# WinGate 8

## ユーザーガイド

---

発売元　Qbik New Zealand Limited

WinGate サイト：WinGate に関する最新情報は以下のサイトをご覧ください。

http://www. wingate.jp/　（日本語）

TechnoBlest

目次

**目次** ..... **2**
**はじめに** ..... **6**
**WinGate について** ..... **7**
WinGate8 の代表的なインターフェース ..... 8
WinGate で取得可能なログ ..... 9
**最小システム必要条件** ..... **10**
**WinGate のライセンスについて** ..... **10**
**WinGate の種類による機能の違い** ..... **11**
**その他のご注意:** ..... **12**
WinGate のインターネット共有接続について ..... 12
インターセプト・プロキシとは？ ..... 13
**試用版、および試用版グレードの変更について** ..... **13**
**WinGate8 からの新機能** ..... **14**
**WinGate7 からの新機能** ..... **14**
**WinGate6 をご利用いただいておりますお客様へのご注意（重要）** ..... **17**
WinGate6 からの変更 ..... 19
WinGate6 からのアップグレードで必要になること（継承されない内容） ..... 19
WinGate がアップデート時に行うこと ..... 19
ユーザー・データーベース選択後に WinGate が行うこと ..... 20
WinGate7、WinGate8 で互換性があり、そのまま継承される内容 ..... 20
WinGate7、WinGate8 で異なって動作する内容 ..... 20
WinGate7、WinGate8 で失われた機能 ..... 21
Kaspersky AntiVirus for WinGate をご利用のお客様へのご注意（重要） ..... 21
**WinGate の主な機能とその概要** ..... **22**
サービス ..... 22
プロキシサービス機能 ..... 23
その他の機能 ..... 23
WinGate アップデート ..... 24
**WinGate の新規インストール** ..... **25**
インストールの前に（重要） ..... 25
**WinGate インストールチェックシート** ..... **27**
インストールの開始 ..... 28
**WinGate8.x のアップグレード（WinGate8 最新バージョンの適用、および WinGate7 からのアップグレード）** ..... **35**
アップグレード時の注意点 ..... 35
アップグレード時の注意点（WinGate 8.1.0 へのアップグレード） ..... 35
アップグレード前の確認事項 ..... 36
インストール方法 ..... 38
インストール共通手順 ..... 40
**旧バージョンからのアップグレード（WinGate6.xからのアップグレード）** ..... **44**

バージョンアップの際の注意点（必ずお読みください）....44
WinGate6 から WinGate8 で引き継がれない設定....44
ユーザー・データーベースについて....45
メールサーバー機能をご利用いただいておりお客様へのご注意....45
WinGate7 以降で変更される機能....45
WinGate7、および WinGate8 で失われた機能....46
バージョンアップを行う前に（最終確認のお願い）....46
WinGate6.6 から WinGate 最新版へのアップグレード....47
スタートアップメニューの重複について....54
インストール完了後の注意点、および確認事項....55
その他の旧バージョン（WinGate2.x、WinGate3.x、WinGate4.x）からのバージョンアップについて....56
**WinGate のアンインストール....57**
**インストール完了後に行う内容（新規インストール）....59**
ライセンスアクティベーション....59
WinGate Management へのログイン....66
WinGate users database engine を指定した場合、の Administrator パスワードの設定方法....72
**インストール完了後に確認する内容（新規インストール）....73**
必要となるサービス、サーバー機能の追加....73
ネットワーク接続の確認（重要）....73
Notifications（通知）....76
ログ取得内容の確認（重要）....79
ログのクリーンナップ....80
DNS Client（DNS クライアント）設定の確認....80
使用しない機能の停止....81
**クライアントマシンの構成....82**
はじめに....82
クライアントマシンでの TCP/IP のインストール....82
クライアントマシンの TCP/IP 設定（DHCP の構成）....82
**WinGate 詳細....84**
WinGate Management（WinGate マネージメント）について....84
メニューバー....86
WinGate Management 各項目の概要....88
各項目、および機能の説明....89
Welcome（ようこそ）....89
Monitoring（モニタリング）....89
Activity（アクティビティ）....89
Dashboard（ダッシュボード）....90
DHCP....90
Email....91
Notifications（通知）....92
Timeline（タイムライン）....92

VPN ....98
Web Access Control（Web アクセス・コントロール） ....98
Control Panel（コントロール・パネル） ....103
Certificates（証明書） ....103
Credential rules（信任ルール） ....104
Data（データー） ....105
DNS Client（DNS クライアント） ....106
Event（イベント） ....108
Extended Networking（拡張ネットワーキング） ....108
HTTP Cache（HTTP キャッシュ） ....116
Licensing（ライセンス） ....124
Logging（ロギング） ....125
Module（モジュール） ....130
Network Connections（ネットワーク接続） ....131
Notifications Settings（通知設定） ....132
Performance counters（パフォーマンス・カウンター） ....133
Permissions（権限） ....134
Policy（ポリシー） ....135
Scheduled Events（スケジュール・イベント） ....136
Services（サービス） ....137
サーバー、サービス機能について ....140
個々のサービス固有の設定 ....155
User and Groups（ユーザーとグループ） ....161
VPN Settings（VPN 設定） ....169
WinGate Update（WinGate アップデート） ....169
Utilities（ユーティリティ） ....174
**WinGate 設定例 ....175**
クライアント PC から WWW Proxy Server を使用して Web サイトを参照 ....175
WinGate のプロキシ機能を使用してメールの送受信を行う（POP3 Proxy、TCP Mapping） ....177
Extended Networking（拡張ネットワーク）の NAT を使用する方法 ....183
WinGate インターネットクライアント（WGIC）を使用するクライアントの構成 ....183
WGIC のインストール ....183
クライアントマシンでのアプリケーションの実行 ....187
WinGate インターネット・クライアントの構成 ....187
クライアント PC の FTP クライアントソフトウェアから FTP を行う ....189
**WinGate メールサーバー機能 ....190**
メールサーバーの設定 ....190
**WinGate でよく利用される設定の事例 ....199**
ご注意：ポリシーに関して ....199
WWW Proxy Server でユーザー認証を行う ....199
ユーザーに特定の Web サイトのみの表示を認める、または特定の Web サイトの表示を許可しない。 ....211

決められた IP アドレスからの接続を許可する（または許可しない）①（ポリシー）.....216
決められた IP アドレスからの接続を許可する（または許可しない）②（Web アクセスコントール）.....225
プライベートアドレスの接続のみを許可する.....230
特定のページをキャッシュしない.....236
WinGate で発生したイベントを管理者に通知する.....249
多段プロキシの設定.....254
URL により使用する上位プロキシサーバーを振り分ける.....255
**通常のメンテナンス.....262**
**WinGate 設定情報の保存と復元.....263**
WinGate8.0.4 以降のバージョンをご利用の場合.....268
**WinGate のアクティベーションについて.....272**
ハードウェア、OS トラブル時などの WinGate アクティベーション情報の解除.....272
**トラブルシューティング.....273**
WWW Proxy を使用して Web サイトが表示できない.....273
WinGate のパフォーマンスに関するトラブルシューティング.....275
Extended Networking の無効化.....277
ログの確認方法について.....277
Diagnostic ログに記録される WWW Proxy server 関連のエラーとその内容について.....278
**アップグレード保証期間の確認.....279**
**アップグレード保証更新、Kaspersky AntiVirus for WinGate の購読期限更新の適用.....279**
**WinGate の種類、ユーザー数を変更した場合の適用方法.....282**
**お問い合わせに関して.....283**

## はじめに

この度は WinGate をご使用いただき、誠にありがとうございます。
WinGateは現在ご使用いただいております環境にインストールいただく事により、インターネット・ゲートウェイ・サーバ、プロキシサーバー、またメールサーバーとして動作するように自動的に構成されますが、WinGate は多くの機能を持っており、WinGateをご利用目的に合わせてご利用いただくためには、ネットワーク環境や使用環境に合わせて、より適切な設定を行っていただく必要があります。
WinGate のインストールを行う前に、WinGate の機能や設定内容をご理解いただく事により、より円滑に WinGate をご使用いただくことができます。

本書では、WinGate8.x の概要、及びインストールからご使用いただくまで、そして代表的な設定情報を記述しております。
より詳細な設定に関しましては、弊社までお問い合わせください。

WinGate8 をご使用いただく際に、本書をお役立ていただけると幸いです。

また、本書の内容は随時最新の情報に更新されております。最新のユーザーガイドに関しては、弊社 Web サイトをご参照ください。

### ご注意

1. 本書の内容は将来予告なしに変更する事があります。
2. 本ソフトウェア、及び本書を運用いただき生じた結果につきましては、一切の責任を負いかねますことをご了承ください。

### 著作権

Copyright © 2015 TechnoBlest Inc. All Rights Reserved.
Copyright © 2015 Qbik New Zealand Limited
このマニュアルの一部、または全てを許可なく複写する事はできません。

### 商標

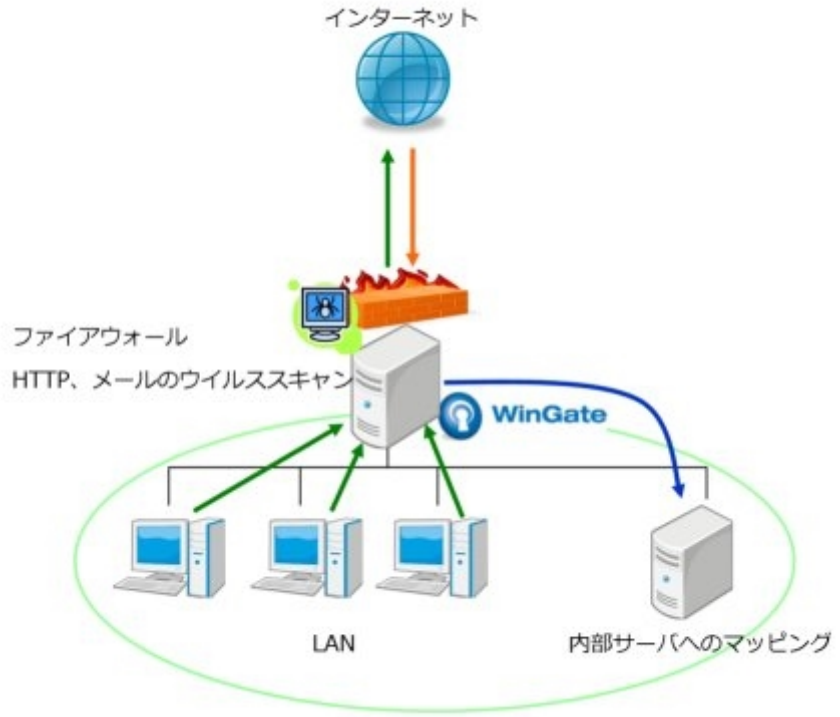
Windows は米国 Microsoft 社の登録商標です。その他、記載されている会社名、製品名等は各社の登録商標、または商標です。

**WinGate について**

WinGate はインターネット・ゲートウェイとして構成可能な統合型プロキシサーバ・ソフトウェアです。
プロキシサーバーとしての動作をはじめ、多くの機能を使用してインターネットの共有接続を提供いたします。
WinGate の主な機能は以下の通りです。

- ◆ プロキシ、NAT、WinGate インターネット・クライアントによる、インターネット接続の共有
- ◆ WinGate VPN による VPN（ヴァーチャル・プライベート・ネットワーク）のサポート
- ◆ ファイアウォール機能によるネットワークの保護
- ◆ 強力なポリシー機能によるアクセス制限
- ◆ ログファイル、アクティビティ、タイムラインによるユーザーの監視・管理
- ◆ WinGate メールによるメールサーバーの統合（POP3 サーバー、SMTP サーバー、IMAP4 サーバー）
- ◆ 他

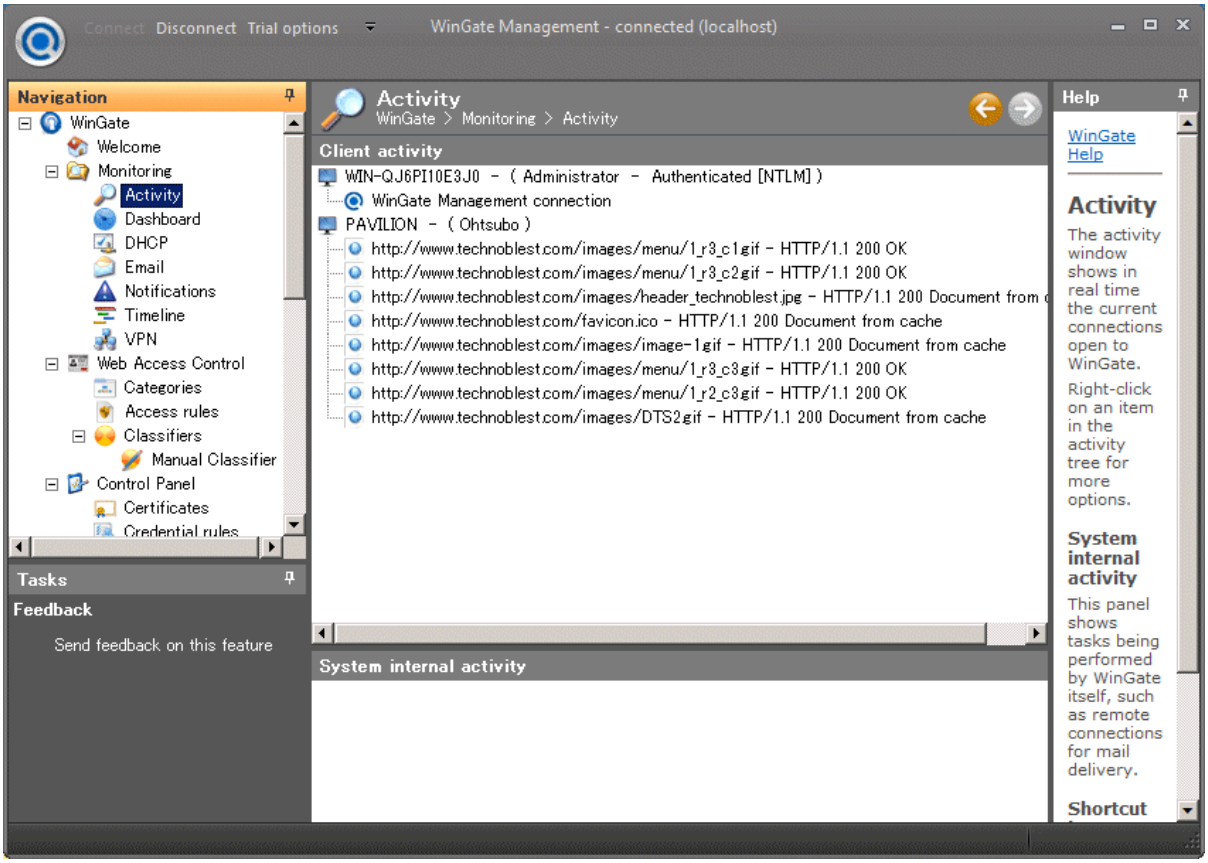
このように WinGate は多くの機能をもっており、全ての機能を同時に使用することが可能です。
しかしながら、お客様の環境では必要としない機能があるかもしれません。
WinGate の機能をご理解いただき、目的にあった WinGate の構成を行っていただくために本書を利用ください。



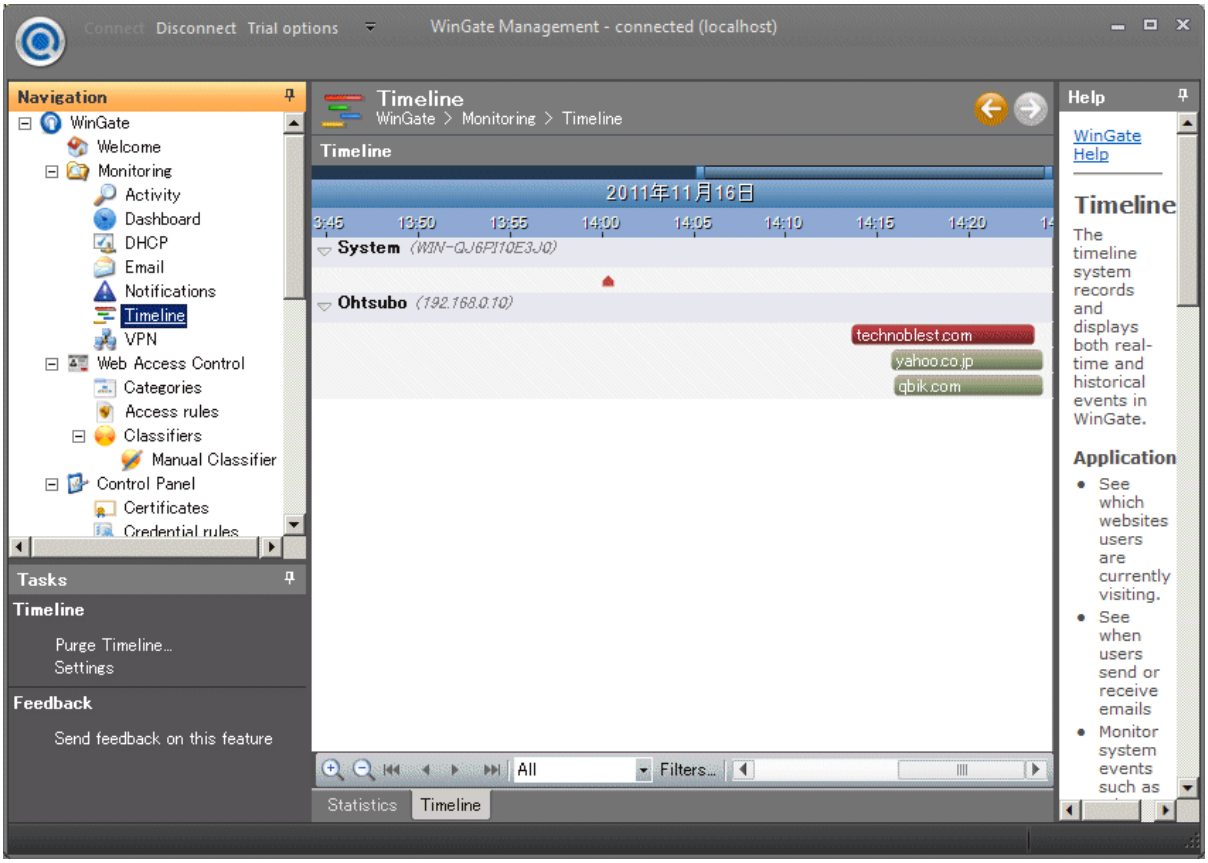

WinGate は Windows のシステムサービスとして動作する WinGate エンジンと設定や管理を行う管理ツールである WinGate マネージメントに分かれます。WinGate の動作は、タスクトレイに表示される WinGate エンジンアイコンで確認することができます。

## WinGate8 の代表的なインターフェース

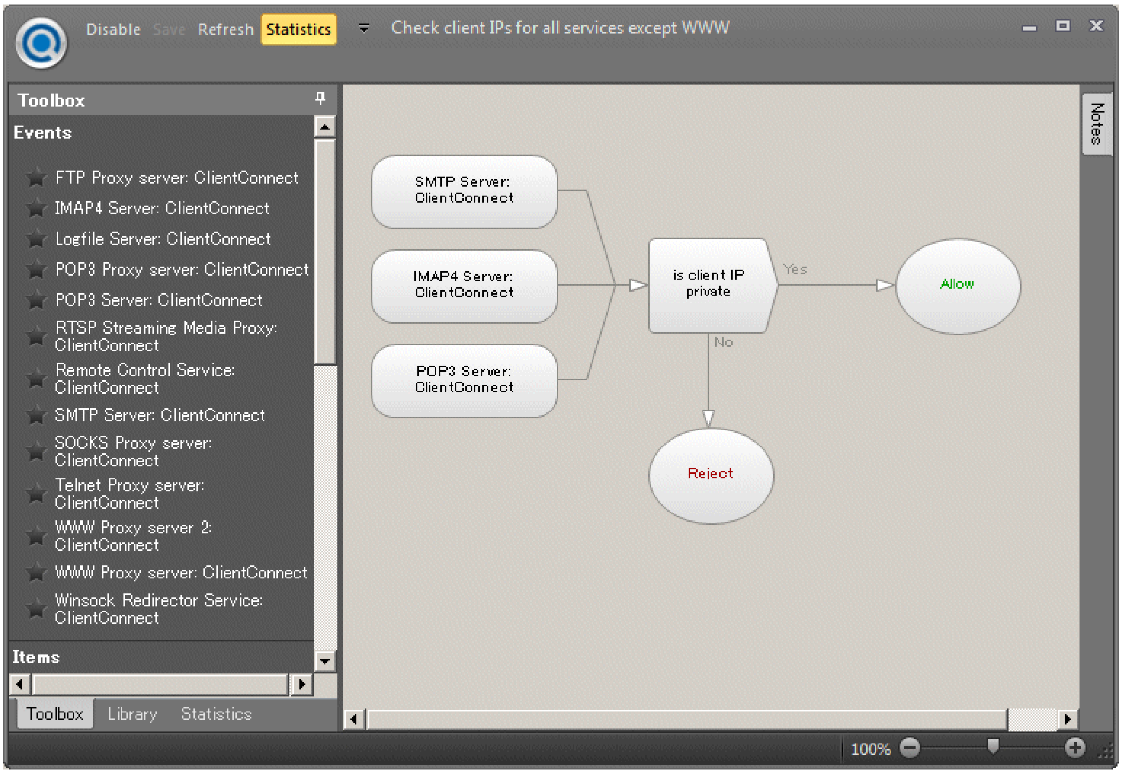
WinGate マネージメント（WinGate Management）




タイムライン（Timeline）



ポリシー・システム




**WinGate で取得可能なログ**

WinGate8 では、サービス毎のログ(診断ログ)とは別に WWW Proxy Server、WinGate NAT、SMTP deriver Service などの Usage(使用)ログを W3C 形式(Standard 版では利用できません)でログを取得することができます。WWW Proxy Server の Usage ログはデフォルトで、以下の様なログを取得いたします。

```
#Software: WinGate        Format Id: {5092B986-E5E7-4A2C-8486-CA43E684D5C6}    Format Name: W3C Logger Format
#Version: 2.0
#Date: 2011-12-21 17:41:15
#Fields: date   time      cs-username   session-id   time-taken   c-ip   c-agent   s-ip   cs-method   cs-uri   cs-uri-query   sc-status
                cs-bytes  sc-bytes      cs-protocol  cs(Referer)
#Remark: TimeZone: +00:00   FieldInfo: [WinGate.Class.HTTPSession]   (5,Date)   (6,Time)   (4,User Account)   (2,Session ID)  (2,Time Taken)(4,Client IP)
                (4,User Agent) (4,Server IP)  (4,HTTP Method)   (4,URL)   (4,URL Query) (2,HTTP Status)   (2,CS Bytes)   (2,SC Bytes)   (4,CS Protocol)
                (4,CS Header %s)
2011-12-21      08:41:15  unknown   2   0   192.168.0.10   "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"   192.168.0.23
                GET       http://www.technoblest.com/   -   304   588   235   http   -
2011-12-21      08:41:15  unknown   2   0   192.168.0.10   "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"   192.168.0.23
                GET       http://www.technoblest.com/tb.css   -   304   602   234   http   http://www.technoblest.com/
```

**最小システム必要条件**

- CPU： 1GHz 以上のプロセッサ(2GHz 以上を推奨)
- メモリ： 4GB 以上の RAM（Kaspersky AntiVirus for WinGate を使用する場合は 8GB 以上を推奨）
- オペレーションシステム（OS）:
  Windows 2003、2008、7、Windows8、Windows Server 2012（R2 を含む）
  ※サーバーOS での使用を強く推奨いたします。
  （Windows8、および Windows Server 2012 は、WinGate7.3 以降で対応）
  ※64bit OS 環境では、32bit アプリケーションとして動作いたします。
  ※OS が持つ機能は、その OS が持つ設定や制限に準じます。
  ※仮想マシン環境での動作に関しましては、VMware、Hyper-V などで動作を確認しておりますが、サポートは、WinGate に関する内容のみの対応となります。仮想マシン環境固有の問題に関しましては対応させていただくことができません。
  ※Windows Server 2012 では、Windows の ECN 機能の影響を受ける場合がございます。
- 利用可能な TCP/IP ネットワーク （※NIC チーミングをサポートしておりません。）
- 利用可能なインターネット接続

**※WinGate インターネットクライアント（WGIC）は Windows Vista、2008、7、8、2012 に対応しておりません。**
**（WGIC は、WinGate の Winsock redirector Service を使用する接続のみで使用され、WGIC を使用しない場合でも NAT やプロキシは使用いただくことができます。）**

WinGate は、32bit アプリケーションとして動作いたしますが、より大規模なユーザー環境では、より高性能な CPU、大きいメモリを搭載いただくことで、より高速な環境を実現することができます。
また、より高速なハードディスク環境は、WinGate のキャッシュレスポンスを、より高速化いたします。

WinGate は、ログの保存、キャッシュ情報の保存などに HDD 容量を使用いたします。
使用される容量は、WinGate のご利用状況などにより異なりますので、試用版などをご利用いただき、実際のサイズをご確認ください。

**WinGate のライセンスについて**

WinGate のライセンスは、構成される 1 つの WinGate 毎に必要となります。仮想 OS 環境などで複数の WinGate を同時に起動する場合、その OS で構成される WinGate 毎にライセンスが必要となります。（2 つの WinGate を使用する場合、WinGate を 2 本ご購入いただく必要があります。）
WinGate のユーザー数は、同時接続数となり、ユーザー数を超える接続があった場合、WWW Proxy server では、接続数を超えたクライアントからブラウザに英文で使用できないことを示すメッセージが表示され、Web サイトの参照などを行うことができません。他のサービスでは、ユーザー数を超える接続があった場合、リクエストは WinGate により切断されます。
弊社では、WinGate を使用する可能性のある台数のユーザー数をご購入いただくことをお勧めしておりますが、使用状況などから WinGate を使用する同時接続数が WinGate を利用するクライアント台数未満でも、ご利用いただくことができます。（ユーザー数を超える接続があった場合、新たなクライアントは、他のクライアントの接続が終了し、ユーザー数未満になるまで WinGate を利用できません。）

新規購入いただきました WinGate のライセンスには、1 年間のアップグレード保証が含まれます。アップグレード保証には、開発元がアップグレード保証の期間内であることを必要とする最新バージョンをリリースした際に最新バージョンにアップグレードできる権利、および弊社技術サポートが含まれます。
アップグレード保証の有効期限は、WinGate Management の Licensing（ライセンス）より確認いただくことができます。
アップグレード保証の更新は、有償にて承ることができます。アップグレード保証更新については、弊社までお問い合わせください。

**WinGate の種類による機能の違い**

WinGate はご利用目的に合わせて 3 種類のグレードをご用意しております。
それぞれ以下の違いを持ちます。
お客様の使用用途に合わせて、WinGate の種類をお選びください。

| Standard 版 | Professional 版 | Enterprise 版 |
|---|---|---|
| Dashboards: 1<br>ダッシュボードの数：1 | Dashboards: 2<br>ダッシュボードの数：2 | Dashboards: 無制限<br>ダッシュボードの数：無制限 |
| Notification plans: 1<br>通知プランの数：1 | Notification plans: 2<br>通知プランの数：2 | Notification plans: 無制限<br>通知プランの数：無制限 |
| Cache volumes: 1<br>キャッシュボリューム数：1 | Cache volumes: 1<br>キャッシュボリューム数：1 | Cache volumes: 無制限<br>キャッシュボリューム数：無制限 |
| Mailbox volumes: 1<br>メールボックスのボリューム数：1 | Mailbox volumes: 1<br>メールボックスのボリューム数：1 | Mailbox volumes: 無制限<br>メールボックスのボリューム数：無制限 |
| | Active Directory support<br>アクティブディレクトリをサポート | Active Directory support<br>アクティブディレクトリをサポート |
| | W3C usage logging<br>W3C 形式でのログ | W3C usage logging<br>W3C 形式でのログ |
| | Scripting support (Lua / JScript)<br>スクリプトサポート | Scripting support (Lua / JScript)<br>スクリプトサポート |
| | Use files in data lists<br>データリストのファイル参照 | Use files in data lists<br>データリストのファイル参照 |
| | Bandwidth Control<br>帯域幅制御 | Bandwidth Control<br>帯域幅制御 |
| | DMZ | DMZ |
| | | HTTP キャッシュルール |
| | | HTTPS インセプション |
| | | VPN |
| | | Threshold checking in monitored data<br>モニターされたデーターによるスレッショルドチェック |
| | | Custom DHCP options<br>カスタム DHCP オプション |
| | | Web-based Administration<br>Web ベースの管理 |
| | | Remote shell<br>リモートシェル |
| | | Performance counters<br>パフォーマンス・カウンター |
| | | Advanced policy items<br>詳細ポリシーアイテム |
| | | Advanced WinGate events<br>詳細 WinGate イベント |
| | | Advanced Schema objects<br>詳細スキームオブジェクト |
| | | Advanced adapter settings<br>詳細アダプタ設定 |

**その他のご注意：**

WinGate の ENS 機能一部は、Windows ファイアウォール機能と重複する場合があります。また、Windows ファイアウォール機能が有効である場合、WinGate の各プロキシサーバーに対するポートを Windows ファイアウォールでオープンしていただく必要がある場合がございます。Windows ファイアウォールの設定に関しては、マイクロソフト社へご確認ください。

**WinGate のインターネット共有接続について**

WinGate では 3 つのインターネット共有方法をサポートしております。これらの方法は同時にご使用いただく事が可能であり、もちろん単体でもご使用いただく事ができます。

1. 各プロキシサービスによるプロキシ接続による共有
2. WinGate インターネットクライアント（WGIC）による共有
3. NAT 機能による共有

それぞれの方法には以下のような特徴があります。

| | NAT | WGIC | プロキシ |
|---|---|---|---|
| クライアント PC の容易な構成 | ☆☆☆ | ☆☆ | ☆ |
| 速度 | ☆☆☆ | ☆☆ | ☆☆ |
| セキュリティ | ☆☆ | ☆☆☆ | ☆☆☆ |
| 構成 | ☆ | ☆☆ | ☆☆☆ |
| OS の互換性 | ☆☆☆ | ☆ | ☆☆ |
| ソフトウェアの互換性 | ☆☆☆ | ☆☆☆ | ☆☆ |
| 内向き接続の受け入れ | ☆ | ☆☆☆ | ☆☆ |

各接続方法には幾つかの注意事項があります。

- **プロキシ**

  クライアント PC のアプリケーション（ブラウザなど）で、プロキシサーバーを指定する必要があります。
  プロキシサーバーに対応していないアプリケーションをご使用いただく事はできません。
  WinGate の各プロキシサーバーを使用します。
  各プロキシサーバーでポリシー制限を行う事により、プロキシサーバー毎にポリシーを設定することができます。

- **NAT**

  クライアントマシンでは特に設定を行う必要はありません。（ゲートウェイに WinGate PC が指定されている必要があります。ルータのように WinGate を使用することができます。）
  TCP/IP をサポートする OS ではれば、OS の種類を選びません。
  アプリケーションでプロキシサーバーを指定する必要はありません。
  WinGate の ENS 機能の一部として動作します。
  ※利用するには WinGate で ENS がインストールされている必要があります。
  ※ネットワークインターフェースが 2 つ（内部、外部）必要となります。

- **WGIC**

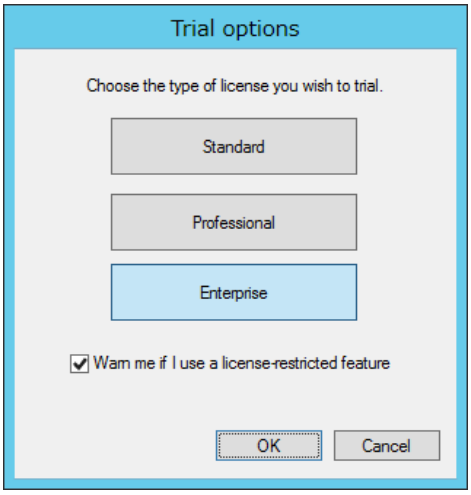
  クライアントマシンに WGIC をインストールする必要があります。
  WGIC は Windows のみの対応となりますので、他の OS ではご使用いただく事ができません。
  アプリケーションでプロキシサーバーを指定する必要はありません。

ほとんどのインターネット・アプリケーションをサポートします。
接続は WinGate の Winsock リダイレクトサービスを使用します。

**<u>これら 3 つの接続方法はそれぞれ同時に使用する事ができますので、クライアントマシンの環境やお客様のネットワーク環境に合わせて、接続方法を選択、運用していただく事が可能となります。</u>**
また、WinGate ではインターセプト・プロキシを各プロキシサーバーで設定いただく事ができます。

**インターセプト・プロキシとは？**
トランスペアレント・リダイレクションは、NAT、WGIC の接続を WinGate 内部で WinGate の各プロキシサーバーがインターセプトする機能です。
これにより WinGate の NAT で受けた接続を WinGate 内部でプロキシがインターセプトし、実際はプロキシ機能を使用させる機能となります。
例えば NAT 接続を WWW Proxy Server でインターセプトした場合、NAT 接続では、ユーザー認証、詳細なログ情報の取得、HTTP Cache の利用、ポリシーによる URL 制限などが行えないため、NAT 接続を WWW Proxy Server でインターセプトすることにより、これらの WWW Proxy Server の利点を利用することが可能となります。また、WinGate を使用するクライアントでは、WinGate の NAT 機能を使用するため、クライアント ソフトウェアでプロキシ設定を行うことなく、かつプロキシ使用を意識させることなく、WinGate の WWW Proxy Server の各機能を使用することができます。
インターセプト・プロキシの詳しい詳細については、本書の「トランスペアレントの設定」をご参照ください。

**試用版、および試用版グレードの変更について**
WinGate は、試用版として 30 日間、全ての機能をご利用いただくことができます。
弊社では、WinGate をご購入いただく前に、試用版にて設定や動作をご確認いただくことをお願いしております。
試用版をご利用いただくには、WinGate インストール後に試用版としてアクティベーションを行っていただく必要がございます。（試用期間の情報は、WinGate Management 内の Licensing より確認いただく事ができます。
また、WinGate Management へログインした状態で表示される Trial options（試用版オプション）により試用版として利用する WinGate の種類を選択することができます。
これにより、実際にご購入を検討いただいております WinGate の種類と同じ動作を試用版でお試しいただけます。




オプション：Warn me if I use a License-restricted feature（ライセンスによって制限される機能を使用した場合に警告）
試用版で利用する WinGate の種類を変更した場合、WinGate の再起動が必要となります。

**WinGate8 からの新機能**

WinGate8 は、WinGate7 からのアップグレード版として幾つかの変更を適用しております。WinGate6 をご利用いただいておりますお客様は、WinGate7 からの変更点をご確認ください。

◆ **HTTP キャッシュ機能の刷新**
WinGate7 で採用されたデーターベース型のインデックス形式から、より高速で大容量のキャッシュに対応したキャッシュシステムへ変更されました。
これにより、より容易に大容量のキャッシュを高速にご利用いただくことが可能となりました。
また、キャッシュからの除外や独自のルール設定が可能なキャッシュ ルール機能も追加されました。

◆ **ネットマスクによる信任ルール**
新任ルールでネットマスクによる範囲指定が可能となりました。

◆ **HTTPS コンテンツのフィルタリング、キャッシュ**
中間証明書の使用により、HTTPS コンテンツのフィルタリング、キャッシュが可能となります。これは WinGate で作成した中間証明書をクライアントへ配布することにより可能となります。

◆ **Timeline データーベースの変更**
大規模な Timeline データーベースに対応するために、デフォルトデータベースを MDB から SQLite へ変更しました。(8.1.0 以降)

◆ **その他**
WinGate7 から多くの機能修正を適用するとともに、利便性向上のため細かな機能追加を多く適用しております。

より詳細な情報については、WinGate Web サイト リリースノートページをご参照ください。

**WinGate7 からの新機能**

WinGate7 では、多くの新機能を採用しております。

◆ **イベント管理**
刷新されたイベント機能は、WinGate で発生する様々なイベントに基づき、様々なアクションを実行することができます。特定のイベントが発生した場合に電子メールで通知を行うことや動作を指定することができます。また、イベントの内容は集中管理され、容易に運用することができます。

◆ **サービス**
**ネットワーク・サービス**
インターネット共有アプリケーションとして、WinGate は、WinGate ユーザー、およびアプリケーション・プロトコルのネットワーク管理を行うために、様々なネットワーク・サービスを提供します。各サービスは、特定のネットワーク接続に関するクライアント要求答えるように設計されています
WinGate は DHCP サービスによりクライアントへ IP アドレスを割り当てることや、DNS サービスによりクライアントへインターネット DNS 参照の機能を提供します。WWW プロキシサービスでは、ウェブ・ブラウザでのプロキシ使用のコントロールを提供するためにデフォルトでインストールされます。また、お客様が必要とする場合、他のプロキシサービスを追加することもできます。
WinGate 7 は、SMTP、POP3 サーバー機能を持ち、WinGate ユーザーがメールボックスを持つメールサーバーとして利用することもできます。
**コンポーネント・サービス**
WinGate は必要に応じて、コンポーネント・サービスをインストールすることができます。それらのコンポーネント・サービスは、停止、開始、構成することができます。

◆ **データー**

新しいデータシステムはグローバルなデータオブジェクトを作成する機能を WinGate 管理者に提供します。グローバル・データは、リスト、ストリング、ブールを持ち、これらの値は WinGate で構成されるときアクセスされる事ができます。
また、データシステムは WinGate のコンポーネントとオペレーティングシステム性能のカウンタを監視するデーターを提供します。

◆ **ポリシー・システム**
WinGate 7 は、WinGate 内で発生するイベントを制御し応答する新しいポリシー・システムを提供します。
新しいポリシー・システムでは選択されたイベントが発生した際に、実行されるポリシーを作成することができます。
新しいポリシー・システムは、グラフィカルなフローチャートにより作成することができ、単純なポリシーから複雑な複合的なポリシーを作成することができます。ポリシー内ではサービスの停止やリストの参照、電子メールの送信など多様な条件を複合的に作成することができます。

◆ **ユーザー管理**
WinGate は、インターネットへのユーザアクセスを制御する目的に領できるユーザー・データーベースを提供します。ユーザー・データーベースには、WinGate にビルトインされているユーザー・データーベース、WinGate がインストールされているコンピュータのオペレーティングシステムのユーザー・データーベース、または Active Directory ユーザー・データーベースを使用することができます。
WinGate のすべてのユーザデータベースオプションは、NTLM 認証をサポートします。WinGate を通してインターネットにアクセスする際に、WinGate で認証を利用することにより、制限を適用すると共に、ユーザーを監視することができます。

◆ **権限（パーミッション）**
権限機能は、ユーザーが何を見て、どのようなアクセスを持ち、WinGate 管理コンソールコンソール内で何をすることができるかを決定するのを助けます。

◆ **通知**
WinGate 7 は、WinGate に起こるときインシデントを警告するために包括的な通知システムを追加しました。通知システムでは、特定の通知プランやスケジュールの一部として実行される Lua Script イベントプロセッサを使用することで Lua スクリプトを実行することができます。（メールの送信イベントによって。特定のイベントが発生した際に電子メールで通知することもできます。）

◆ **タイムライン**
タイムライン機能は、時間の経過にそって、ユーザーのウェブアクティビティをグラフ表示するとともに、システムイベントの発生をグラフ内に表示します。

◆ **新しいロギング**
WinGate7 では、ログ形式に W3C 形式を採用いたしました。ログの保存ディレクトリの変更や取得項目を詳細に設定できるようになりました。
また、ログの保存期間を設定することが可能です。

◆ **Web アクセス・コントロール**
特定のウェブサイトと URL へのユーザアクセスを制御できる、Web アクセス・コントロール機能を追加しました。WWW Proxy サーバーを通じて要求されたるセッションに対して、作成可能なカテゴリーに分けてアクセスの拒否、許可を設定することができます。また、アクセス・ルールでは、ユーザーやグループ毎のアクセス制御にも対応「いたします。

◆ **HTTP キャッシュ**
WinGate7 では、クライアントから要求された HTTP ファイルの保存と検索を提供する新しいキャッシュシステムを導入しました。HTTP キャッシュはボリュームに保存されたキャッシュファイルを組織化するためにインデックス

データベースを使用します。これにより HTTP キャッシュボリュームの検索速度が高速化されました。
キャッシュボリュームは、管理を容易にするために複数のボリュームを作成することができます。また、HTTP キャッシュインデックスを保存する他のデーターベースを指定することができます。

**WinGate アップデート**

WinGate7 では、新しい WinGate 更新システムを導入いたしました。WinGate は自動的に WinGate の更新を確認し、ダウンロード、およびインストールを行うことができます。これは Kaspersky AntiVirus for WinGate などの WinGate プラグインに対しても動作いたします。

**WinGate6 をご利用いただいておりますお客様へのご注意（重要）**

**WinGate6 をご利用いただいておりますお客様は、こちらの内容を必ずご参照ください。**

WinGate7、WinGate8 は、WinGate6 より非常に多くの新機能、仕様変更を適用しており、WinGate の機能の一部は、異なるサービスへ変更され設定情報を引き継ぐことができません。また、一部の機能は継承されず失われておりますことにご注意ください。

WinGate6 よりバージョンアップを行う場合には、これらの内容にご注意ください。

WinGate6 からのアップグレード方法に関しては、インストールの章をご参照ください。

WinGate6 から WinGate7、WinGate8 の主な変更点は以下の通りです。

| WinGate6 | WinGate7、8 | 説明 |
|---|---|---|
| WinGate エンジン | WinGate エンジン | 以前のバージョンで、WinGate エンジンは WinGate の機能性のかなりの部分を保持し、操作していました。WinGate 7 以降では、WinGate エンジンは、モジュールの構造で作成されています。コンポーネントは、ロード、アンロード、そして、それらの機能性を WinGate(と他のコンポーネント)に供給することができます。WinGate エンジンは、WinGate スキーマを通してこれらのコンポーネントを組織化して管理します。 |
| ENS（拡張ネットワーキング） | ENS（拡張ネットワーキング） | WinGate は WinGate でネットワークセキュリティを管理するために、継続して ENS 構成を提供します。ENS ドライバーは、拡張ネットワーク・サービス(NAT、ファイアウォール、帯域幅制御、ゲートウェイモニタ)を含んでいます。 |
| GateKeeper | WinGate マネージメント | WinGate マネージメントコンソールは、旧バージョンの Gatekeeper ユーザーインタフェースから変更されます。WinGate マネージメントコンソールは、完全に新しいユーザーインタフェースに変更され、より操作性を向上しています。WinGate マネージメントのインターフェースは、WinGate を管理するために再設計されました。 |
| WinGate システムとプロキシ・WinGate サービス | サービス | WinGate の新しいモジュール構造により、主なサービスは任意に追加する必要がります。WinGate 7 は、デフォルトでは、システムとプロキシサービスをインストールしません。WinGate は、インストール直後、デフォルトで WWW Proxy サーバーをインストールします。WinGate 7 以降では、インターセプト・プロキシを提供しますが、これはインターセプト(インターセプトプロキシ)に変更されます。 |
| システムとサービスポリシー・ポリシーシステム | ポリシー・システム | WinGate 7 以降は、完全に新しいポリシー・システムを提供します。<br>WinGate は、その機能性の多くの部分をイベントからなお応答に基づき作成されていいます。新しいポリシー・システムは、WinGate で発生したイベントに基づいたポリシ |

| | | |
|---|---|---|
| | | ーを作成することができます。これは、ポリシーが指定されたイベントの発生により処理できることを意味しています。<br>以前の WinGate では、ポリシーを作成するためにフィルターと基準を選択することができました。<br>WinGate 7 以降では、ポリシーの内容はイベントの発生を含むフローチャートにより作成することができます。新しいポリシー・システムでは、フローチャートのステップを作成するために使用する事ができる、さまざまな強力なツールを持っています。<br>特定のシステムやプロキシサービスに基づく、システムとサービスポリシーの概念はなくなりました。<br>**アップグレードを行った場合、以前のバージョンで作成されたポリシー設定を継承することはできません。** |
| スケジューラ | スケジュール・イベント | スケジュールシステムは、スケジュール・イベント・システムに変更されました。新しいスケジュール・イベント・システムは、必要とするスケジュールで発生するイベントを発生させます。 |
| ロギング | ロギングシステム | 以前のバージョンで利用することができたログファイルサーバは、新しいロギングサービスに置き換えられました。ログは、全てのログ情報を統括するグローバル・ログ、または個々のサービス毎に保存される自身のログを選択することができます。取得するログ情報は、幾つかのレベルから選択することができます。<br>新しいログシステムは、W3C 形式のログとなるため、サードパーティ製の W3C ログ解析ツールで分析を行うことも可能です。 |
| ユーザー・データーベース | ユーザー・データーベース | WinGate 7 以降では、WinGate で使用するユーザコントロールと管理のために、3 つのユーザー・データーベースのオプションを提供します。<br>それは NTLM 認証サポートを提供する WinGate ユーザー・データーベースを保有します。<br>また、WinGate がインストールされている Windows オペレーティングシステムのユーザー・データーベースを使用する Windows Users と Group コネクタを持ちます。<br>もう一つの方法として、WinGate 7 は Active Directory ユーザーデーターベース・コネクタを持ちます。 |
| キャッシュ | HTTP キャッシュ | HTTP キャッシュ機能は、WinGate8 で刷新されました。より高速で大容量なキャッシュシステムを可能とします。 |
| Winsock リダイレクトサー | Winsock リダイレクトサ | Winsock リダイレクトサービス(WRS)は、デフォルトでイ |

| | | |
|---|---|---|
| ビス | ービス | ンストールされません。WinGate インターネット・クライアントは、ウインドウズ・オペレーティングシステム(Windows2000、XP、Server2003)のみで、利用することができることに注意してください。WRS は、新しいポリシーにおいて、使用するアプリケーションコントロールを提供します。 |

**WinGate6 からの変更**

WinGate7、8 はバージョン 6 から大幅な進化を遂げました。
WinGate6 と WinGate7、WinGate8 での変更については、一つ前のセクションをご参照ください。
現在お客様が WinGate 6(WinGate 6 ライセンスを所有しアップグレード保証の期間内である場合)を使用している場合、少しの変更により WinGate8 にアップグレードすることができます。
WinGate 8 インストーラーは、以前のインストールと以下に基づくアップグレードがないかどうか WinGate サーバーを調べるでしょう:

**WinGate6 からのアップグレードで必要になること（継承されない内容）**

**以下の機能は WinGate6 から引き継ぐことができません。WinGate8 インストール後は、新たに設定を行っていただく必要がございます。**

- **ポリシー設定は、バージョン 6、またはそれ以前のバージョンから継承されません。**
  WinGate 6 で作成された、如何なるポリシー設定も引き継ぐことができません。新しいポリシー・システムで新しくポリシーを作成する必要があります。

- **キャッシュの内容とキャッシュポリシーは継承されません。**
  WinGate 8 の新しい HTTP キャッシュは、完全に新しいインデックスと保存システムを使用します。アップグレードさせた後にデフォルトで HTTP キャッシュ・サービスを提供するために、WinGate は新しい HTTP キャッシュボリュームを作成します。

- **スケジュールされたイベントは継承されません。**
  WinGate8 は、完全に新しいスケジュール・イベント・システムを持ちます。

- **プラグイン**
  古いプラグイン(Kaspersky AntiVirus For WinGate など)は、互換性がありません。WinGate 8 との互換性を持ったバージョンへアップデートする必要があります。

**WinGate がアップデート時に行うこと**

- **現在の設定に基づくユーザー・データーベース選択**
  WinGate は、お客様が WinGate 6 で使用している現在のユーザー・データーベースを調査し、WinGate 8 のための適切なユーザー・データーベースを決定するでしょう。
  それらは以下の選択です:

  1. **WinGate ユーザー・データーベース**
     WinGate ユーザー・データーベースが使用されている場合、WinGate 8 は、WinGate ユーザー・データーベースを使用し続けることを選択します。

  2. **Windows ユーザーとグループ**
     WinGate 6 で WinGate がインストールされているサーバーのオペレーティングシステム・ユーザー・データベースを使用していると、WinGate は、ローカルのオペレーティングシステムデータベースを使用

し続けるように、WinGate は Windows ユーザーとグループコネクタを選択します。

3. **Active Directly**
   WinGate 6 で Active Directly とドメイン・コントローラ・ユーザーデータベースを使用する設定がされている場合、WinGate 8 は Active Directly ユーザーデーターベース・コネクタを選択します。

**ユーザー・データーベース選択後に WinGate が行うこと**

新しいユーザー・データーベースに電子メール・メールボックスを移動します。
IMAP 形式へのメールボックスへ移されます。
WinGate 8 は、POP3、IMAP4 メールボックス間には、区別が全くありません、すべてのメールボックスが IMAP 形式で保存されます。ユーザーが、POP3 プロトコルを使用して、WinGate メールボックスにアクセスすることを望む場合、ユーザーは受信トレイフォルダーにアクセスすることができるだけでしょう。

