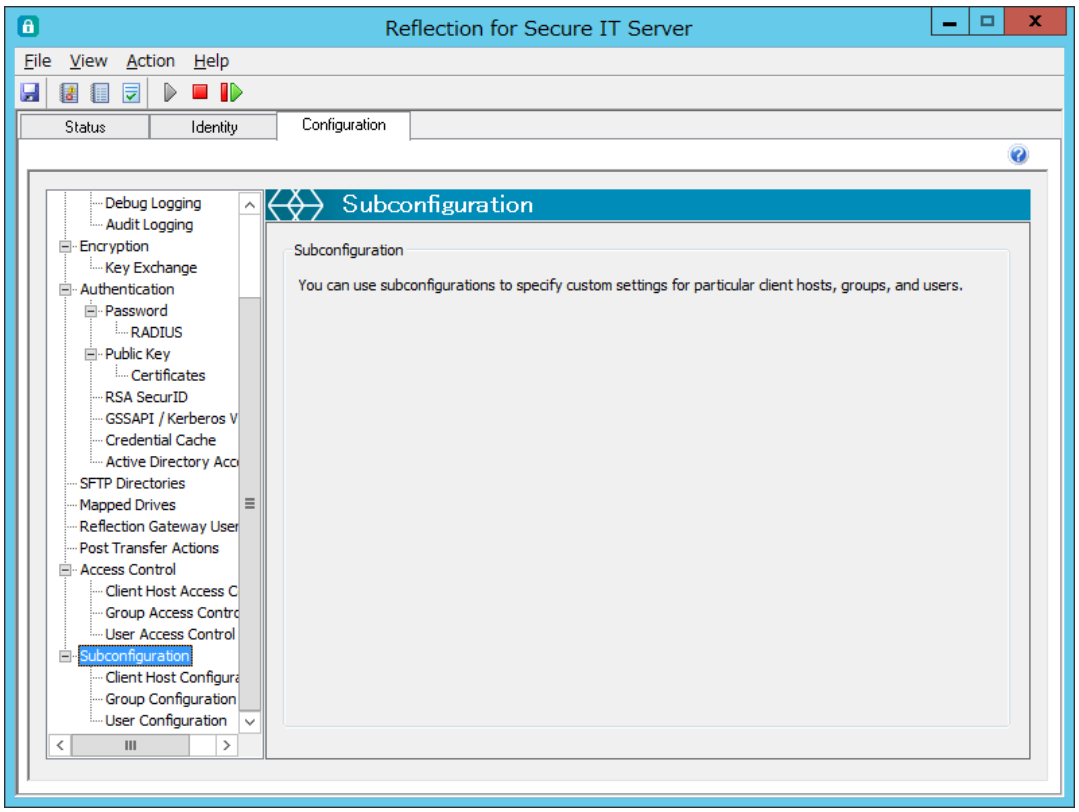
ドメインユーザ名指定の書式は、①ドメイン名/ユーザ名 ②ドメイン名¥¥ユーザ名　のいずれも可能です。

注記：

記述内容の一致判定は正規表現規則に従います。

ドメイン名．ユーザ名 の書式でも一見動作する場合が多いのですが、メタキャラクタ ″.(ドット)″ と解釈され、改行を除く任意の一文字扱いになります。よって、″.(ドット)″の位置を別な文字に置き換えた内容とも合致することになります。