仮定されたユーザーは信任ルールに移されます。そして、マルチユーザー・マシンは信任ルールに移されます。

WinGate 6 で設定された、仮定されたユーザー、またはマルチユーザー・マシンは、WinGate 7 で適切な新しい信任ルールを作成します。

**WinGate7、WinGate8 で互換性があり、そのまま継承される内容**
**これらの設定項目は、継承されますがインストール完了後には、必ず設定項目をご確認ください。**

- 既存のサービス構成
- 既存の拡張ネットワーキング設定
- 既存のメール設定
- 既存のネットワーク接続設定
- ダイアルアップ設定

**WinGate7、WinGate8 で異なって動作する内容**

- **ロギング**
  WinGate 8 は、完全に新しいログシステムを持ちます。

- **スケジューラ**
  WinGate 8 は、完全に新しいスケジューラ・イベント・ステムを持ちます。

- **ポリシー**
  WinGate8 では、システムとサービスポリシーの概念はありません。すべてのポリシーが、WinGate 内で発生したイベントに基づき構成されるポリシー・システムで構成されます。

- **フィルタリング**・プラグインとキャッシュは、必要とする場合、各サービスベースで有効、無効にすることができます。

- **ファイアウォールタブ**
  WinGate ファイアウォール・アクティビティを表示するためのパネルはありません。すべてのファイアウォール・アクティビティは、WinGate NAT と呼ばれるログに記載されます。WinGate 管理コンソールのコントロール・パネル、ロギングパネルで参照することができます。

**WinGate7、WinGate8 で失われた機能**

**WinGate8 は、WinGate6 の以下の機能を持ちません。これらの機能をご利用いただいております場合、代替え機能をご検討ください。**

- **Java ログイン**
  Java ログインはサポートされません。これは WWW 認証に置き換えられました。

- **隔離**
  WinGate8 は、隔離機能を持ちません。WinGate プラグインの Kaspersky AntiVirus によってスキャンされた HTTP、SMTP、および POP3 Proxy トラフィックは、許可(クリーンである場合)、またはスキャンの結果に基づき拒否されるだけです。

- **プロキシでのドリップフィード**
  これは必要に応じてプラグインで扱われます。

- **SMTP Proxy Server**
  TCP Mapping サービスにて同様の動作を行うことができます。

- **ログファイルサーバ**
- **Telnet コマンドライン管理インターフェース**

**Kaspersky AntiVirus for WinGate をご利用のお客様へのご注意（重要）**

Kaspersky AntiVirus for WinGate の旧バージョンと WinGate8 用の Kaspersky AntiVirus for WinGate は互換性がありません。また、設定情報を継承することができません。

Kaspersky AntiVirus for WinGate がインストールされた WinGate6.x へ WinGate7 を上書きインストールした場合、WinGate8 のインストーラーは、旧バージョンの Kaspersky AntiVirus for WinGate を自動的にアンインストールします。

WinGate8 へアップグレード後、手動で Kaspersky AntiVirus for WinGate のインストールを行い、再度設定を行う必要がございますことにご注意ください。

**WinGate の主な機能とその概要**

WinGate は以下のサービスを持ちます。
「デフォルトインストール」の記載があるものは、インストール直後にデフォルトでインストールされ開始されます。それ以外の項目は必要に応じて、手動で追加・設定を行ってください。
その他の機能の詳細については、各サービスの解説ページをご参照ください。

**サービス**

◆ DHCP Service （デフォルトポート:67　変更不可）
DHCP サービスは、WinGate を DHCP サーバーとして動作させるサービスです。このサービスが有効となっている場合、WinGate は、設定可能な DHCP サーバーとして動作します。WinGate の DHCP Service を利用する事によりマシン名を WinGate 内で利用する事が可能となります。

◆ Winsock Redirect Service （デフォルトポート:2080）
Winsock リダイレクトサービスは、WinGate インターネットクライアント（WGIC）により使用されます。クライアント PC で WGIC が使用される場合、接続は Winsock リダイレクトサービスで受け付けられます。

◆ GDP Service（デフォルトポート:368　変更不可）
GDP サービスは、WGIC が WinGate サーバーを発見するために使用されます。

◆ DNS Service（デフォルトポート:53　変更不可）
クライアントマシンへ DNS サーバーの機能を提供します。レコードなどを持つことはできません。名前解決は WinGate マシンの TCP/IP 設定で設定された DNS サーバー、または DNS リゾルバ設定により設定された DNS サーバーが使用されます。（DNS プロキシのような機能となります。）

◆ Remote control Service（デフォルトポート:808） [ **デフォルトインストール** ]
リモート・コントロールサービスは、WinGate マネージメントが WinGate サーバーにログインするために使用されます。このサービスが停止された場合、WinGate マネージメントは自身の、またはリモートの WinGate へログインすることはできません。

◆ SMTP delivery service [ **デフォルトインストール** ]
WinGate から電子メールを送信する場合に使用されるサービスです。

◆ POP3 Server（デフォルトポート:110）
WinGate のメールサーバー機能の POP3 Server となります。
※POP3 Proxy Server とは異なります。

◆ SMTP Server（デフォルトポート:25）
WinGate のメールサーバー機能の SMTP Server となります。
※SMTP Proxy Server とは異なります。

◆ IMAP4 Server（デフォルトポート:143）

WinGate のメールサーバー機能の IMAP4 Server となります。

**プロキシサービス機能**

◆ FTP Proxy Service（デフォルトポート：21）
FTP プロキシサーバーとして動作します。

◆ POP3 Proxy Service（デフォルトポート：8110）
POP3 プロキシサーバーとして動作します。メールクライアントから利用するためには、メールクライアントでの区切り文字を使用したアカウント設定が必要となります。

◆ RTSP Proxy Service (デフォルトポート：554)
Real Time Streaming Protocol プロキシサーバーとして動作します。

◆ SOCKS Proxy Service（デフォルトポート：1080）
Socks プロキシサーバーとして動作します。対応する SOCKS バージョンは、4、5 となります。

◆ Telnet Proxy Service（デフォルトポート：23）
telnet プロキシサーバーとして動作します。

◆ VDOLive Proxy Service（デフォルトポート：7000）
VDOLive プロキシサーバーとして動作します。

◆ WWW Proxy Server（デフォルトポート：80） [ **デフォルトインストール** ]
WWW(HTTP) プロキシサーバーとして動作します。

◆ XDMA Proxy Service（デフォルトポート：8000）
XDMA プロキシサーバーとして動作します。

◆ TCP/UDP マッピング
TCP や UDP 接続を決められたサーバーへマッピングする場合に使用します。接続を受け付けるポートとマッピング先のサーバー、ポートを指定します。

**その他の機能**

◆ HTTP Cache（HTTP キャッシュ）
キャッシュ機能は、WWW Proxy Server で参照された Web サイトの情報をキャッシュし、同じリクエストがあった場合に、キャッシュ内の情報を使用することにより高速表示とネットワークリソースの節約を行うことができます。キャッシュサイズやキャッシュの内容を設定することができます。

◆ Timeline（タイムライン）
WinGate の WWW Proxy Server で参照された URL、ダウンロードされたサイト、WinGate の起動などをグラフ表示します。

◆ DHCP

WinGate の DHCP サービスを使用した場合に、DHCP によって割り当てられた内容の表示や解放を行うことができます。

◆ Web アクセスコントロール

ポリシー設定は別に、お客様によって作成されたカテゴリー毎に、WWW Proxy Server でアクセスを許可、拒否するサイトなどの設定を行うことができます。また、制限の対象になったカウントの確認も可能となります。

◆ イベント

WinGate 内で発生するイベントにより様々なアクションを実行することができます。ルールに違反する挙動があった場合に電子メールを配信するといった事も可能となります。

◆ スケジュール・イベント

WinGate で行われる動作をスケジューリングすることができます。デフォルトでは、ログファイルのローテーション等がスケジューリングされています。この他にも WinGate の停止、開始などもスケジューリングできます。

◆ 拡張ネットワーキング（ENS）

NAT、ファイアウォール、ポートセキュリティ、帯域幅制限など、ENS ドライバーにより提供される機能の設定を行います。ポートセキュリティでは、WinGate マシンに対する接続をポート単位でどのように取り扱うかを制御することができます。

◆ VPN（エンタープライズ版、および VPN 購入ユーザー様のみ）

WinGate VPN の設定を行います。（他社 VPN との接続や他社 VPN 網内での挙動を制御するものではありません。）

◆ DNS クライアント

WinGate がインターネットアクセスを行う際に使用する DNS サーバーの設定や DNS キャッシュの設定などを行います。

◆ サーバー証明

WinGate で使用されるサーバー証明書の作成などを行います。

**WinGate アップデート**

WinGate の自動更新の確認や自動更新の適用方法などを構成します。

**WinGate の新規インストール**

**インストールの前に（重要）**

WinGate は、NAT 機能、メールサーバー機能、プロキシ機能、ファイアウォール機能など、多くの機能を持っており、これらは同時に使用することが可能です。これらは非常に有効な機能ですが、お客様の環境によっては幾つかの機能は、不要であるかもしれません。また、不要な WinGate の機能が動作する事により、ネットワーク内での予期せぬ動作や意図しない WinGate の動作を行ってしまう場合もあります。WinGate のインストール前に以下の内容を確認し、目的に合わせたインストール、設定を行ってください。（これらはインストール後に変更することも可能となります。）

◆ **WinGate の拡張ネットワーキング（ENS）機能は必要とするか？（重要）**

ENS は Windows のシステムドライバとして動作し、NAT、ファイアウォール、ポートセキュリティの機能を提供します。

ENS はインストールすることが推奨され、特に NIC が 2 枚の構成で、1 つがインターネット接続、1 つが LAN 側の様な構成では、外部からの不要な接続から保護するためにインストールが特に推奨されます。（NAT 機能のだけの無効化なども可能となります。）

一方で、NIC1 枚で LAN 内のプロキシサーバーとしてだけと使用する場合には、ENS が不要となる場合があります。ご利用をいただく WinGate の機能に応じて、ENS の有無を事前に決定してください。

◆ **WinGate メールサーバー機能（POP3 Server , SMTP Server）は必要か？**

WinGate は、プロキシ機能と異なる、ドメイン、メールアカウントを構成可能なメールサーバー機能を持ちます。

**重要：このメールサーバー機能は、プロキシ機能とは異なることにご注意ください。**

WinGate をメールサーバーとして使用する必要がなく、POP3 プロキシ、SMTP プロキシを使用する場合は、WinGate メールサーバー機能はインストールされる必要がないかもしれません。（両方が重複したポートで構成された場合、メールサーバー機能が優先されます。

◆ **その他に必要な WinGate の機能は何か？**

WinGate はメールサーバー機能の他にも、DHCP サービス、DNS サービスを持ちます。ネットワーク内や同一コンピュータに、これらのサーバサービスが既に使用されている場合は、サーバーが競合し意図しない動作を招く場合もあります。

インストール前に、どのサービスが不要で、どのプロキシが必要とされるかをご確認ください。

WinGate の幾つかのサービスは、削除することはできません。（無効とすることができます。）

プロキシサーバーは削除することができます。

◆ **ユーザー・データーベースは何を使用するか？**

WinGate は、認証やメールアカウントなどに使用可能なユーザーを設定することができます。

このユーザーは、WinGate が独自で持つユーザー・データーベース以外にも、Windows ユーザー・データーベース、Active Directly ユーザー・データーベースを使用することができます。

インストール完了後に、使用するユーザー・データーベースを使用する選択を行うことができます。

※ユーザー・データーベースは、WinGate の管理ツールである WinGate マネージメントへのログインにも使用されます。

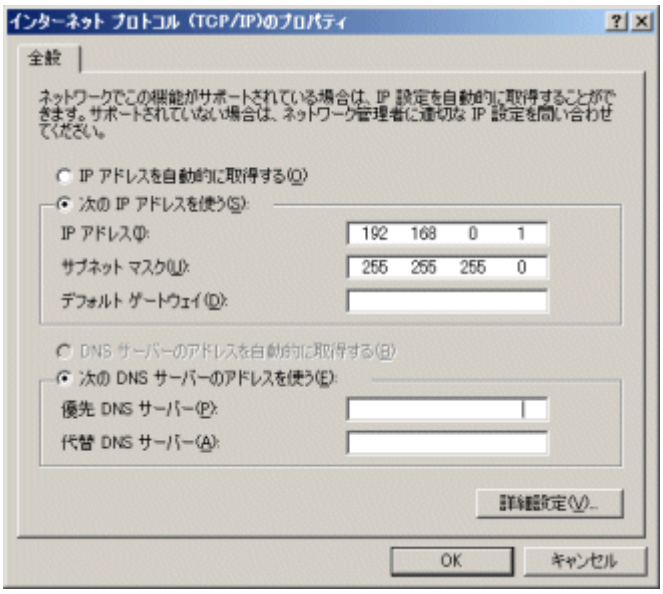
インストール後に Windows ユーザー・データーベース、Active Directly ユーザー・データーベースを選択した場合は、WinGate マネージメントのログインに、指定したユーザー・データーベースの管理者、パスワードでログイ

ンする必要があります。
また、Active Directly ユーザー・データーベースを使用する場合には、WinGate マシンは、Active Directly のメンバーである必要があります。

◆ **WinGate サーバーPC のネットワーク環境の確認**

WinGate はインストール完了後に、ポートセキュリティ、バインドポリシーで使用される NIC の用途を自動で構成します。
しかし、この自動構成がネットワーク構成の意図した設定に検出されない場合がございます。
インストール前に WinGate で NIC やゲートウェイがどのように使用されるべきであるかを、ご検討ください。
WinGate をインストールする前に目的にあったネットワークインターフェースの構成を行っていただく事により、より円滑にインストール作業を行っていただく事ができます。
インターネットへの接続環境、およびクライアントマシンからの接続を受け付けるインターフェースの設定が完了していることを確認してください。
クライアントからの接続を受け付けるインターフェースは、スタティック（静的）な IP アドレスが設定されていることが推奨されます。
Windows の TCP/IP の設定より事前に設定を行ってください。

**Windows の TCP/IP 設定画面**




※NIC が 2 枚の構成で、1 つの NIC2 がクライアントからの接続を受け付ける専用のインターフェースである場合、WinGate がゲートウェイとなるためこの例のようにデフォルトゲートウェイ、DNS サーバーを持つ必要はありません。一方でインターネットに接続される側に NIC は、確実にインターネットへ接続できる環境としてください。
※NIC が 1 枚の構成である場合、WinGate が接続を受け付ける NIC と WinGate がインターネットへアクセスするための NIC は同一の NIC で行われるため、インターネットへ接続できる設定としてください。（既にインターネットへの接続環境を持っている場合は、WinGate 用に変更の必要はありません。）

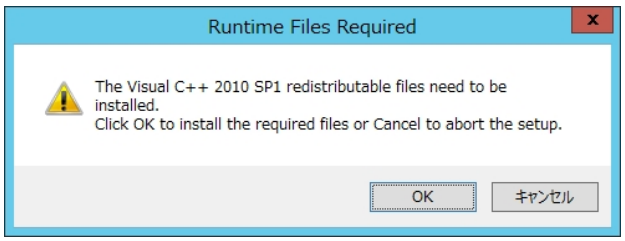
**WinGate インストールチェックシート**

| | | | |
|---|---|---|---|
| **コンピュータが持つ NIC** | | | |
| ① 名前 | IP アドレス | 用途: 内部 ・ 外部 | |
| ② 名前 | IP アドレス | 用途: 内部 ・ 外部 | |
| ③ 名前 | IP アドレス | 用途: 内部 ・ 外部 | |
| **インストール時に選択する機能** | | | |
| 拡張ネットワーキング（ENS） | ☐ | Windows ユーザー・データーベースの利用 | ☐ |
| **利用するサービス** | | | |
| DHCP Service | ☐ | Winsock Redirect Service | ☐ |
| GDP Service | ☐ | DNS Service | ☐ |
| Remote Control Service | ☐ | POP3 Server | ☐ |
| SMTP Server | ☐ | IMAP4 Server | ☐ |
| **利用するプロキシサービス** | | | |
| FTP Proxy Server | ☐ | Logfile Sever | ☐ |
| POP3 Proxy Server | ☐ | SOCKS Proxy Server | ☐ |
| Telnet Proxy Server | ☐ | VDO Live Proxy Server | ☐ |
| WWW Proxy Server | ☐ | XDMA Proxy Server | ☐ |
| | | | |
| **インストール後の確認事項** | | | |
| ネットワーク接続の用途の設定 | | インターネット接続 | |
| 不要なサービスの停止 | | 各プロキシの利用 | |
| 不要なプロキシの削除 | | 各サービスの利用 | |
| 各バインドの設定 | | | |
| **メモ** | | | |
| | | | |

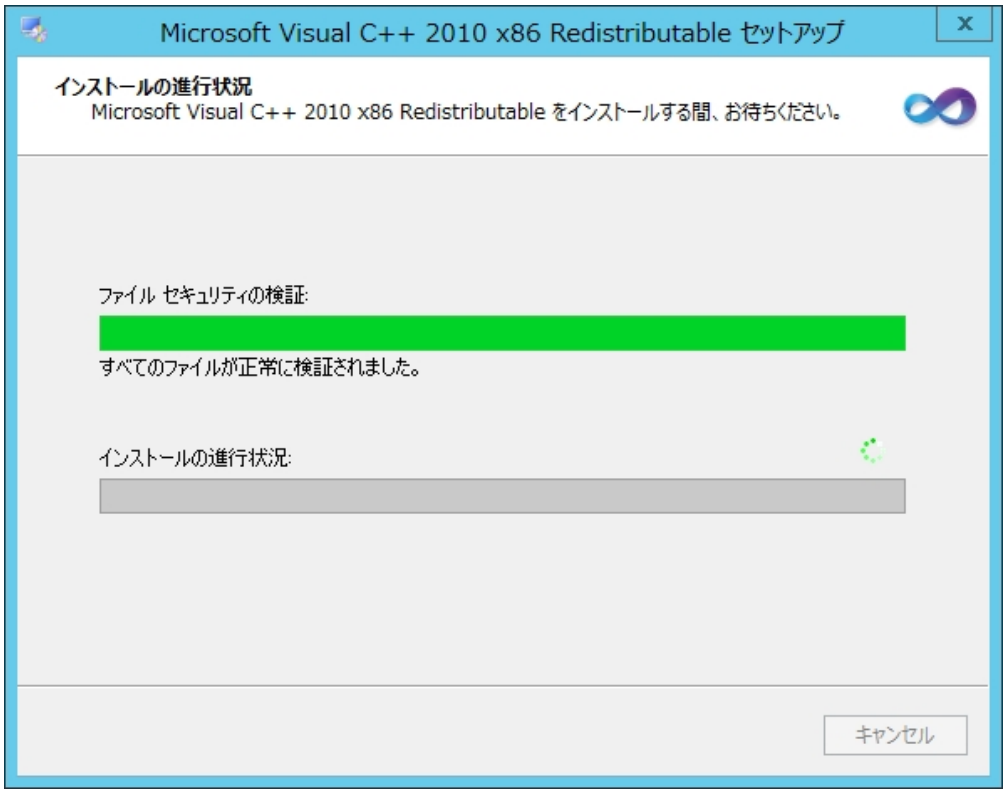
本チェックシートはインストールの確認用などにご利用ください。

**インストールの開始**

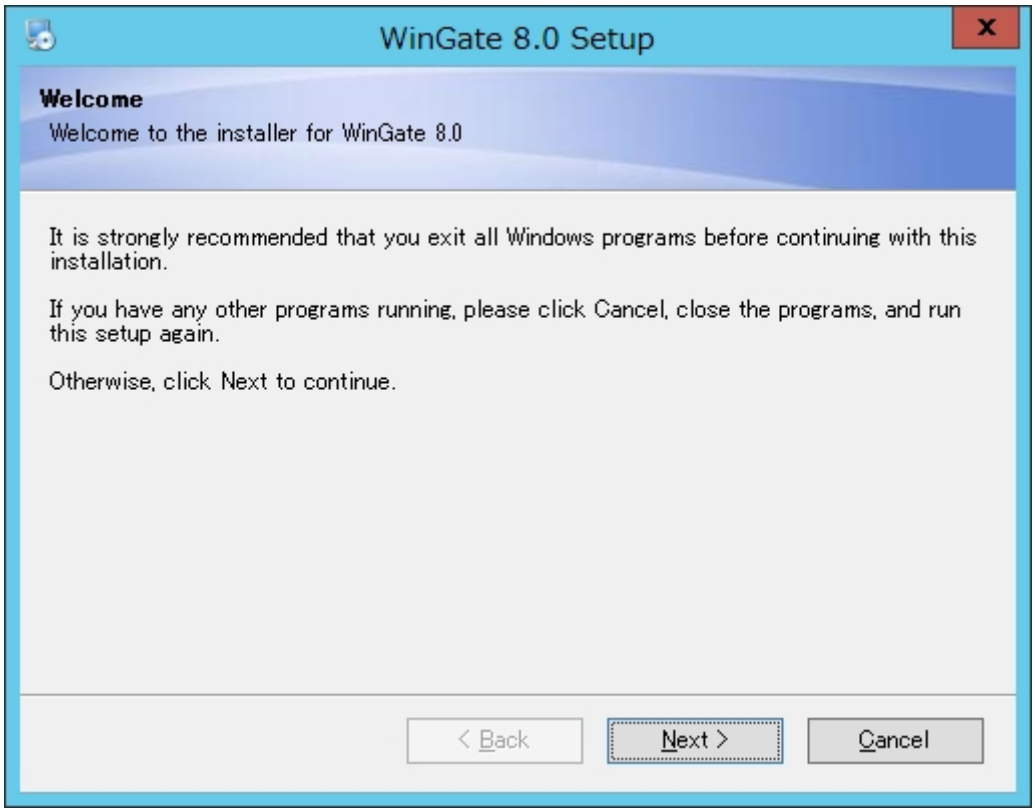
1. WinGate のインストールプログラムを実行します。




Windows Server 2012 などでは、環境によって Visual C++ 2010 SP1 再配布パッケージのインストールが必要となるダイアログが表示される場合があります。
このダイアログが表示された場合、OK ボタンをクリックして Visual C++ 2010 SP1 再配布パッケージのインストールを行ってください。

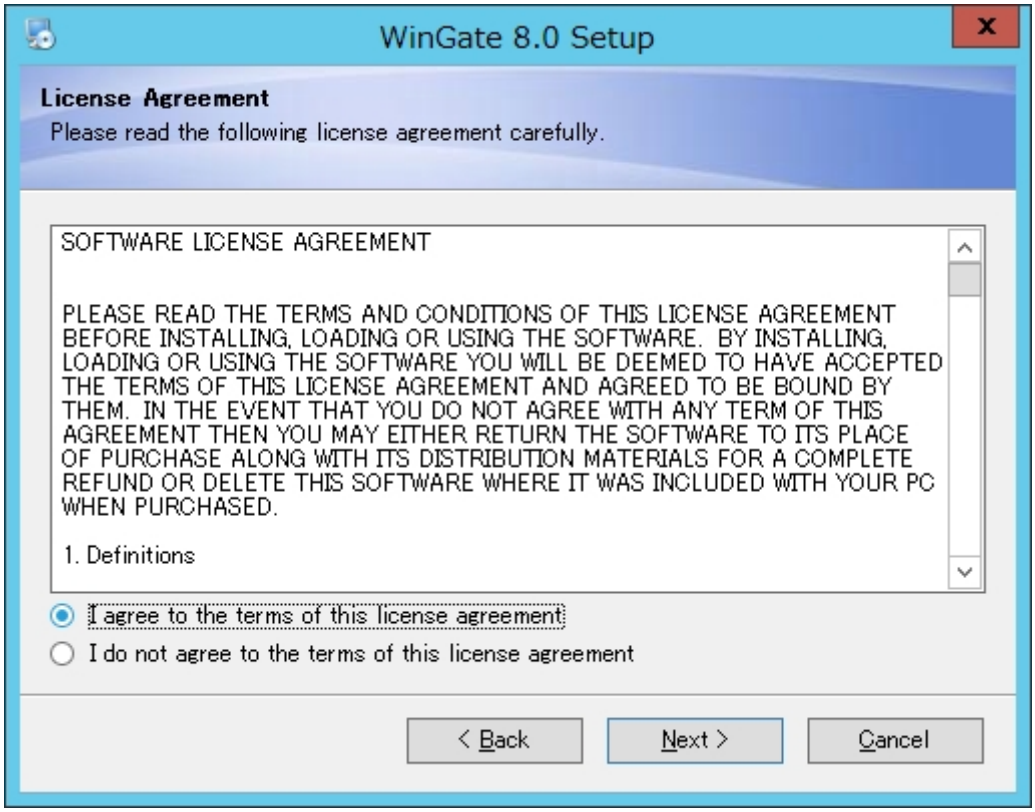


2. インストーラーが開始されます。



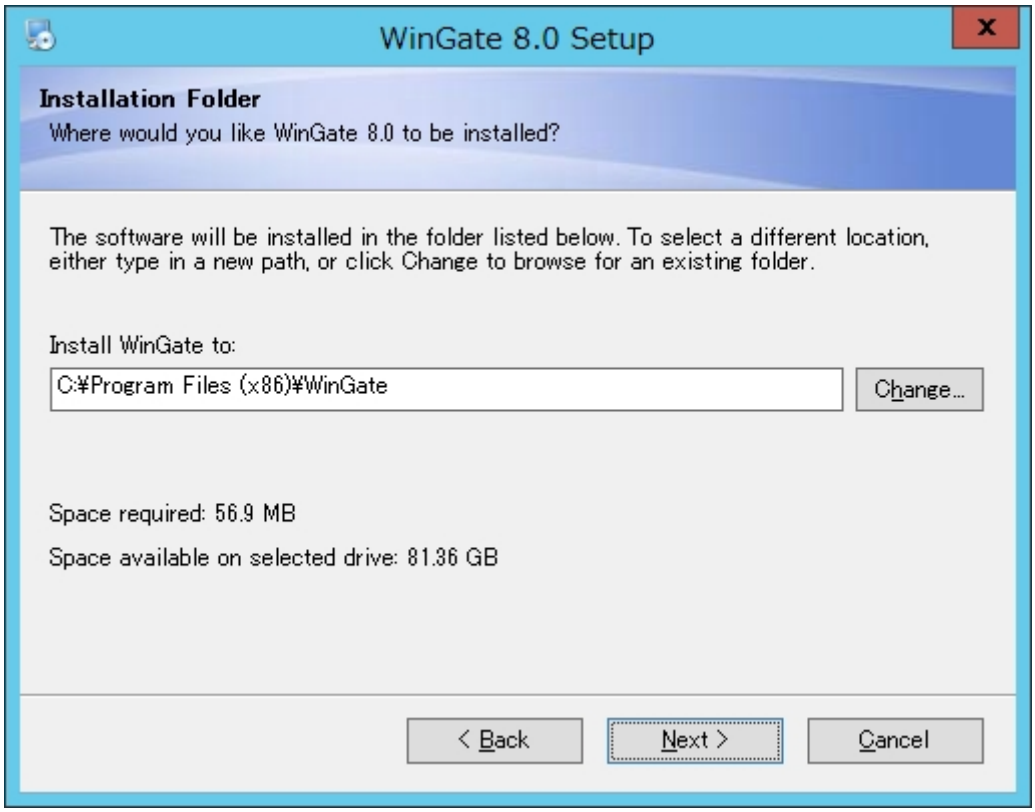

Welcomeダイアログが表示されます。起動している他のプログラムがある場合は、終了いただく事をお勧めいたします。Cancel（キャンセル）ボタンでインストールをキャンセルすることができます。
問題がない場合、「Next」をクリックして、次へ進みます。

3. License Agreement（ライセンス許諾）が表示されます。




同意いただける場合は「I agree to the terms of this License agreement」（ライセンス許諾に同意）を選択して「Next」ボタンで次へ進みます。

4. Installation Folder（インストールフォルダ）が表示されます。

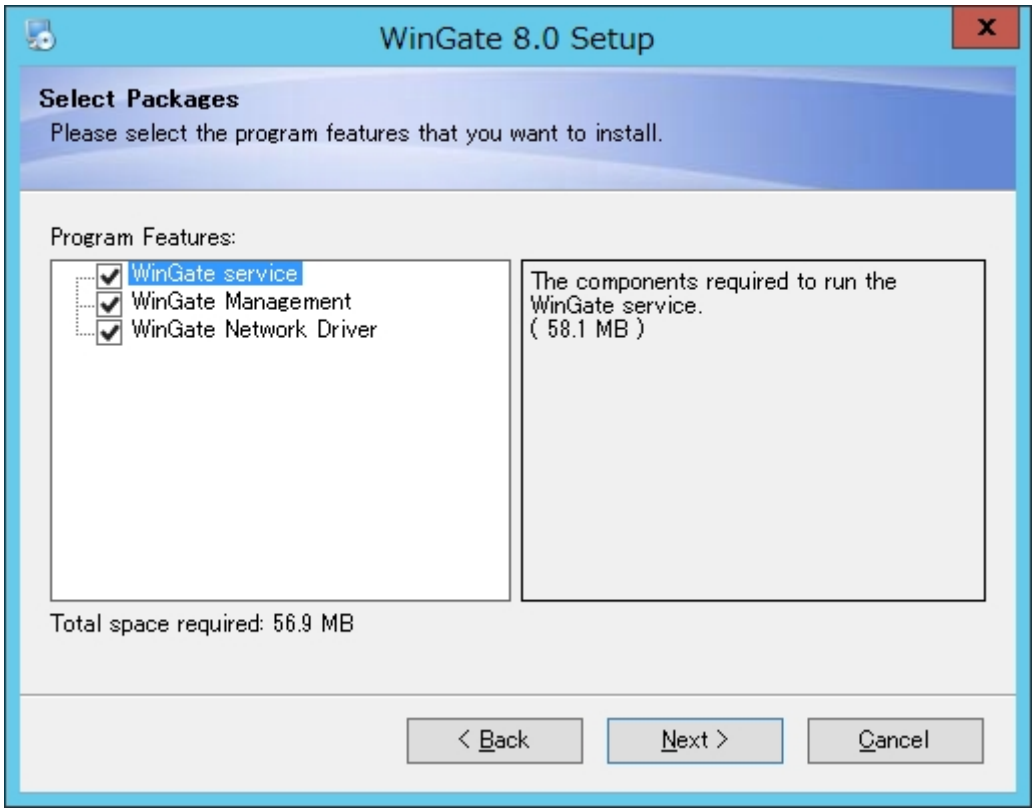



WinGate をインストールするフォルダーを選択します。インストールフォルダーは、51.0MB の空き容量が必要となります。（Space available on selected driver:）には、指定されたフォルダーの現在の空き容量が表示されております。

デフォルトでは C:¥Program files(x86)¥WinGate にインストールされます。変更する場合は「Change」ボタンをクリックして、フォルダーの参照ダイアログよりインストールディレクトリを指定してください。

設定が完了いたしましたら「Next」ボタンで次へ進みます。

5. Select Packages ダイアログが表示されます。

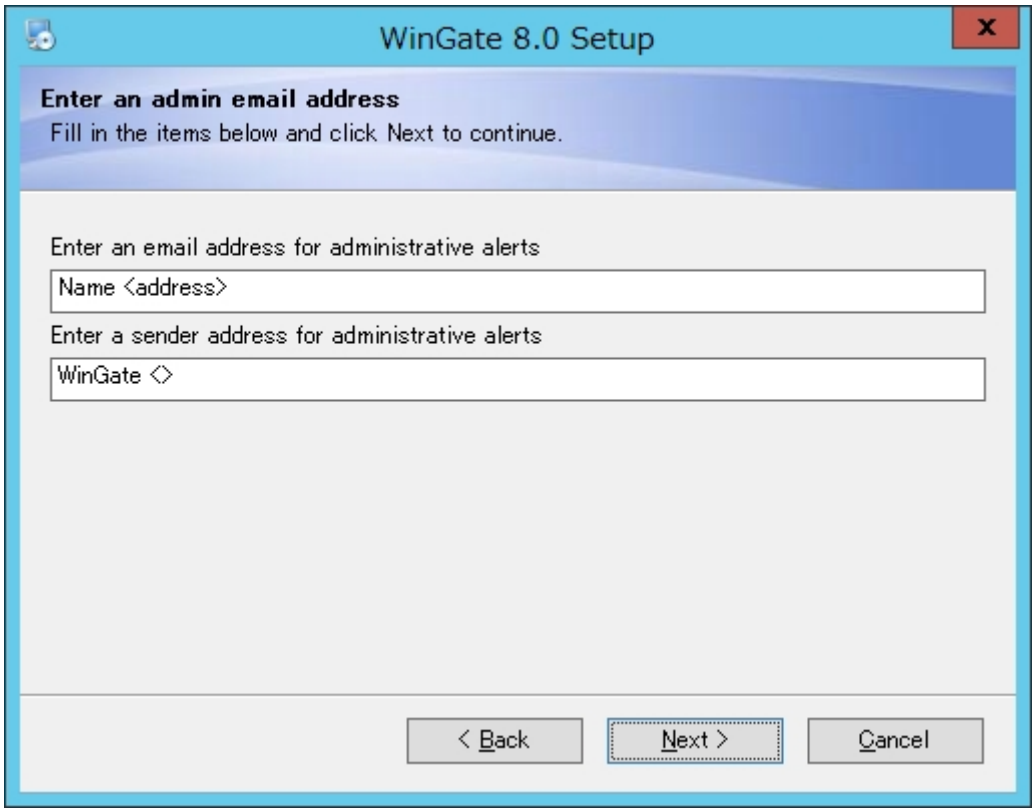



ここでは、インストールする WinGate のパッケージを選択します。
選択項目の内容は以下の通りです。
WinGate Service = WinGate の各サービスとなります。WinGate をプロキシサーバーなどとして使用する場合は、この項目が選択されている必要があります。
WinGate Management = WinGate の管理ツールである「WinGate Management」（WinGate マネージメント）をインストールします。
WinGate Network Driver = WinGate のファイアウォール、VPN、NAT 機能を使用する場合には、こちらを選択します。

**ご注意：**一般的な WinGate のインストールでは、WinGate Service、WinGate Management のみが選択される必要があります。
**WinGate Network Driver は、WinGate へ Extended Network Driver をインストールします、ファイアウォール、VPN、NAT 機能を使用しない場合は、この項目を選択する必要はありません。（例プロキシサーバーとしてのみ WinGate を使用する場合など）**

選択が完了いたしましたら「Next」ボタンで次へ進みます。

6. Enter an admin email address が表示されます。

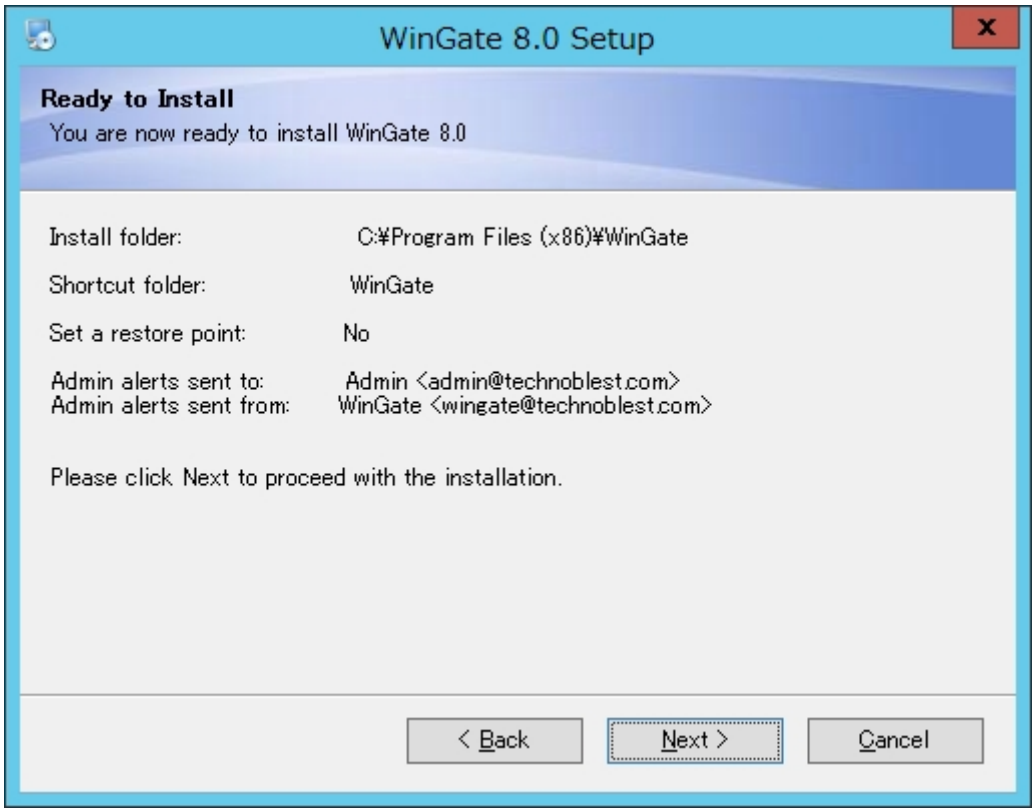



ここでは、WinGate インストール完了後に、警告などを配信する管理者の電子メールアドレスを入力してください。（必須ではありませんが入力をいただかない場合、インストール完了後にポリシー設定で警告が表示されます。）

ここで設定した電子メールアドレスへ警告メールを配信するには、インストール完了後に配信設定を行う必要があります。

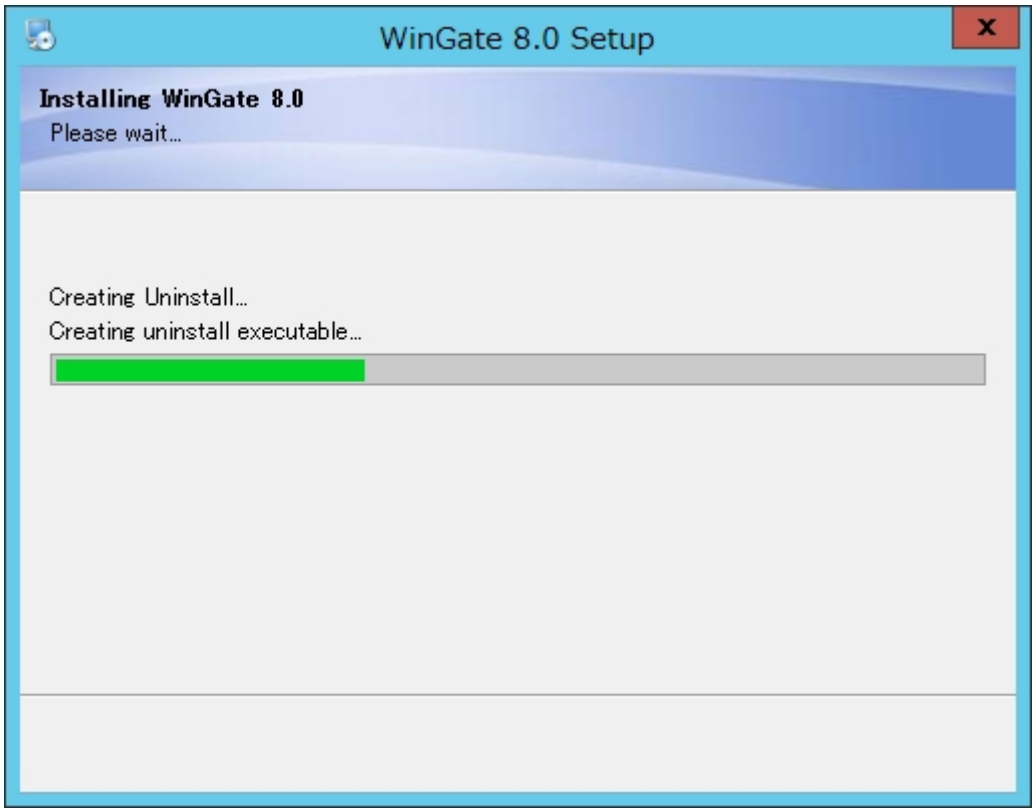
設定が完了いたしましたら「Next」で次へ進みます。

7. Ready to Install が表示されます。

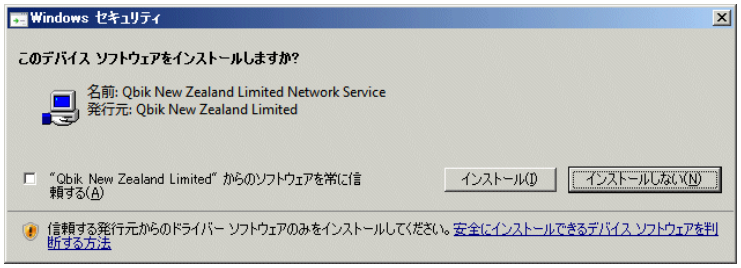



インストールの準備が完了いたしました。
これまでのダイアログで設定した内容が表示されますので、これらの内容に問題がない場合は、「Next」ボタンでインストールを開始します。内容を修正する場合は「Back」ボタンで必要な箇所まで戻り、設定を変更してください。

8. インストールが開始されます。

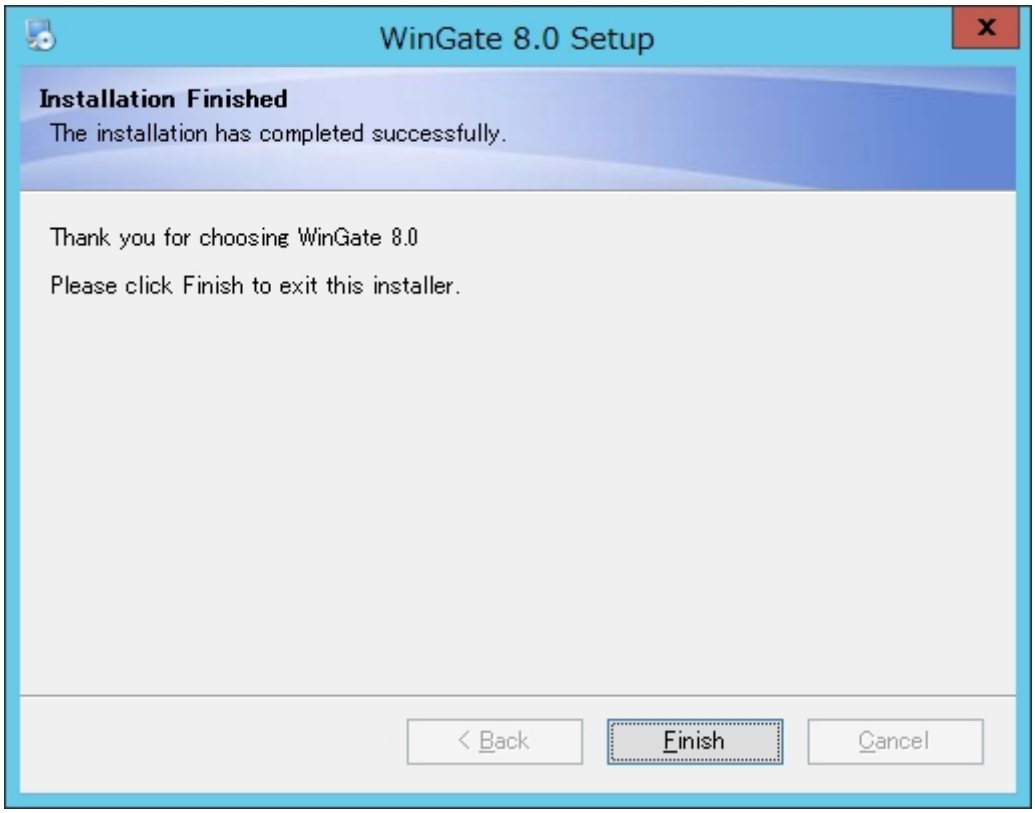


WinGate Network Driver を選択した場合、インストール途中に Windows セキュリティダイアログが表示される場合があります。(Windows Server 2008 など)



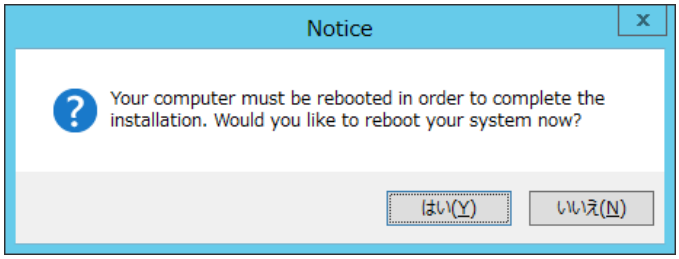

このダイアログが表示された場合、「インストール」「を選択してWinGateのインストールを継続してください。

9. Installation Finished が表示されます。




以上で WinGate のインストールは完了となります。Finish ボタンをクリックして、インストールを終了してください。

10. ダイアログが閉じられた後、WinGate Network Driver のインストールを選択している場合は PC の再起動を促す以下のダイアログが表示されます。




「はい」をクリックすると PC の再起動を行います。WinGate Network Driver のインストールを選択していない場合、PC の再起動は必須ではありませんが、再起動いただく事をお勧めいたします。

以上でインストールは完了となります。

**WinGate8.x のアップグレード（WinGate8 最新バージョンの適用、および WinGate7 からのアップグレード）**

WinGate の機能追加、機能修正はアップグレードによりのみ提供されます。

WinGate の開発元では、機能追加や機能修正を適用するために最新バージョンをリリースいたします。

最新バージョンを適用いただくことにより、新機能や機能修正を適用いただくことができます。（機能修正のみをおこなうパッチのリリースはございません。機能修正を適用するには、最新バージョンへアップグレードいただく必要があります。）

**アップグレード時の注意点**

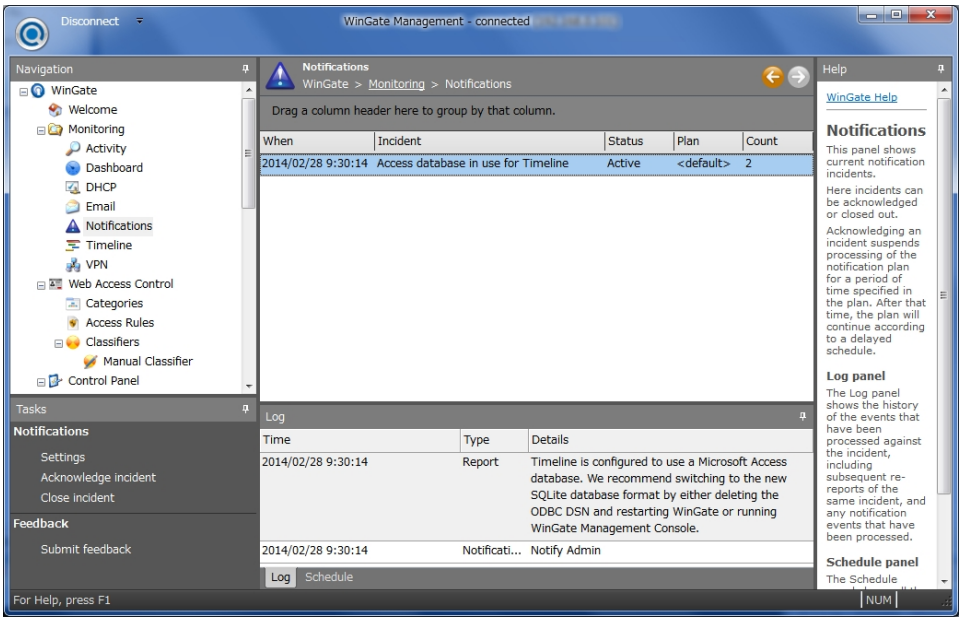
**ご注意：WinGate のアップグレード インストールを行う際は、WinGate エンジンが停止いたします。**
**インストール完了後は、PC の再起動を行っていただくことをお勧めいたします。（WinGate Network Driver をインストールいただきました場合、再起動は必須となります。）**

**ご注意：WinGate7 からアップグレードする場合、既存のキャッシュ情報、キャッシュボリュームは、全て削除されます。**
**アップグレード完了後に再設定いただく必要があります。**

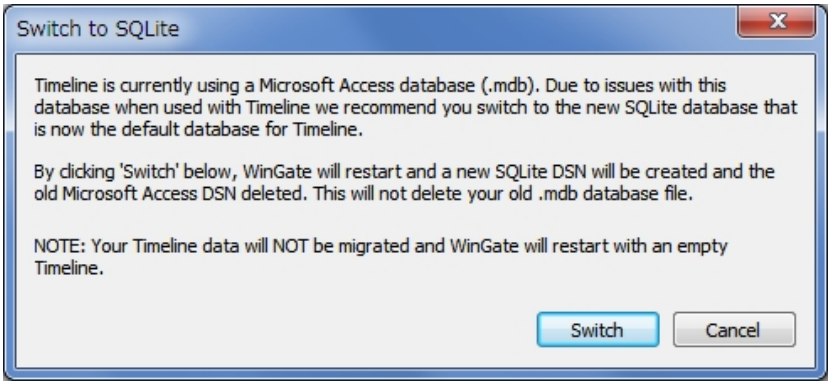
**アップグレード時の注意点 （WinGate 8.1.0 へのアップグレード）**