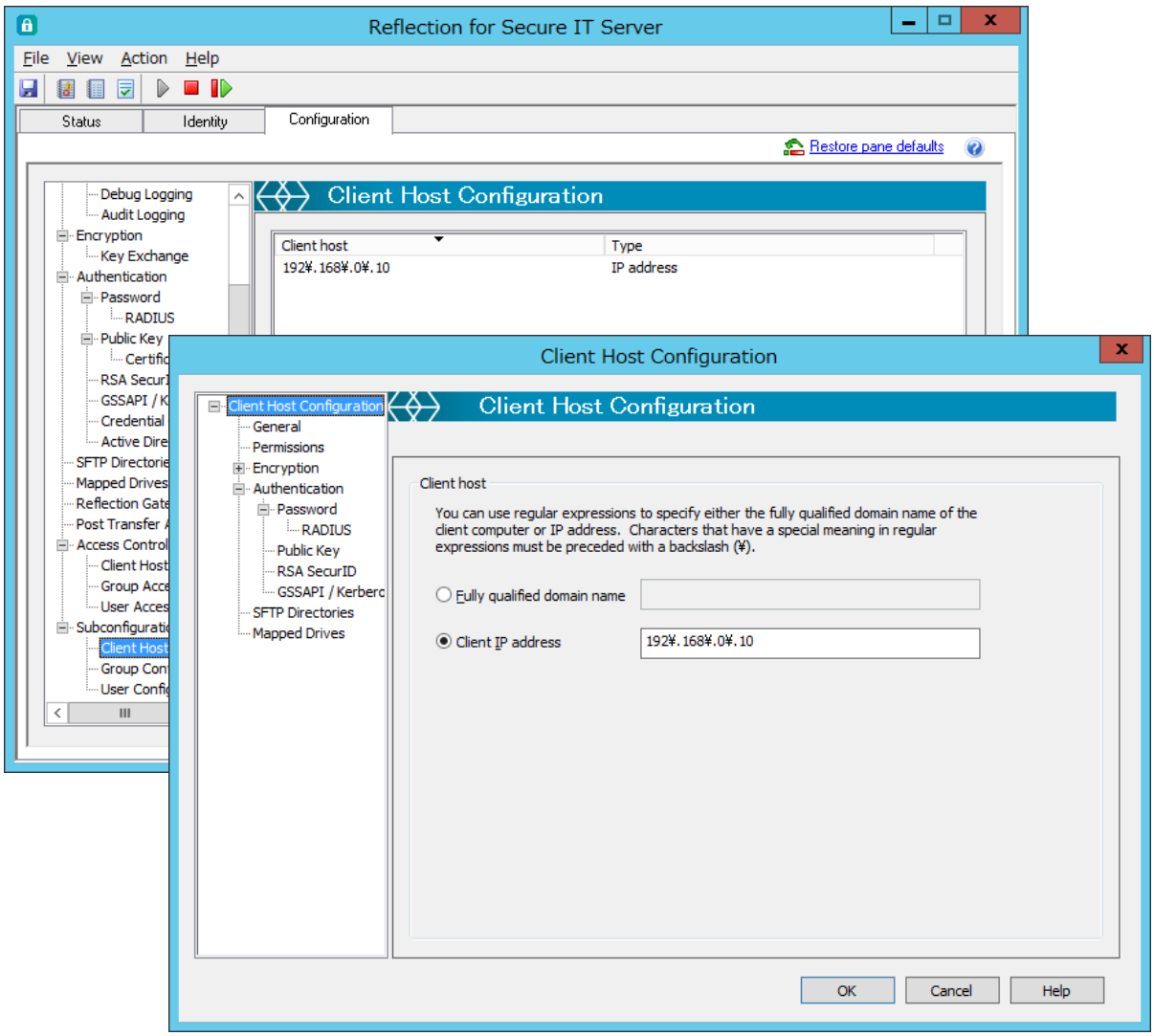
4.2.27 [Subconfigration] 設定画面



これまでの設定内容は導入したマシン共通に適用されます。これに対し、クライアント(Client Host Configuration) /グループ(Group Configuration) /ユーザ(User Configuration) 個別にサブコンフィギュレーション(Subconfiguration)を指定し、共通設定内容より高優先の指定が可能です。

RSIT Windows サーバは、次の順位で設定内容を読み込み、後から読み込んだ内容を上書きします。
①共通設定 ⇒ ② Client Host 個別設定 ⇒ ③ Group 個別設定 ⇒ ④ User 個別設定
よって最終的には、④>③>②>① の優先順位にて設定内容が適用されます。