**ご注意**：WinGate8.1.0 では、Timeline（タイムライン）機能で使用されるデーターベースが、MDB から SQLite へ変更されました。

WinGate8.1.0 へアップグレード後、WinGate Management へログインすると以下のような通知が表示されます。




Timeline を選択すると以下のようなダイアログが表示され、データーベースの変更を行うかを決定します。



**ご注意**:Timeline のデーターベースを変更した場合、以前の Timeline データーベースは継承(統合)されません。また、Microsoft Access DSN は、削除されます。
**ご注意:変更を適用するには、WinGate の再起動が必要となります。**

Timeline で使用されるデーターベースを SQLite へ変更するには「Switch」ボタンをクリックして、ダイアログの指示に従い WinGate の再起動を行ってください。

Timeline で使用されるデーターベースを変更しない場合は、「Cancel」ボタンをクリックしてください。

以前の MDB データーベースは、小規模なユーザー向けとなり、今回の変更により使用される SQLite は、中/大規模なユーザーで WinGate を使用しているお客様で強く推奨されます。

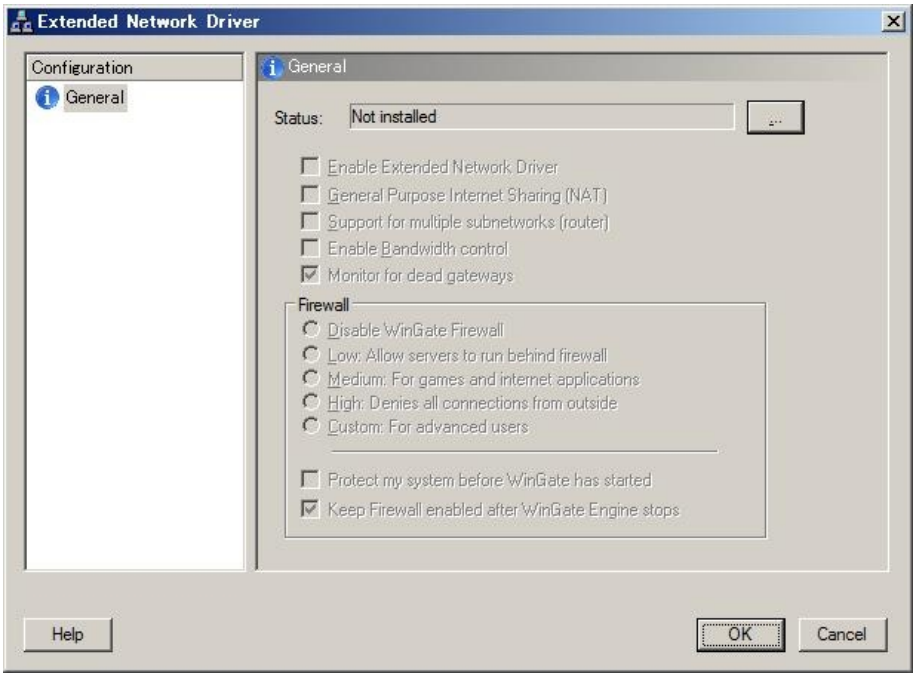
**アップグレード前の確認事項**
最新バージョンをインストールする前に、以下の内容をご確認ください。

- **アップグレード保証の有効期間**
  アップグレード保証の有効期間が経過している場合、最新バージョンを適用するために、有償でアップグレード保証を更新いただく必要がある場合がございます。
  WinGate Management の Licensing よりアップグレード保証の有効期限をご確認ください。
  アップグレード保証期限内の場合は、最新バージョンを適用いただくことができます。アップグレード保証の有効期限が経過している場合は、最新バージョンを適用できない場合がございます。詳細に関しては、弊社 Web サイトのダウンロードページをご参照いただくか、弊社までお問い合わせください。

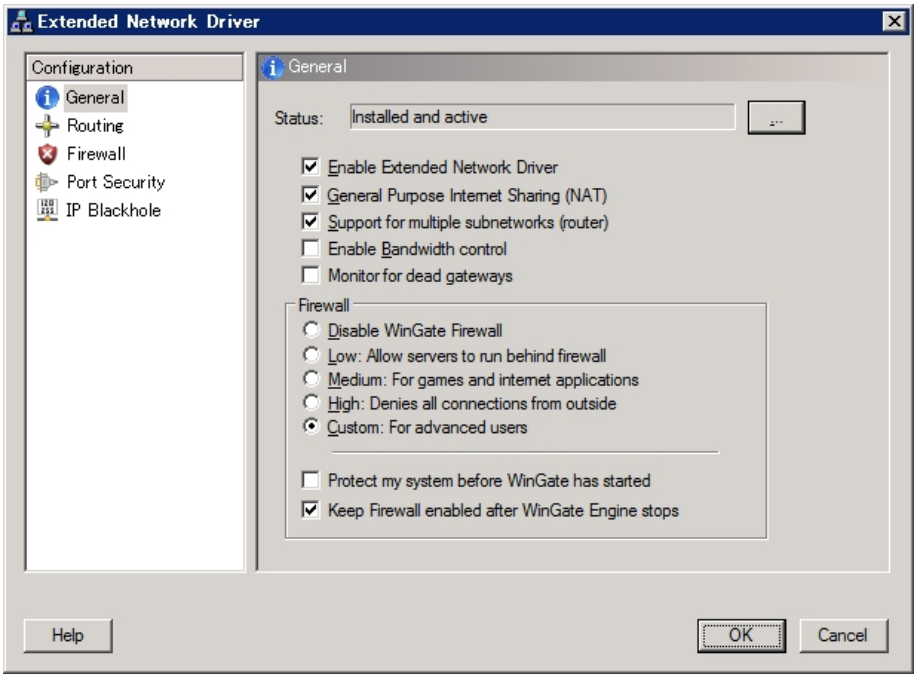
  **WinGate8.0.0 について**
  2013 年 6 月 1 日時点で、アップグレード保証の有効期限内である場合は、現在のライセンスキー情報で、そのまま WinGate8.0.0 を利用いただくことができます。2013 年 6 月 1 日時点でアップグレード保証有効期限が切れている場合は、WinGate8 へアップグレードいただく事ができません。アップグレード保証の更新をご検討ください。

- **設定情報のバックアップ**
  最新バージョンへのアップグレードは、最新バージョンのインストーラーを実行し、上書きインストールによりアップグレードされます。
  設定情報を引き継いだインストールが可能となりますが、念のため事前に設定情報やログ情報などを保存いただくことをお勧めいたします。設定のバックアップ方法に関しては、本ユーザーガイドをご参照ください。

- **重要:WinGate Network Driver インストール有無の確認**
  WinGate のインストーラーは、WinGate Network Driver インストールの有無を検知いたしません。
  **WinGate Network Driver を使用していない場合は、インストーラーで WinGate Network Driver のインストールを手動で外していただく必要があります。**
  事前に WinGate Network Driver がインストールされているかを WinGate Management でご確認ください。
  WinGate Network Driver がインストールされていない場合、WinGate Management の Extended Networking をクリックすると以下のように Status に Not installed と表示されています。




インストールされている場合、以下のように Status は、Installed and active と表示されます。




◆ **Kaspersky AntiVirus for WinGate**

Kaspersky AntiVirus for WinGate がインストールされている場合、必ず先に Kaspersky AntiVirus for WinGate のアップデートを先に行ってください。

**インストール方法**

最新バージョンをインストールするには 2 つの方法があります。

1. 弊社 WinGate Web サイトより最新バージョンのインストーラーをダウンロードして、インストールする方法
2. WinGate Management の WinGate Update で最新バージョンを確認、ダウンロードしてインストールする方法

1. **弊社 WinGate Web サイトより最新バージョンのインストーラーをダウンロードして、インストールする方法**

   ① http://www.wingate.jp/ へアクセスし、ダウンロードページを開きます。

   ② ページ内から最新バージョンのリンクをクリックしてインストーラーをダウンロードします。

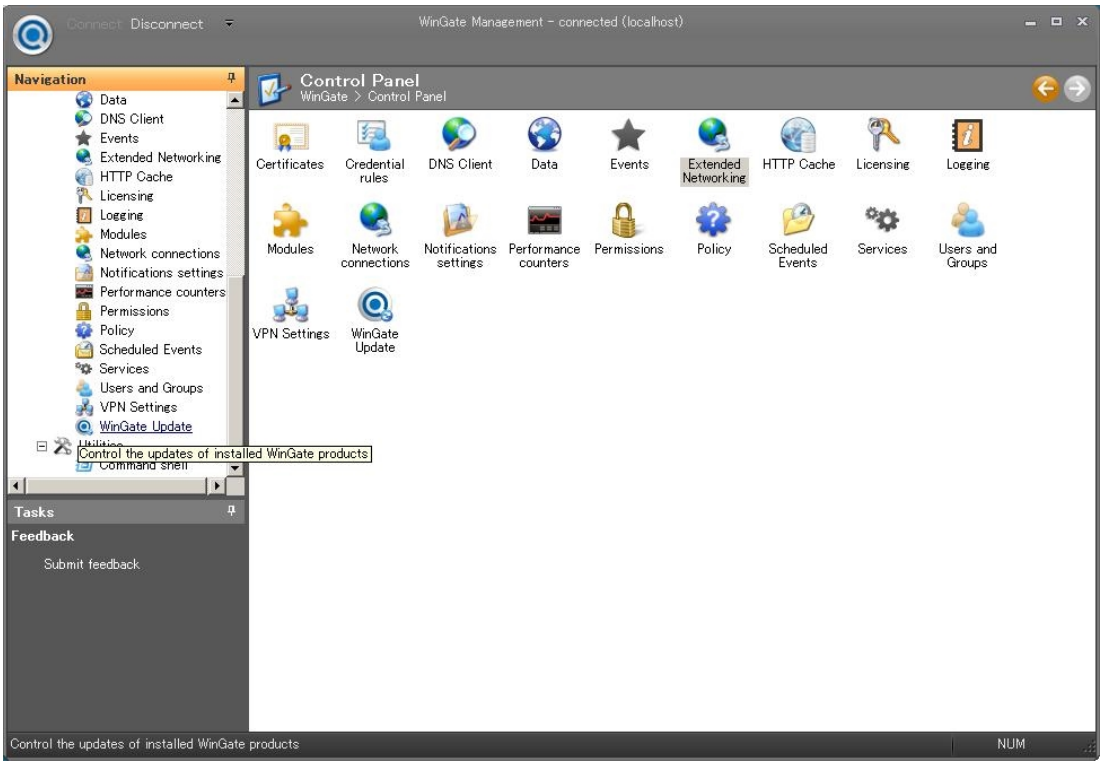
   ③ ダウンロードしたインストーラーを WinGate がインストールされている PC の任意の場所に置きます。

   これ以降の手順は、共通となります。

2. WinGate Management の WinGate Update で最新バージョンを確認、ダウンロードしてインストールする方法

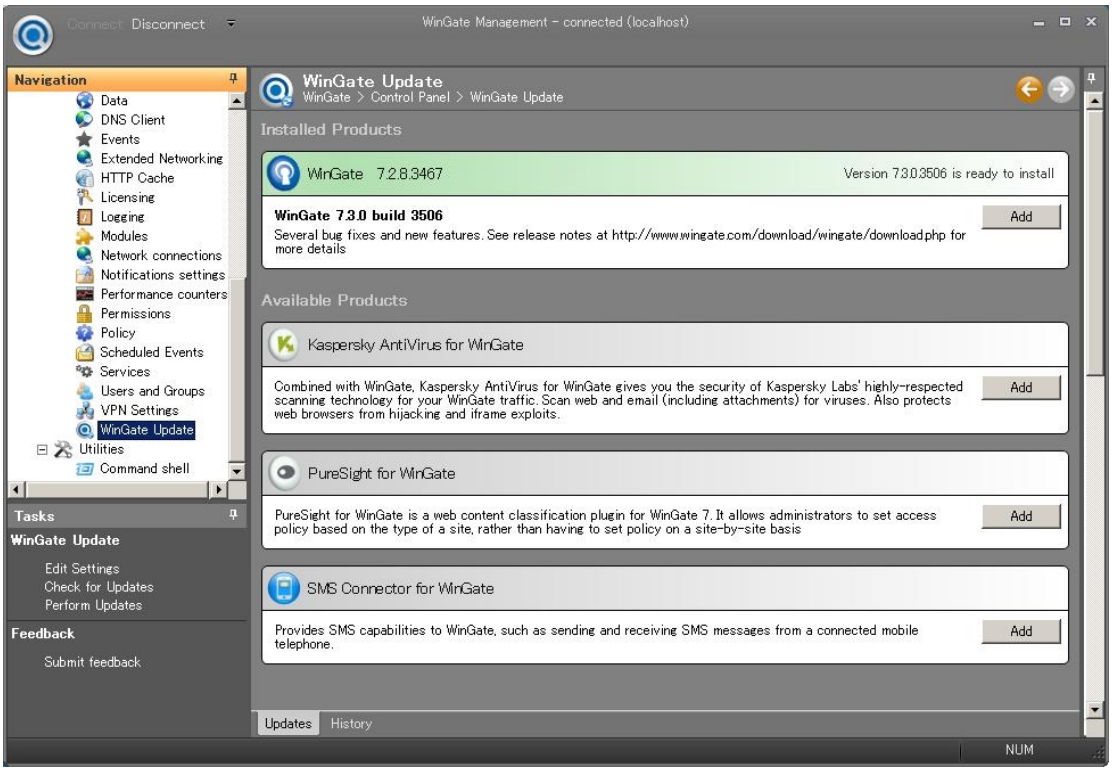
   ① WinGate Management へログインします。

   ② Navigation より WinGate Update を選択します。



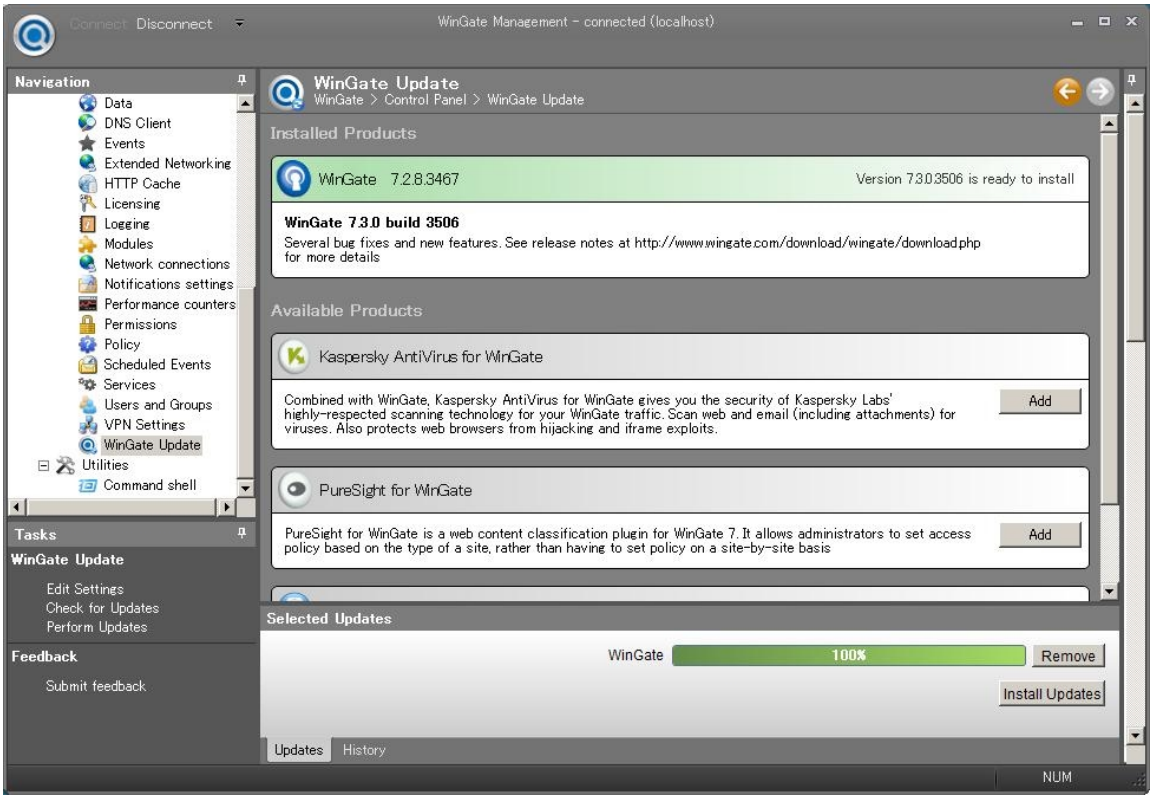

   ③ WinGate Update の設定により、最新バージョンが認識されている場合、Installed Products の WinGate に最新バージョンが表示されます。

   最新バージョンがリリースされている状況で、最新バージョンが表示されていない場合、Navigation の下にございます Tasks の WinGate Update より Check for update をクリックしてください。




④　適用する製品にある「Add」ボタンをクリックします。

画面下の Selected Update に WinGate が表示されますので「Start download」ボタンをクリックしてダウンロードを開始します。




⑤　ダウンロードが終了いたしましたら Install Update ボタンをクリックしてインストールを開始します。

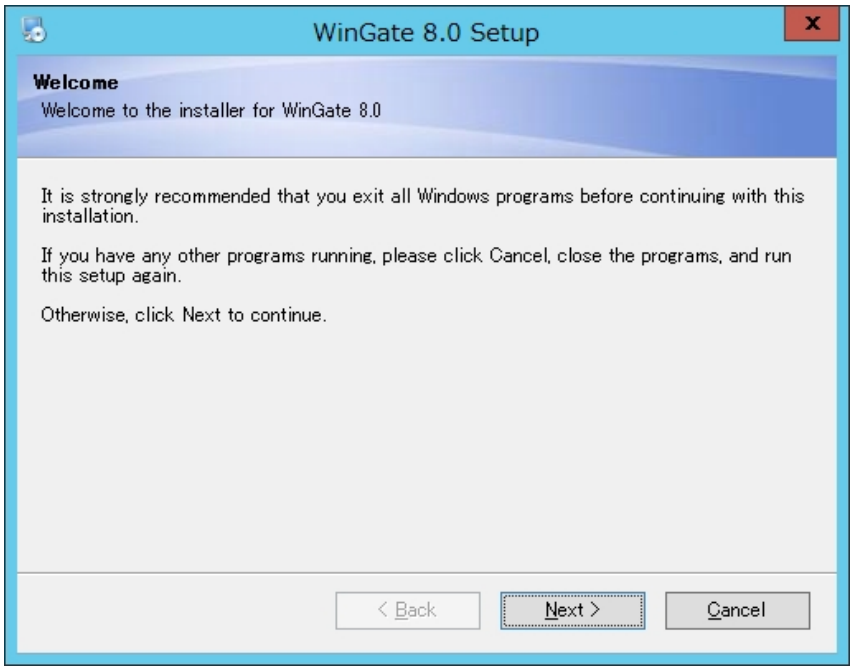
これ以降の手順は、共通となります。（※Kaspersky AntiVirus for WinGate がインストールされている場合、必ず先に Kaspersky AntiVirus for WinGate のアップデートを行ってください。）

**インストール共通手順**

何れの方法の場合もインストールを開始すると、WinGate のインストーラーが開始されます。

アップグレードインストールは、新規インストールと共通の手順となります。 インストーラーの指示に従いインストールを行ってください。

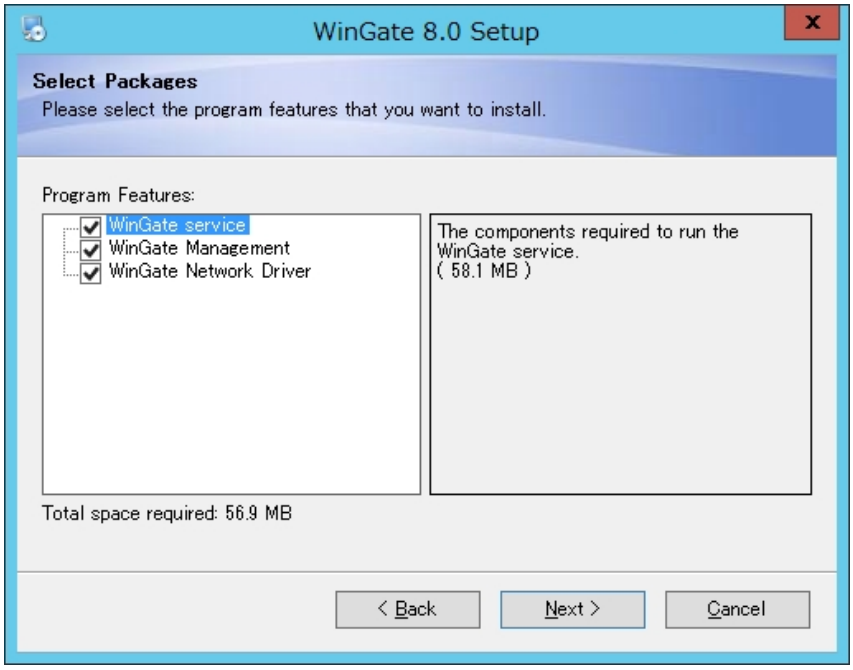
1. インストーラーが開始されます。




Welcomeダイアログが表示されます。起動している他のプログラムがある場合は、終了いただく事をお勧めいたします。Cancel（キャンセル）ボタンでインストールをキャンセルすることができます。

問題がない場合、「Next」をクリックして、次へ進みます。

2. Select Packages ダイアログが表示されます。




ここでは、インストールする WinGate のパッケージを選択します。

選択項目の内容は以下の通りです。

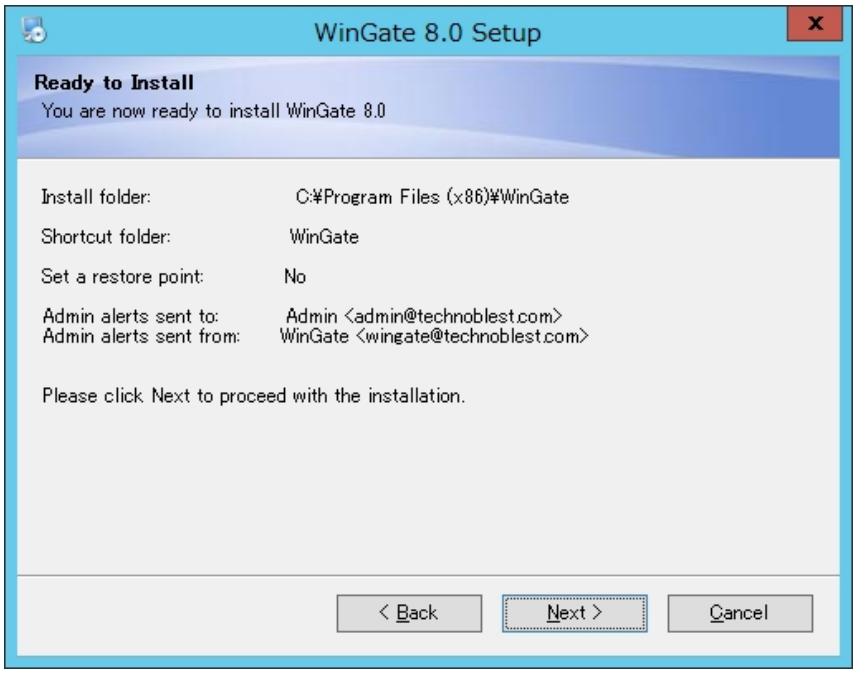
WinGate Service = WinGate の各サービスとなります。WinGate をプロキシサーバーなどとして使用する

場合は、この項目が選択されている必要があります。
WinGate Management = WinGate の管理ツールである「WinGate Management」（WinGate マネージメント）をインストールします。
WinGate Network Driver = WinGate のファイアウォール、VPN、NAT 機能を使用する場合には、こちらを選択します。

**※重要※　ご注意：**WinGate のインストーラーは、WinGate Network Driver インストールの有無を検知いたしません。
**WinGate Network Driver を使用していない場合は、インストーラーで WinGate Network Driver のインストールを手動で外していただく必要があります。 チェックされた状態でインストールを行うと、WinGate Network Driver がインストールされます。**

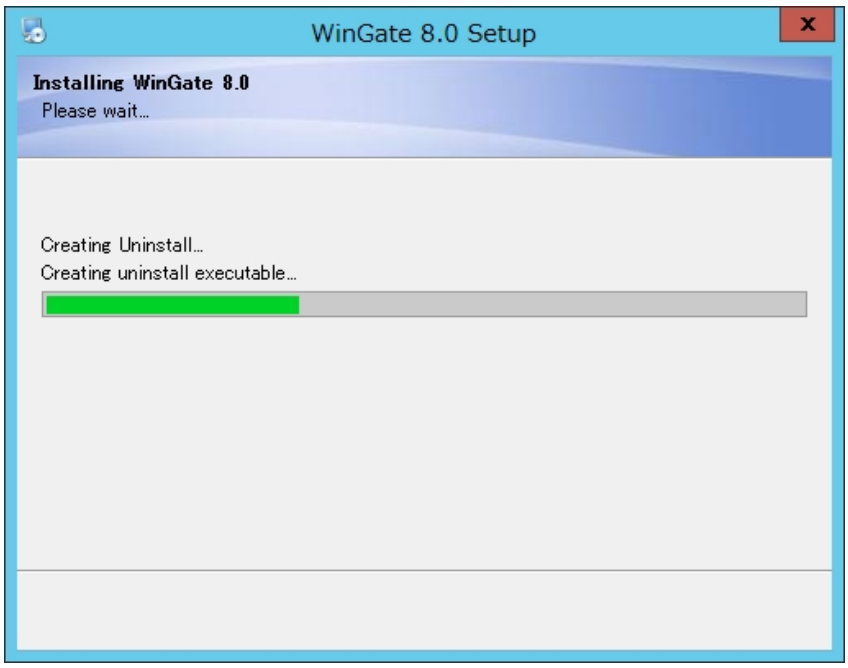
選択が完了いたしましたら「Next」ボタンで次へ進みます。

3. Ready to Install が表示されます。

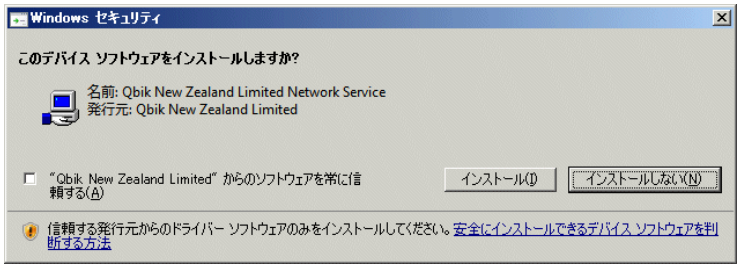



インストールの準備が完了いたしました。
これまでのダイアログで設定した内容が表示されますので、これらの内容に問題がない場合は、「Next」ボタンでインストールを開始します。内容を修正する場合は「Back」ボタンで必要な箇所まで戻り、設定を変更してください。

4. インストールが開始されます。

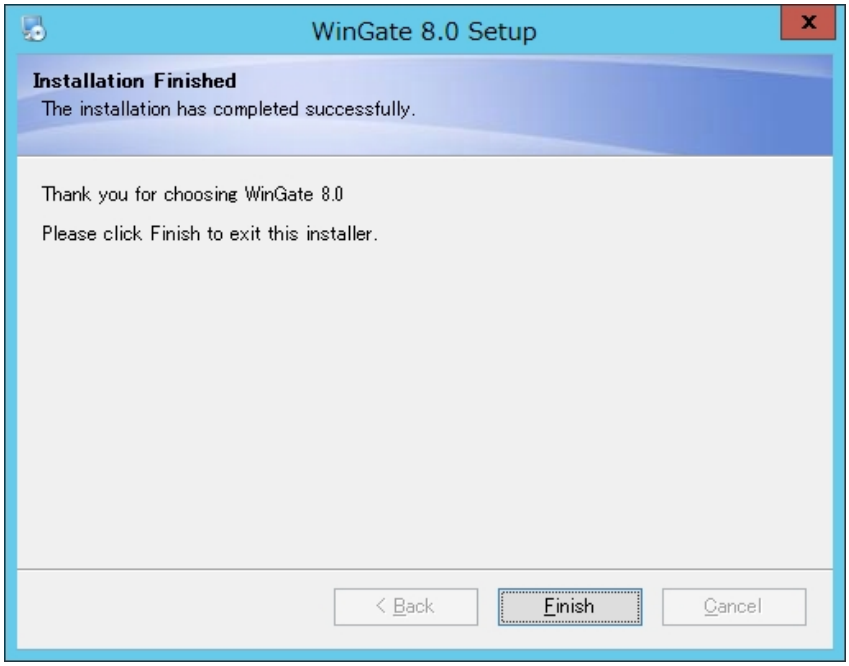



WinGate Network Driver を選択した場合、インストール途中に Windows セキュリティダイアログが表示される場合があります。



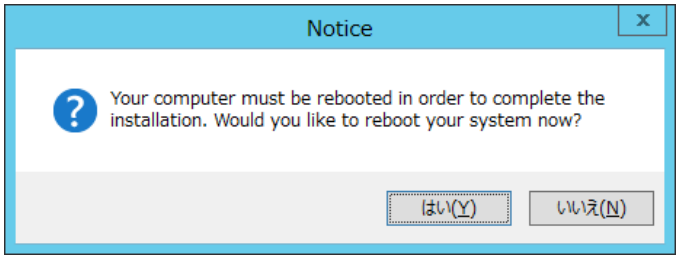

このダイアログが表示された場合、「インストール」「を選択してWinGateのインストールを継続してください。

5. Installation Finished が表示されます。




以上で WinGate のインストールは完了となります。Finish ボタンをクリックして、インストールを終了してください。

6. ダイアログが閉じられた後、WinGate Network Driver のインストールを選択している場合は PC の再起動を促す以下のダイアログが表示されます。




「はい」をクリックすると PC の再起動を行います。
WinGate Network Driver のインストールを選択していない場合、PC の再起動は必須ではありませんが、再起動いただく事をお勧めいたします。

以上でアップグレードインストールは完了となります。
インストール完了後は、必ず以前の設定情報が引き継がれているかを WinGate Management よりご確認いただき、クライアントからの WinGate の利用など動作確認を行ってください。

### 旧バージョンからのアップグレード（WinGate6. x からのアップグレード）

WinGate6.x 以前の WinGate がインストールされている環境から WinGate8 へアップグレードいただくことにより、最新版の機能、および最新版で修正された内容を適用いただくことができます。

**ご注意：**バージョンアップを行うには、2013 年 6 月 1 日時点でアップグレード保証の期限内である必要があります。アップグレード保証期限の確認は、GateKeeper のヘルプ（Help）メニュー、ライセンス管理（License Management）より表示されます、Qbik ライセンスビューアで、登録されているライセンスをクリックいただき、下の欄にございます「VERSION PROTECTION EXPIRY:」に表示されている日付となります。
インストール前に、必ずアップグレード保証の日付をご確認いただき、この範囲内であるかをご確認ください。
アップグレード保証の期限が過ぎている場合は、有償でアップグレード保証の更新を行う必要があります。
アップグレード保証更新については、ライセンスキー情報をお書き添えのうえ、sals@technoblest.com まで電子メールをお送りください。折り返し価格情報などをご返信させていただきます。

**ご注意：**WinGate6 以前のバージョンをご利用いただいておりますお客様は、WinGate8 への上書きアップグレードをサポートしておりません。一旦アンインストールを行い、新規に WinGate8 をインストールくださいますようお願い申し上げます。

**バージョンアップの際の注意点（必ずお読みください）**
WinGate8 は、WinGate6 から大幅な機能変更ができ要されており、一部の機能の上書きインストールによる設定情報の引き継ぎができません。また、幾つかの機能は WinGate7 以降で失われております。
Kaspersky AntiVirus for WinGate がインストールされている場合、WinGate8 の Kaspersky AntiVirus for WinGate は、旧バージョンの Kaspersky AntiVirus for WinGate と互換性がなく、設定情報の継承が行われないことにご注意ください。（※上書きインストールにより、旧バージョンの Kaspersky AntiVirus for WinGate は自動的にアンインストールされます。WinGate インストール完了後に、別途 Kaspersky AntiVirus for WinGate のインストール、設定を行う必要があります。）
**弊社では、WinGate6 と WinGate7 以降の機能の違いや WinGate7 以降の設定などを事前にご確認いただくために、テスト環境にて WinGate7 以降の試用版をご利用いただき、テストを実施いただくことをお勧めいたします。**
WinGate8 への上書きインストールを行う際は、これらの内容をご理解いただいたうえで、アップデートを行ってください。
また、**可能となります場合は、WinGate8 の新規にインストール,再設定いただくことを強くお勧めいたします。**

以下は、それらの情報を簡単にまとめた内容となります。（詳細に関しては「WinGate6 をご利用いただいておりますお客様へのご注意（重要）」の章をご覧ください。

**WinGate6 から WinGate8 で引き継がれない設定**

- **ポリシー**
  各サービス、プロキシ、システムで設定されたポリシーは、引き継がれません。WinGate7 のポリシーで新たに設定する必要があります。
- **キャッシュ**
  キャッシュされた内容、キャッシュ設定など既存のキャッシュ情報、設定は引き継がれません。WinGate7 の HTTP

キャッシュで新たに設定を行う必要があります。

- **スケジューラ**
  スケジューラの設定内容は引き継がれません。WinGate7 のスケジュール・イベントで新たに設定する必要があります。
- **プラグイン**
  Kaspersky AntiVirus for WinGate などのプラグイン、および設定内容は引き継がれません。また、過去のバージョンとも互換性がありませんので、WinGate7 インストール完了後は、新たにプラグインをインストール、設定する必要があります。
- **SMTP Proxy Server**
  SMTP Proxy Server がインストールされた環境に、WinGate7 を上書きインストールした場合、WinGate7 では、SMTP Proxy Service がそのまま作成されますが、現在マッピング先などの情報を引き継ぐことができません。
  SMTP Proxy Server をご利用いただいております場合、WinGate7 インストール完了後に TCP Mapping サービスにて、SMTP 用のマッピングサービスを作成してください。
  詳細に関しては、本書の設定例の章をご覧ください。

**ユーザー・データーベースについて**

WinGate6 から上書きインストールを行った場合、WinGate8 は既存のユーザー・データーベースを調査し設定情報を引き継ぎますが、WinGate8 への上書きアップデート完了後は、必ず既存のユーザー・データーベース情報が正しく移行されているかをご確認ください。

**引き継がれる設定内容**

- 現在のサービス構成
- 現在の拡張ネットワーキング（Extended networking）構成
- 現在のメール設定
- 現在のネットワーク接続構成
- ダイアルアップ構成

**メールサーバー機能をご利用いただいておりお客様へのご注意**

WinGate8 への上書きインストールを行った場合、新しいユーザー・データーベースに電子メール・メールボックスを移動します。
これは全て IMAP 形式へのメールボックスへ移動されます。
WinGate 7 は、POP3、IMAP4 メールボックス間には、区別が全くありません、すべてのメールボックスが IMAP 形式で保存されます。ユーザーが、POP3 プロトコルを使用して、WinGate メールボックスにアクセスすることを望む場合、ユーザーは受信トレイフォルダーにアクセスすることができるだけとなるのでご注意ください。

**WinGate7 以降で変更される機能**

以下は WinGate7 以降で変更されています。内容が異なりますので、新たに設定を行う必要がある場合がございます。

- **ロギング**
  WinGate8 では、新たに W3C 形式のログに変更されております。（WinGate Professional 版、Enterprise

版のみ） また、ログの保存ディレクトリ、取得内容も異なりますので、インストール完了後は、Logging より設定を行ってください。

- **ファイアウォールタブ**
  WinGate8 では、ファイアウォールタブはありません。Logging の WinGate NAT ログの項目でブロックした情報を確認することができます。

**WinGate7、および WinGate8 で失われた機能**

以下の機能は WinGate8 では失われております。これらの機能をご利用いただいております場合は、これらの機能が利用いただけないことをご理解いただいた上で WinGate7 のアップグレードを行ってください。

- **Java 認証**
  Java 認証機能を WinGate8 で使用することはできません。NTLM 認証をベースとした WWW 認証への変更をご検討ください。
- **Kaspersky AntiVirus for WinGate の隔離機能**
  WinGate8 は、隔離機能を持ちません。WinGate プラグインの Kaspersky AntiVirus によってスキャンされた HTTP、SMTP、および POP3 Proxy トラフィックは、許可(クリーンである場合)、またはスキャンの結果に基づき拒否されるだけです。
- **プロキシでのドリップフィード**
  これは必要に応じてプラグインで自動的に制御されます。
- **SMTP Proxy Server**
- **ログファイルサーバ**
- **Telnet コマンドライン管理インターフェース**

**バージョンアップを行う前に（最終確認のお願い）**

◆ バージョンアップを行う前に、バージョンアップを行うシステムが、先に記述されているシステム用件を満たしているかご確認ください。

◆ 以前の WinGate で拡張ネットワーキング（Extended networking）をインストールしていない場合、本バージョンで拡張ネットワーキング（Extended networking）をインストールすることにより、ネットワークの構成に、いくつかの重要な変更を加える場合があります。

◆ WinGate7 以降で引き継がれない機能、失われた機能の影響がご理解いただけているかを再度ご確認ください。

◆ Kaspersky AntiVirus for WinGate は、WinGate8 をインストールする際に削除されます。WinGate8 インストール完了後にインストールしてください。

**WinGate6.6 から WinGate 最新版へのアップグレード**

以下の手順により WinGate 6.6.x 英語版から最新バージョンへアップグレードいただくことができます。

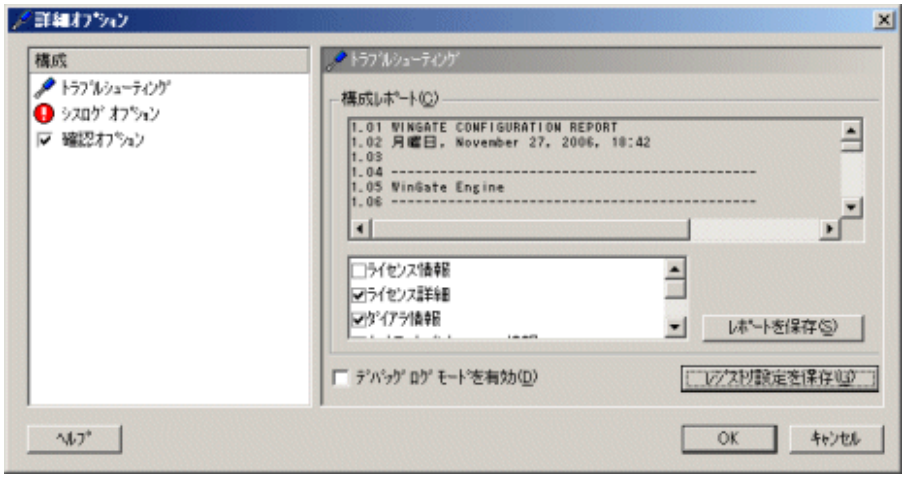
**ご注意:アップグレードを行う際は、必ず WinGate の設定情報をバックアップしてください。また、ログ情報などに関しても、必要に応じてバックアップを行ってください。**

1. WinGate の設定情報のバックアップ

   ご注意:レジストリ情報の保存により保存されるのは WinGate の設定情報のみとなります。ログやメールデータなどは保存されません。

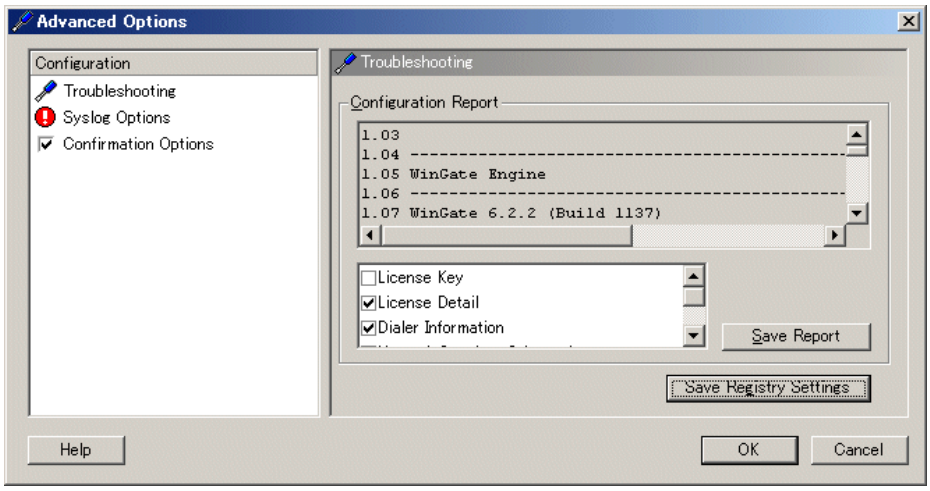
   WinGate 6.6 日本語版のバックアップ

   GateKeeper のオプションメニュー → 詳細 → 詳細オプション・ダイアログで「レジストリ情報を保存」ボタンをクリックし、レジストリファイルを WinGate のインストールディレクトリ以外の任意の場所に保存します。




   WinGate6.x 英語版の設定情報のバックアップ

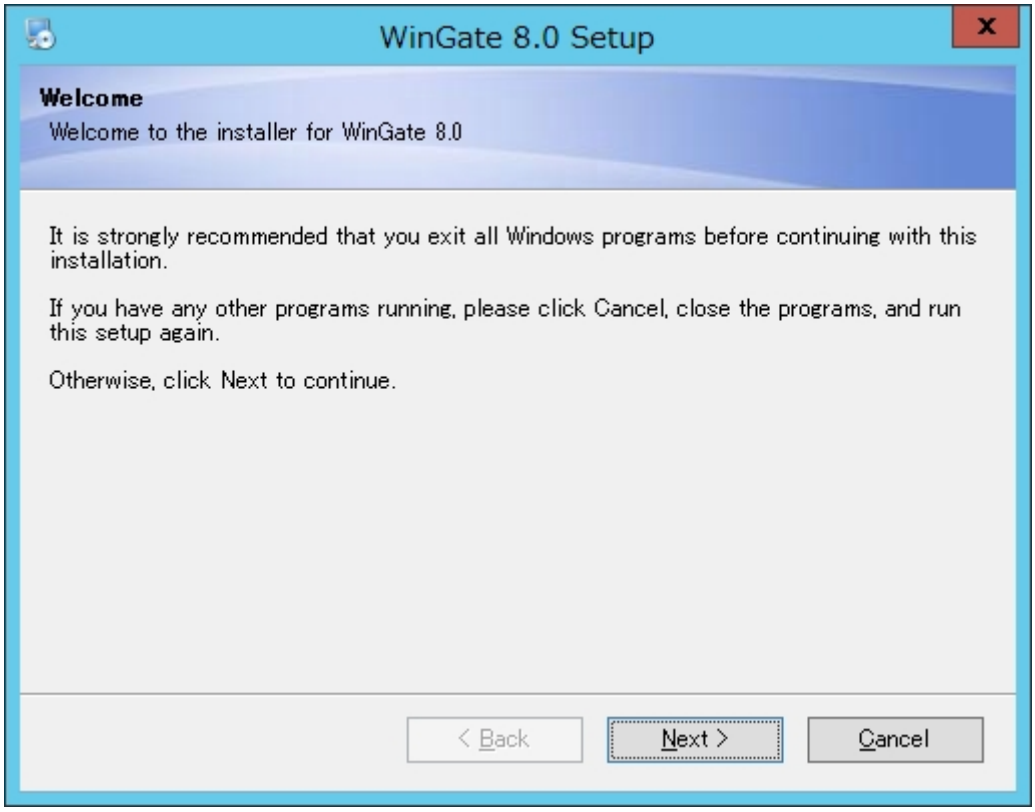
   GateKeeper の Options メニュー → Advanced → Advanced Options ダイアログで「Save Registry Settings」ボタンをクリックし、レジストリファイルを WinGate のインストールディレクトリ以外の任意の場所に保存します。




2. WinGate7 のインストールプログラムを実行します。

   (GateKeeper を実行している場合、終了してください。WinGate エンジンは開始された状態でも問題はありません。インストール時に自動的に停止されます。)

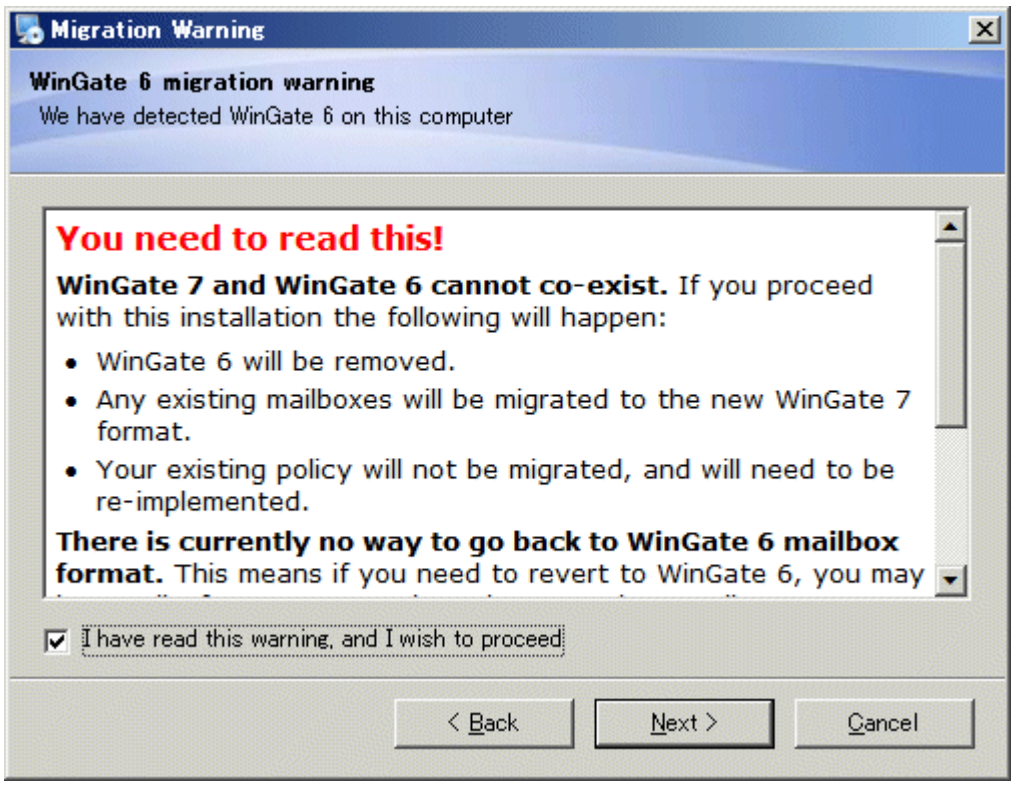
3. Welcome ダイアログが表示されます。




起動している他のプログラムがある場合は、終了いただく事をお勧めいたします。Cancel（キャンセル）ボタンでインストールをキャンセルすることができます。

問題がない場合、「Next」をクリックして、次へ進みます。

4. WinGate8 のインストーラーは WinGate6 がインストールされていることを検出し、WinGate6 migration warning（WinGate6　移行警告）ダイアログを表示します。




警告内容は下記の通りとなります。

必ずお読みください！

WinGate 7、WinGate8 と WinGate 6 は共存することができません。このインストールを継続すると、以下の内容が発生します。:

- WinGate 6 は削除されます。
- どんな現在のメールボックスは、新しい WinGate7 以降のフォーマットに移行されます。
- 現在のポリシーは移行されません。そしてポリシーを再設定する必要があります。

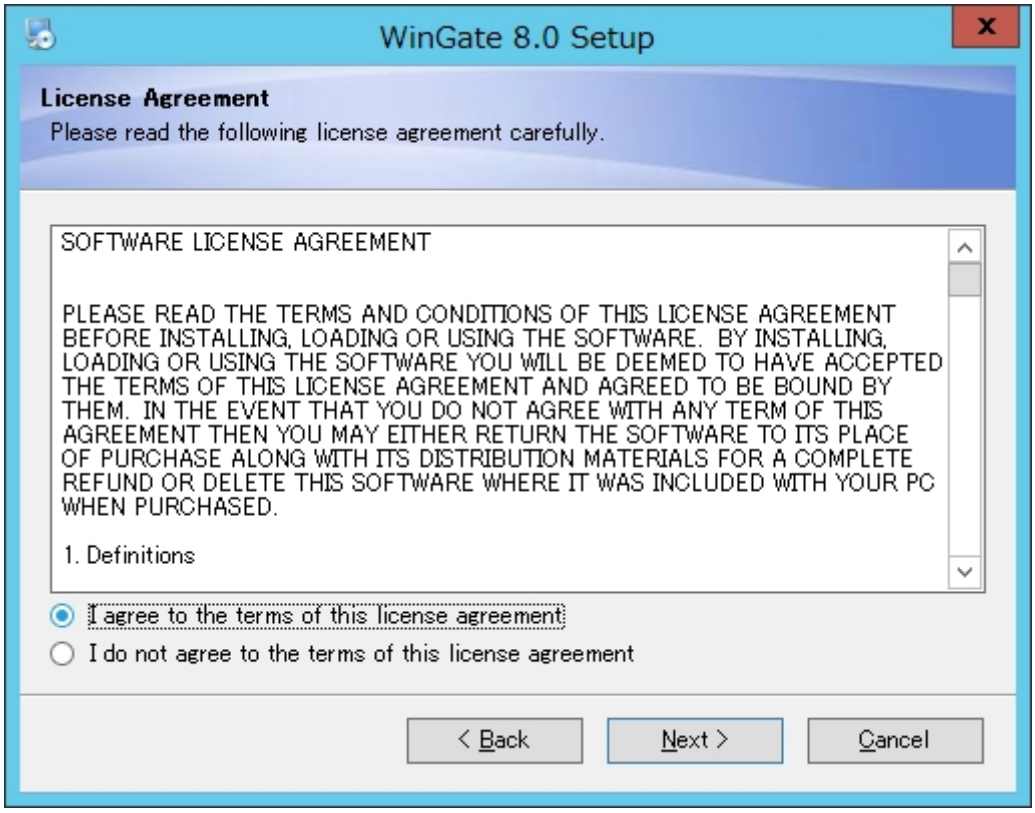
**WinGate 6 メールボックス形式に戻す方法はありません。**これは、お客様が WinGate 6 へ戻す必要がある場合、メール情報を失うことを意味します。もし、お客様が WinGate にホストメールを使用していないなら、WinGate6 へ戻り、WinGate レジストリのバックアップを取ることができます。

**WinGate7 を展開する前に、これがお客様の望む製品であることを確実にしてください。**弊社は、WinGate7 を展開する前に、テスト環境で WinGate7 を評価いただくことをお勧めいたします。

本件に関するご質問がございます場合、WinGate サポート( support@wingate.com )へご連絡ください。(日本のお客様は wg_support@technoblest.com へご連絡ください。)

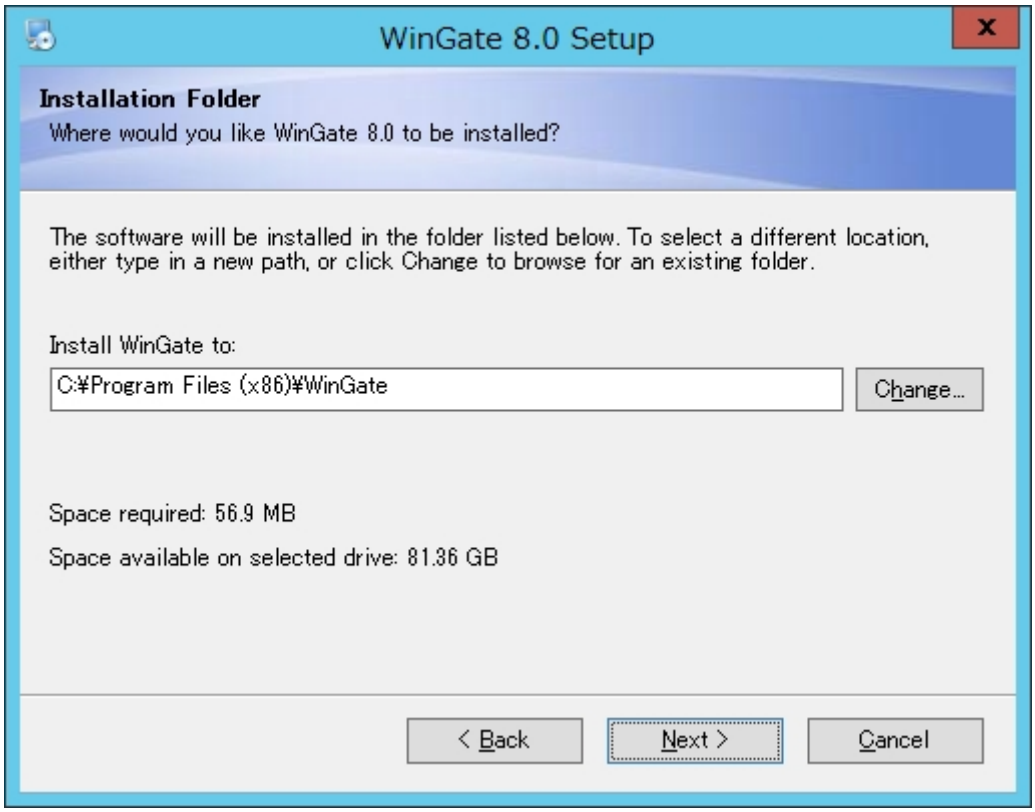
これらの内容をご確認いただき、問題がない場合は「I have read this warning, and I wish to proceed」(私はこの警告を読み、継続することを望みます。)をチェックし「Next」ボタンで次へ進みます。

5. License Agreement(ライセンス許諾)が表示されます。




同意いただける場合は「I agree to the terms of this License agreement」(ライセンス許諾に同意)を選択して「Next」ボタンで次へ進みます。

6. Installation Folder（インストールフォルダ）が表示されます。

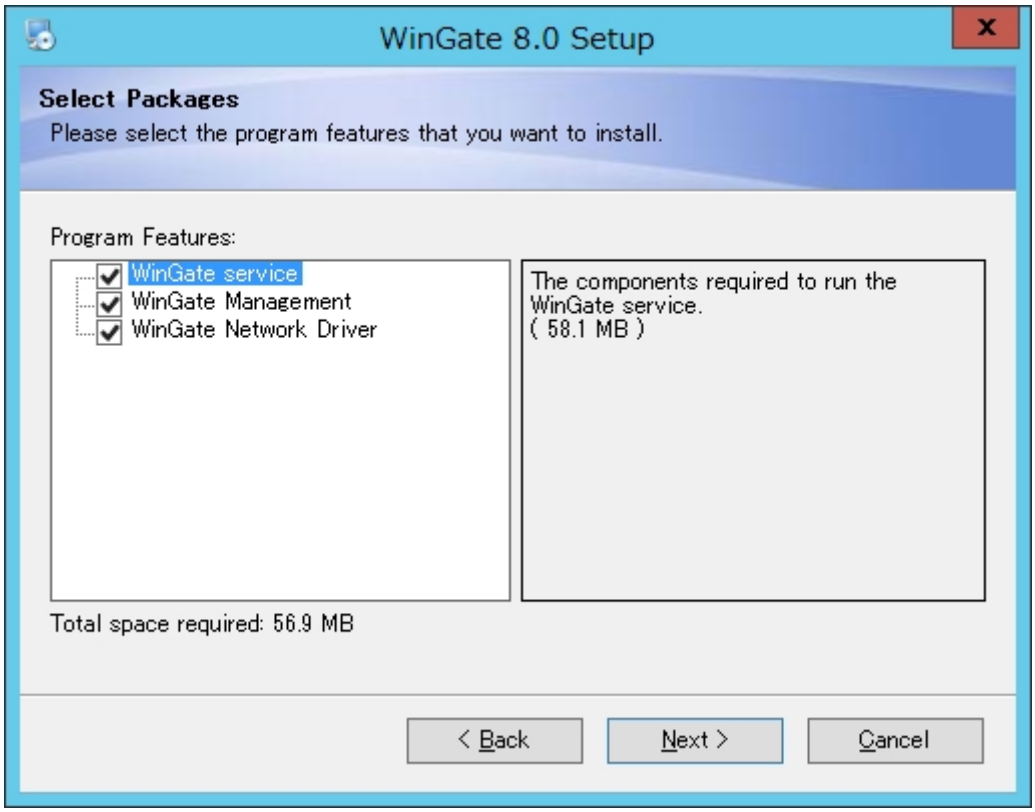



WinGate をインストールするフォルダーを選択します。インストールフォルダーは、51.0MB の空き容量が必要となります。（Space available on selected driver:）には、指定されたフォルダーの現在の空き容量が表示されております。

デフォルトでは C:¥Program files(x86)¥WinGate にインストールされます。変更する場合は「Change」ボタンをクリックして、フォルダーの参照ダイアログよりインストールディレクトリを指定してください。

設定が完了いたしましたら「Next」ボタンで次へ進みます。

7. Select Packages ダイアログが表示されます。

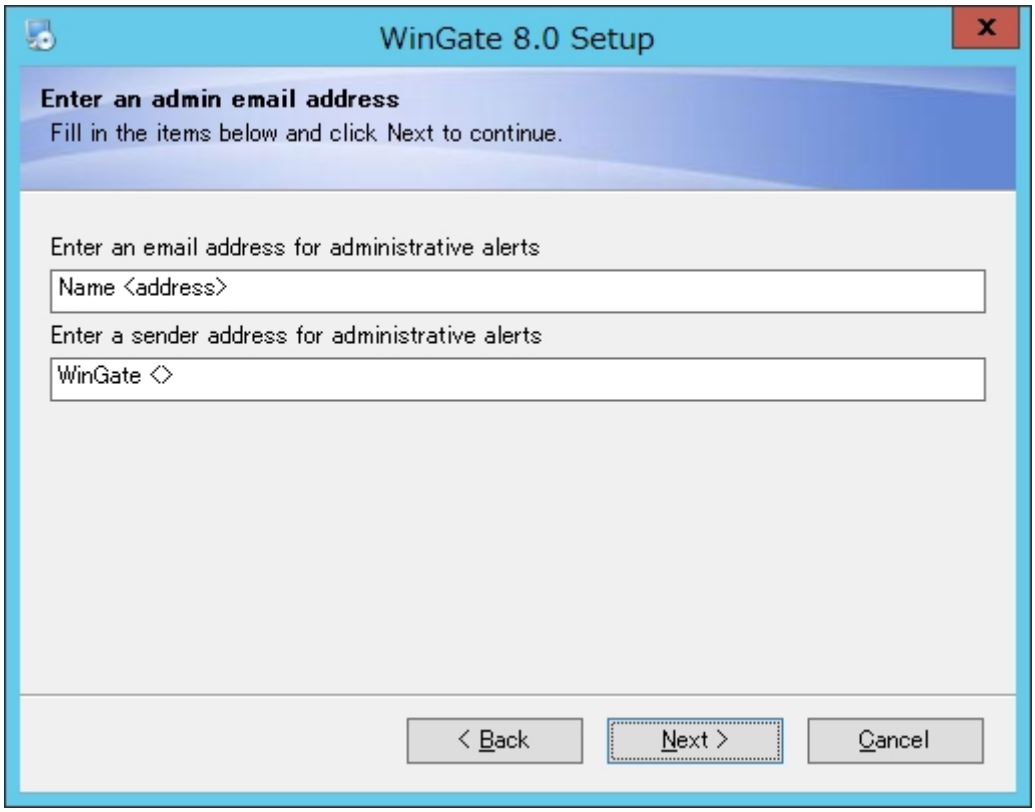



ここでは、インストールする WinGate のパッケージを選択します。
選択項目の内容は以下の通りです。
WinGate Service = WinGate の各サービスとなります。WinGate をプロキシサーバーなどとして使用する場合は、この項目が選択されている必要があります。
WinGate Management = WinGate の管理ツールである「WinGate Management」（WinGate マネージメント）をインストールします。
WinGate Network Driver = WinGate のファイアウォール、VPN、NAT 機能を使用する場合には、こちらを選択します。

**ご注意：**一般的な WinGate のインストールでは、WinGate Service、WinGate Management が選択される必要があります。
WinGate Network Driver は、WinGate へ Extended Network Driver をインストールします、ファイアウォール、VPN、NAT 機能を使用しない場合は、この項目を選択する必要はありません。（例プロキシサーバーとしてのみ WinGate を使用する場合など）

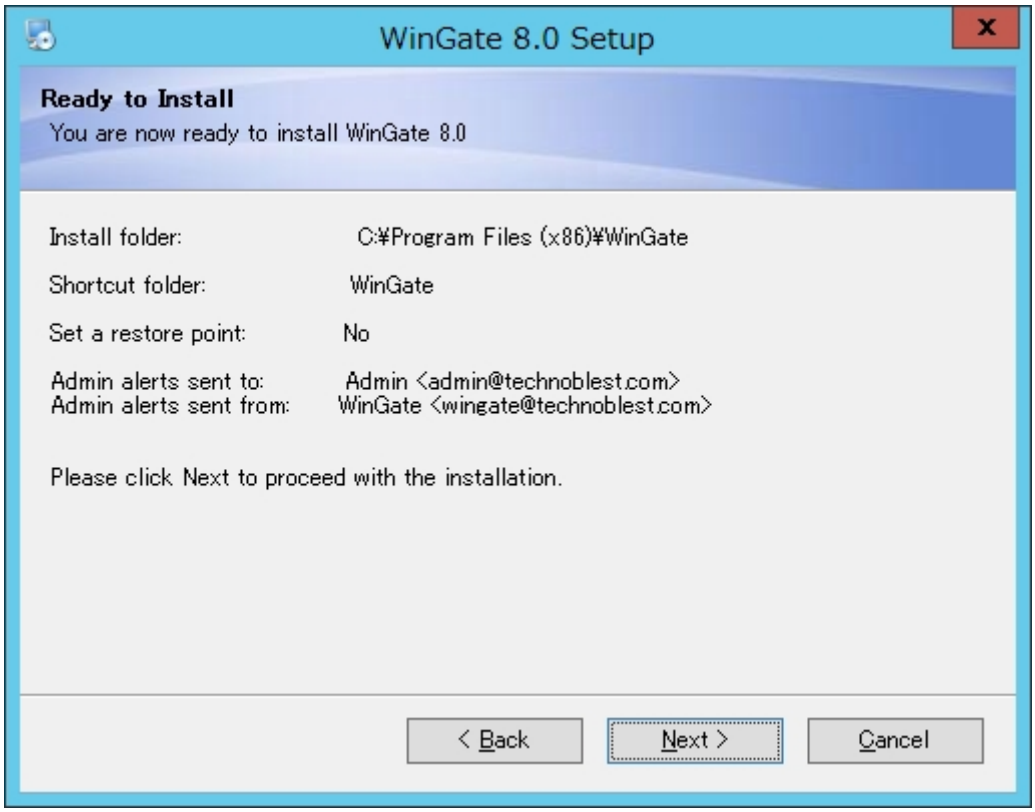
選択が完了いたしましたら「Next」ボタンで次へ進みます。

8. Enter an admin email address が表示されます。



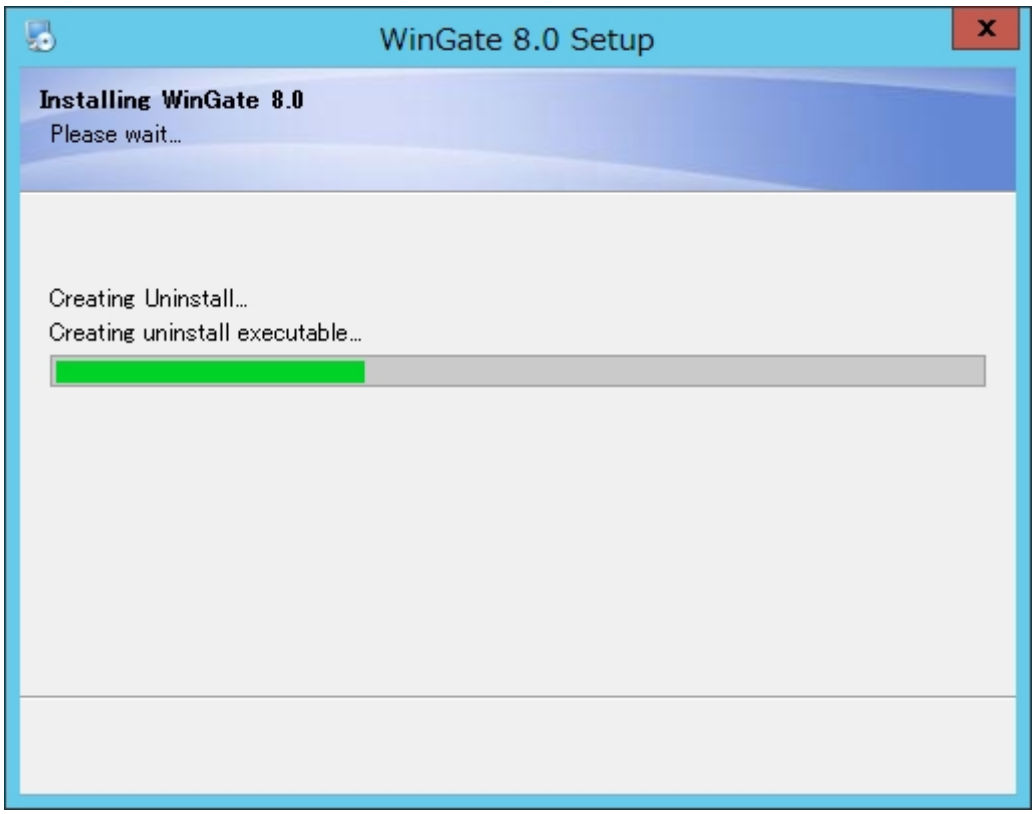

ここでは、WinGate インストール完了後に、警告などを配信する管理者の電子メールアドレスを入力してください。
（必須ではありませんが入力をいただかない場合、インストール完了後にポリシー設定で警告が表示されます。）
ここで設定した電子メールアドレスへ警告メールを配信するには、インストール完了後に配信設定を行う必要があります。
設定が完了いたしましたら「Next」で次へ進みます。

9. Ready to Install が表示されます。

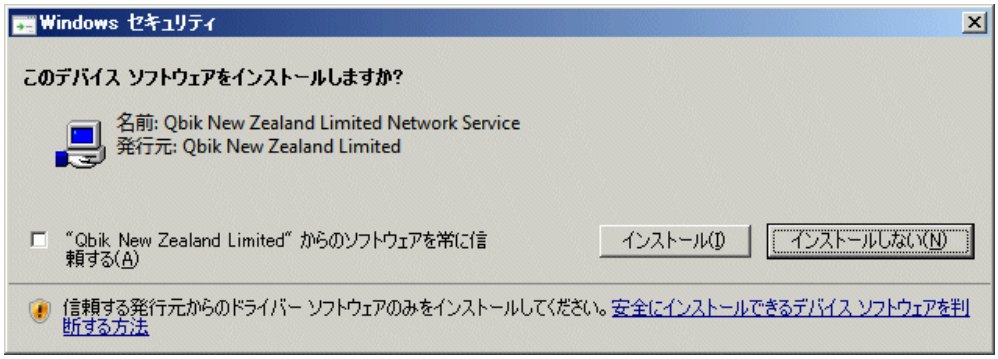


インストールの準備が完了いたしました。
これまでのダイアログで設定した内容が表示されますので、これらの内容に問題がない場合は、「Next」ボタンでインストールを開始します。内容を修正する場合は「Back」ボタンで必要な箇所まで戻り、設定を変更してください。

10. インストールが開始されます。

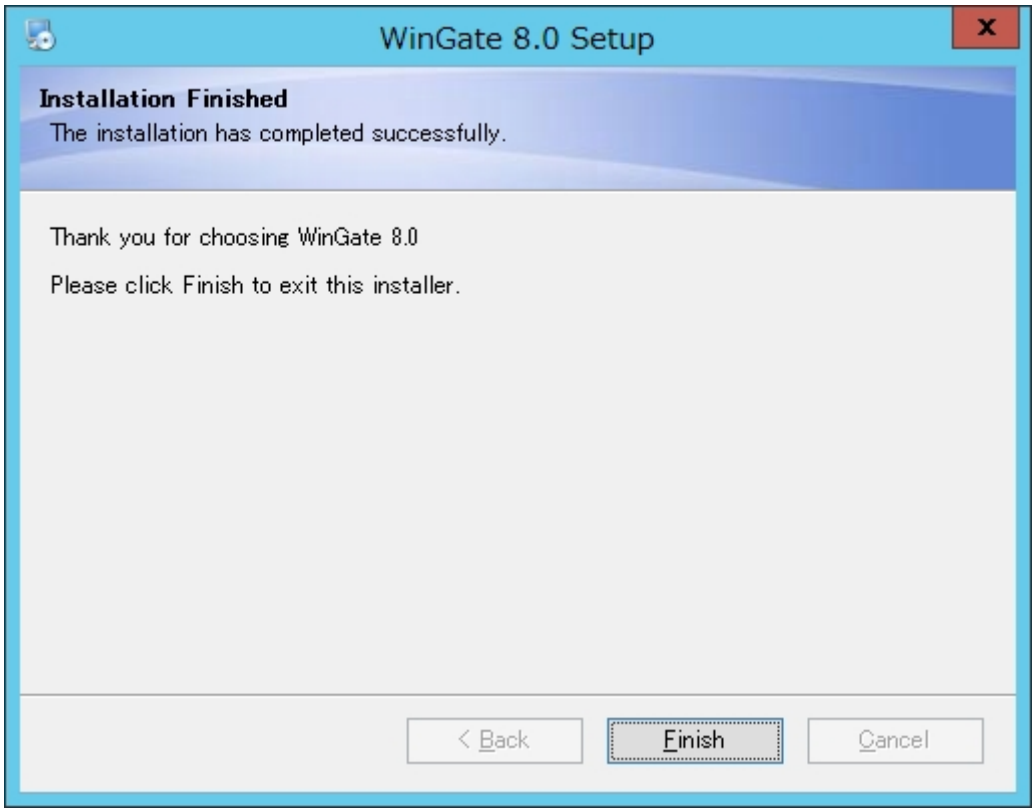



WinGate Network Driverを選択した場合、インストール途中にWindowsセキュリティダイアログが表示される場合があります。



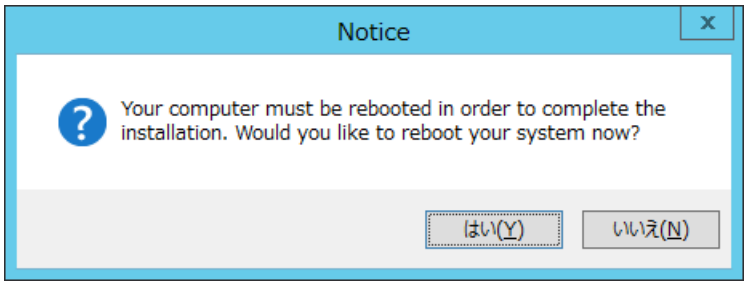

このダイアログが表示された場合、「インストール」「を選択して WinGate のインストールを継続してください。

11. Installation Finished が表示されます。




以上で WinGate のインストールは完了となります。Finish ボタンをクリックして、インストールを終了してください。

12. ダイアログが閉じられた後、WinGate Network Driver のインストールを選択している場合は PC の再起動を促す以下のダイアログが表示されます。




「はい」をクリックすると PC の再起動を行います。

WinGate Network Driver のインストールを選択していない場合、PC の再起動は必須ではありませんが、再起動いただく事をお勧めいたします。

以上でバージョンアップは完了となります。

再起動完了後に、WinGate マネージメントを開始して、以前の情報が引き継がれているかをご確認ください。また、継承されない機能については、新たに設定を行ってください。

**スタートアップメニューの重複について**

Windows のスタートアップメニューに、旧バージョンのスタートアップ項目が残る場合があります。スタートアップメニューが重複している場合、手動で WinGate エンジンモニタ（WinGate Engine Monitor）、および WinGate VPN を削除してください。

**インストール完了後の注意点、および確認事項**

上書きインストールを行った場合、以下の項目をご確認ください。

- WinGate8 は、WinGate6 で使用されていたユーザー・データーベースを継承します。WinGate Management へログインする際には、WinGate6 で使用していた、ユーザー・データーベースのログイン情報でログインしてください。
  また、ユーザー・データーベースで、ユーザーが正しく認識されているかをご確認ください。

- インストール完了後に初めて WinGate Management へログインすると、アクティベーション（Activation）を必要とする警告が表示される場合があります。
  これは WinGate8 で、新たにライセンスキー情報を認識しアクティベーションする必要があるためです。
  アクティベーション・ウィザードの指示に従い、現在お持ちのライセンスキー情報でアクティベーションを行ってください。
  2013 年 6 月 1 日時点で、アップグレード保証の有効期限内である場合は、現在のライセンスキー情報で、そのまま WinGate8 を利用いただくことができます。2013 年 6 月 1 日時点でアップグレード保証有効期限が切れている場合は、WinGate8 へアップグレードいただく事ができません。アップグレード保証の更新をご検討ください。
  ※アクティベーション完了後、WinGate の再起動が必要となります。

- 各サービスの設定が引き継がれているかをご確認ください。
  継承できない機能以外は、上書きインストールにより継承されているかをご確認ください。
  また、WinGate8 では、WinGate6 では削除できなかった一部のサービスを削除することができます。
  使用する必要がないサービスについては、WinGate Management の Services より、不要なサービス上で右クリックを行い Remove（削除）より削除してください。
  **ご注意：SMTP Proxy Server は、上書きインストールにより継承されているように表示されますが、マッピング先などの設定を持つ事ができず、設定は継承されておりません。**
  **SMTP Proxy Server をご利用いただいておりました場合は、SMTP Proxy Server を一旦削除し、新たに TCP Mapping Service を作成して、設定を行ってください。**

- ログの保存ディレクトリ、およびログ保存期間
  上書きインストールを行った場合、デフォルトのログ保存ディレクトリは C:¥Program Files¥WinGate¥（64bit OS では、C:¥Program Files(x86)¥WinGate¥ ）となります。
  以前のログ情報は C:¥Program Files¥WinGate¥Logs フォルダーに残されますが、ログの互換性がないため、新たにログ保存nディレクトリを指定してください。
  ログ保存ディレクトリの設定は WinGate Management の Navigation、Logging の Settings、Logs base path より設定することができます。
  新たなディレクトリを作成いただき、ログ保存ディレクトリとしていただくか、以前のログフォルダを移動する方法などが考えられます。（ログ保存ディレクトリを変更しても、以前のログ情報は移動されません。）
  デフォルトでは、60 日間に設定されており、60 日前のログは自動的に削除されます。

その他の確認事項に関しては、本書のインストール後の確認の章をご覧ください。

**その他の旧バージョン（WinGate2.x、WinGate3.x、WinGate4.ｘ）からのバージョンアップについて**

WinGate6.x 以前のバージョンをご使用いただいております場合、上書きインストールを行っても、設定情報を引き継いだバージョンアップ、または正しいバージョンアップを行っていただく事ができません。

**弊社ではこれらのバージョンからアップグレードいただく場合には、新規インストール、新規設定をお願いしております。**

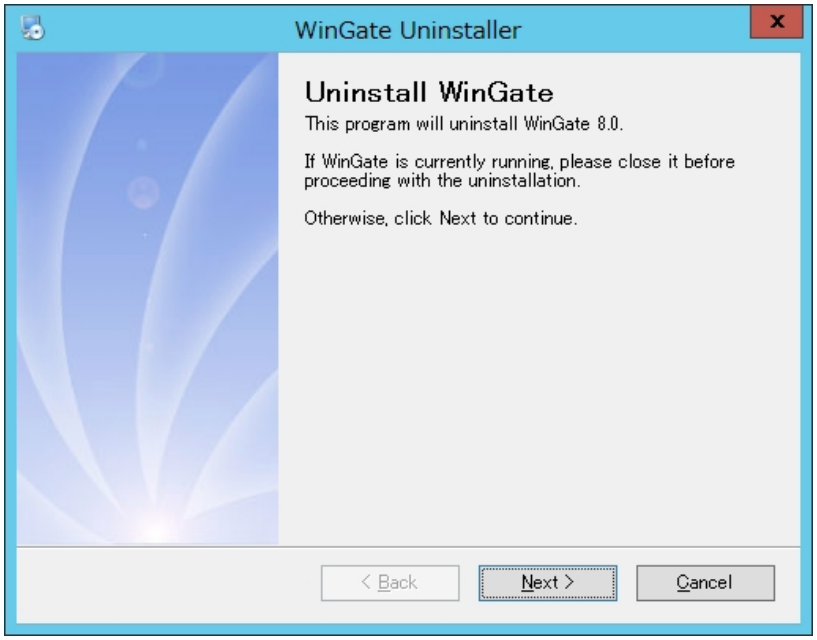
**WinGate のアンインストール**

WinGate のアンインストールは、Windows のスタートメニュー、WinGate、Uninstall WinGate（WinGate のアンインストール）を実行、または Windows コントロール・パネルより行うことができます。

**ご注意：WinGate のアンインストールを行うことにより、WinGate の全ての設定情報、ログ情報などが失われます。WinGate に関する情報が必要となります場合は、必要に応じて事前にバックアップを行ってください。**

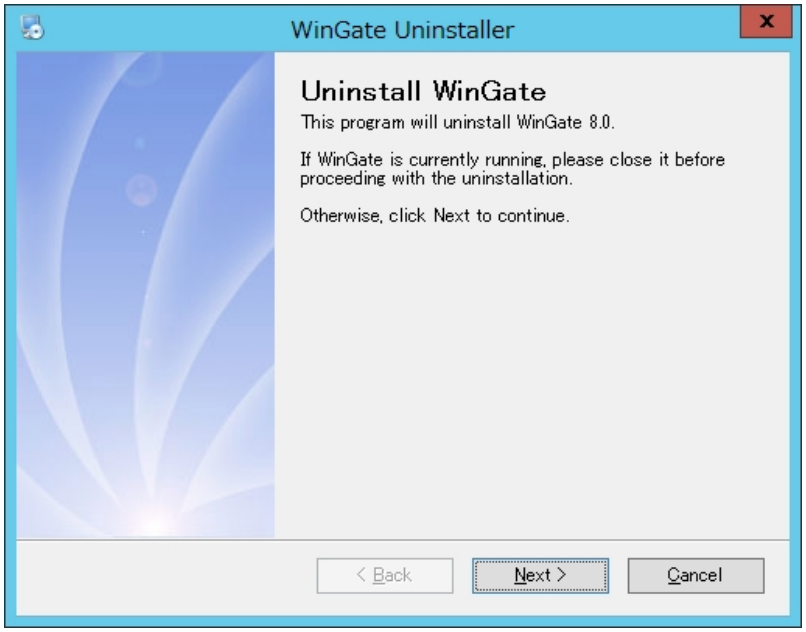
アンインストールを行う場合は、WinGate エンジンは開始されている状態でも問題はありませんが、GateKeeper は閉じていただく事をお勧めいたします。アンインストールは以下の手順で実行されます。

1. Uninstall WinGate e（WinGate のアンインストール）ダイアログが表示されます。



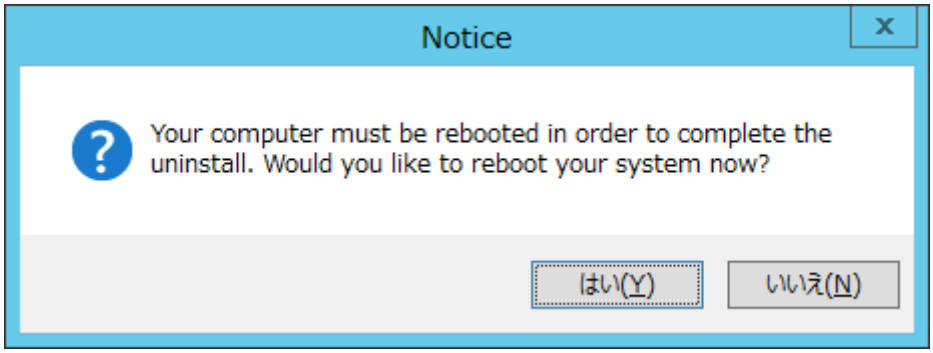

「Next」クリックして次へ進みます。

2. アンインストール開始が開始され、終了すると「Uninstall successful」ダイアログが表示されます。




「Finish」ボタンをクリックして、インストールを完了します。

3. アンインストールが完了すると再起動を促すダイアログが表示されます。




「はい」をクリックして、PC の再起動を行ってください。

以上で WinGate のアンインストールは完了となります。

### インストール完了後に行う内容（新規インストール）

WinGate の新規インストール完了後には、WinGate の使用を開始するために幾つかの設定を行う必要があります。

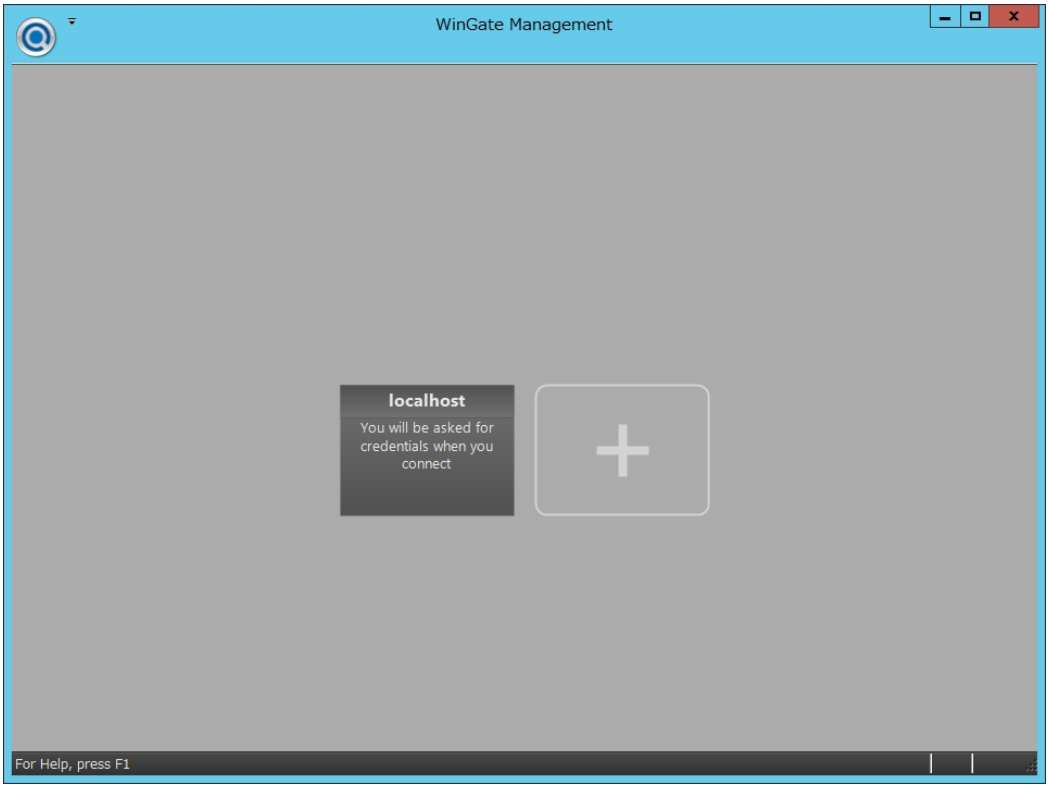
- ライセンスアクティベーション（**WinGate の再起動が必要**）
  WinGate をご利用いただくには、ライセンスのアクティベーションを実施いただく必要があります。アクティベーションが完了するまで WinGate をご利用いただくことはできません。
  アクティベーションは、インターネット経由、または他のインターネット接続可能なマシンからのオフラインアクティベーションをサポートします。詳細な方法に関しましては、本書のアクティベーションの章をご覧ください。

- ユーザー・データーベースの選択（**WinGate の再起動が必要**）
  WinGate は、WinGate で使用するユーザー・データーベースに WinGate ユーザー・データーベース、Windows ユーザー・データーベース、Active Directory ユーザー・データーベースを選択いただく事ができます。（これらの 3 種類を併用することはできません。）
  ご利用の目的に合わせてユーザー・データーベースを選択してください。
  WinGate ユーザー・データーベースは、WinGate 独自のユーザー・データーベースとなり、WinGate マネージメントでユーザーの追加、削除などの管理を行うことができます。
  Windows、Active Directory ユーザー・データーベースでは、ユーザーの管理はそれぞれのユーザー・データーベースに依存いたします。また、これらのユーザー・データーベースを使用した場合には、WinGate マネージメントへのログインにも。これらのユーザー・データーベースの管理者アカウントを使用いたします。
  Active Directory ユーザー・データーベースを使用する場合、WinGate マシンは Active Directory のメンバーである必要があります。

### ライセンスアクティベーション

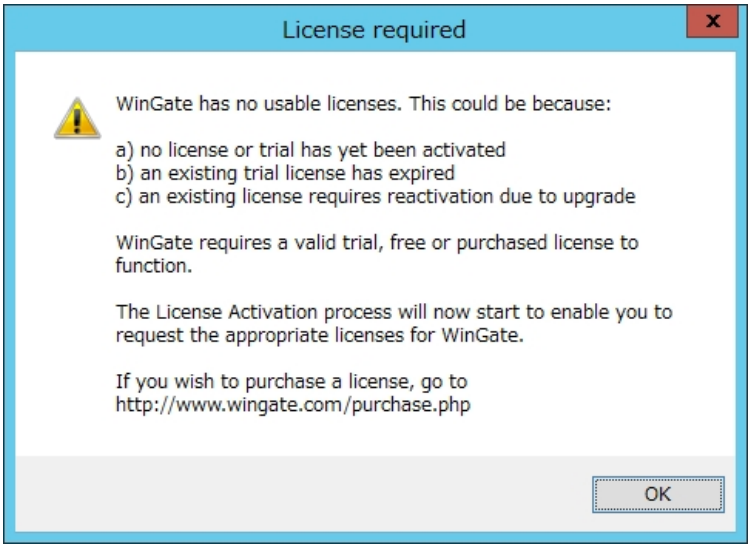
WinGate をご利用いただくには、ライセンスキー情報の入力とアクティベーションが必要となります。
試用版をご利用いただく場合にも、試用版としてのアクティベーションが必要となります。
初回起動時のログイン、およびアクティベーション手順は以下の通りとなります。

1. 新規インストール後に WinGate 起動した場合、管理ツールである「WinGate Management」を起動すると、WinGate Management ダイアログが開きます。




ログインを行うため、WinGate Management 内に表示されている Localhost をクリックします。

2. License required ダイアログが表示されます。

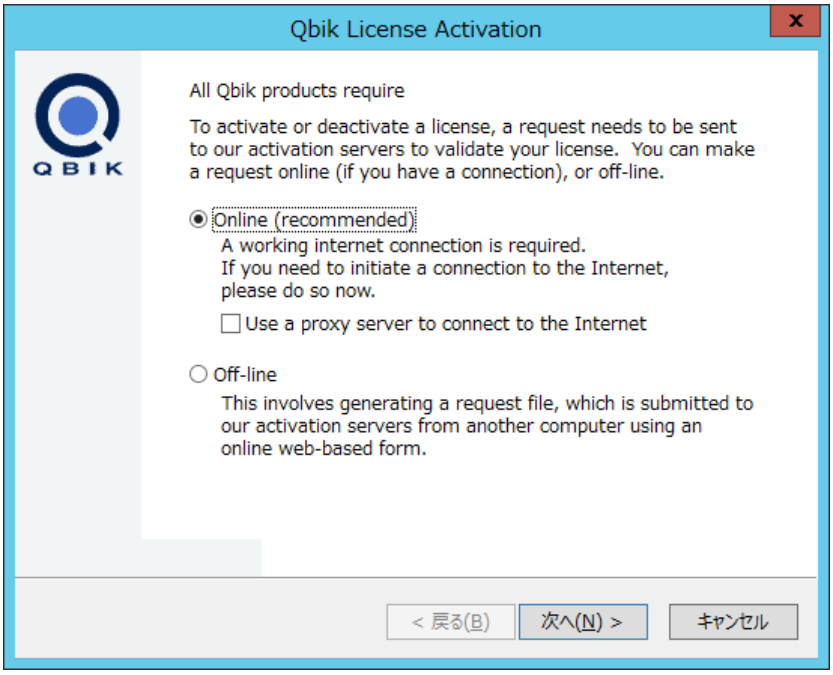



このダイアログは、以下の場合に表示されます。

- 新規インストールなどで正規版・試用版ライセンスがアクティベートされていない場合
- 試用版の試用期間が終了した場合
- アップグレード保護の期間が終了しアップグレード保護の更新が必要な場合

OK ボタンをクリックします。

3. Qbik License Activation ダイアログが表示されます。




アクティベーションは、インターネット経由（推奨）、および電子メールによるオフラインアクティベーションが可能となります。

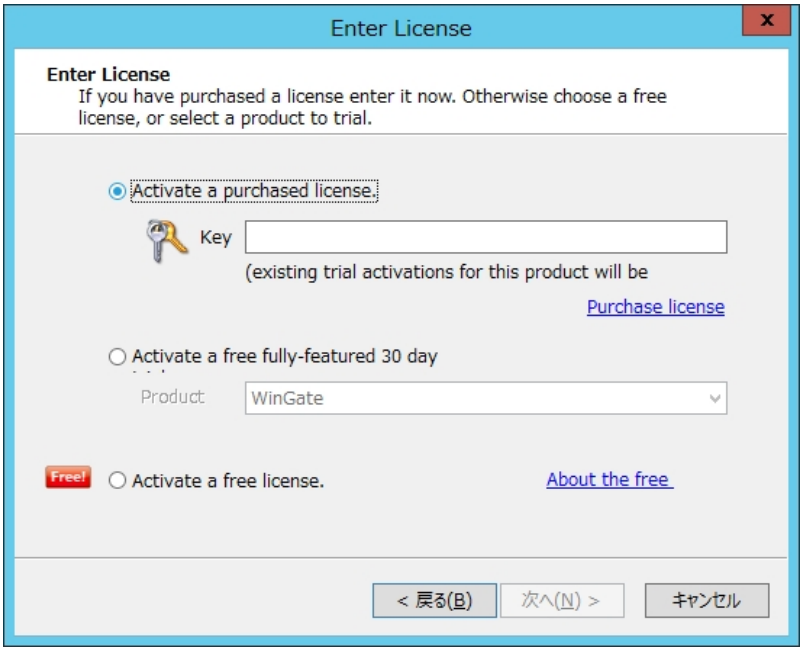
WinGate PC がインターネット接続環境を持つ場合には、Online（オンライン）を選択して、インターネット経由でのアクティベーションを実行してください。**（推奨）**

WinGate PC がインターネット接続環境を持たない場合は、Off-line（オフライン）を選択して、電子メールによるアクティベーションを行ってください。

アクティベーション方法を選択して「次へ」をクリックします。

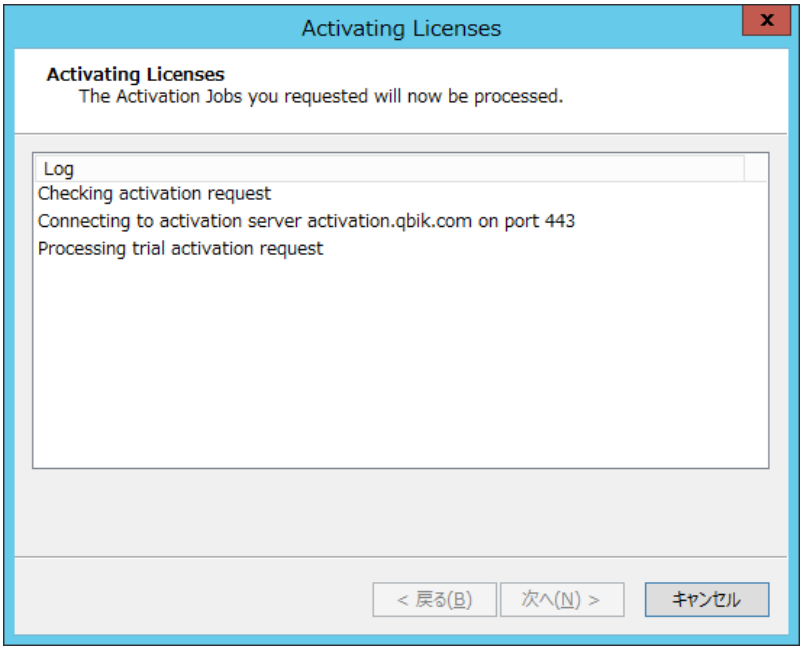
4. **オンラインアクティベーション**

Online を選択し「次へ」ボタンをクリックすると以下のダイアログが表示されます。

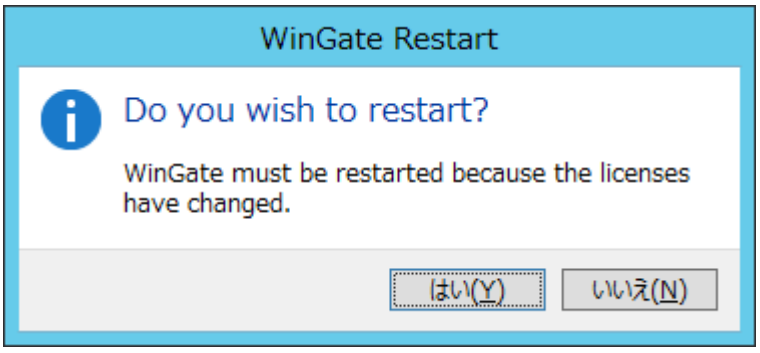



既にライセンスキー情報をお持ちの場合は、Activate a purchased license を選択し Key 欄にライセンスキー情報を入力して「次へ」ボタンをクリックしてください。

試用版をご利用いただく場合は、Activate a free 30 day trial を選択し Product ドロップダウン・メニューで試用版として利用する製品を選択し「次へ」ボタンをクリックしてください。



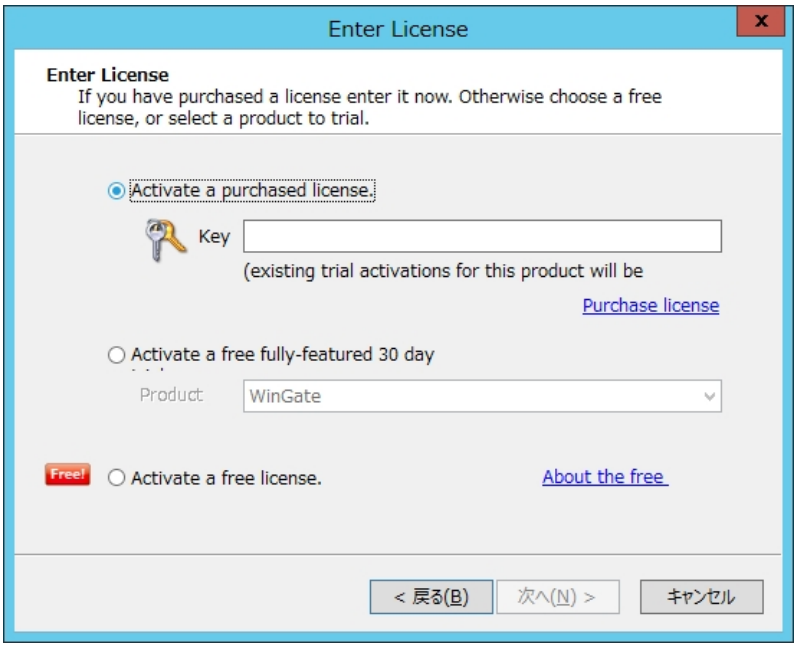

アクティベーションが開始され、完了すると「succeed」（成功しました）と表示されますので完了ボタンをクリックしてください。
以上でオンラインアクティベーションは完了となります。




ライセンスを有効にするために WinGate を再起動する必要があります。ダイアログの指示に従い WinGate の再起動を行ってください。

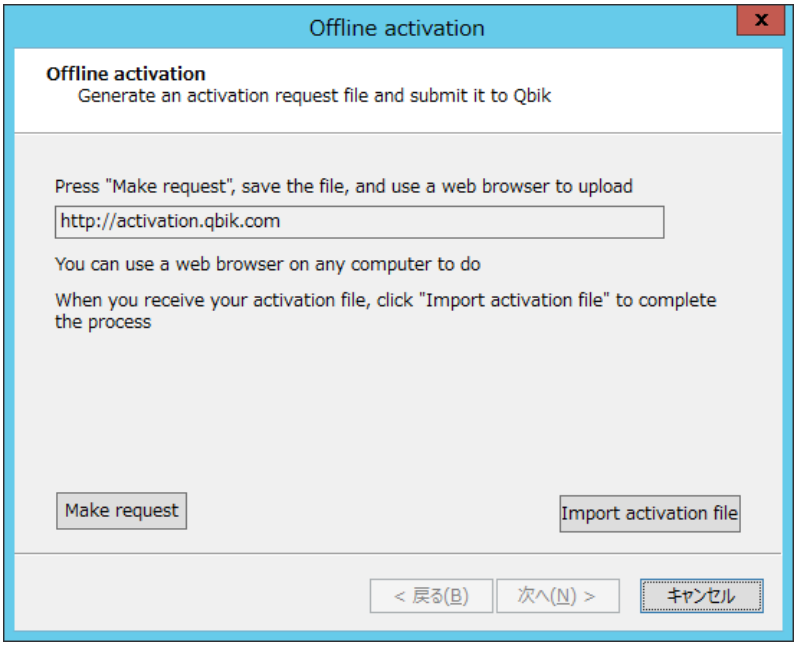
1. **オフラインアクティベーション**

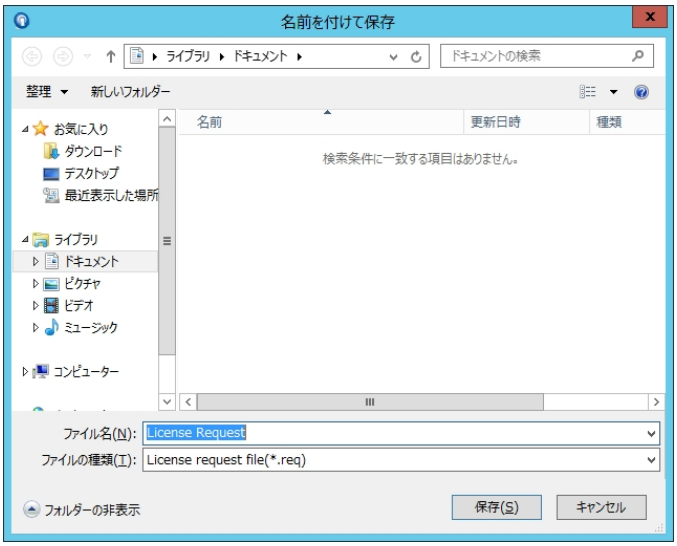
Off-line を選択し「次へ」ボタンをクリックすると以下のダイアログが表示されます。