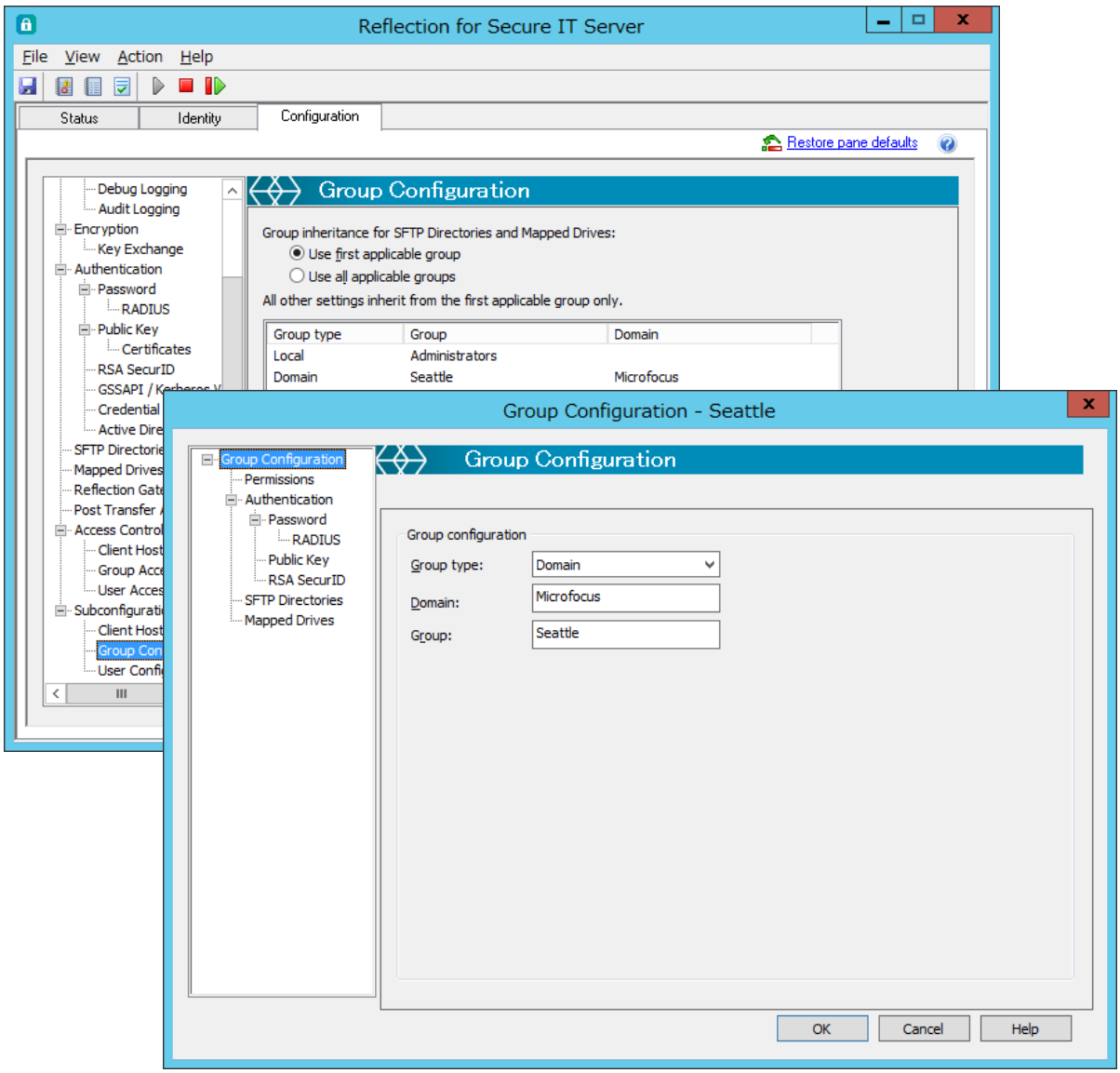
4.2.28 [Client Host Configration] 設定画面



設定画面内［Add］、［Edit］ボタンをクリックし、［Client Host Configuration］ダイアログボックスを表示し、指定クライアント(Client Host)に対して共通設定内容よりも高優先の個別指定をします。