既にライセンスキー情報をお持ちの場合は、Activate a purchased license を選択し Key 欄にライセンスキー情報を入力して「次へ」ボタンをクリックしてください。

試用版をご利用いただく場合は、Activate a free 30 day trial を選択し Product ドロップダウン・メニューで試用版として利用する製品を選択し「次へ」ボタンをクリックしてください。






名前を付けて保存ダイアログが表示されますので、任意の場所へファイルを保存してください。

インターネットアクセスが可能なマシンに保存したファイルを保存し、ブラウザで http://activation.qbik.com/ へアクセスします。

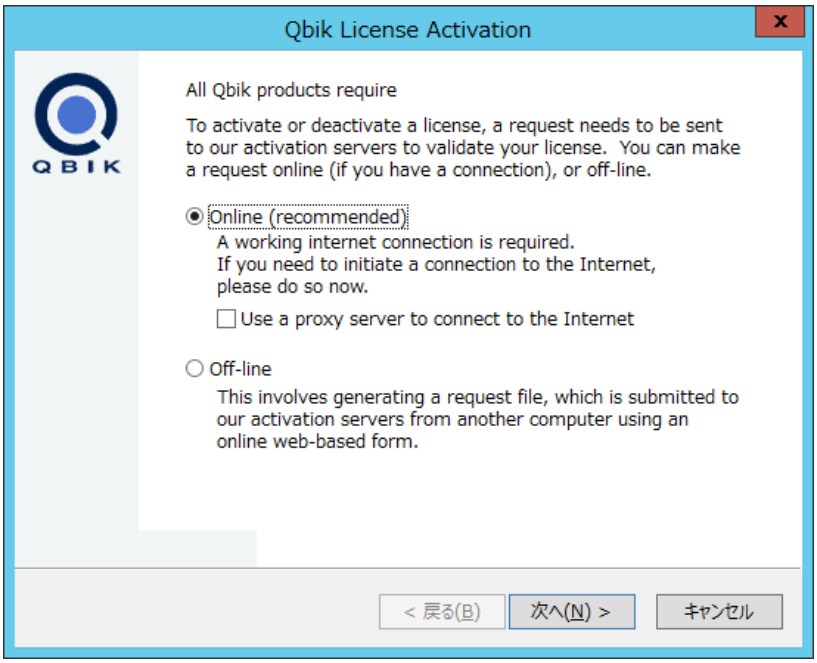
WinGate 開発元である Qbik New Zealand 社の Offline activation ページが表示されますので、「Choose file:」で参照ボタンをクリックして先程保存したファイルを指定してください。

指定が完了いたしましたら「Upload」ボタンをクリックしてください。

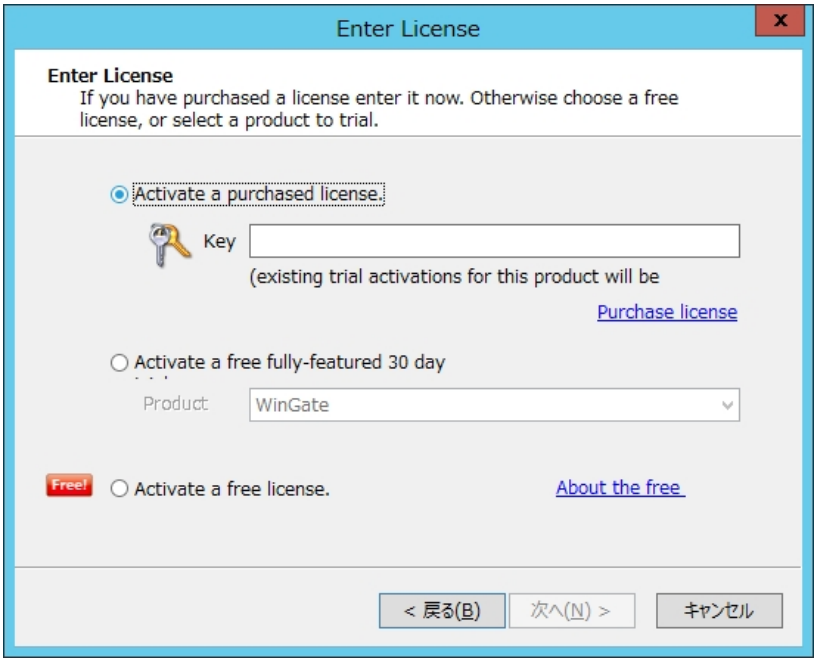
暫くするとブラウザでファイルの保存を促す表示がされますので、ファイルを任意の場所に保存してください。

保存したファイルを WinGate PC で読み込み可能なようにします。

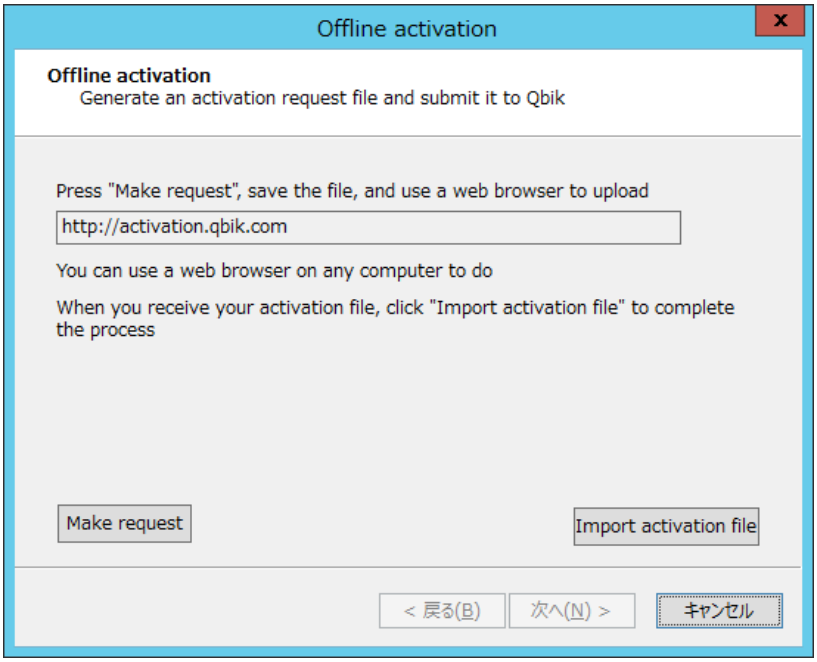
WinGate Management を開始するとアクティベーションを行うためのダイアログが表示されます。




Off-line を選択し「次へ」ボタンをクリックします。




キー情報の入力、または試用版の選択を行い、「次へ」ボタンをクリックします。

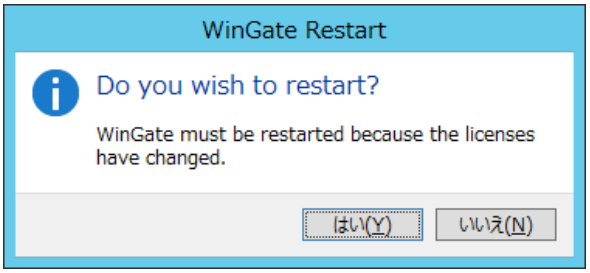



Import activation file（アクティベーションファイルのインポート）を選択し、ダウンロードしたファイルを指定します。

インポートが完了いたしましたら「完了」ボタンをクリックします。

以上でオフラインアクティベーションは完了となります。

ライセンスを有効にするために WinGate を再起動する必要があります。ダイアログの指示に従い WinGate の再起動を行ってください。



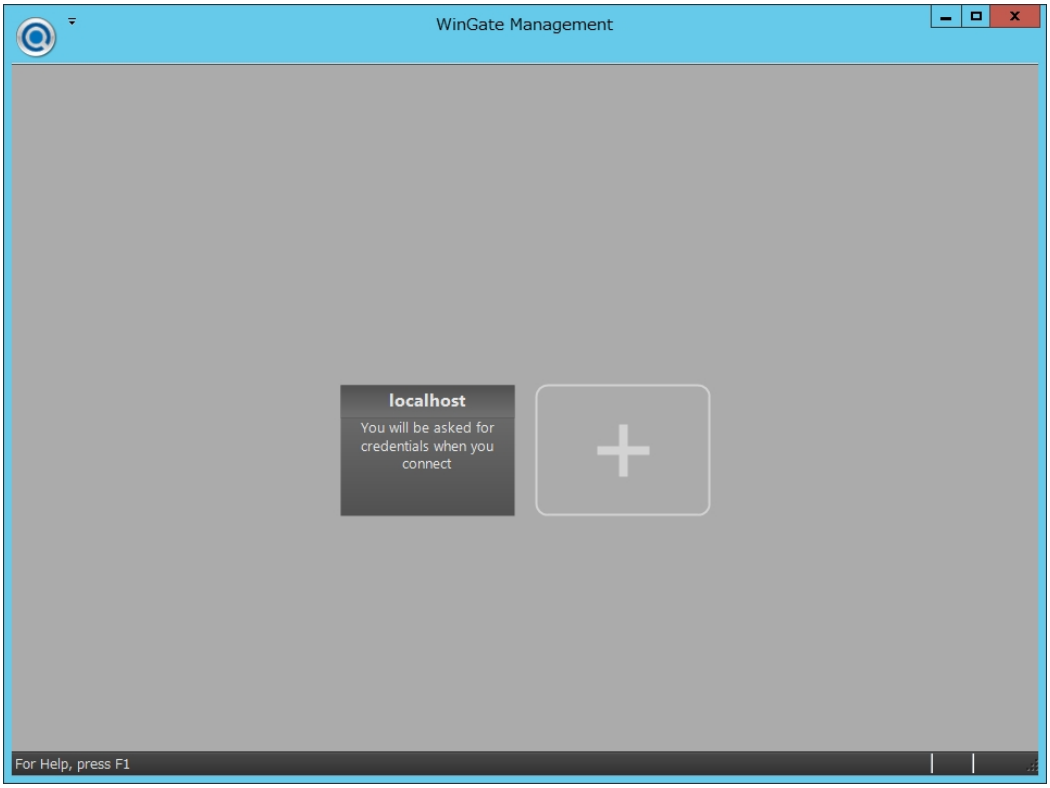
**WinGate Management へのログイン**

WinGate の構成を行うためには、WinGate の管理ツールである「WinGate Management」（WinGate マネージメント）を使用して、WinGate エンジンに接続する必要があります。

タスクトレイに表示されている WinGate エンジンモニタ、または Windows のスタートアップメニュー、WinGate より「WinGate Management」（WinGate マネージメント）を選択して WinGate Management を開始してください。

WinGate エンジンに接続するにはユーザー名とパスワードが必要となります。

WinGate Management を開始すると中央にログイン先へのリンクが表示されます。（図 1）

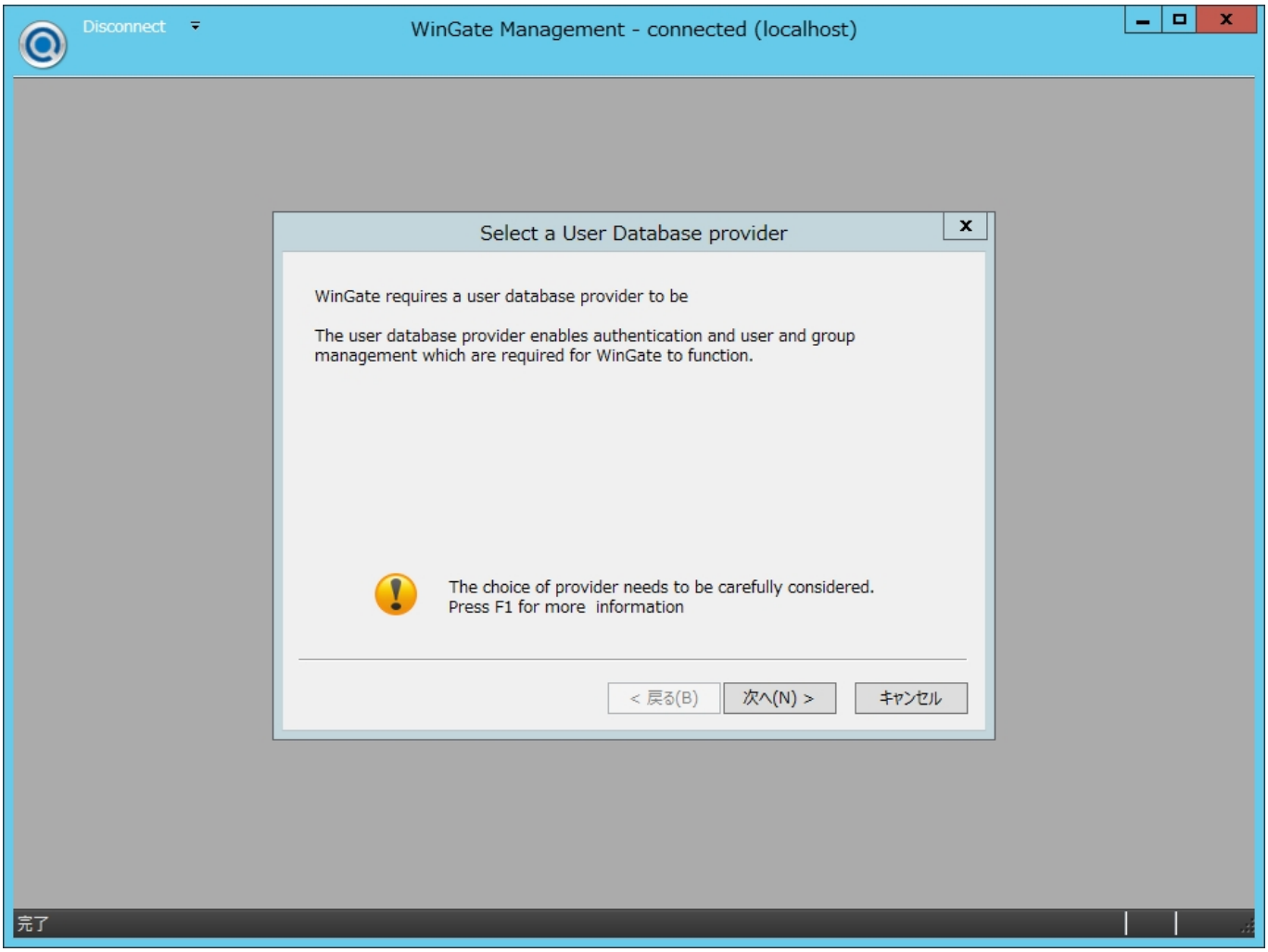



（図 1）WinGate Management 開始時の画面

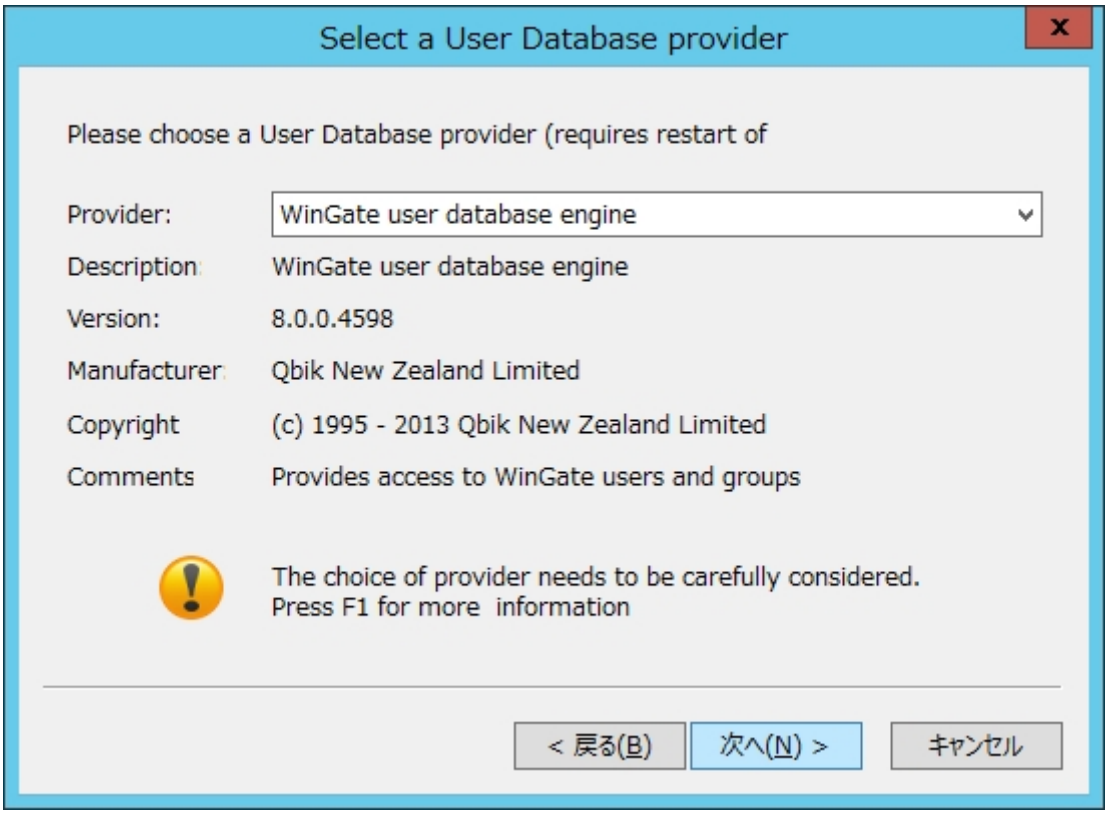
デフォルトでは「Localhost」が追加、このままの状態で、Localhost をクリックします。

WinGate Management は、WinGate の Remote Control Service を使用して WinGate エンジンへ接続します。このサービスは初期状態で「127.0.0.1」（localhost）にバインドされています。（これはこのアドレスがマシンの外部からは見えないアドレスであり、セキュリティ面を考慮してあるためです。）

初めて WinGate をインストールした直後に WinGate Management で接続を行うと「Select a User Database Provider」（ユーザー・データベース・プロバイダーの選択）ダイアログが表示されます。（旧バージョンからアップグレードを行った場合は、旧バージョンのユーザー・データーベースを引き継いでいますので、Select a User Database Provider ダイアログは表示されません。）




「次へ」ボタンをクリックします。




このダイアログでは、WinGate で使用するユーザー・データーベースの種類を選択します。

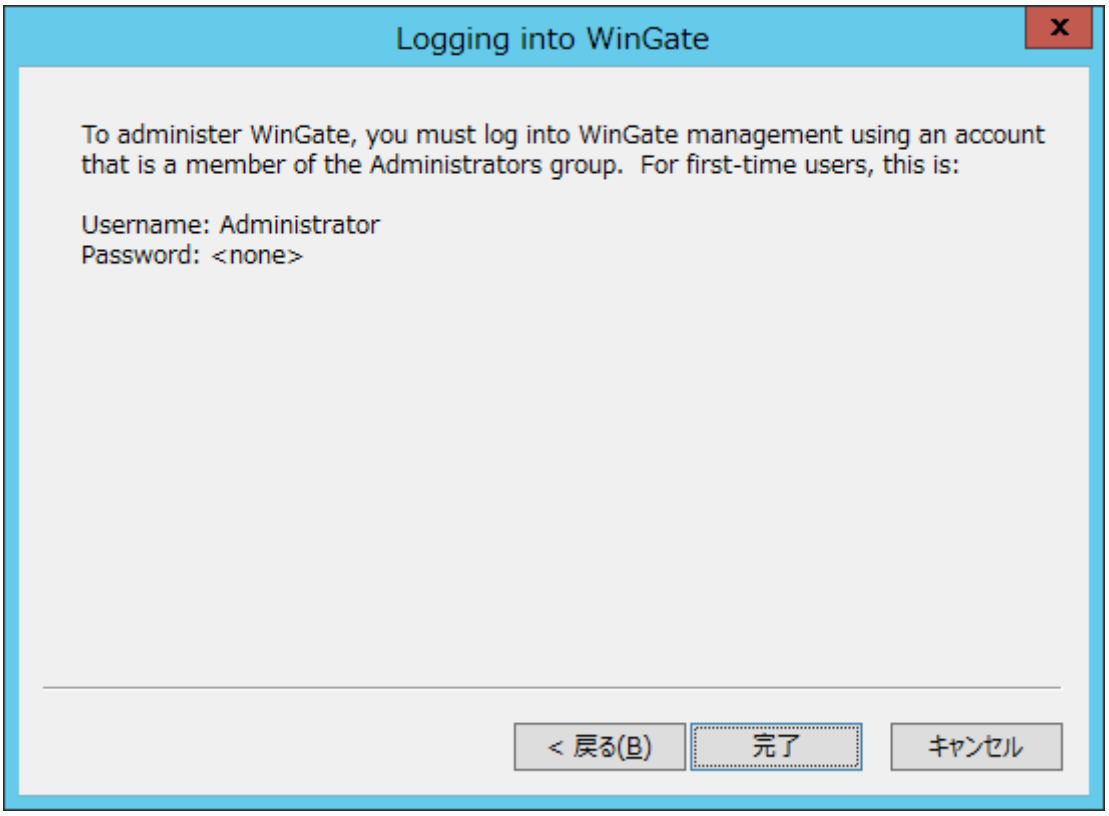
選択できるユーザー・データーベースは、以下の 3 種類です。

1. Active Directly Connector（アクティブ・ディレクトリ・コネクタ）
   このオプションを選択した場合、WinGate は Active Directly ユーザー・データーベースを使用します。
   ご注意：Active Directly Connector を使用する場合、WinGate　PC は、Active Directly のメンバーである必要があります。
   Active Directly Connector　を使用するには WinGate Professional、または WinGate Enterprise ライセンスが必要となります。

2. Windows Users and Groups Connector（Windows ユーザーとグループコネクタ）
   このオプションを選択した場合、WinGate は WinGate がインストールされている PC の Windows ユーザー・データーベースを使用します。（※Windows Home を使用している場合は、この選択を使用しないでください。編集するまでローカルユーザーとグループは利用することができません。）

3. WinGate users database engine（WinGate ユーザーデータベース・エンジン）
   このオプションを選択した場合、WinGate は WinGate 独自のユーザー・データーベースを使用します。

選択が完了いたしましたら「次へ」ボタンをクリックします。
Active Directly Connector を選択した場合




WinGate を管理するためには WinGate　Management へドメイン管理者グループメンバーのアカウントでログインする必要があることを示すメッセージが表示されます。

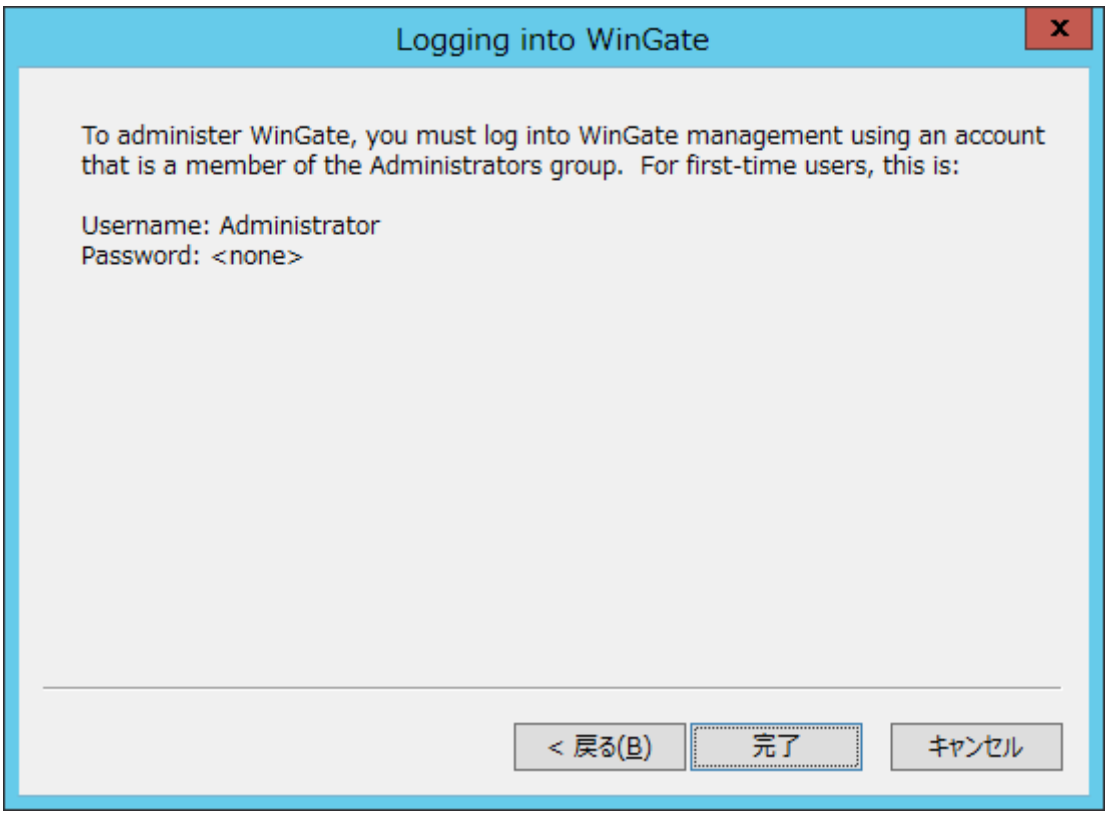
Windows Users and Groups Connector を選択した場合
WinGate を管理するためには WinGate　Management へローカル管理者グループのアカウントでログインする必要

があることを示すメッセージが表示されます。

WinGate users database engine を選択した場合

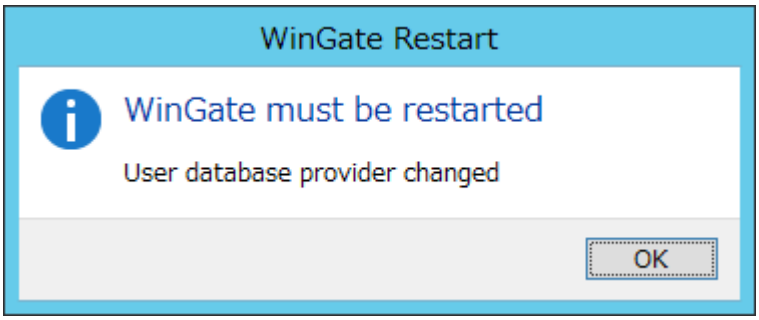
WinGate Management へログインするためには、WinGate ユーザーデータベーの管理者グループのアカウントでログインする必要があることを示すダイアログが表示されます。

ユーザー・データーベースでアカウントが設定されていない、初回のログインでは Username（ユーザー名）: Administrator、Password（パスワード）:（空白）でログインします。



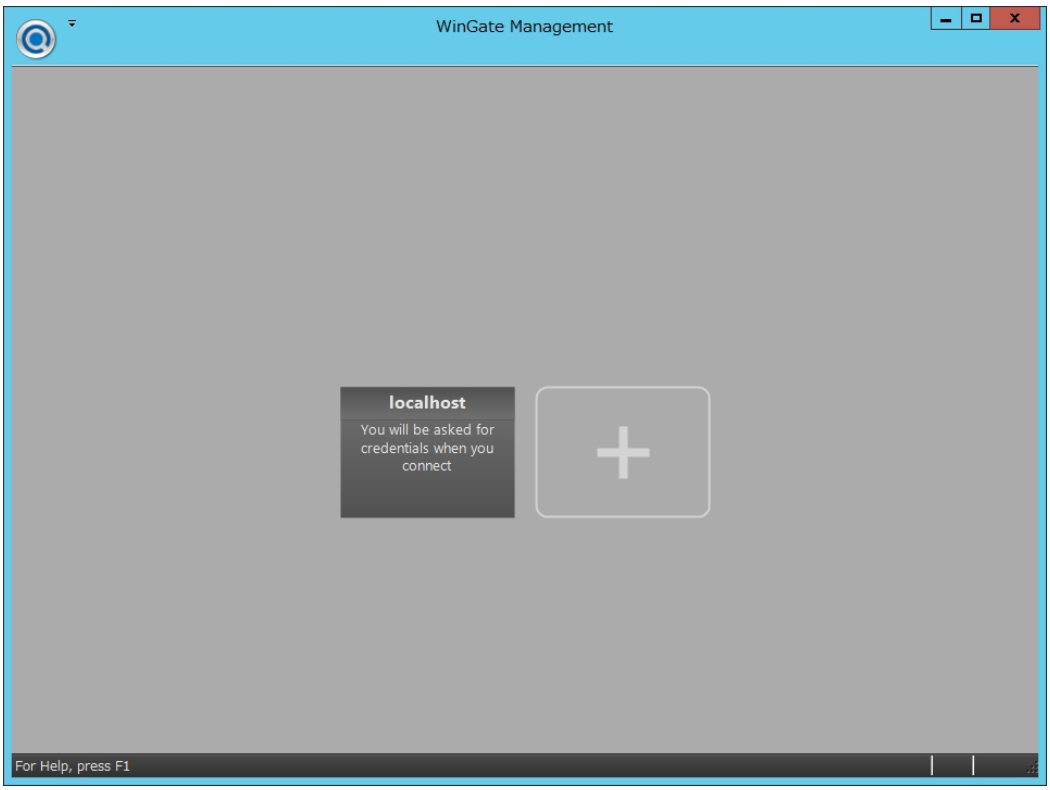
何れの選択の場合でも完了ボタンをクリックして、ユーザー・データーベースの選択を終了してください。

ユーザー・データーベースの選択が完了すると WinGate は、新しいユーザー・データーベースを認識するために再起動する必要があります。




ダイアログの指示に従い WinGate の再起動を行ってください。

WinGate の再起動完了後に WinGate Management を開始すると以下の画面となります。




画面中央の Localhost をクリックし

WinGate Security ダイアログが表示されます。

Windows Users and Groups Connector、Active Directly Connector を選択した場合で、Windows で使用している現在のユーザーアカウントが管理者権限を持つアカウント、または Administrator アカウントである場合は、Log on as current Windows user を選択して、現在の Windows ユーザーアカウントでログインしてください。

WinGate users database engine や Log on as current Windows user で表示されているアカウント以外を使用する場合は、Use another account をクリックして、ログインに使用するアカウントを、入力してログインしてください。

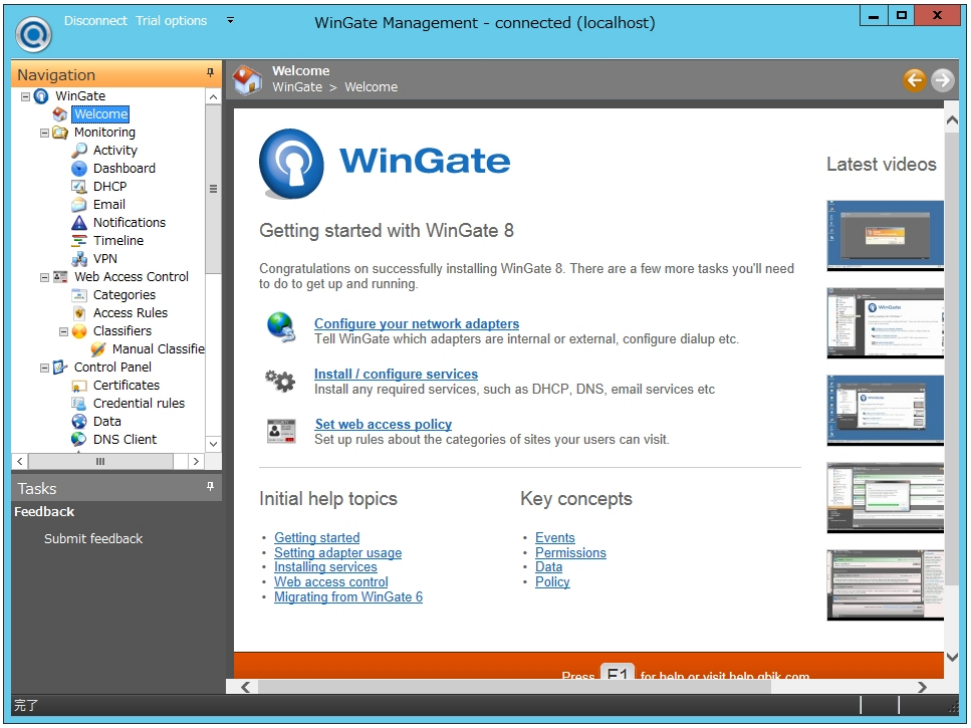
Save changes to profile を選択すると、入力したログインプロファイルが保存されます。

WinGate users database engine を指定した場合、初回のログインは Administrator、パスワードは空白でログインできます。
ログインが完了すると WinGate Management が表示されます。

**WinGate users database engine を指定した場合、の Administrator パスワードの設定方法**

WinGate Management ログイン後に、Navigation より Users and groups を選択します。中央に表示されますユーザーとグループの一覧から Administrator を選択し、右クリックで選択できるメニューから Set Password を選択します。表示されるダイアログで、New password、Confirm 欄に設定するパスワード入力して OK ボタンで終了します。

次回、ログイン時より設定したパスワードがログインに必要となります。




ログイン直後の WinGate Management 画面

以上で WinGate Management への初回ログインは完了となります。

この後は WinGate Management を使用して、お客様の環境に合わせた WinGate の構成を行ってください。

### インストール完了後に確認する内容（新規インストール）

新規インストールを行い、アクティベーション、ユーザー・データーベースの選択を行うと、WinGate を使用する準備が整いました。WinGate マネージメントへログインし、使用するために必要な設定を行ってください。

WinGate の使用を開始するにあたり、最小限以下の内容を確認してください。

#### 必要となるサービス、サーバー機能の追加

WinGate は、新規インストールで以下の、サービス、サーバーを持ちます。

| 名前 | 使用内容 | 削除の可否 |
|---|---|---|
| Performance counters | WinGate の Performance counters で WinGate 内の情報を収集されるために使用されます。<br>通常、このサービスを停止する必要はありません。 | 不可 |
| Remote Control Service | WinGate Management から WinGate エンジンに通信するために使用されます。<br>**ご注意：このサービスを停止した場合、WinGate エンジンと WinGate Management の通信が行えなくなり、WinGate Management でログインできなくなります。**<br>**必要となります場合以外は、停止やポートの変更を実施しないでください。** | 不可 |
| SMTP delivery Service | メール配信を行う場合に、WinGate が内部的に使用するサービスとなります。SMTP Server や SMTP Proxy とは異なります。 | 不可 |
| Scheduler | WinGate のスケジューラー・サービスとなります。停止した場合、WinGate の Scheduled Event で設定された内容は全て実行されません。 | 不可 |
| WWW Proxy Server | WWW Proxy（HTTP Proxy）サーバー機能となります。 | 可 |
| Web Admin service | ブラウザベースで WinGate の管理を行う場合に使用されるサービスとなります。現在は、アカウントのメールボックス設定やユーザー/グループ管理の一部のみが利用できます。 | 不可 |

ご利用をいただく機能に応じて、POP3 Proxy や DNS、DHCP サービスなどの追加を行ってください。

#### ネットワーク接続の確認（重要）

WinGate は、各サービス、プロキシサーバーのバインド設定で利用されるダイナミックなバインドをサポートします。

ダイナミックなバインドは、WinGate が利用可能なインターフェースを自動的に検出して、内部（Internal）か外部（External Interface）のどちらかであるか判断し、分類（IP アドレスの詳細に基づきます）します。

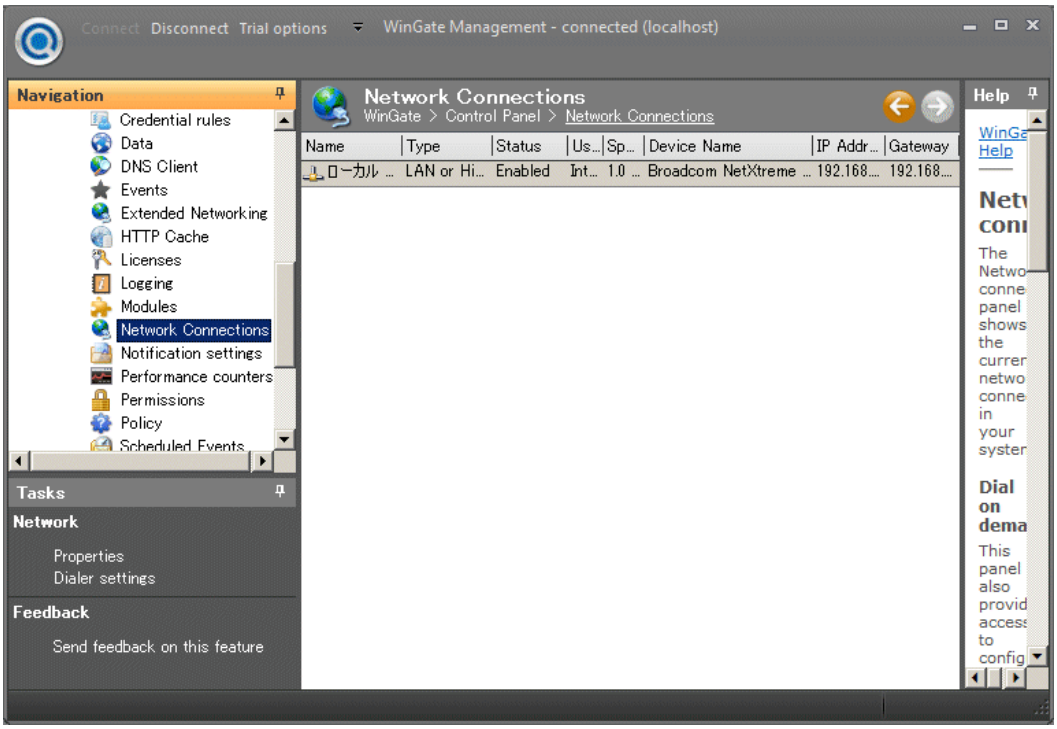
各サービス、サーバーのバインド構成は、デフォルト設定では、基本的にこの判断に基づき構成されます。

各サービス、プロキシのバインド構成は、デフォルトでは任意の内部アダプタとループバックアドレスにバインドさ

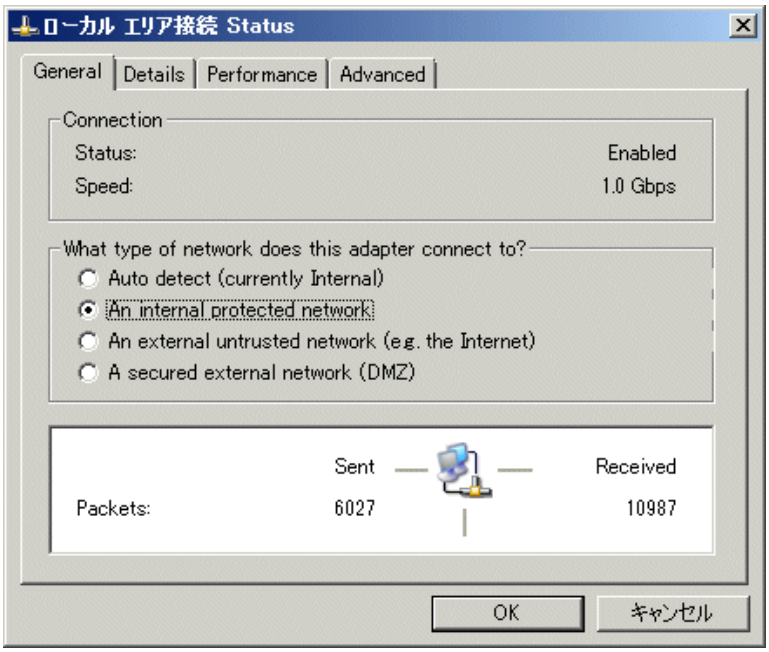
れる設定となります。
これはネットワーク接続で内部として認識・設定されているアダプタの IP アドレスがバインドされ、そのアダプタで接続が受けつかられることを意味します。
WinGate のネットワーク接続機能は、NIC の構成などから、内部、外部を自動検知いたしますが、この自動検知は必ずしも正しく検知できるわけではありません。
また、新たに NIC が追加された場合や、NIC の IP アドレスが変更された場合も、WinGate は自動的に変更・追加を検知し分類を行いますが、これも認識直後は自動検知として設定されます。

弊社では、自動検知の内容を必ずご確認いただき、可能な場合は手動で内部、外部の設定を行っていただく事をお願いしております。
**インストール直後、NIC や IP アドレスの変更があった場合は必ず、この項目を確認してください。**
また、この内部、外部の認識は ENS 機能のファイアウォール、ポートセキュリティ、NAT 機能などの設定にも反映され、利用されます。

**ネットワークインターフェースの確認方法**
WinGate のダイナミック・バインドは WinGate マシンで利用可能なネットワークインターフェース（ダイアルアップ接続を含む）を自動的に検出して、WinGate Management の Network Connections で利用可能なネットワーク・アダプタを表示します。




設定の確認を行うネットワーク接続をダブルクリックして、そのネットワーク接続のプロパティを表示します。




上記の図では Auto detect（自動検知）で currently Internal（現在は内部）と表示されていることから、このネットワーク接続は現在 WinGate では内部の保護されたネットワーク用のインターフェースであると認識されています。（認識が正しい場合でも手動で設定いただくことをお勧めいたします。）

設定項目の内容は以下の通りです。

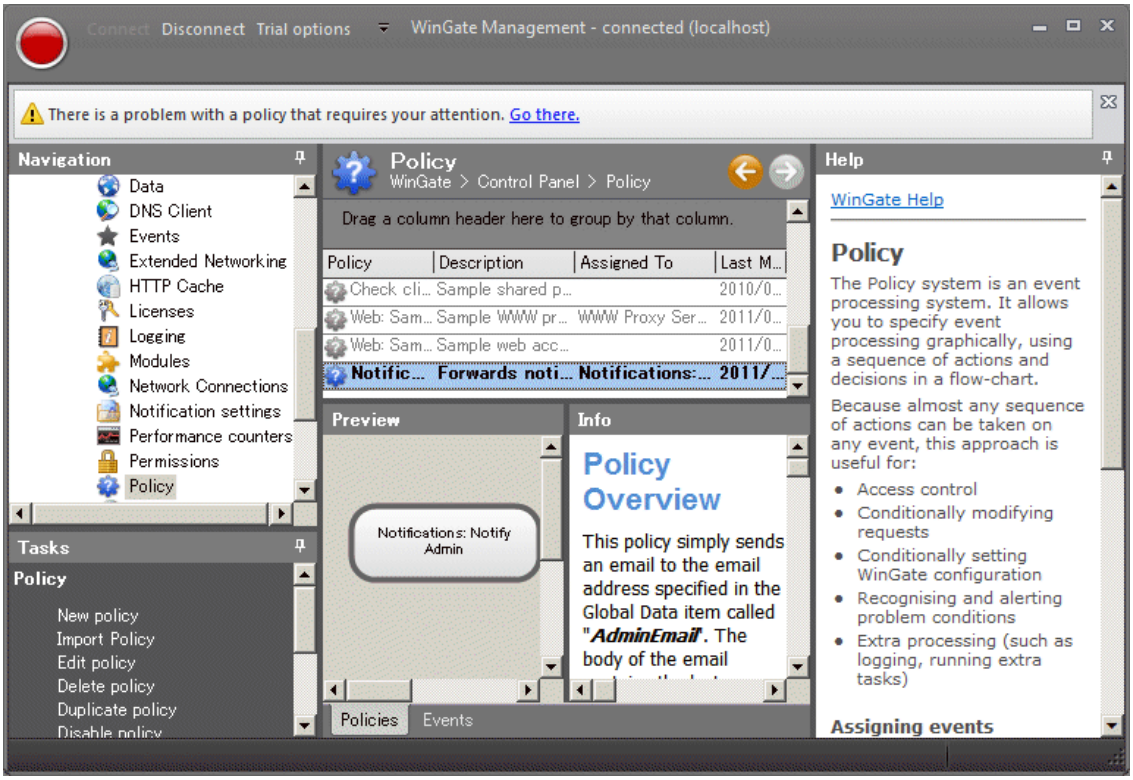
- Auto detect
  自動検知　カッコ内には、自動検知での構成が表示されます。currently Internal は内部、currently External は外部用となります。
- An Internal protected network
  内部の保護されたネットワークとなります。WinGate がクライアントから接続をうけるインターフェースは、通常、この設定となります。
- An external untrusted network (e.g. the Internet)
  信頼されない外部ネットワークとなります。NIC2 枚構成で、インターネットへ接続される側のインターフェースは、通常この設定をなります。
- A secured external network(DMZ)
  安全な外部のネットワーク（DMZ）となります。NIC3 枚構成で WinGate により DMZ を構成し、DMZ へ接続されるインターフェースは、通常この設定となります。

もし自動検知の内容がネットワークの構成に反している場合などは、適切な設定を選択いただくことにより、任意にネットワークインターフェースのタイプを変更することができます。

**※この変更は WinGate の全てのバインド、ファイアウォール構成に影響します。**

**Notifications（通知）**

インストール後、WinGate Management へログオンし、通知される内容があると左上のアイコンが赤く点滅し、WinGate の Notifications（通知）機能により、通知が表示される場合があります。




これは、管理者の電子メールアドレスの設定を促す通知となります。

この通知を消すには、Policy（ポリシー）をクリックし以下の設定変更を行ってください。

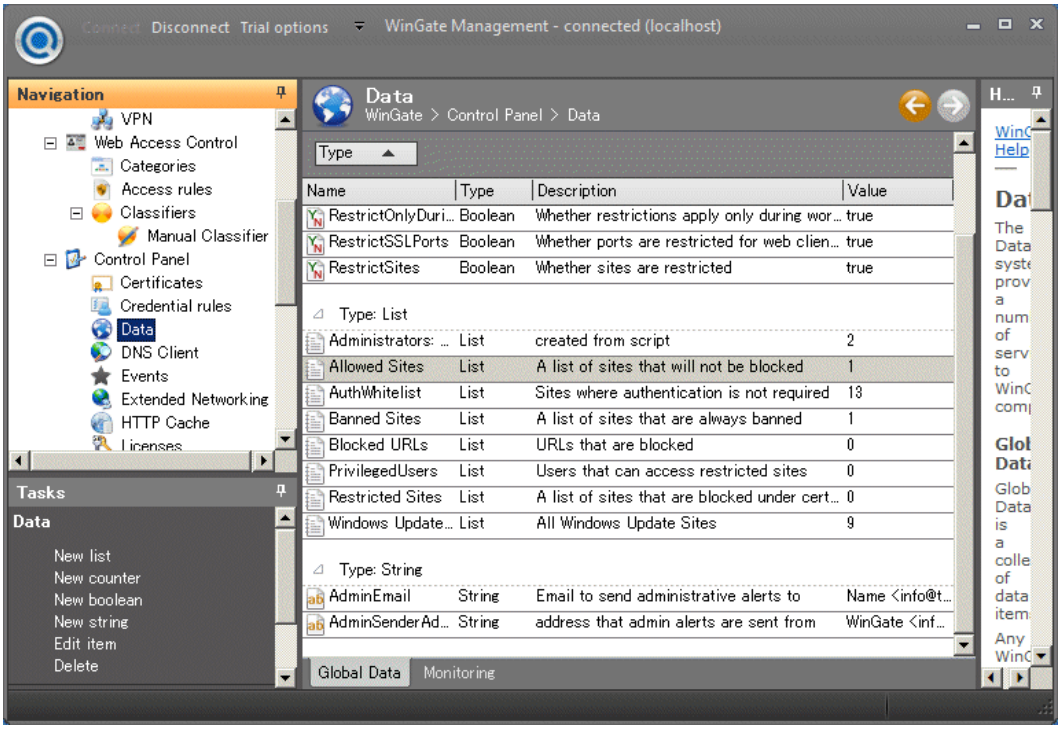
**管理者電子メールアドレスへの通知機能を利用しない場合**

Policy の太字で表示されている「Notification handler」を選択し、右クリックで Delete Policy を選択して、このポリシーを削除してください。

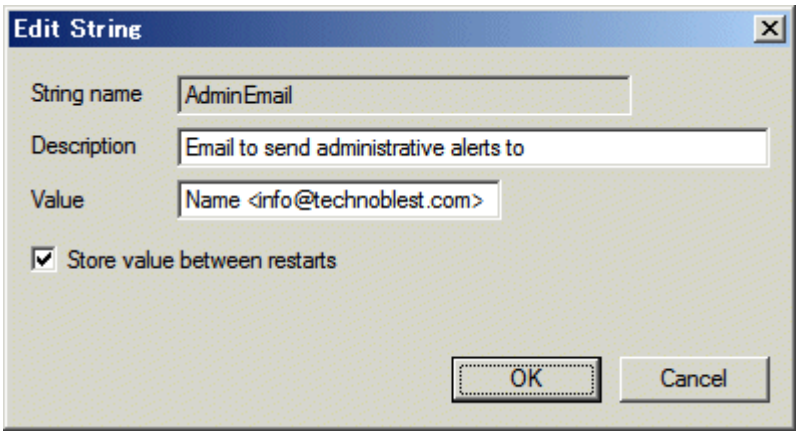
**管理者電子メールアドレスへの通知機能を利用する場合**

WinGate Management の Navigation から Data をクリックします。

下のタブで Global Data を開きます。




Type: String にある AdminEmail をダブルクリックで開きます。




Value（値）の欄に送信先の電子メールアドレスを入力します。

（Store value between restart をチェックした場合、設定内容は WinGate を再起動するまで適用されません。

同様に AdminSenderAddress をダブルクリックし、送信元の電子メールアドレスを入力します。

実際に通知を受け取るには、Wingate Email 機能でメールサーバーの機能を設定する必要があります。

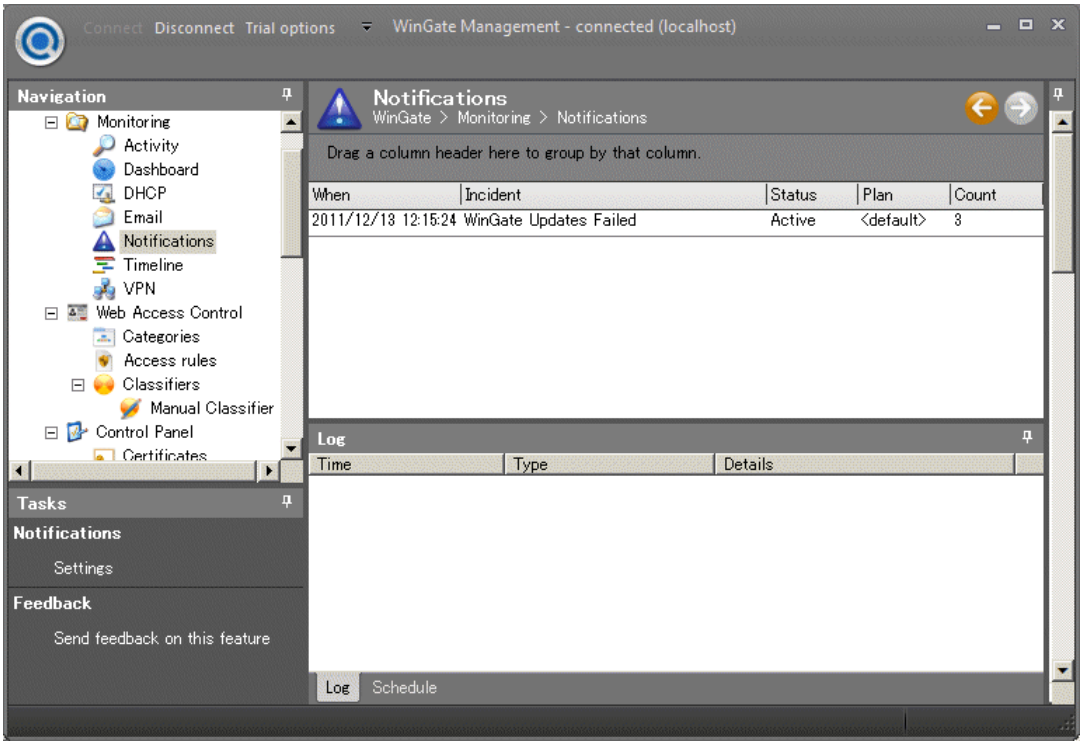
**Notifications の処理について**

WinGate で通知があった場合、WinGate Management へログイン後、左上のアイコンが赤く点滅し通知があることを知らせます。

その場合、Notifications を開くことで赤い点滅は終了しますが、次回ログイン時に同様の警告が通知されます。

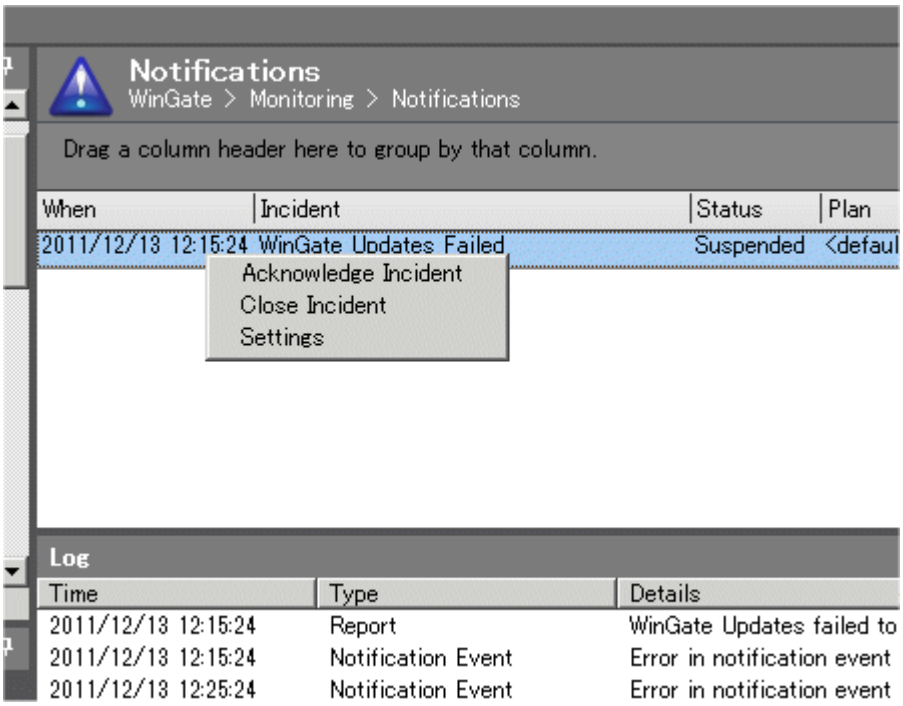
通知内容を把握した場合、以下の方法で通知を消すことができます。

Notifications を開きます。




表示されている通知を確認します。

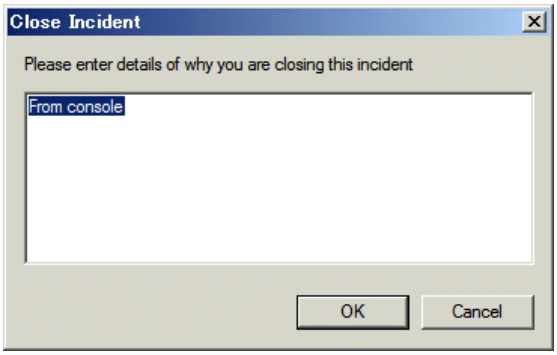
表示されている通知を選択して、右クリックします。




上記のメニューが表示されます。

**Acknowledge Incident**（承認したインシデント） この通知内容を承認し、表示に残す場合は、これを選択してください。

Close Incident（インシデントを閉じる） この通知内容を閉じる場合は、これを選択してください。

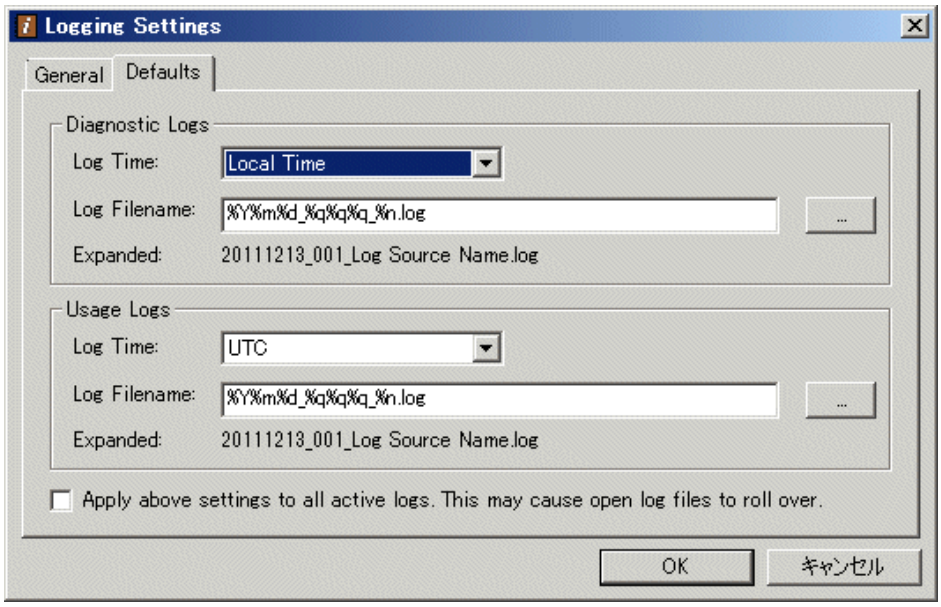



Close Incident ダイアログが表示されますので、閉じる理由を入力してください。
選択した場合、通知内容は WinGate Management から消去されます。

**ログ取得内容の確認（重要）**

WinGate のログはデフォルトでは、WinGate インストールフォルダーの Logs フォルダーに保存されます。
ログは Diagnostic（診断）ログと Usage（使用）ログの、2つのログから構成されています。
Diagnostic ログはデフォルトでは、警告（Warning）ログだけを記録し、全て Global.log という一つのログファイルに集約して保存されます。
警告（Warning）ログは、主に WinGate の各サービスなどで発生したエラーのみを記録します。
これをサービス毎に取得する場合には、Logging の Sources タブで設定を変更してください。

Usage ログは、WinGate の WWW Proxy Server などで使用されるログになります。（WWW Proxy Server は Diagnostic ログも持ちますが、Diagnostic ログは診断用として別に記録されます。）
Usage ログはデフォルトではログに記録する時刻を UTC（協定世界時）で記録します。
これをローカル時刻に変更するには、WinGate Management の Navigation から Logging を選択し、Tasks から Settings をクリックします。

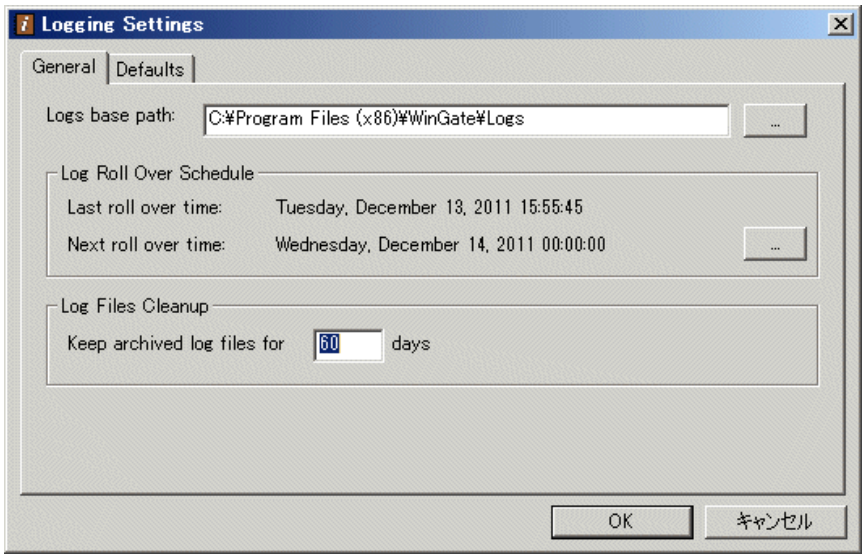



Defaults（デフォルト）タブの Usage Logs で Log Time から「Local Time」を選択します。
Apply above settings to all active logs. This may cause open log file to roll over.（全てのアクティブなログに上記の設定を適用する。これは開いているログファイルをロールーバーします。）を選択した場合、すぐに変更内容を適用し、現在のログファイルをロールーバーして、新しいログファイルに適用します。）

**ログのクリーンナップ**

WinGate のロギング機能は、デフォルトでは、60 日間で古いログ情報を削除していきます。

これを変更する場合は、WinGate Management の Navigation から Logging を選択し、Tasks から Settings をクリックします。

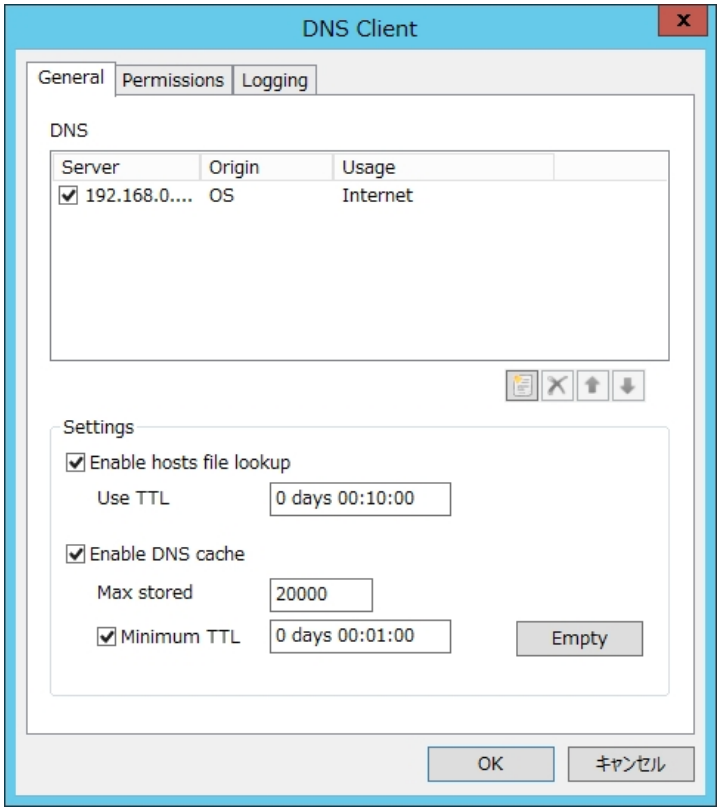



General（全般）タブの Log Files Cleanup よりログファイルのアーカイブを保持する日数を設定してください。

**ご注意**：ログ保存期間は、任意に指定する必要があります。（ログを削除しない設定はありません。）

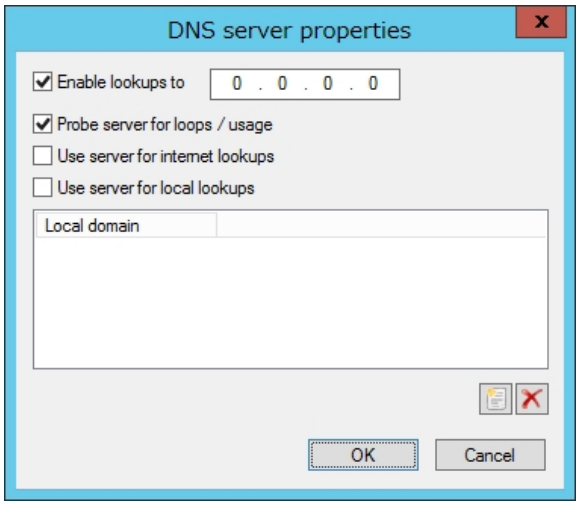
**DNS Client（DNS クライアント）設定の確認**

DNS Client は、WinGate 自身がインターネットアクセスする際に使用する DNS サーバーを指定する項目となります。




WinGate はデフォルトでは、OS の TCP/IP 設定で指定されている DNS サーバーを自動的に取得し、使用用途

（Usage）を決定します。
ここで、DNS サーバーが表示されていない場合は、右下のボタンより手動で DNS サーバーを追加してください。
また、使用用途（Usage）が Internet となっていない場合、WinGate はその DNS サーバーをインターネット接続の名前解決に使用できないため、Web ページなどの表示を行えない場合があります。この場合、表示されている DNS サーバーをダブルクリックし、DNS server properties より「Use server for internet lookups」（サーバーをインターネット参照に使用）を選択してください。




**使用しない機能の停止**

お客様の環境によっては、WinGate の持つ機能で必要としない機能があるかもしれません。WinGate を使用する目的に合わせて、使用しない機能を停止してください。
お客様の環境によって使用しない場合がある機能としては、以下の機能がございます。

- HTTP Cache（HTTP キャッシュ）
  HTTP キャッシュ機能は、WinGate の WWW Proxy Server 機能でリクエストされた内容をキャッシュし、同じリクエストがあった場合に、キャッシュ情報を利用して Web 表示の高速化を図る機能となります。
  この機能を筆四用としない場合は、HTTP Cache の設定画面より機能を無効としてください。

- Timeline（タイムライン）機能
  タイムラインは、WinGate Management 内でグラフにより WinGate を経由した Web アクティビティ（WWW Proxy の使用）を表示する機能となります。
  デフォルトでは、タイムライン機能は、データーベースに MDB を使用するため大規模な環境では、WinGate に高い負荷を与える場合がございます。
  大規模な環境では、タイムライン機能を停止、タイムライン・データーベースにサード パーティー製のデーターベースを使用、またはタイムラインのパージ間隔を短くしていただくことをお勧めいたします。
  詳細に関しては、トラブルシューティングの章をご覧ください。

## クライアントマシンの構成

### はじめに

ネットワーク内の WinGate サーバーの準備が完了したら、次にクライアントマシンのセットアップを行います。WinGate サーバーを利用するクライアントコンピュータは、WinGate サーバーに TCP/IP を使用して接続できる構成となっている必要があります。

クライアントマシンへのネットワークインターフェースのセットアップ方法は、ご利用するハードウェアの説明書の指示に従ってください。

クライアントの要件はクライアントで行わせる内容により異なります。しかし、どのような場合でも、クライアントマシンを構成する前に、WinGate サーバマシンのセットアップが完了している事をお勧めいたします。

クライアントマシンのセットアップを行う前に、クライアントマシンで TCP/IP がインストールされ、動作していることを確認してください。クライアントマシンから WinGate サーバーへの接続は TCP/IP を使用して行われますので、TCP/IP が正しく動作しない場合、WinGate サーバーを利用することはできません。これはクライアントマシンとして利用される全てのオペレーションシステム（Windows、MacOS、Linux）全てに適用されます。

### クライアントマシンでの TCP/IP のインストール

Windows はデフォルトで TCP/IP をほとんど全ての環境にインストールされているでしょう。TCP/IP がデフォルトでインストールされる場合、これらの設定を変更する必要はないでしょう。

既に TCP/IP がインストールされる場合、再び TCP/IP をインストールする必要はありませんが、TCP/IP が適切に動作しているかをテストする事ができます。TCP/IP の問題があった場合、TCP/IP の再インストールしてください。

TCP/IP のインストール、再インストールは使用する OS やハードウェアのより異なります。ご使用いただいておりますOS、ハードウェアのオンラインヘルプ、または取り扱い説明書をご参照ください。

### クライアントマシンの TCP/IP 設定（DHCP の構成）

WinGate は DHCP サービスによって、クライアントの TCP/IP 構成を自動的に行うことができます。多くの理由から、WinGate の DHCP サービスをご使用いただく事を推奨いたしますが、お客様のネットワーク構成や環境によっては、WinGate の DHCP サービスをご使用いただけない場合が考えられます。

クライアント構成では以下のアプローチが考えられます。:

1. クライアントマシンの TCP/IP は WinGate の DHCP サービスを使用して構成されます。
2. クライアントマシンの TCP/IP はネットワーク上の別の DHCP サーバーを使用して構成されます。
3. クライアントマシンの TCP/IP は手動で構成されます。（DHCP は使用しません）

各アプローチでのクライアントマシンの設定は以下の通りとなります。

1. **WinGate の DHCP サービスを使用するクライアントの設定**

   これは推奨されるアプローチです。ご使用いただいておりますオペレーションシステムの TCP/IP 設定で、IP アドレスを自動的に取得する設定がされていれば、DHCP は自動的にマシンで WInGate を使用するように構成されるでしょう

   例：Windows XP での TCP/IP の設定

   1.Windows のスタートメニューをクリックします。

2.「コントロール・パネル」を選択します。
3.「ネットワーク接続」を開きます。（クラッシック表示）
4.接続に使用する「ローカルエリア接続」アイコンを右クリックして、「プロパティ」を選択します。
5.インターネットプロトコル（TCP/IP）を、ダブルクリックします。
6.「全般」タブで「IP アドレスを自動的に取得する」を選択します。
7.同様に「DNS サーバーのアドレスを自動的に取得する」を選択します。
8.OK をクリックしてダイアログを終了します。

終了すると、Windows は DHCP サーバーを探し、自動的に IP アドレス等の情報を WinGate の DHCP サービスから取得するでしょう。正しく情報が取得されない場合、コンピュータの再起動をお試しください。

Windows XP 以外の OS に関しても TCP/IP の設定で「IP アドレスを自動的に取得する」設定を行っていただくことにより、構成が可能となります。（OS の種類によってはコンピュータの再起動が必要となる場合がございます。）

**2. 他の DHCP サーバーを使用するクライアントの構成**

既に他の DHCP サーバーを使用している場合、構成によっては既存の DHCP サーバーに変更を加える必要があるかもしれません。
WinGate の NAT 機能をご使用いただく場合、既存の DHCP サーバーの「ルータ」オプションを WinGate サーバーの IP アドレス（接続を受け付けている）に設定してください。この変更を行うことにより、クライアントマシンが WinGate の NAT をご使用いただくことができます。
また、DHCP の競合を防止するため、WInGate の DHCP を停止いただく必要があるかもしれません。
WinGate の DHCP の停止方法は、本書の 28 ページをご参照ください。

**3. DHCP を使用しないクライアントの設定**

このアプローチはあまり推奨される構成ではありませんが、既存のネットワーク DHCP を使用しない構成がされている場合、この構成となることが考えられます。
この構成を行う場合は、既存のネットワークポリシーにしたがって TCP/IP の設定を行ってください。
（IP アドレスの競合を防止するために、各クライアントで異なる IP アドレスを構成いただく必要があるでしょう。）
また、WinGate の NAT をご使用いただく場合、TCP/IP 設定のゲートウェイで WinGate サーバーの IP アドレス（接続を受け付けている）に設定する必要があることにご注意ください。

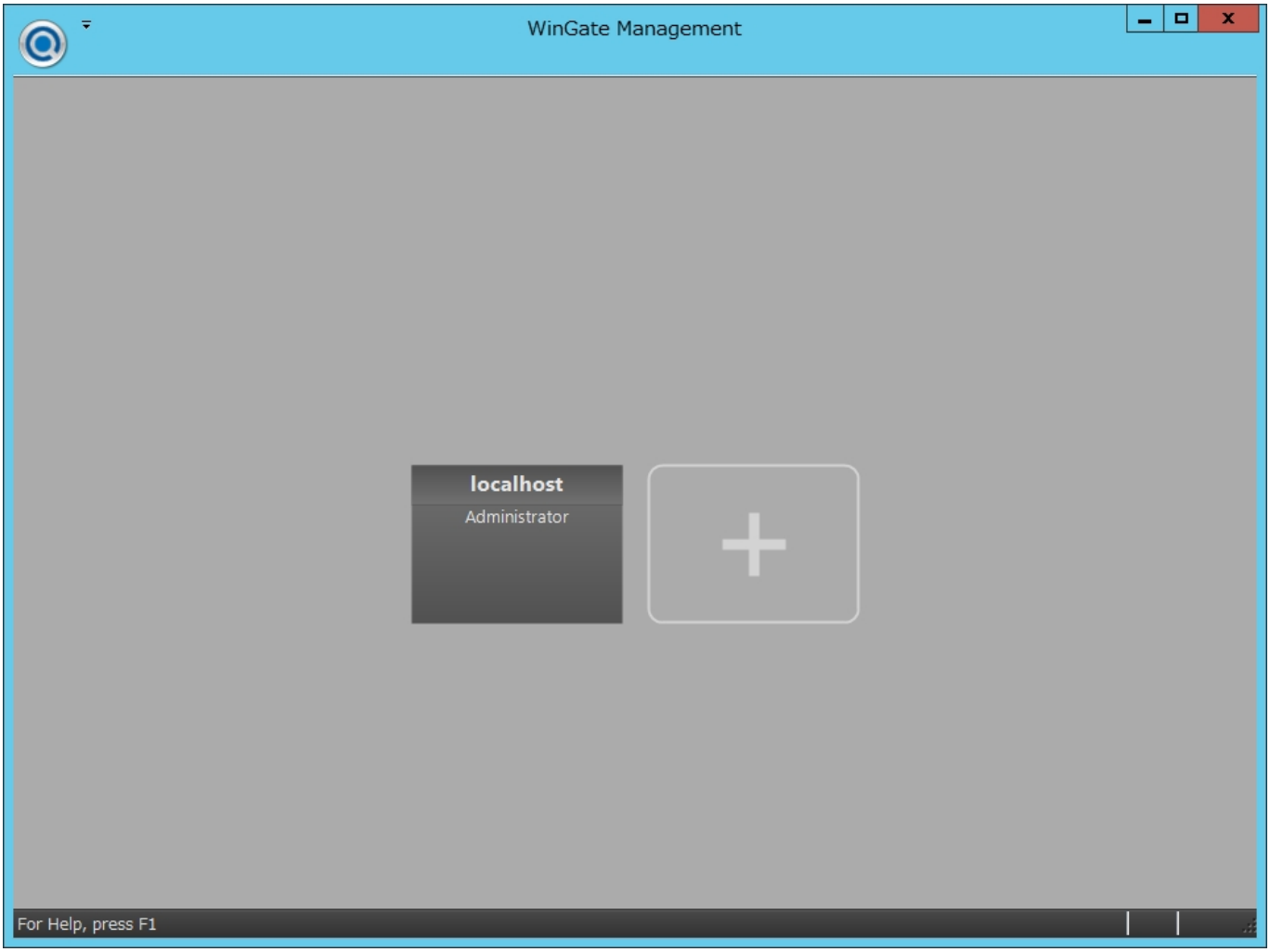
**※ WinGate の DHCP サーバーを使用していない場合、WinGate Management のアクティビティにマシン名を表示することができません。この場合、クライアントマシンの IP アドレスが表示されます。**

**WinGate 詳細**

**WinGate Management（WinGate マネージメント）について**

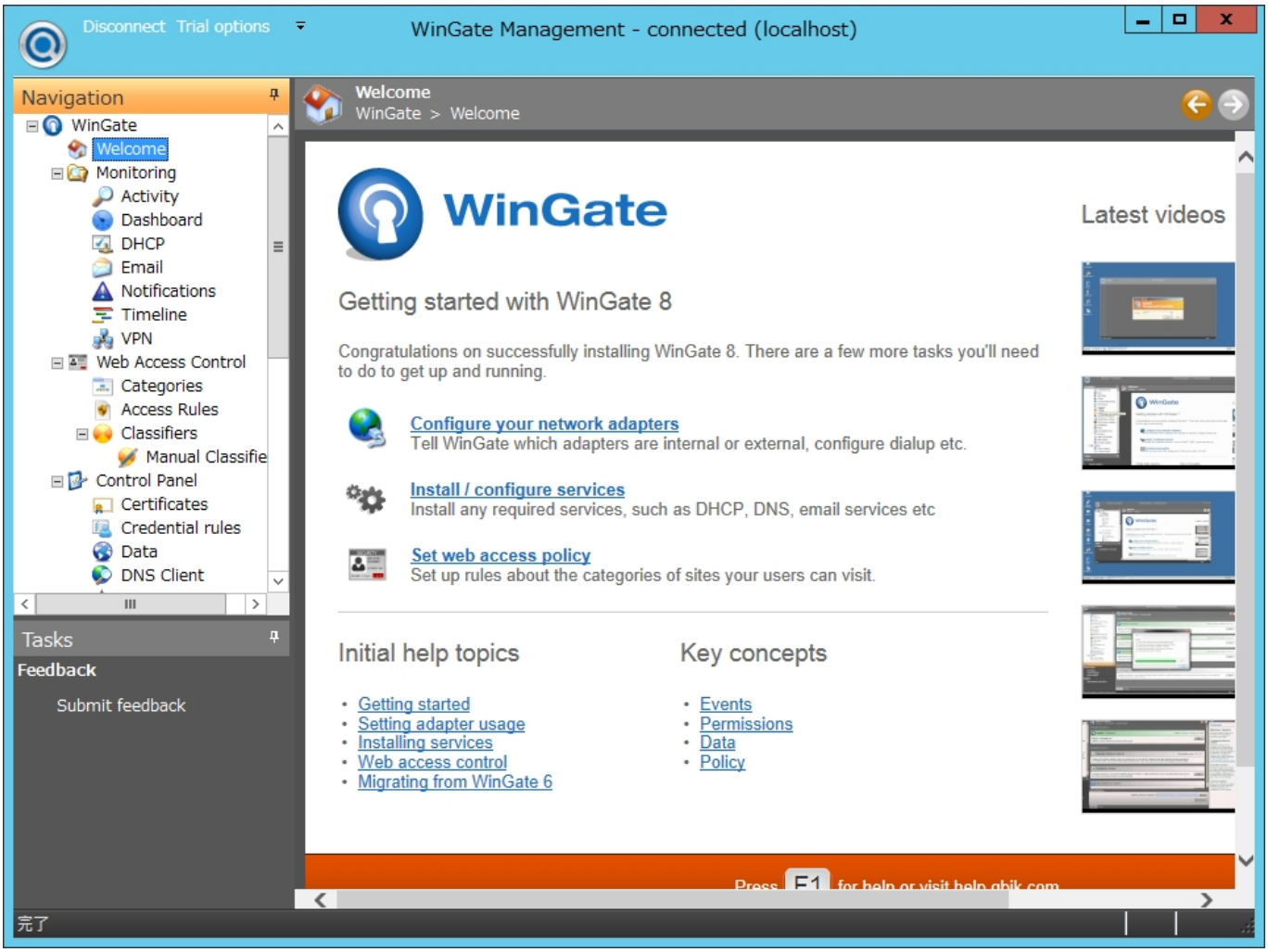
WinGate は WinGate Management を使用することにより制御、構成されます。
WinGate Management はすべての構成、モニター、およびコントロールのために暗号化された TCP/IP リンク上で WinGate とコミュニケートします。
WinGate Management は構成に使用されますが、WinGate の動作自体には、不可欠なものではありません。

TCP/IP 接続を持つリモートマシンから WinGate Management を使用して、WinGate へリモートアクセスいただくことも可能となります。（※WinGate Pro 版以上が必要となります。）リモート管理機能を使用することにより、遠隔地からの WinGate の管理、構成も可能となります。




WinGate Management 開始直後は、上記のオンラインオプション・ダイアログが表示されます。接続先を選択し、その後表示される Login information で設定されたユーザー名・パスワードでログインしてください。
Windows ユーザー・データーベースを使用している場合、ログインには Windows ユーザー・データーベースの管理者名・パスワードが使用されるかもしれません。

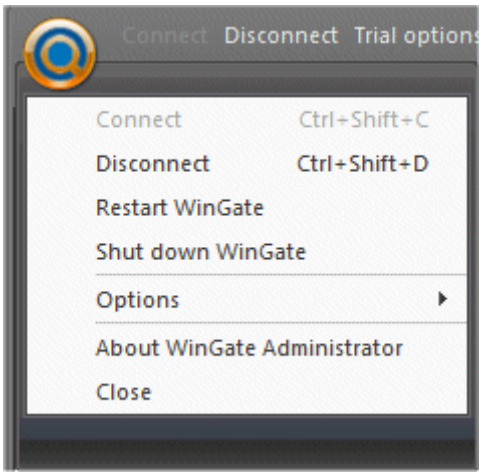
ログインすると次のように画面が表示されます。


Disconnect Trial options
WinGate Management - connected (localhost)
Navigation
WinGate
Welcome
Monitoring
Activity
Dashboard
DHCP
Email
Notifications
Timeline
VPN
Web Access Control
Categories
Access Rules
Classifiers
Manual Classifie
Control Panel
Certificates
Credential rules
Data
DNS Client
Tasks
Feedback
Submit feedback
Welcome
WinGate > Welcome
WinGate
Getting started with WinGate 8
Congratulations on successfully installing WinGate 8. There are a few more tasks you'll need to do to get up and running.
Configure your network adapters
Tell WinGate which adapters are internal or external, configure dialup etc.
Install / configure services
Install any required services, such as DHCP, DNS, email services etc
Set web access policy
Set up rules about the categories of sites your users can visit.
Initial help topics
Getting started
Setting adapter usage
Installing services
Web access control
Migrating from WinGate 6
Key concepts
Events
Permissions
Data
Policy
Latest videos
Press F1 for help or visit help.qbik.com
完了

**メニューバー**

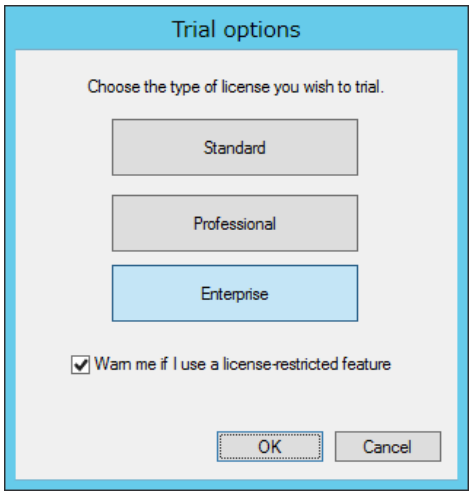
以下は WinGate Management の上部に表示されているメニューバーでご使用いただける項目です。

- **Qbik ロゴマーク**（WinGate Management 左上に表示されている Qbik 社のロゴマークをクリックすると幾つかのオプションを選択できます。）




  - **Connect（接続）**
    WinGate へ接続します。（切断されている際に利用可能です。）
  - **Disconnect（切断）**
    WinGate から切断します。（接続されている際に利用可能です。）
  - **Restart WinGate（WinGate の再起動）**
    WinGate の再起動を行います。再起動中は一旦、接続が切断されます。
  - **Shut down WinGate（WinGate のシャットダウン）**
    WinGate をシャットダウン（停止）します。
  - **About WinGate Administrator**
    WinGate のバージョン情報、インストールされている OS の種類、著作権情報などを含むダイアログを表示します。
  - **Close（閉じる）**
    WinGate Management を終了します。

- **Trial options（試用版オプション）**
  試用版を利用している場合に、このメニューは表示されます。
  Trial options をクリックすると試用版として利用する WinGate の種類を選択することができます。
  これにより、実際にご購入を検討いただいております WinGate の種類と同じ動作を試用版でお試しいただけます。




オプション：Warn me if I use a License-restricted feature（ライセンスによって制限される機能を使用した場合に警告）

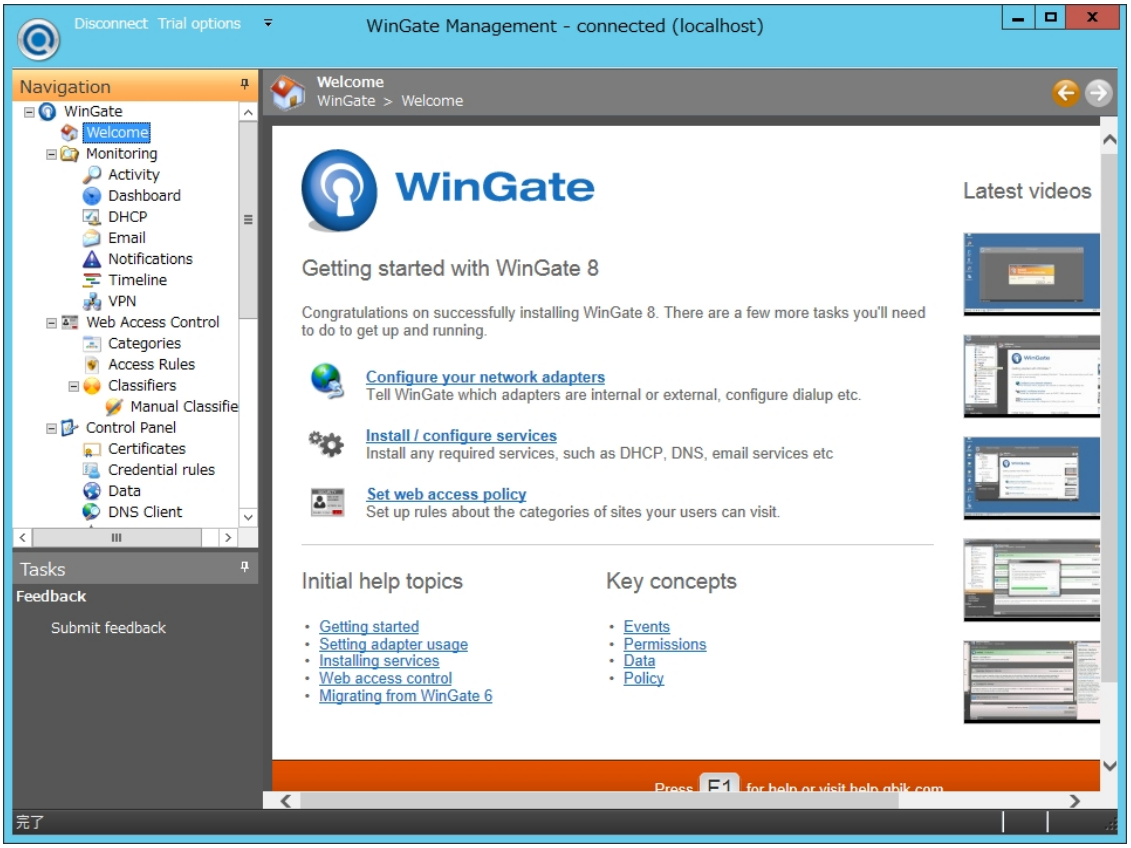
試用版で利用する WinGate の種類を変更した場合、WinGate の再起動が必要となります。

**WinGate Management 各項目の概要**

WinGate Management で設定可能な WinGate の各項目は以下の通りです。

本書では、概要や一般的に使用される機能のみのご説明となっておりますことをご了承ください。詳細な設定方法については、本書に記載がございます一部の機能についての設定方法をご参照いただくか、弊社までお問い合わせください。

WinGate Management は、主に 3 つのパーツから構成されております。




- Navigation（ナビゲーション）パネル

  Navigation はツリー構造で WinGate の利用状況などを表示する「Monitoring」（モニタリング）、WWW Proxy Server でのアクセス制御行う「Web Access Control」（Web アクセス・コントロール）、各種の設定を行う Control Panel（コントロール・パネル）、その他のツールを含む Utilities（ユーティリティ）で構成されます。

- Tasks（タスク）

  画面左下の Tasks では、Navigation で選択した項目で設定選択を行うことができます。項目は Navigation で選択された項目により異なります。

- メインウインドウ

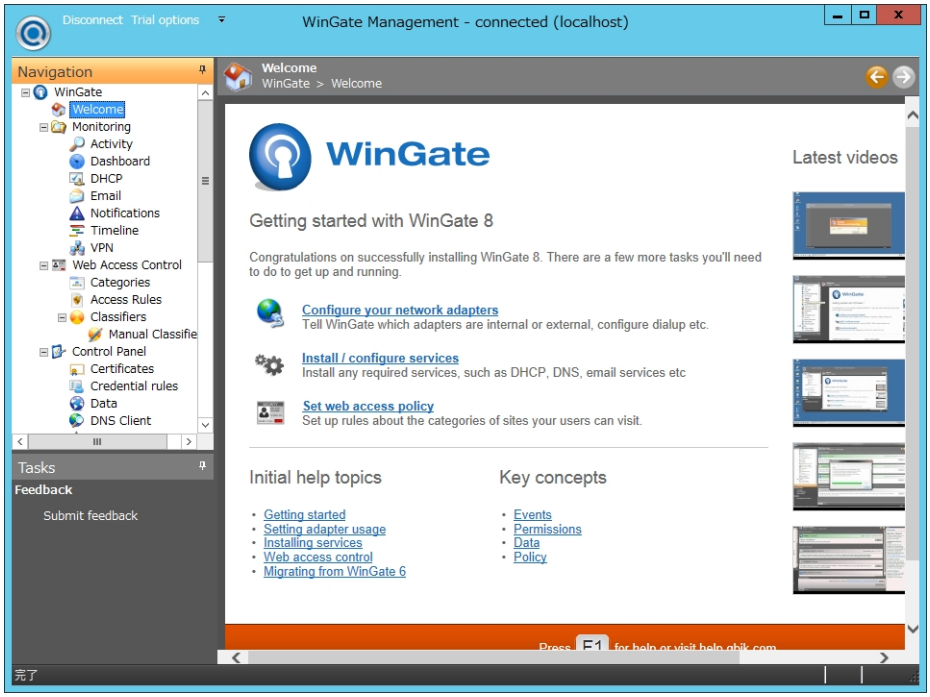
  画面右側のウインドウには、Navigation で選択された広告の設定状況や動作状況などの様々な情報を表示します。

※Navigation で選択された項目の幾つかは、ダイアログが表示され、ダイアログ内で設定を行います。

**各項目、および機能の説明**

以下は、WinGate Management の各項目の内容です。

### Welcome（ようこそ）

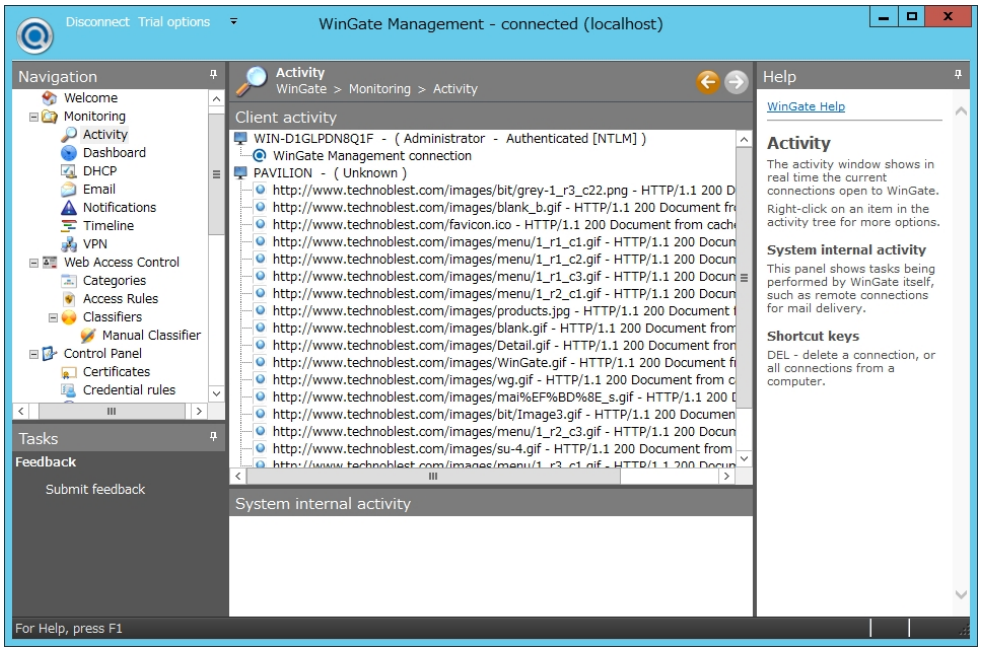



Welcome スクリーンでは、WinGate の開始後の設定に関するショートカットやヘルプへのリンクなどが表示されます。（現在は英語でのご提供のみとなります。）

### Monitoring（モニタリング）

Monitoring は以下の項目から構成されています。

### Activity（アクティビティ）

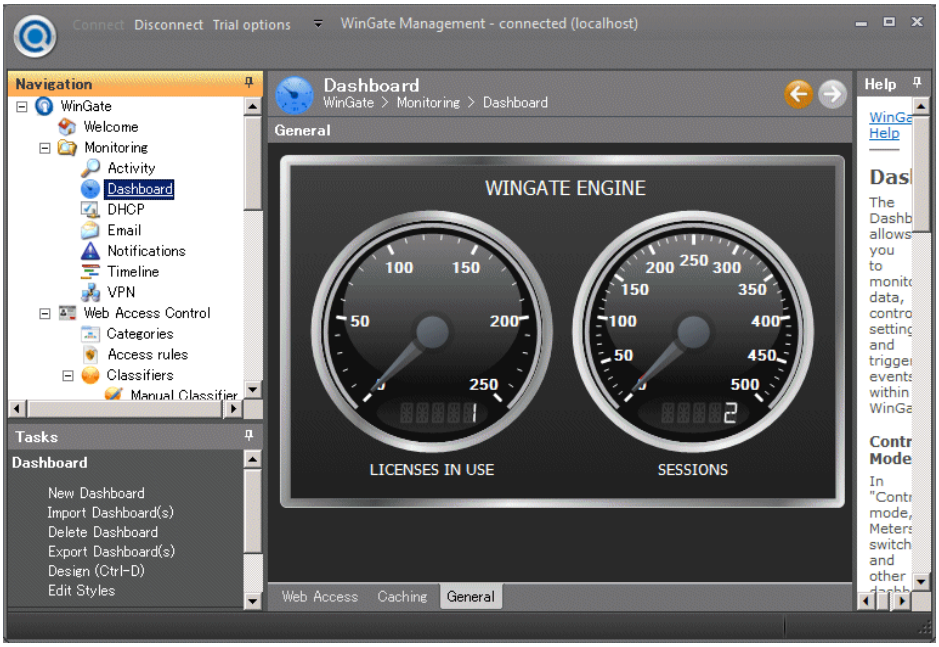



アクティビティには WinGate を利用するユーザーの活動状況がリアルタイムで表示されます。

表示される項目を右クリックする事により、セッションの切断や URL のクリップボードへのコピーなどを行うことが

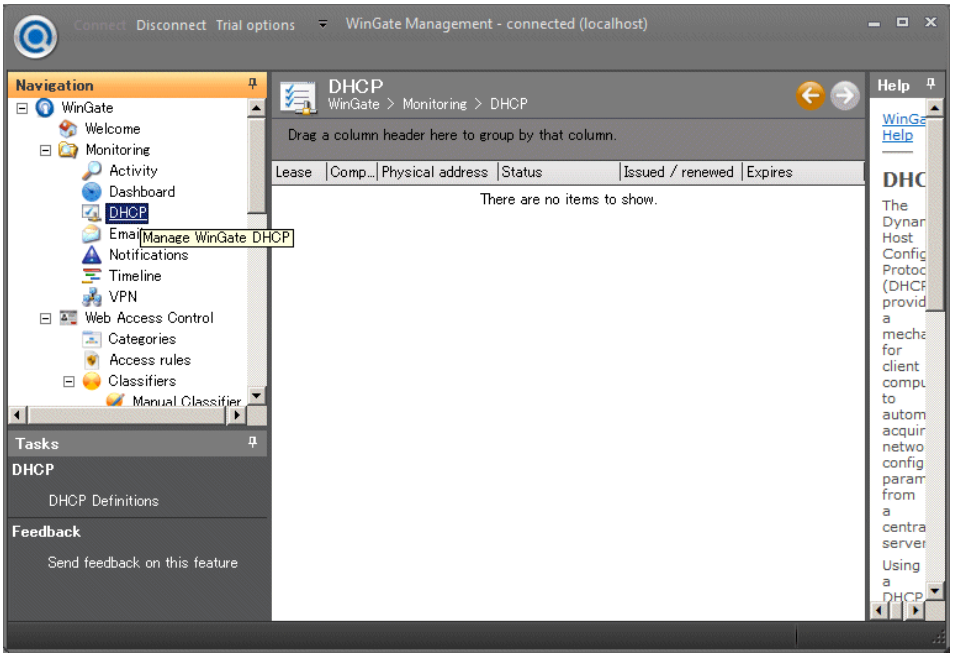
できます。
クライアントからのセッションがなくなっても、一定時間クライアント PC のアイコンは残されます。
Activity での設定項目はありません。

### Dashboard（ダッシュボード）




Dashboard には、WinGate の活動状況を様々な方法で表示します。
デフォルトインストールでは、Web Access、Caching、General の 3 つのタブを持ちます。
Task より Design（デザイン）を選択すると、表示されている Dashboard の内容をカスタマイズすることができます。
また、New Dashboard より新しい Dashboard を追加することもできます。