クライアントとして ドメイン名か IP アドレスにて指定後に、左欄より設定内容を選択し、専用画面を通じて入力編集します。

4.2.29 [Group Configration] 設定画面



設定画面内 [Add]、[Edit] ボタンをクリックし、[Group Configuration] ダイアログボックスを表示し、指定グループ名に対して共通設定内容よりも高優先の個別指定をします。

グループ名を指定後に、左欄より設定内容を選択し、専用画面を通じて入力編集します。

リストに表示のグループは上位行ほど優先されます。[Move up],[Move down]ボタンで操作します。

ユーザが複数グループに所属する場合の扱いについて：

a)設定項目："SFTP Directories", "Mapped Drivers"

・**"Use first applicable group"選択時：**

～リストの中で最上位の該当グループの内容が適用されます。

・**"Use all applicable groups"選択時：**

～リスト中 該当全グループの内容が適用されます。但し 下記詳細条件を配慮します。

①"User login directory"は、リスト中最上位グループの指定内容に従う。

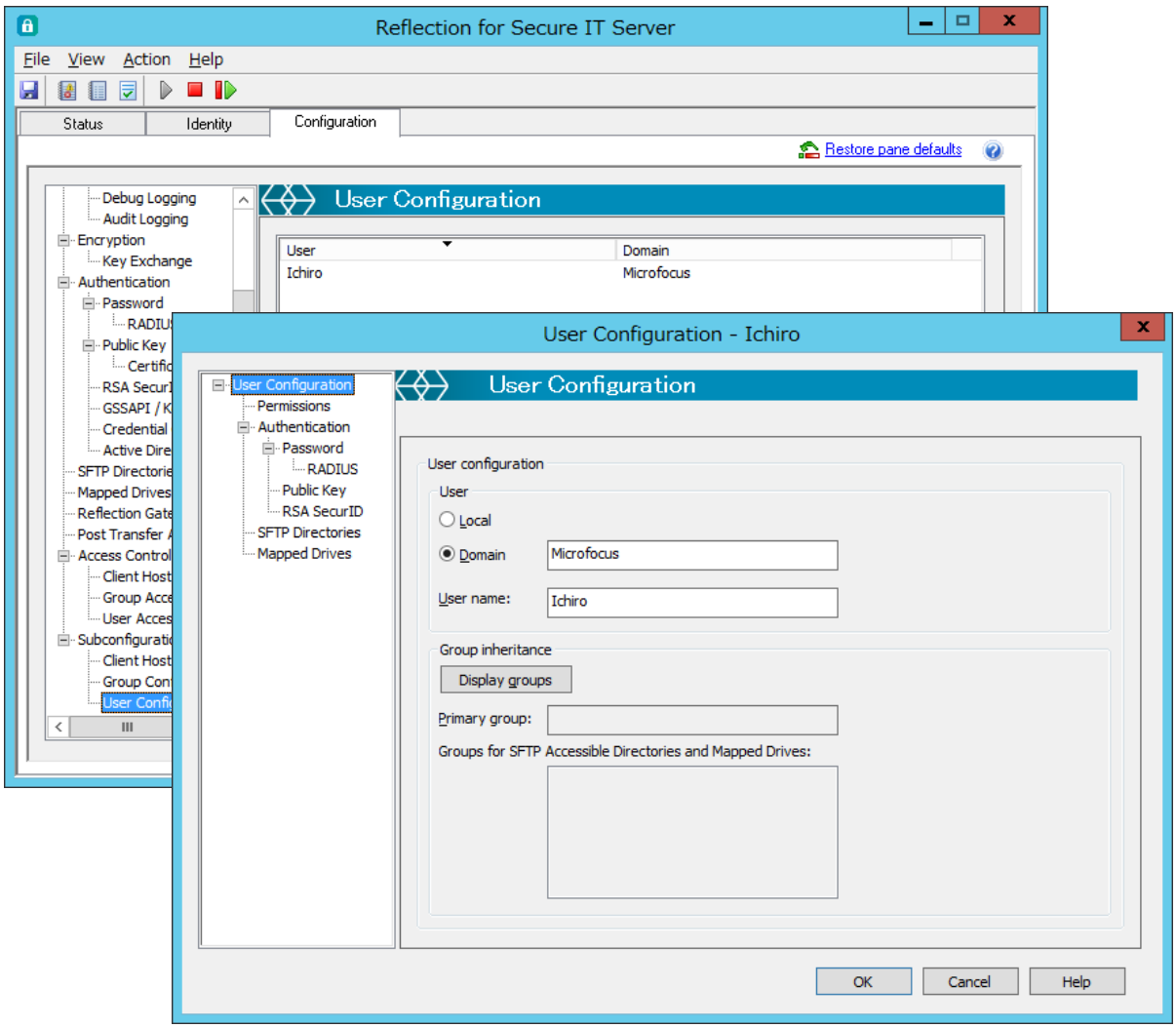
②"Inherit directories","Inherit drivers" を非選択時には、その内容は継承せず。