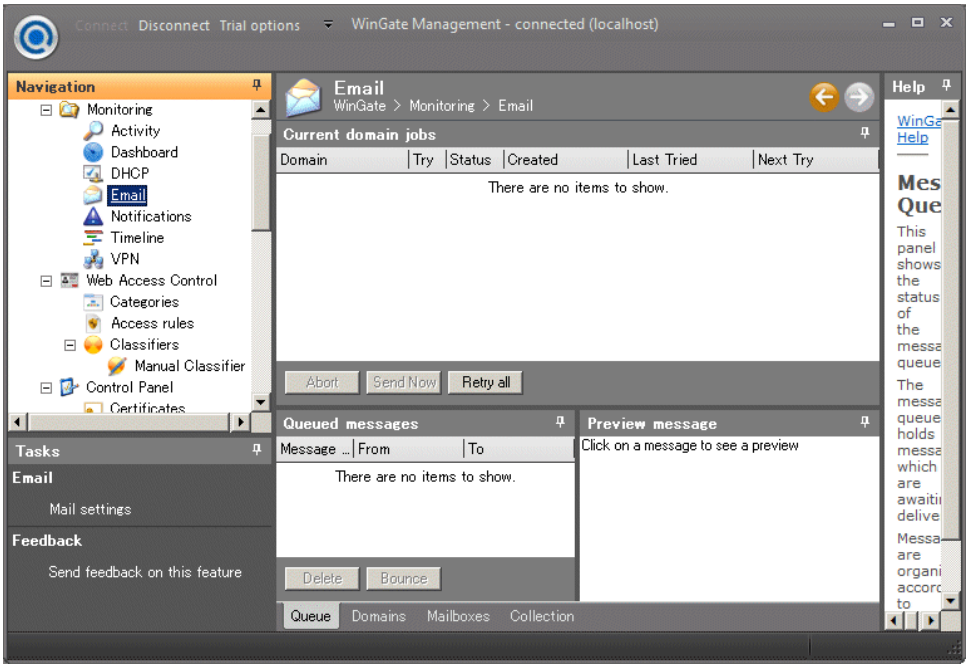
### DHCP



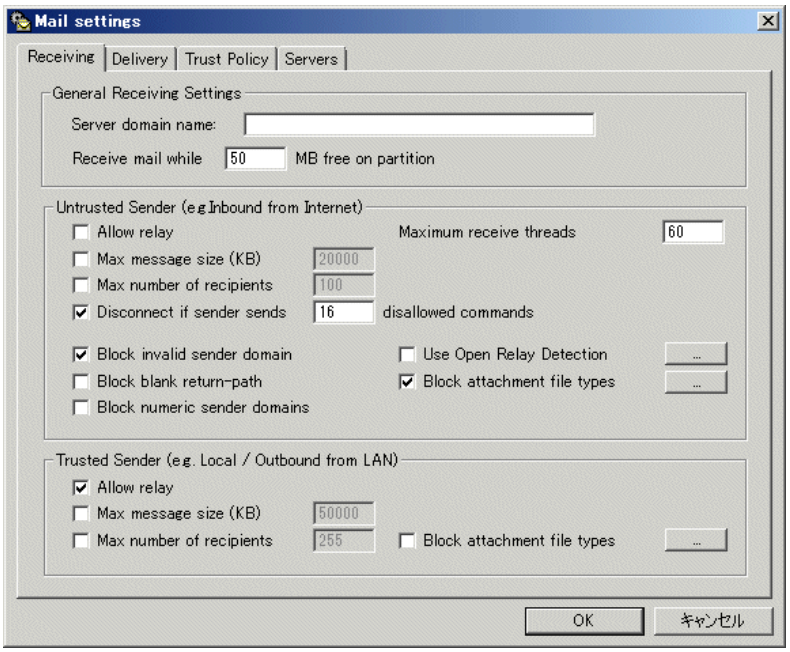

WinGate の DHCP　Service がインストールされている場合、このスクリーンに WinGate に DHCP によって割り当てられた DHCP の内容が一覧で表示されます。

表示されている DHCP リースを選択し右クリックにより「Revoke lease」(リースを破棄)を選択すると、選択した項目の DHCP リースを破棄することができます。また、Task に表示される「Revoke lease」を実行しても、同様の操作を行うことができます。
DHCP Definitions(DHCP 定義)より、定義内容の追加を行うことができます。

**Email**

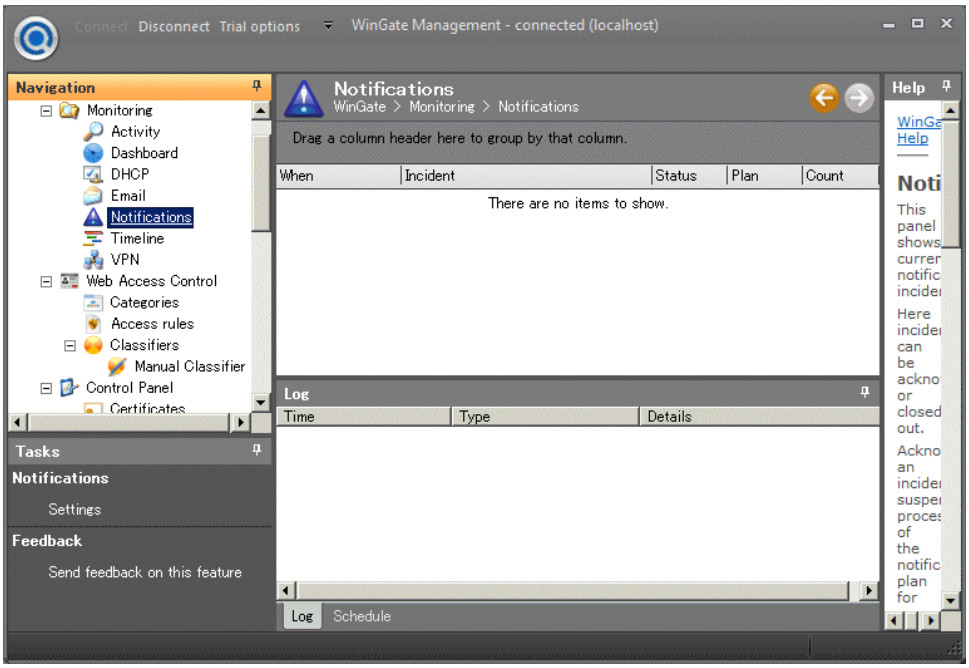



Email では、WinGate のメールサーバーとしての動作状況やメールサーバーの設定を行うことができます。
Tasks の Mail settings(メール設定)をクリックするとメールサーバーの詳細設定ダイアログを表示することができます。



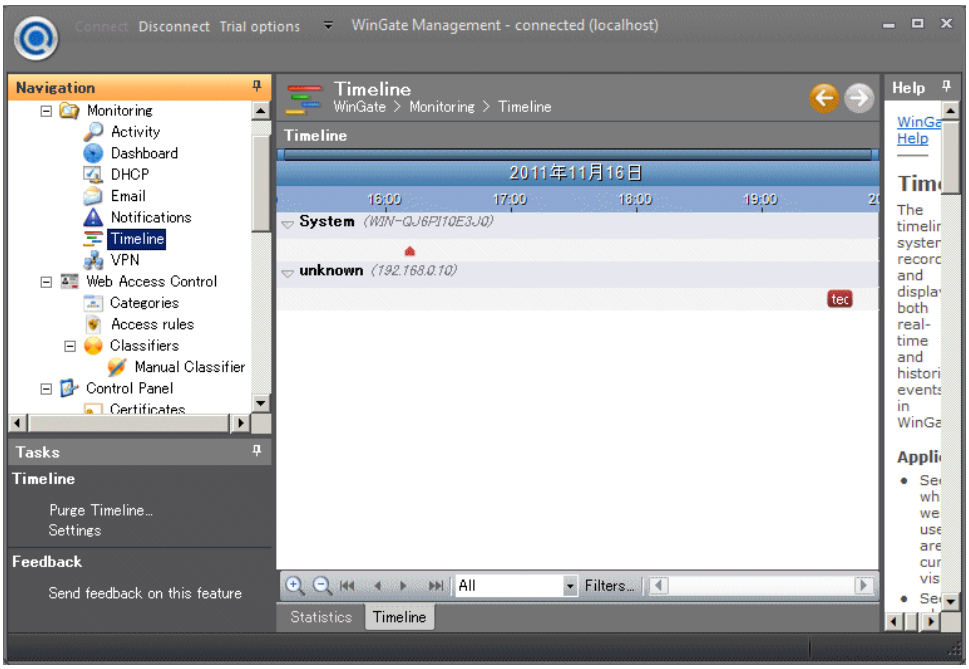

WinGate をメールサーバーとして使用しない場合、または通知機能により管理者向けに電子メールの配信を行わない場合は、これらの設定の必要はございません。

### Notifications（通知）




Notifications には、WinGate から管理者向けの通知がある場合に、それらを表示します。

### Timeline（タイムライン）

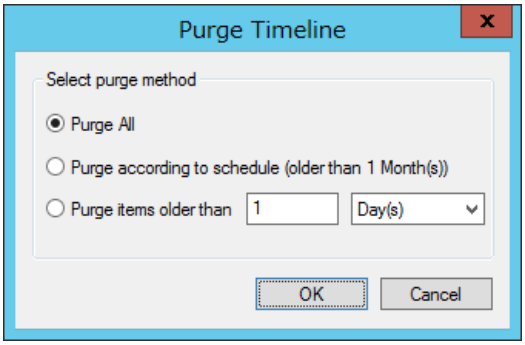



タイムラインは、WinGate のシステムイベント、WWW Proxy Server での活動状況をリアルタイムに記録しグラフ表示します。

タイムライン上のグラフへマウスカーソルを移動することにより、詳細を確認することができます。

また右クリックにより　Open:　XXXXXX　が表示されブラウザでサイト参照することができます。

Tasks の Purge Timeline をクリックすると Timeline を条件に従ってパージ（削除）することができます。

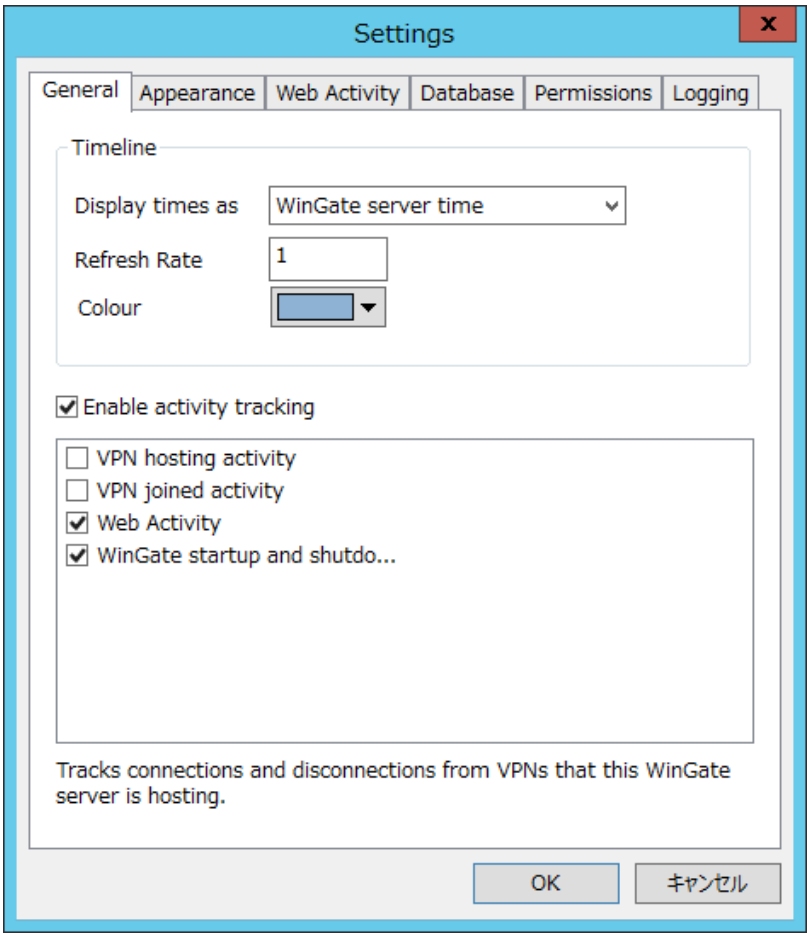



選択項目は、Purge All（全てパージ）、Purge according to schedule(older than 1 Month(s)（スケジュールに従い削除（1 ヶ月より古い）、Purge items than（次より前のアイテムをパージ）となります。

Tasks の Settings をクリックすると、Timeline の内容を設定することができます。

**Settings で行える設定**

General（全般）




ここでは、Timeline の先般的な設定を変更することができます。

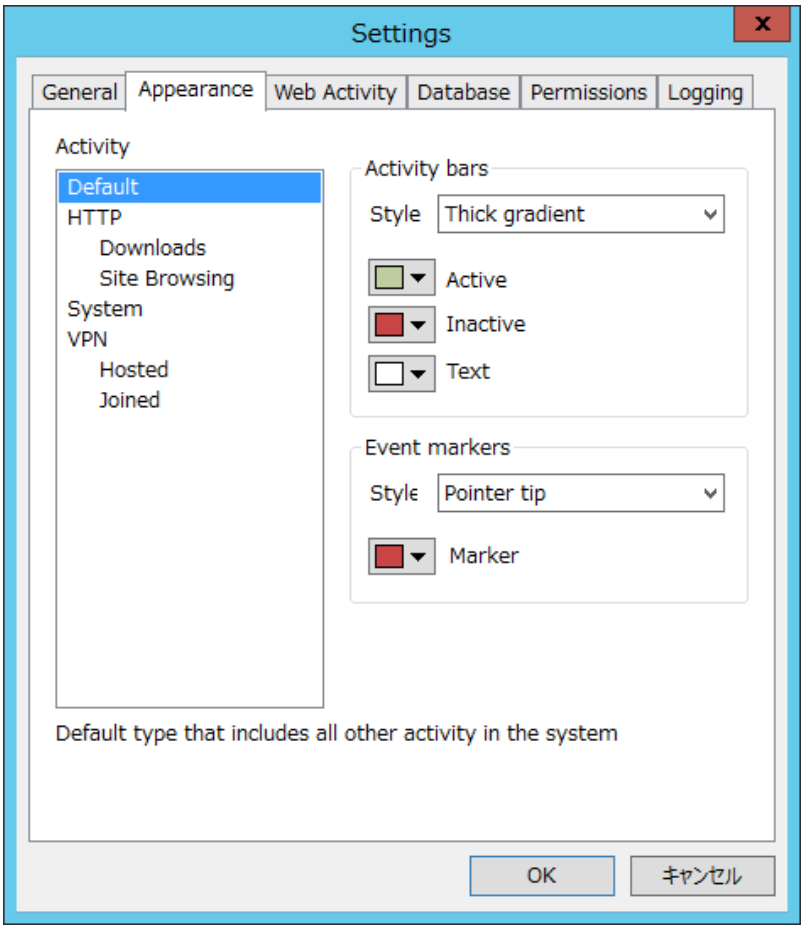
Display time as ＝ Time ラインに表示される時刻を選択することができます。

Refresh Rate(sec) ＝ Timeline が更新されるタイミングを設定することができます。

Coulour Scheme ＝ Timeline 上部の色を変更することができます。

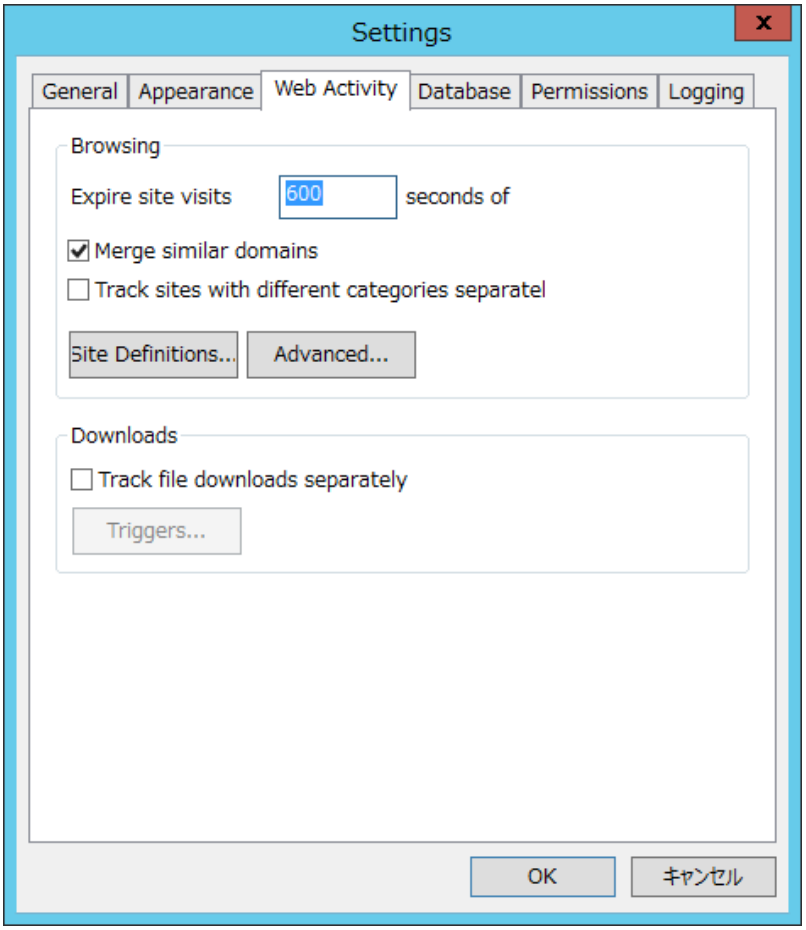
Enable activity tracking ＝ Activity の追跡を有効とするか無効とするかを切り替えます。チェックがされている場合、有効となります。下の段では追跡する Activity を選択することができます。

Appearance（外観）




ここでは Timeline に表示される内容の色を選択することができます。
必要に応じて変更を行ってください。

Web Activity（Web アクティビティ）



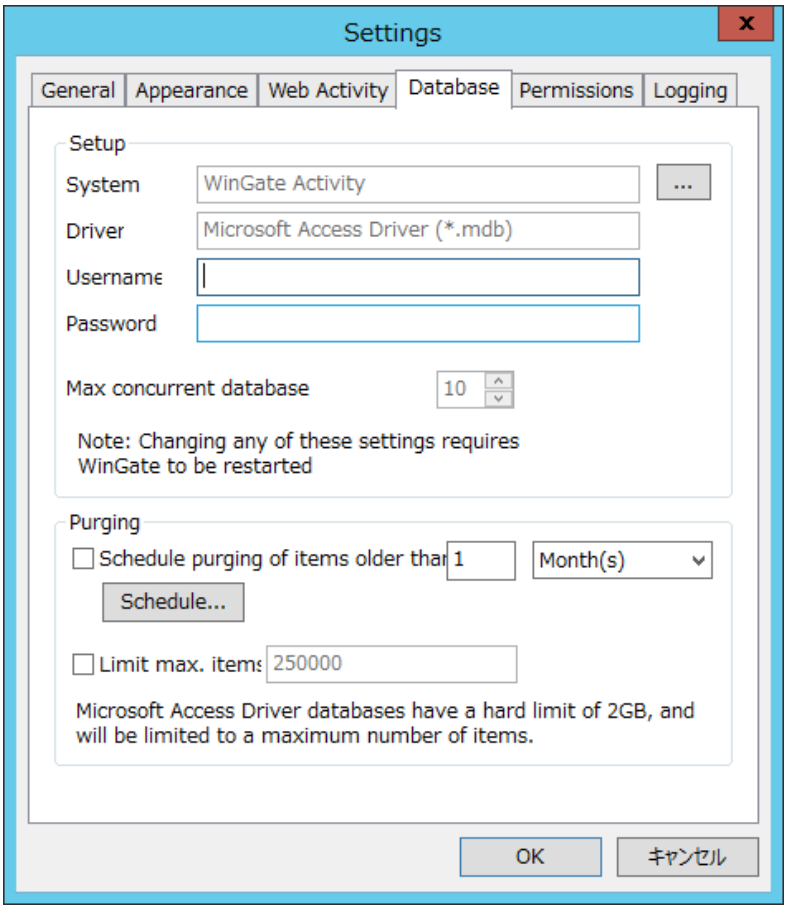

ここでは Timeline に記録する内容を設定することができます。

Browsing（ブラウズ）の Expire site visits after xxx seconds of inactivity では、何秒後にアクティブな状態ではないと判断するかの時間（秒）を設定することができます。Merge similar domains を有効にすると同じドメインは一つのブラフにまとめられます。

Site Definitions（サイト定義）をクリックすると、異なるサイトを一つのサイトとして定義することができます。また、Advanced（詳細）では、追跡をしない URL などを設定することができます。

Downloads（ダウンロード）では、「Track file downloads separately」を有効にすると、ダウンロード活動を追跡し Timeline 上に記録します。Triggers では、ダウンロード追跡のトリガーとなる Mime Type を設定することができます。

Database（データーベース）



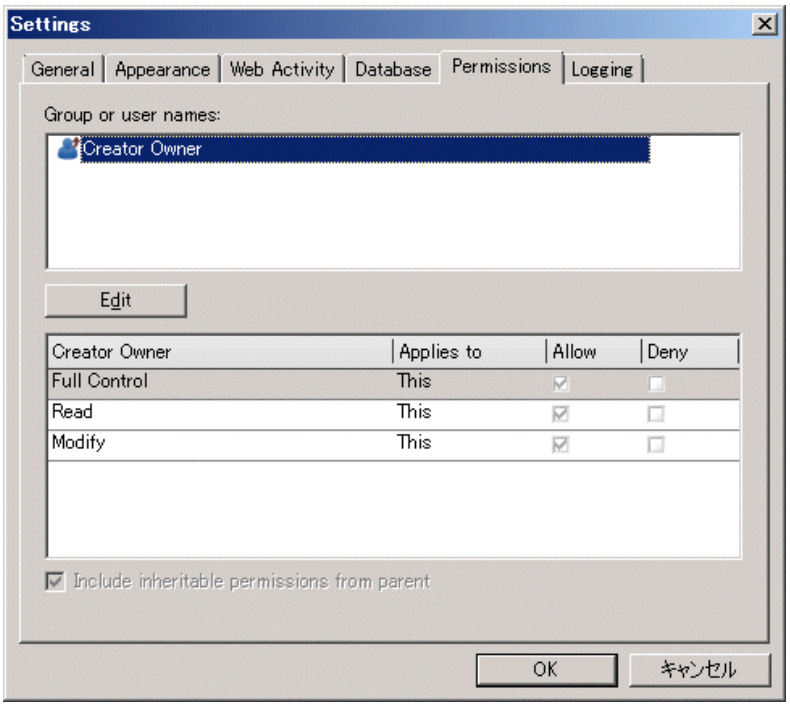

Database では、Timeline の情報を保存するデーターベースを指定することができます。デフォルトは Microsoft Access Driver です。

Purging の Schedule purging of items older than を有効にすると指定した期間の Timeline を自動的にパージ（削除）します。

また、Limit max. items の設定によりデーターベースに記録されるアイテムの最大数を設定することができます。

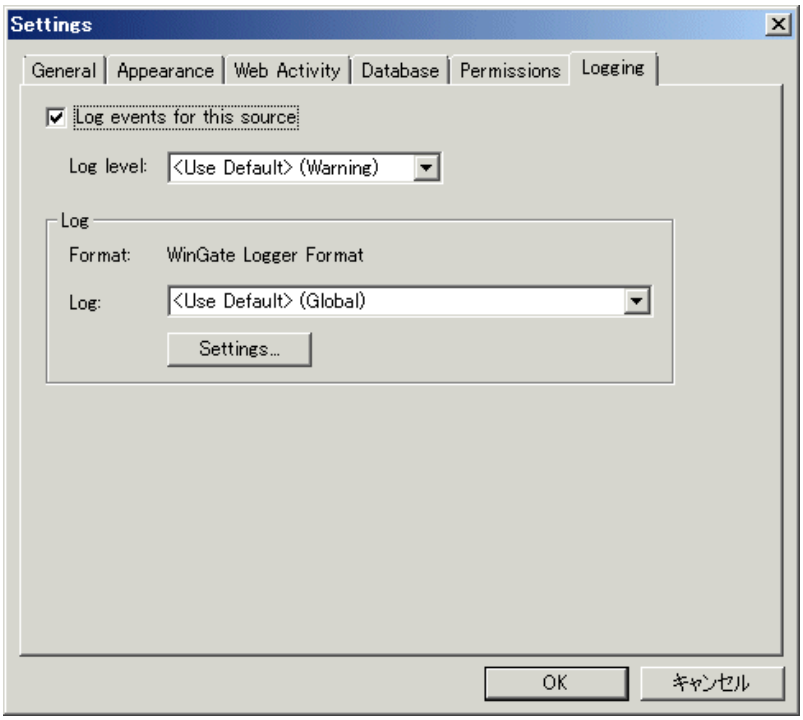
重要：大規模な環境で Timeline 機能を使用した場合、データーベースに保存されるアイテム数が膨大になり、WinGate の動作やパフォーマンスに影響を与える場合があります。これを防止するためには、Timeline のパージ機能、または Limit max. items 設定をご利用ください。

Permissions（権限）



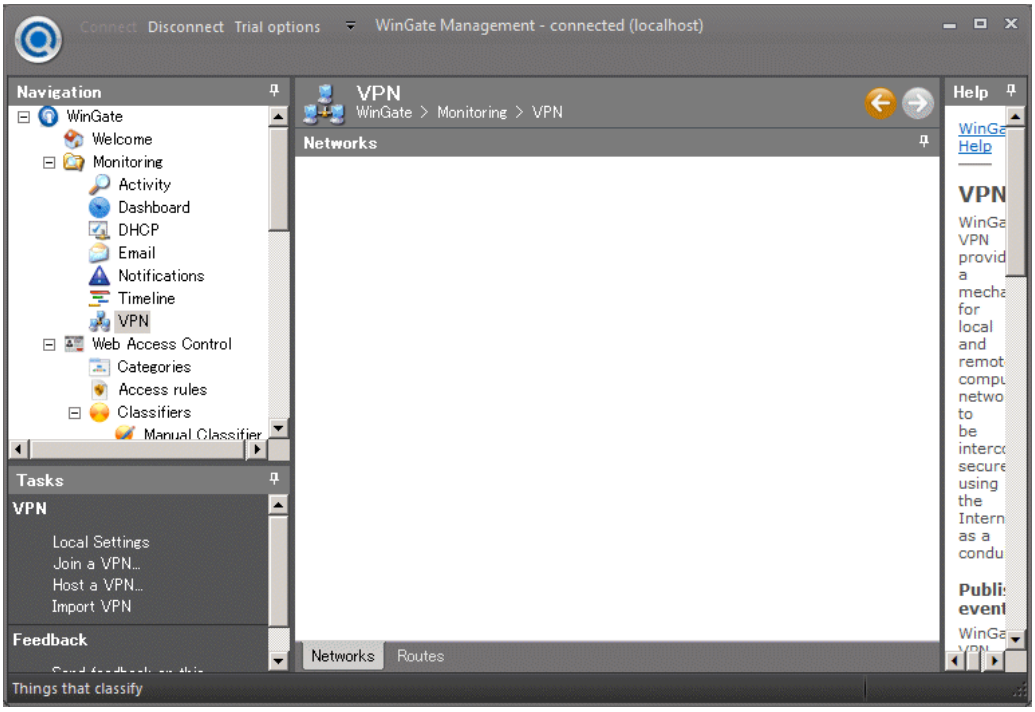

Timeline の権限を設定することができます。

Logging（ロギング）




Timeline のログ取得方法を設定することができます。詳細は、ロギングの章をご覧ください。

### VPN



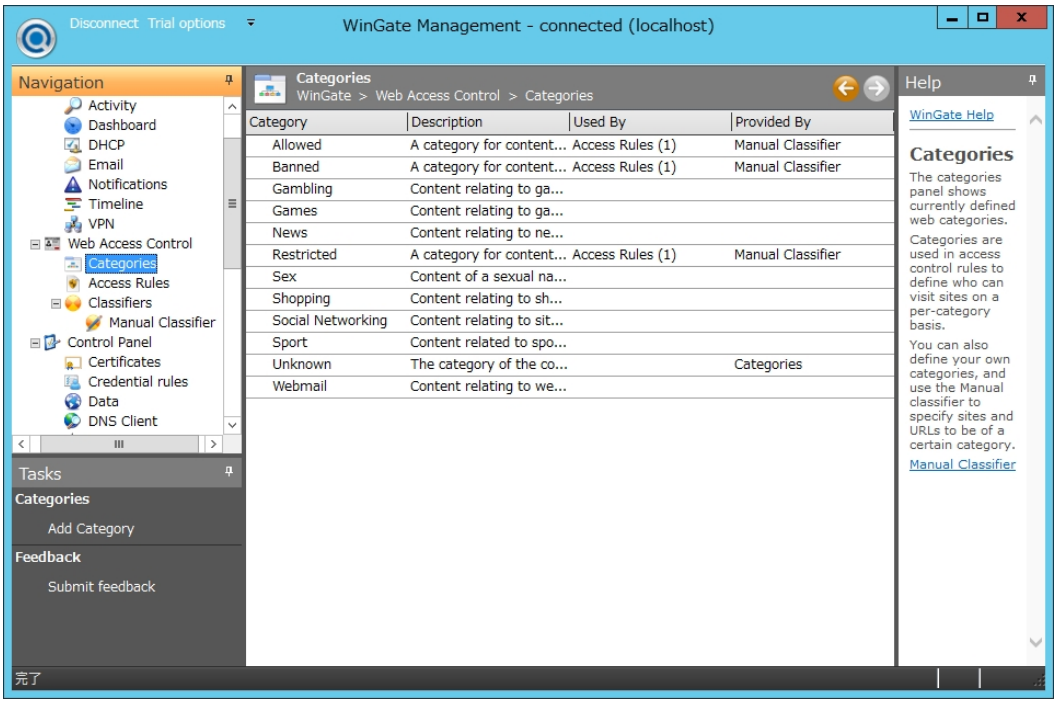

Services で VPN Service がインストールされている場合は、VPN に関する設定を行うことができます。VPN 機能を利用するには、Enterprise ライセンス、または WinGate VPN ライセンスが必要となります。

### Web Access Control（Web アクセス・コントロール）

Web Access Control を使用する事により、容易に WWW Proxy Server による接続を URL、またはドメインによってカテゴリー毎に制御することが可能となります。

Web Access Control は、3 つの要素で構成されています。

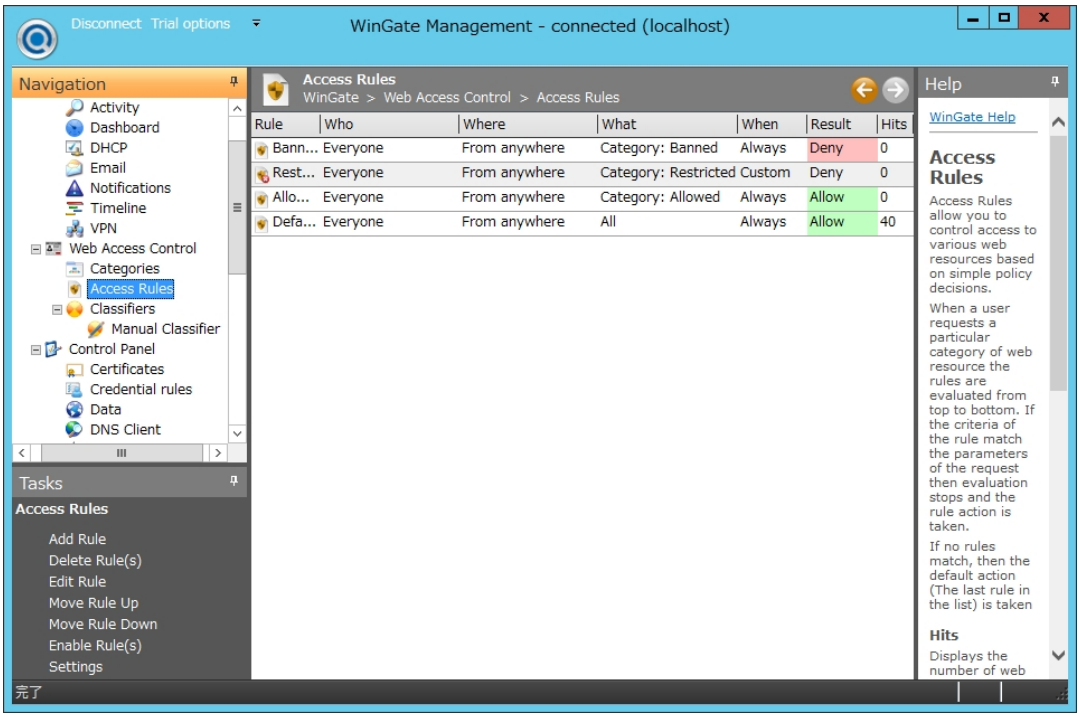
◆ Categories（カテゴリー）




目的に合わせて、手動でアクセス制御を適用するカテゴリーを作成することができます。デフォルトで、幾つかの一般的なカテゴリーが作成されています。

Tasks で Add Category をクリックすることにより、新たにカテゴリーを作成することができます。

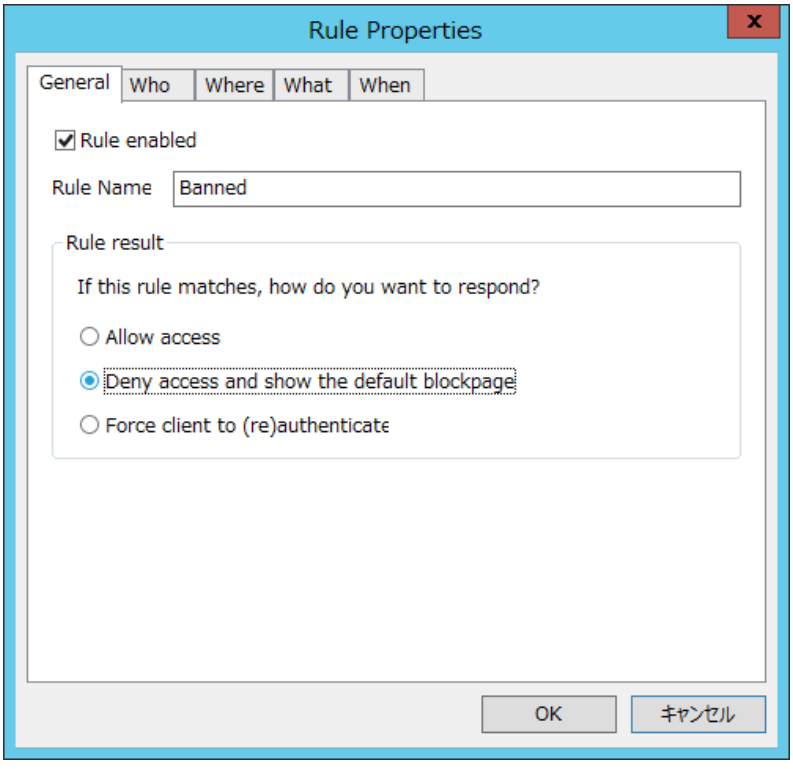
◆ Access rules（アクセス・ルール）




Access rules では、作成する（した）、アクセス・ルールに対する Deny（拒否）／Allow（許可）設定、適用するユーザーやカテゴリー、スケジュールを設定することができます。

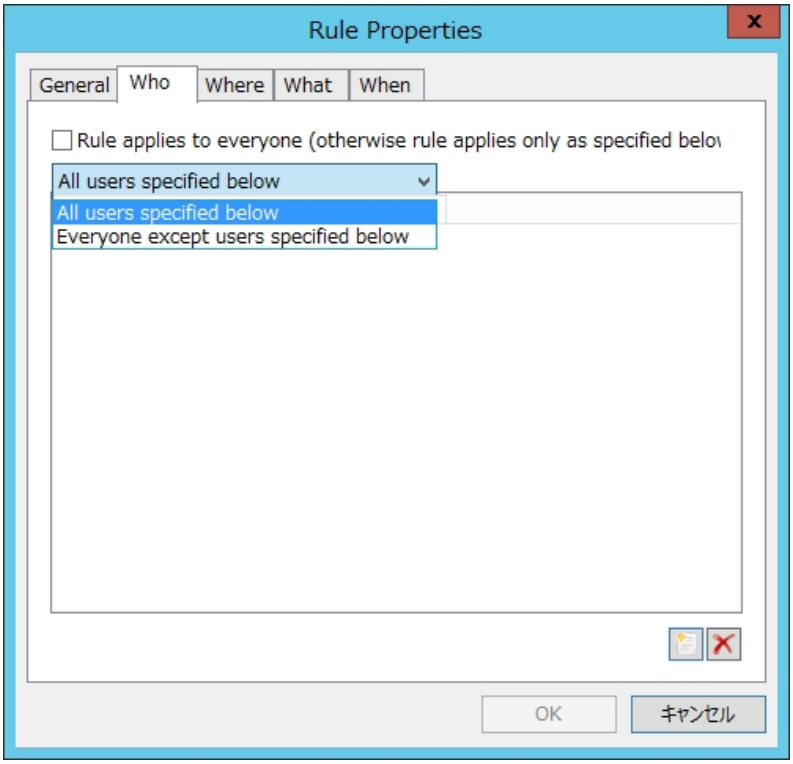
デフォルトでは幾つかのルールが作成されています。

作成した分類に対して、一致した場合にどのようなアクション（拒否、許可）を行い、どのユーザーに適用し、いつ（時間）、そのルールを適用するかを設定します。




ルールの有効・無効の切り替え

Rule Name（ルール名）、Rule result（ルールが一致した場合の動作）

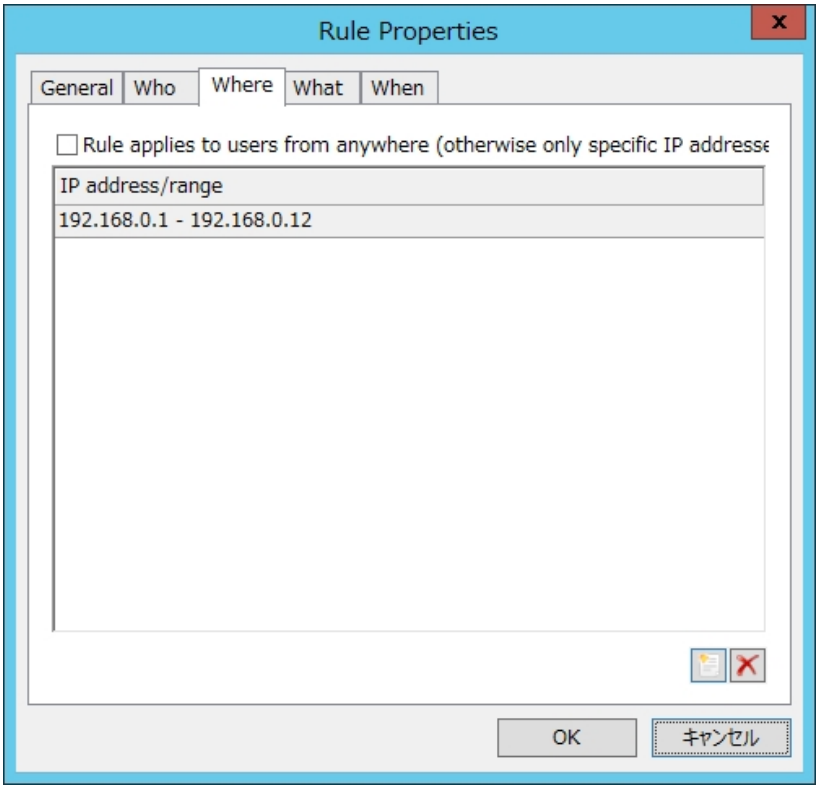



ルールを適用するユーザー、グループの選択

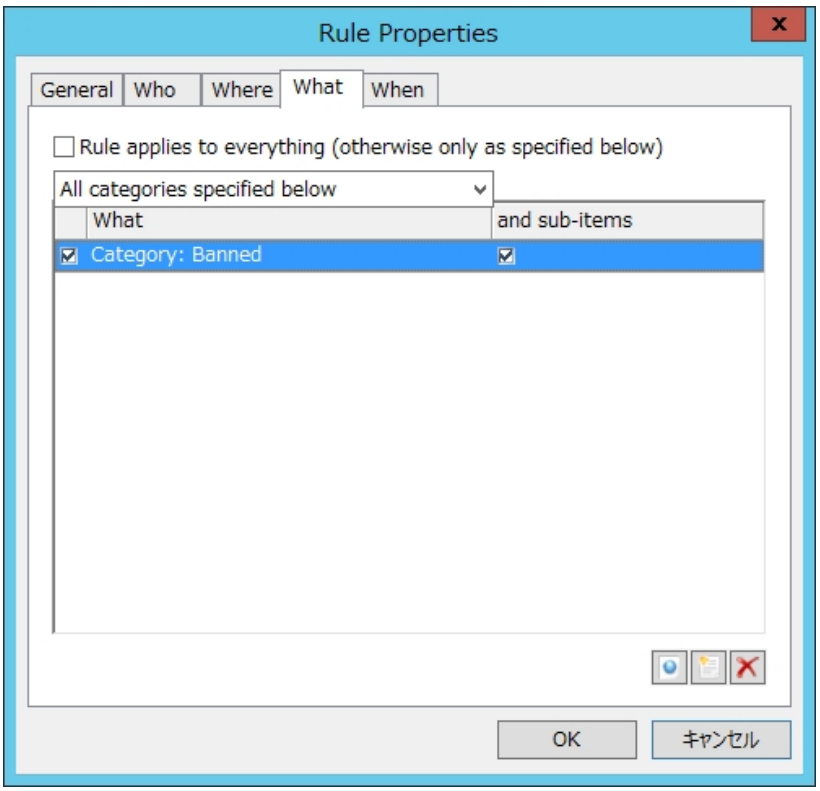
Rule applies to everyone（ルールを全員に適用）を選択した場合は全てのユーザーに適用されます。

All users specified below では、下で指定されたユーザーに、ルールが適用されます。

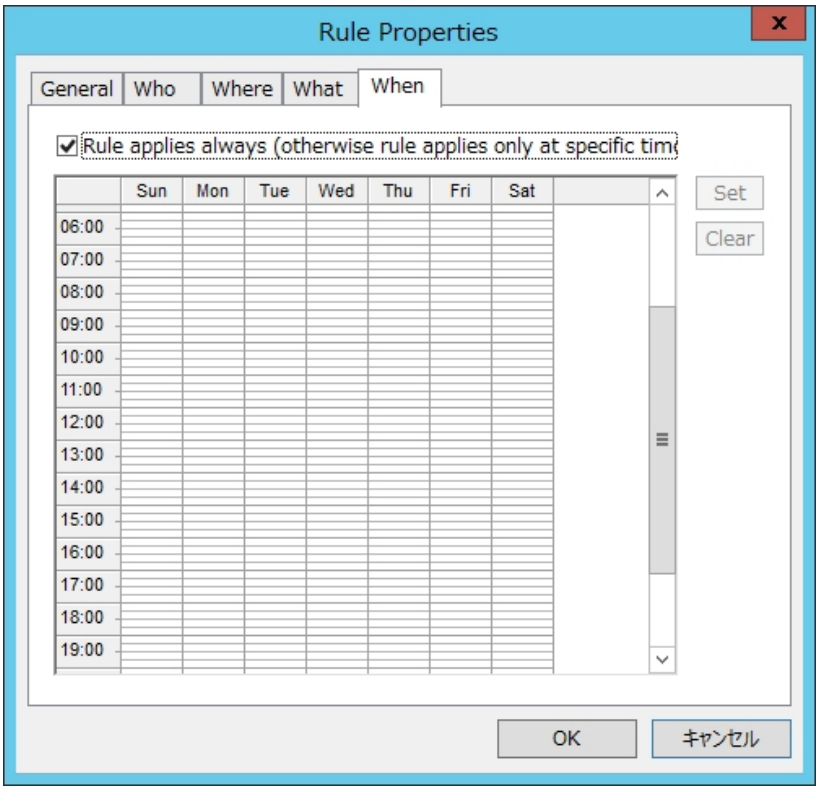
Everyone except users specified below では、以下で指定したユーザー以外にルールが適用されます。