③同一"Virtual directory"名称が重なった場合、リスト中上位のグループ内容を適用。

b)設定項目："Permissions", "Authentication"

～常にリストの中で最上位の該当グループの内容が適用されます。

4.2.30 [User Configration] 設定画面



設定画面内［Add］、［Edit］ボタンをクリックし、［User Configuration］ダイアログボックスを表示し、指定ユーザ名に対して共通設定内容よりも高優先の個別指定をします。

ユーザ名を指定後に、左欄より該当設定画面を選択し、専用の設定画面を通じて入力編集します。

5. 付録

5.1 正規表現ルール

[Access Control]や[Post Transfer Actions]条件判定に使用する正規表現基本ルールを示します。

文字	説明
.	任意の 1 文字に一致。
[ ]	文字クラスを指定し、[ ]で囲まれた文字の中のいずれかに一致。 例えば、[abc] は "a","b", "c" と一致。
^	入力文字列の先頭と一致。
-	範囲を示します。例えば、[0-9]は "0"から"9"の任意の文字に一致。
?	直前のサブ式と 0 回または 1 回一致。 例えば、[0-9][0-9]? は "2"でも"12"でも一致。
+	直前のサブ式と 1 回以上一致。例えば、[0-9]+ は "1"や"13", "456"等に一致。
*	直前のサブ式と 0 回以上一致。
??, +?, *?	修飾子(?, +, *)の直後に"?"を指定し一致パターンを制限。 (?, +, *)単独の場合はできるだけ多数の文字列と一致するのに比べて、直後に"?"を指定した場合はできるだけ少ない文字列と一致。
( )	( )で囲んだ内容をグループ化。
¥, \	エスケープ文字。
$	入力文字列の末尾と一致。
|	選択肢を区切り、左右に置かれた部分正規表現のいずれかに一致。

 # 適用規則:

1) [Post Transfer Actions]の Filter 条件は、Perl 正規表現構文規則に従います。
詳細は、下記解説ページ等を参照下さい。
http://www.boost.org/doc/libs/1_44_0/libs/regex/doc/html/boost_regex/syntax/perl_syntax.html

2) [Access Control]の判定は、Basic Regular Expression (BRE) 構文規則に従います。
また、下記省略表記も適用されます。

文字	説明
¥a, \a	任意英数字一文字：([a-zA-Z0-9])
¥b, \b	空白：([¥¥t])
¥c, \c	任意英字一文字：([a-zA-Z])
¥d, \d	任意十進数一文字：([0-9])
¥h, \h	任意十六進数一文字：([0-9a-fA-F])
¥n, \n	改行：(¥r|(¥r?¥n))
¥q, \q	引用文字列：(¥"[^¥"]*¥")|(¥'[^¥']*¥')
¥w, \w	任意英字：([a-zA-Z]+)
¥z, \z	整数：([0-9]+)