ユーザーのロケーションを指定することができます。

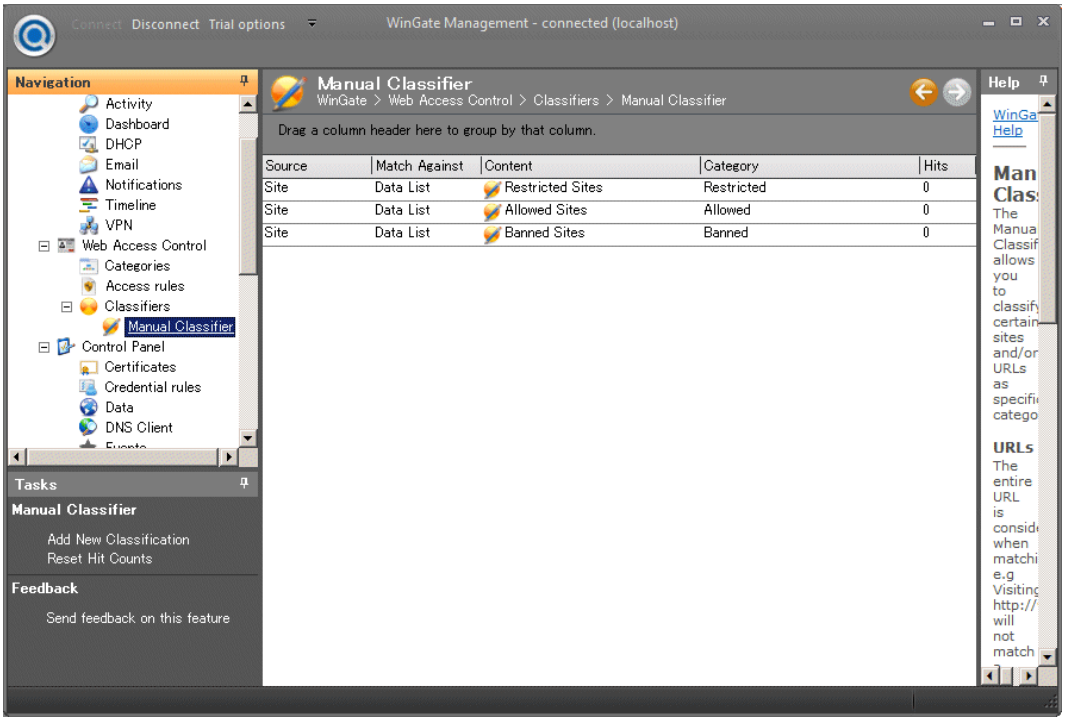



ルールを適用するカテゴリーを選択します。



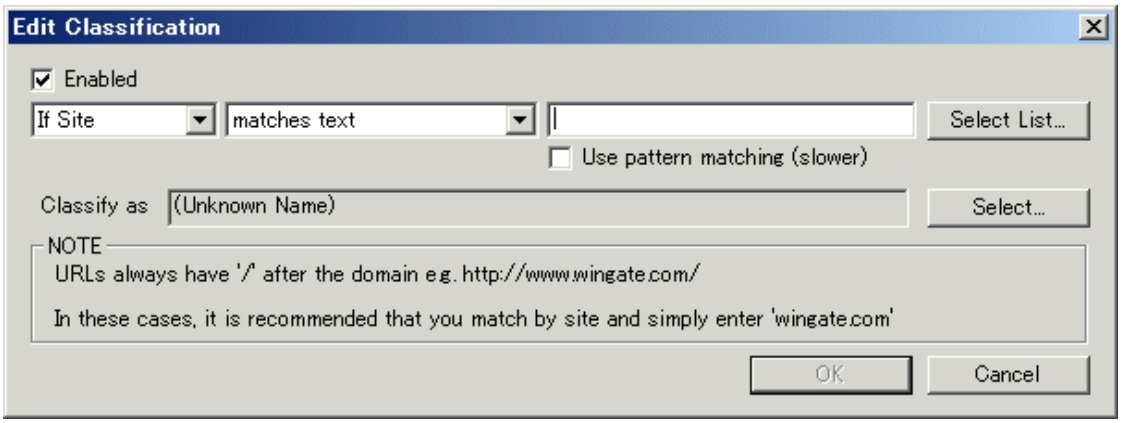

ルールが適用されるスケジュールを選択することができます。

◆ Classifiers（分類）




ここでは、手動で分類を作成、変更することができます。

既存の Classifiers、または Tasks で Add New Classification を選択すると、分類を作成・編集することができます。



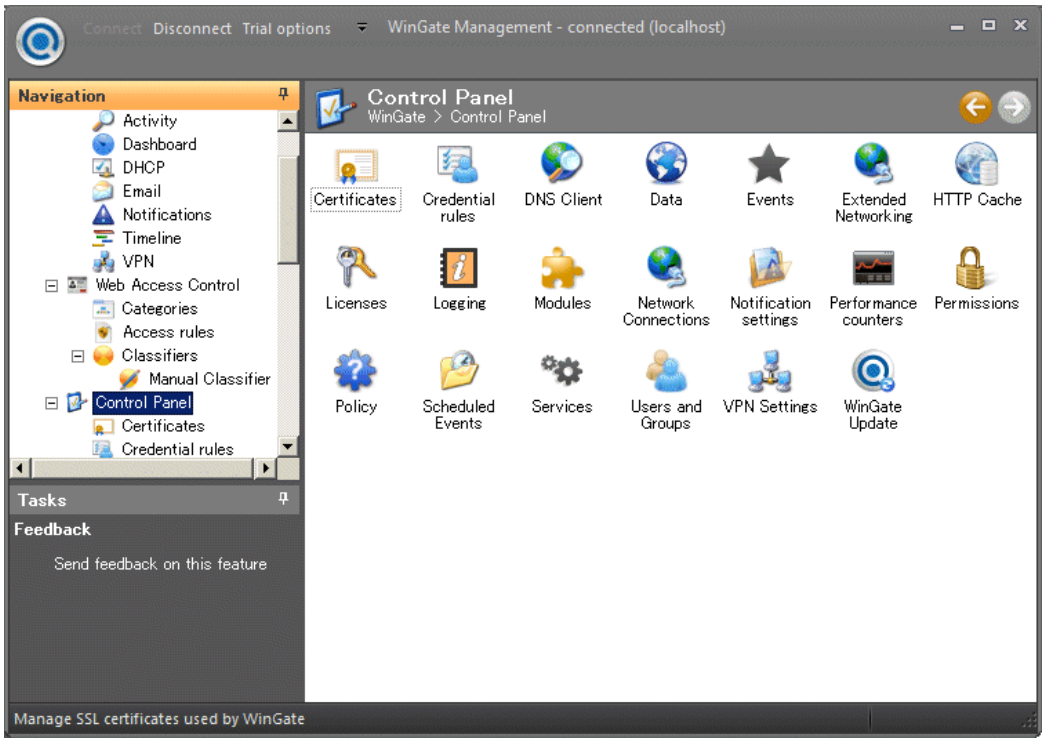

Classification（分類）は、Site（サイト）、URL から選択できます。

また、右側の欄に直接サイト、および URL を記述する。または WinGate の Data からリストを選択することもできます。

Classify as で適用する Categories（カテゴリー）を選択する必要があります。

### Control　Panel（コントロール・パネル）

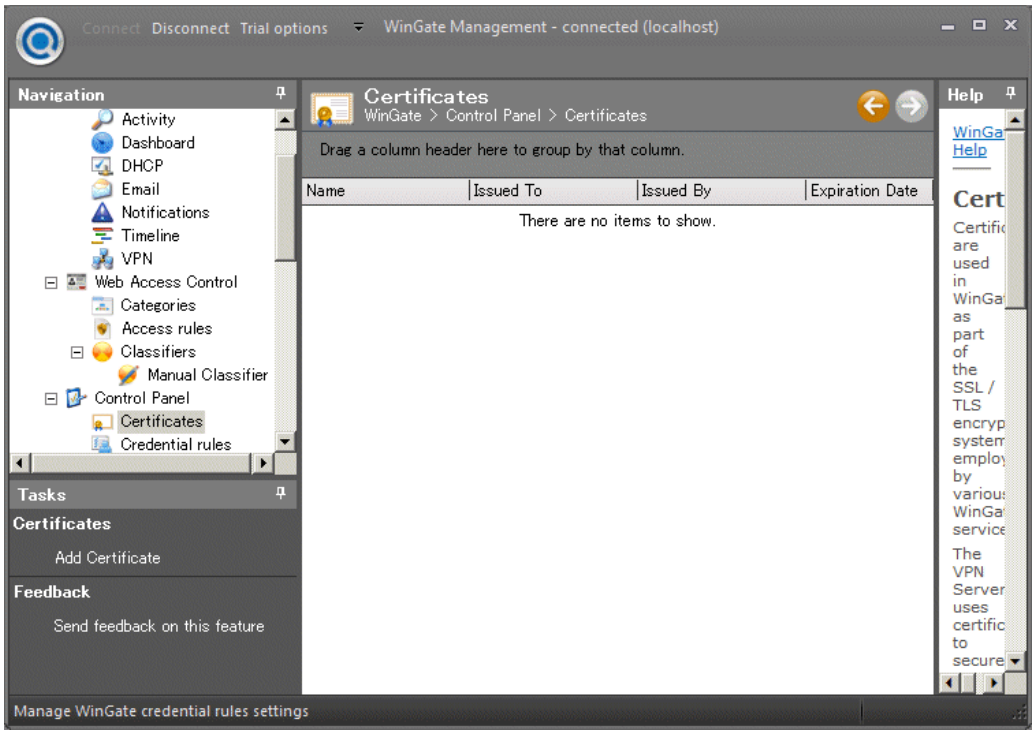
Control　Panel では、WinGate の中心となる様々な設定を行うことができます。




Control　Panel　に表示されるアイコンをクリック、またはツリー表示されている項目をクリックすると、各項目を設定することができます。

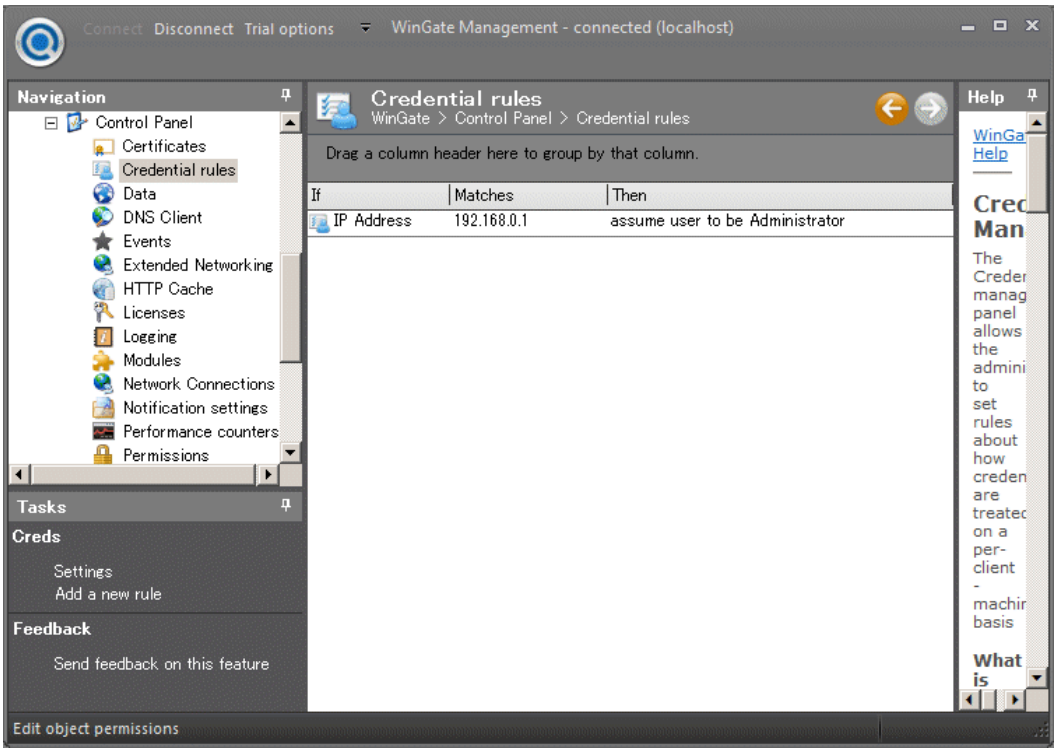
Control　Panel は、以下の内容を含みます。

### Certificates（証明書）




Certificates では、WinGate 内、WinGate VPN で使用されるサーバー証明書を作成、管理することができます。必要に応じて、Add Certificate より証明書を作成してください。

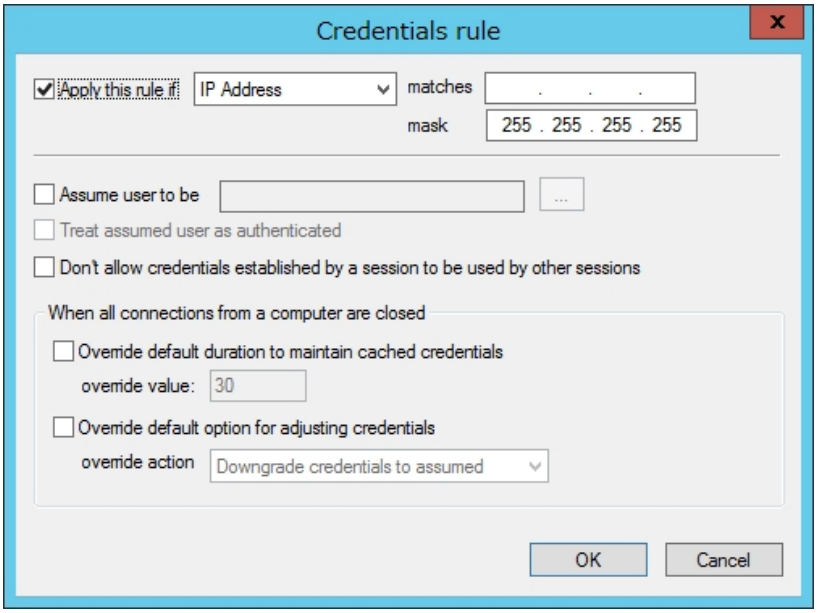
**Credential　rules（信任ルール）**




IP アドレス、マシン名（Computername）、MAC Address（Physical address）とユーザーの関連づけを設定することができます。（以前の WinGate バージョンでは、ユーザーの仮定）

Tasks で Add a new rule（新規ルールの追加）をクリックすると、新しいルールを作成することができます。

編集するルールを選択し、Settings をクリックすると、既存のルールを変更することができます。




Apply this rule if （このルールを次へ適用）で、仮定の際に適用する条件を選択し「matches」（一致）の欄に値を入力してください。

（※MAC アドレスは 00 00 00 00 00 00 00 00 の形式で記述する必要があります。また、Computername を使用する場合は、WinGate の DHCP Service により IP アドレスが割り当てられている必要があります。）

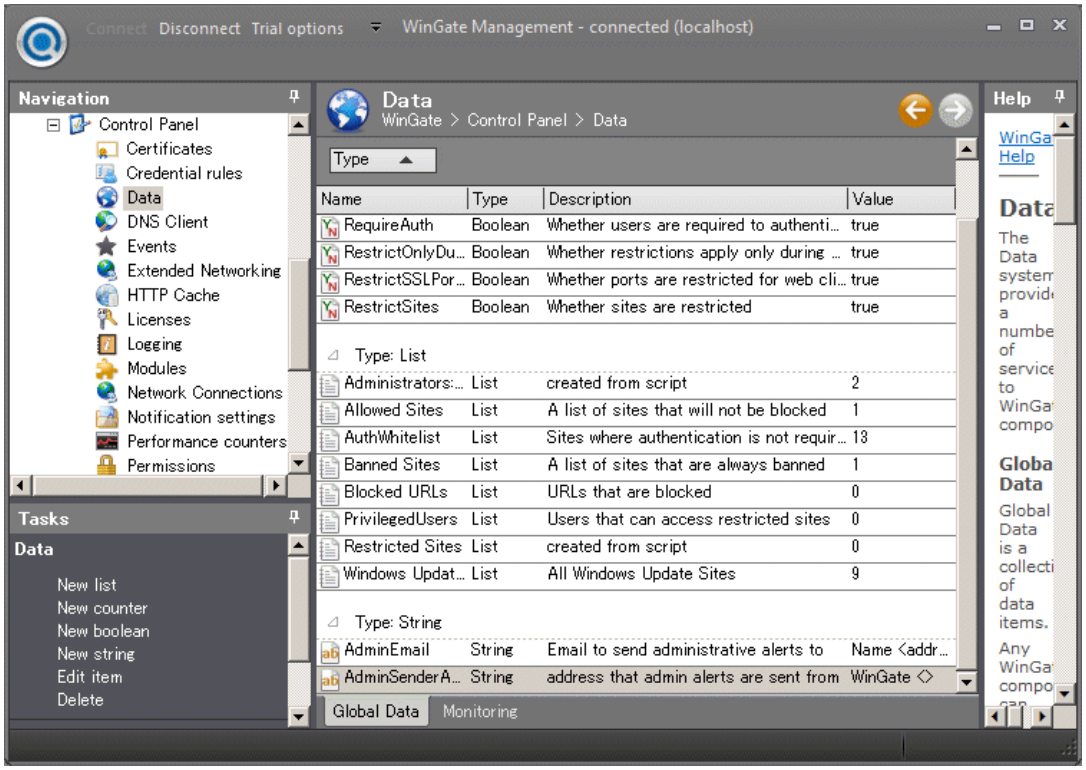
Assume user to be（次のユーザーとして仮定）欄、その条件に一致した場合に仮定するユーザーを選択します。

（右側のボタンよりユーザーを選択することができます。
その他の項目は以下の通りとなります。
Don’t allow credentials established by a session to be used by other sessions（他のセッションによって使用されたセッションを確立された信任として許可しない）＝この項目を有効にすると、一旦ルールにより信任されたセッションから、他の信任を使用したセッションがあった場合に、同一ユーザーとして扱わず multi users（マルチユーザー）として表示、記録します。同じマシンで異なるユーザーや認証情報を使用する場合などは、このオプションを有効にしてください。
※IP アドレスの指定では、* などのワイルドカードや IP アドレスの範囲を使用することはできません。範囲を使用する場合、mask を指定してください。

**Data（データー）**

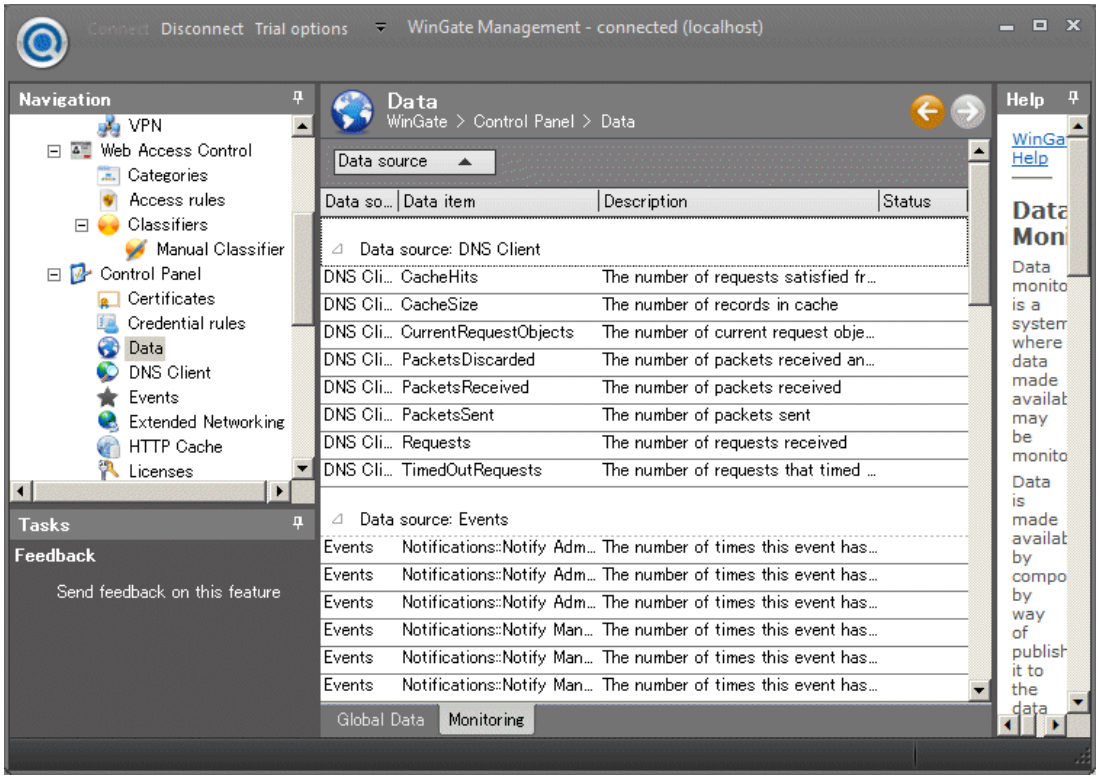
Data は、Global Data と Monitoring の 2 つのタブから構成されています。

Global Data（グローバル・データ）




Global Data では、WinGate 内で使用される Boolean（ブール）、List（リスト）、String（ストリング）を追加、編集、削除することができます。
List では、WinGate のポリシー、プラグイン、Web Access Control で参照されるリストの追加や編集を行うことができます。
また、String では、管理者メールアドレスなどを設定することができます。
必要に応じて、これらの内容を編集してください。

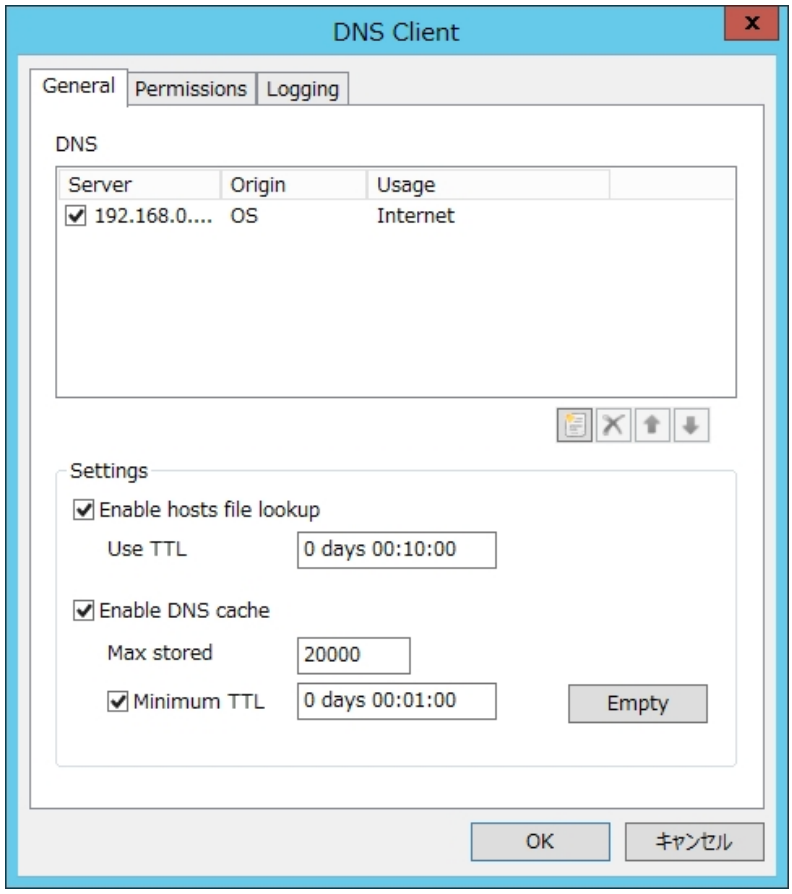
Monitoring（モニタリング）



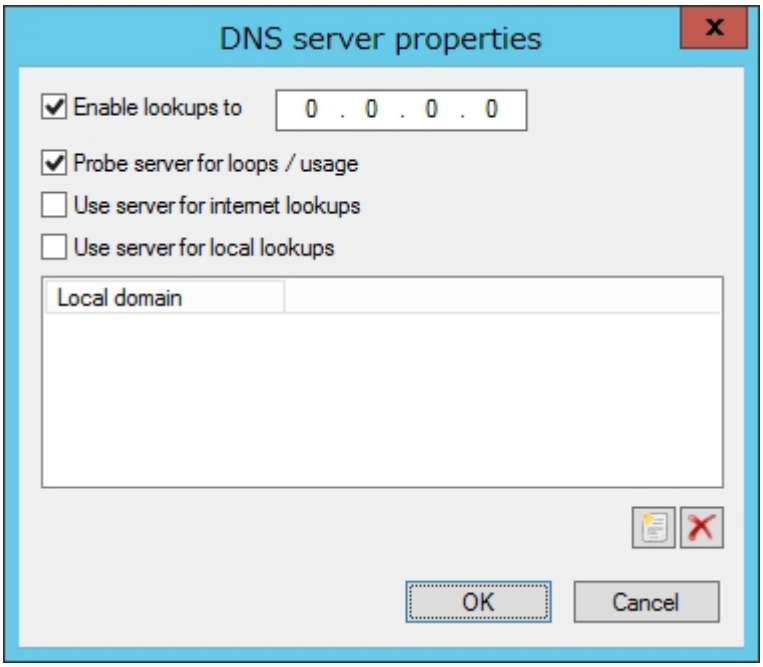

Monitoring では、Dashboard などで使用される WinGate で発生する内容をモニタリングする項目を設定することができます。

必要に応じて、モニタリングする項目の設定を行ってください。

### DNS Client（DNS クライアント）



DNS Client をクリックすると「DNS Client settings」ダイアログが表示されます。
ここでは WinGate が利用する DNS 関連の設定を行うことができます。
DNS Server 欄には、WinGate が名前解決に使用する DNS サーバーが表示されています。デフォルトでは、自動的に Windows の TCP/IP 設定で指定されている DNS サーバーが「Origin」＝「OS」として追加されています。
WinGate サーバーが利用する DNS サーバーを変更、追加する場合は、右下のファイルマークのアイコン（Add a new server）をクリックして新しい DNS サーバーを追加してください。

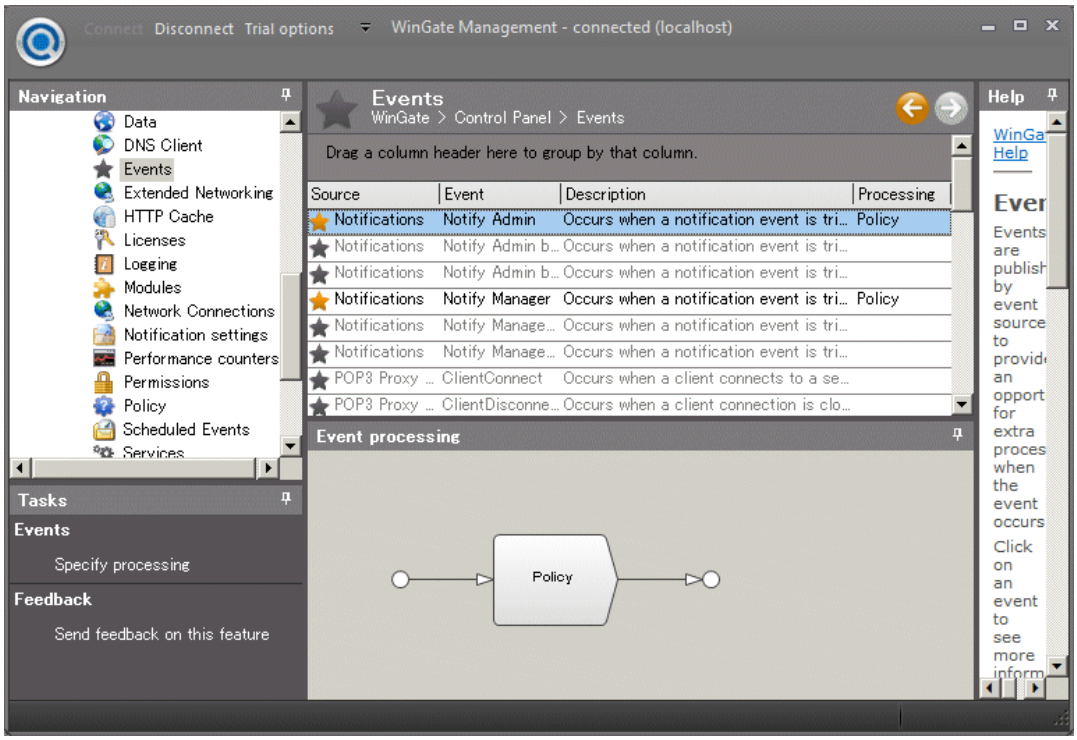



デフォルトで追加されている DNS サーバーは削除することができません。
名前解決に使用する必要がない場合は、左側のチェックボックスをオフにすることで、名前解決にそのサーバーを使用しません。
手動で追加した DNS サーバーは、右下の「×」印のボタンで削除することができます。

Settings では、その他の DNS クライアントの設定を行うことができます。
Enable hosts file lookup を有効にした場合、WinGate は Windows の HOSTS ファイルを参照します。Use TTL の値は、HOSTS ファイルの TEL 値となります。
Enable DNS cache を有効にした場合、WinGate は、メモリに DNS をキャッシュします。「Empty」ボタンでキャッシュされた DNS を削除することができます。Max stored record は、キャッシュに保存する最大レコード数となります。Minimum TTL は、キャッシュするレコードの TTL 最小値となります。

Logging タブでは、DNS Client のログ取得方法を設定することができます。

### Event（イベント）

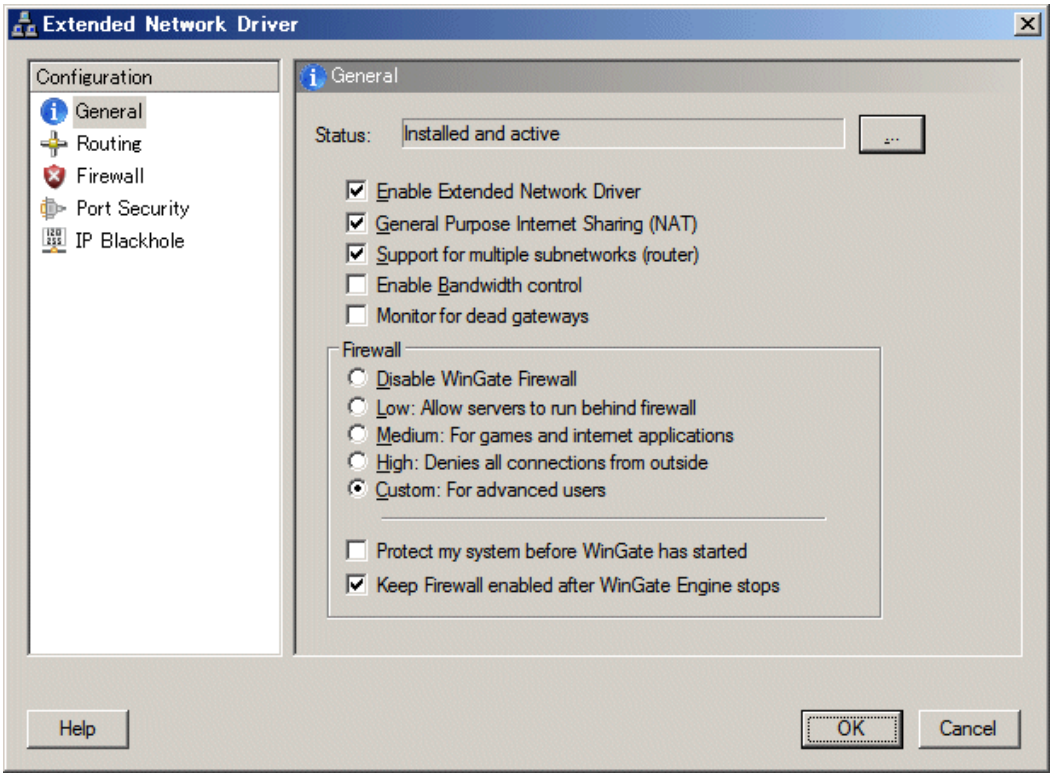



Event では、WinGate で発生するイベントを設定することができます。

WinGate は、WinGate で発生するイベントに基づき様々な動作を実行するように設計されています。

WWW Proxy Server へのクライアントからの接続も、そのイベントの一つです。ポリシーや他の設定でどのようなイベントが使用されているかなどにより、Event の項目は自動的に有効になります。また、Event 単体でもメール配信などの動作を行うことができます。

### Extended Networking（拡張ネットワーキング）



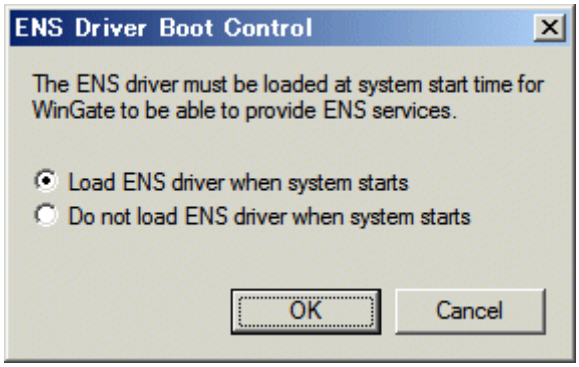

Extended Networking は、インストールいただくことにより、以下の機能を持ちます。

NAT（汎用インターネット共有）
ファイアウォール
ポートセキュリティ
IP ブラックホール

Extended Networking 機能を必要としない場合、インストール時に Extended Networking をインストールしないことを選択することができます。
また、一旦インストールした後でも、全般の「Status」欄、右横にあるボタンで、Extended Networking ドライバーをロードしない設定とすることもできます。
Extended Networking は Windows のシステムドライバとして動作するため、一部の設定を反映するためにマシンの再起動を必要とする場合があります。

各設定画面は、以下の設定を持ちます。

**General（全般）**
全般では、ENS の基本的な設定や状態を確認することができます。
設定は以下の通りです。
Status（状態）
Extended Networking ドライババの状態を表示します。「Installed and active」である場合、インストールされ有効であることを意味します。右側のボタンで ENS の起動状態を設定することができます。




Load ENS driver when system starts　＝システム開始時に ENS ドライバーをロード
Do not load ENS driver when system starts　＝システム開始時に ENS ドライバーをロードしない
ブートコントロール変更後は、マシンを再起動してください。

Enable Extended Network Driver（拡張ネットワークドライバを有効にする）
ENS 機能の有効、無効を選択してください。無効とした場合、ENS に関連した機能は全て使用することができません。

General Purpose Internet Sharing（NAT）
NIC2 枚以上の構成で、内部側インターフェースで NAT 機能を有効とします。
NAT 機能を使用した場合、デフォルトゲートウェイに WinGate の内部側 NIC を持つクライアント PC は、プロキシ設定などを行うことなく、NAT 機能によりインターネットへアクセスできます。

Support for multiple subnetworks(router) （複数サブネットワークのサポート（ルータ））
ルータのように複数のサブネットワークをサポートする場合は、有効としてください。

Enable Bandwidth control（帯域幅制限を有効）
帯域幅制限を使用する場合は、有効としてください。有効とすると ENS の設定画面に帯域幅制限が現れ、設定することが可能となります。

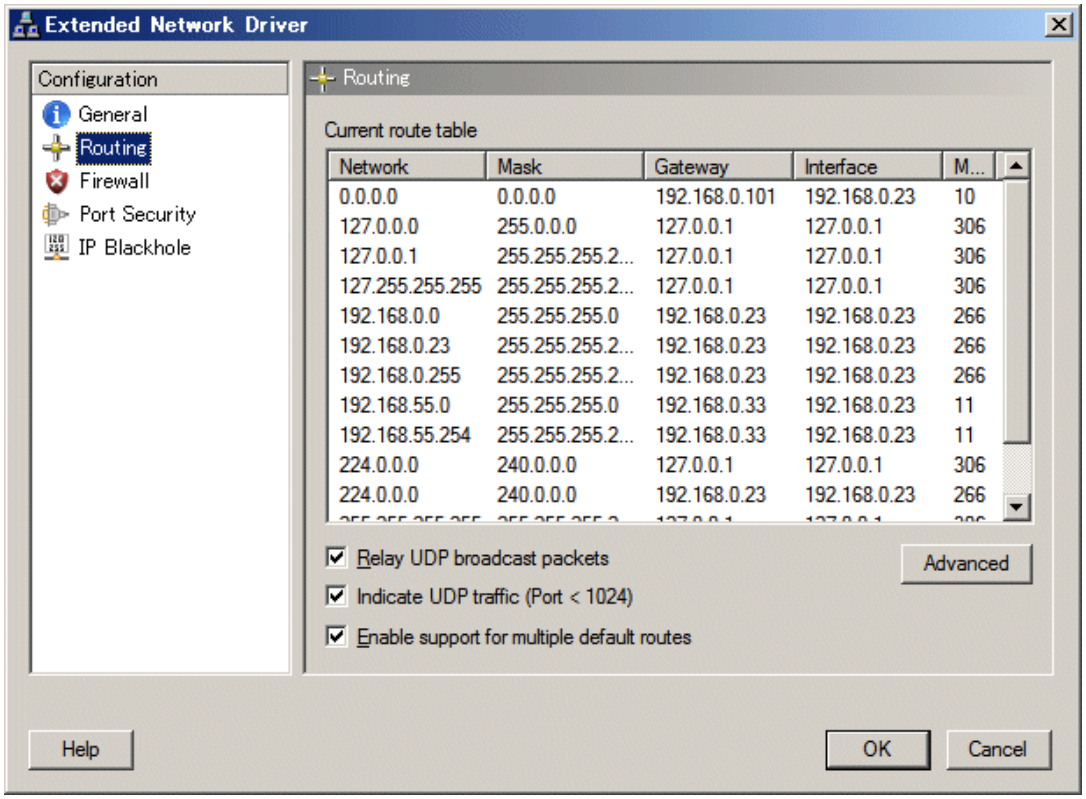
Monitor for dead gateways（無効なゲートウェイをモニター）
無効なゲートウェイを WinGate が監視する場合は、有効としてください。

Firewall（ファイアウォール）
ファイアウォールの基本的な状態を選択することができます。
インターセプト・プロキシや手動でポートセキュリティを設定した場合は、カスタムが選択されます。これらの設定がされている場合は、設定を変更しないでください。

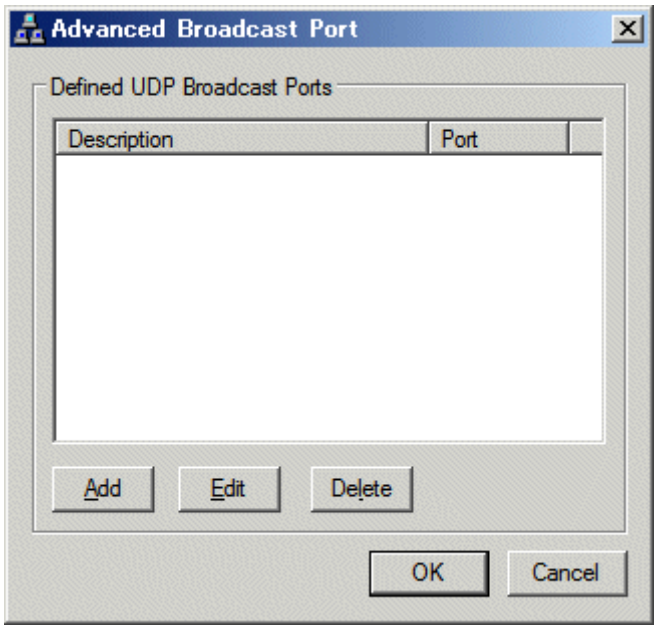
Protect my system before WinGate started（WinGate が開始する前にシステムを保護する）
マシンの再起動時などに WinGate エンジンが開始するまえに、ファイアウォール、ポートセキュリティの内容に基づきマシンを保護する場合は、この設定を有効としてください。

Keep Firewall enabled after WinGate Engine stops（WinGate エンジン停止後もファイアウォールは有効とする）
WinGateエンジンが停止した状態でもファイアウォールの設定を有効する場合は、この設定を有効としてください。（デフォルトは有効）

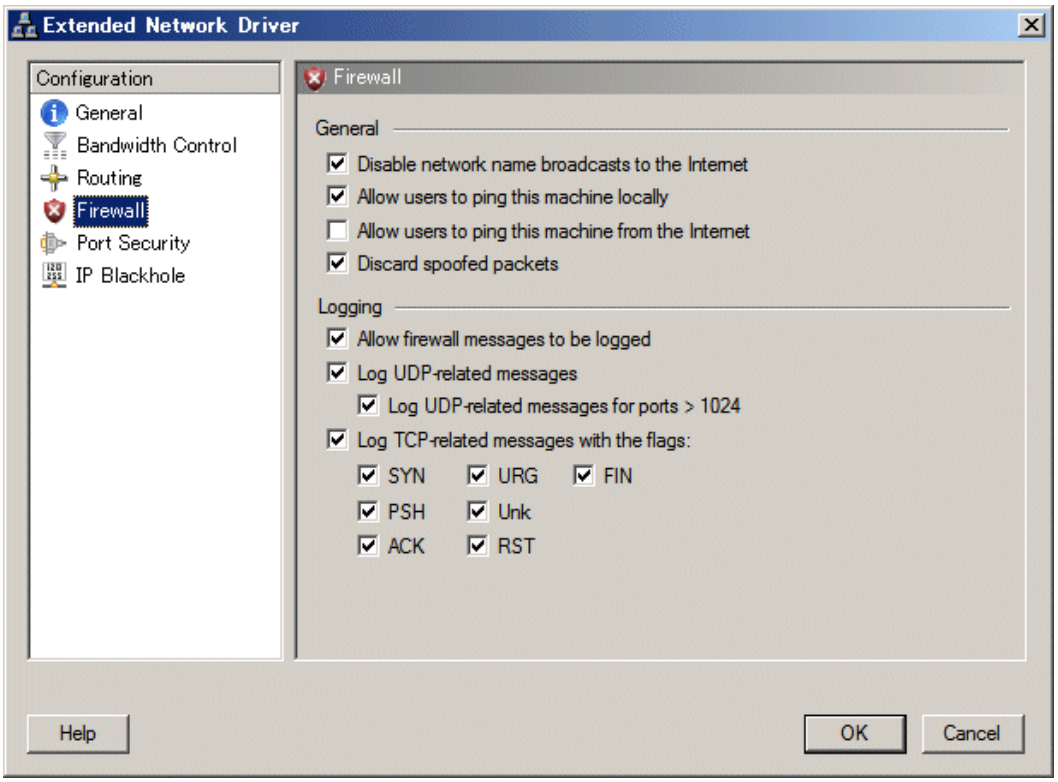
**Routing（ルーティング）**




ルーティングには、WinGate マシンが持つルーティングテーブルの情報が表示されます。
必要に応じて各種の設定を選択してください。
詳細ボタンにより「詳細ブロードバンドポート」ダイアログを表示することができます。



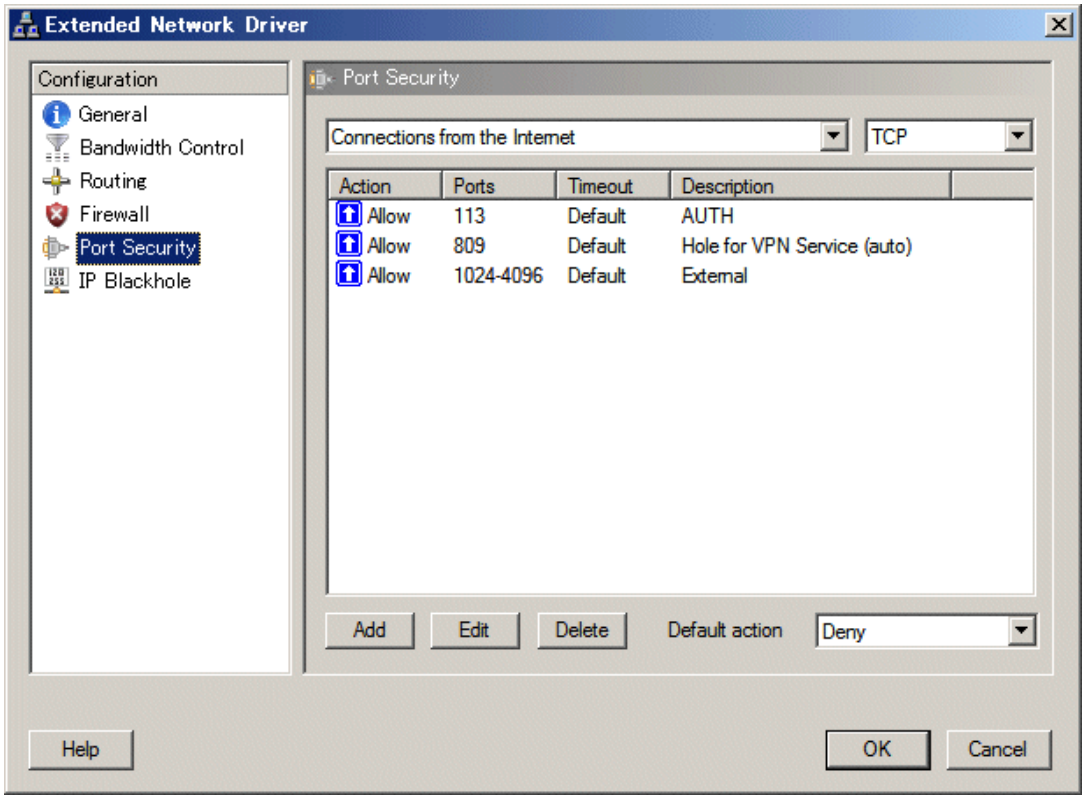

**Firewall ファイアウォール**




ファイアウォールでは、ENS のファイアウォール機能に関する設定を行うことができます。
ファイアウォールは、以下の設定を持ちます。

- Disable network name broadcasts to the internet（インターネットへのネットワーク名のブロードキャストを無効）
  チェックした場合、インターネットへネットワーク名を送りません。
- Allow users to ping this machine locally（ローカルマシンからの Ping を許可）
  チェックされた場合、ローカルマシン（WinGate の内部側のネットワークに属するマシン）から、WinGate への Ping を許可します。
- Allow users to ping this machine from the Internet（インターネットからの Ping を許可）
  チェックされた場合、インターネット（WinGate の外部側ネットワークへ）から、WinGate への Ping を許可します。
- Discard spoofed packets（なりすましパケットを破棄）
  有効にされた場合、なりすましパケットを破棄します。

**Port Security（ポートセキュリティ）**




ポートセキュリティでは、WinGate サーバマシンのポートに対するアクセスに関して様々な設定を行うことができます。これによりインターネットから WinGate マシンの不必要なポートへのアクセス拒否、またはポートリダイレクト、インターセプト・プロキシの関する設定なども確認することができます。
ドロップダウンメニュー（規定アクションを除く）を選択すると、設定されている内容が下の欄に表示されます。

プロキシサーバーなど WinGate のサービスやサーバーで設定された内容は（Auto）として、自動的にポートセキュリティに追加されます。（バインド設定で外部インターフェースにバインドした場合は、インターネットからの接続に自動的に対象となるポートへの接続を許可する内容が追加されます。自動追加された内容はバインド設定変更により自動的に変更、削除されます。）

各選択項目は以下の意味を持ちます。

- **接続の選択**
  最上部のドロップダウン・メニューでは、ポートセキュリティを適用する接続を選択することができます。
  - **Connection from the Internet（インターネットからの接続）**
    インターネット（WinGate で外部として設定されているネットワークインターフェースへの接続）から WinGate PC への接続
  - **LAN　connection to WinGate PC（WinGate PC への LAN 接続）**
    ローカルエリア（WinGate で内部として設定されているネットワークインターフェースへの接続）から WinGate PC への接続
  - **LAN Connection to Internet（インターネットへの LAN 接続）**
    ローカルエリアからインターネットへの接続（トランスペアレントなどに使用されます。）
  - **Connections from the internet to DMZ computers（インターネットから DMZ コンピュータへの接続）**
    インターネットから DMZ（WinGate で DMZ として設定されているネットワークインターフェース

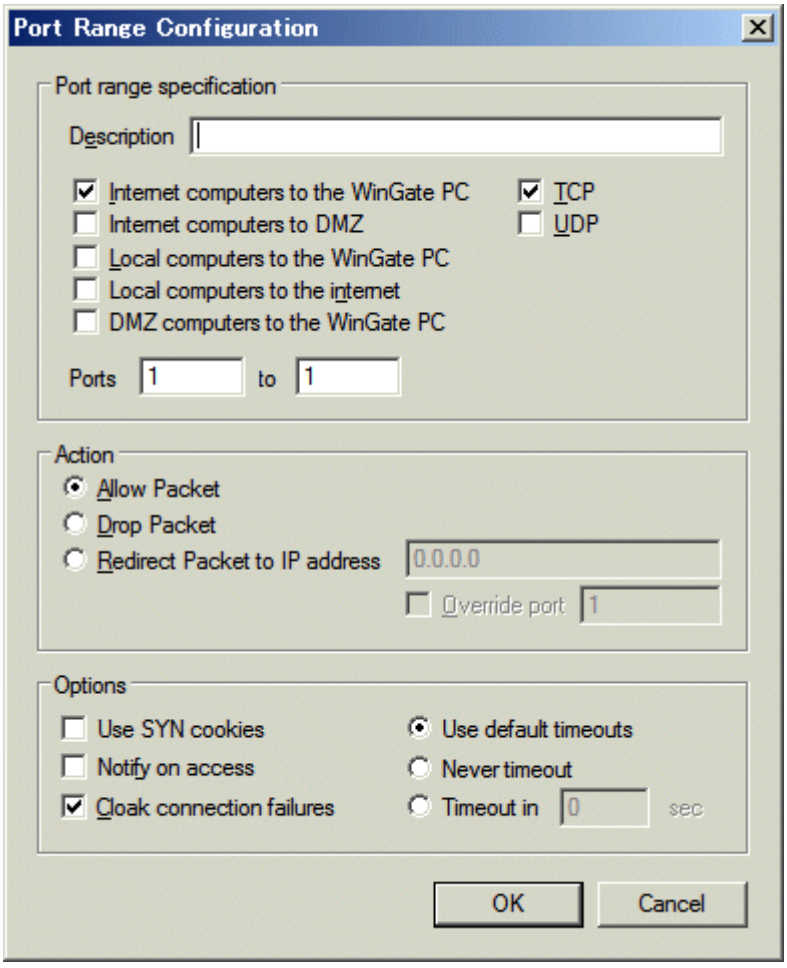
への接続）への接続

- **Connections from DMZ computers to the WinGate PC（DMZ コンピュータから WinGate PC への接続）**
  DMZ 上のコンピュータから WinGate PC への接続

- **プロトコルの選択**
  TCP ・ UDP を選択してください。

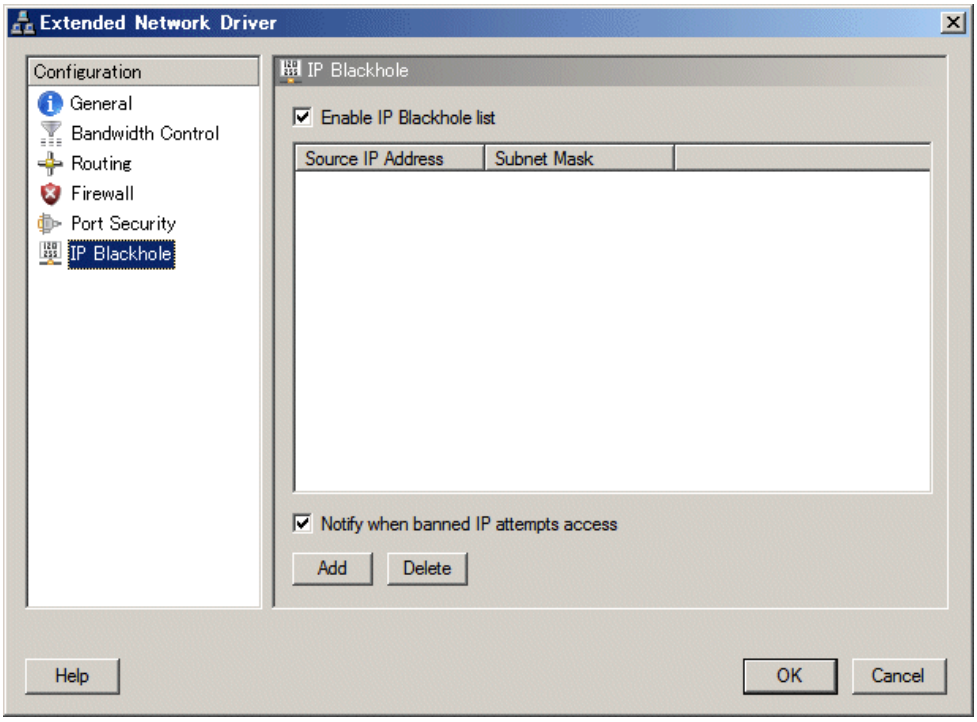
- **Default action（規定アクション）**
  規定アクションでは、選択した接続・プロトコルに対する全体的な動作を選択することができます。
  「許可」を選択した場合は、全てのポートがオープンされるため、インターネットなど外部からの接続に対して不要なポートへのアクセスを許可しない場合、Deny「拒否」を選択してください。

ポートセキュリティは手動で追加することもできます。手動で追加する場合は、Add「追加」ボタンをクリックして Port range specification「ポート範囲の構成」ダイアログを表示してください。




追加する内容に合わせて各項目を選択、入力してください。追加された内容は、ポートセキュリティに表示されます。

**IP ブラックホール**

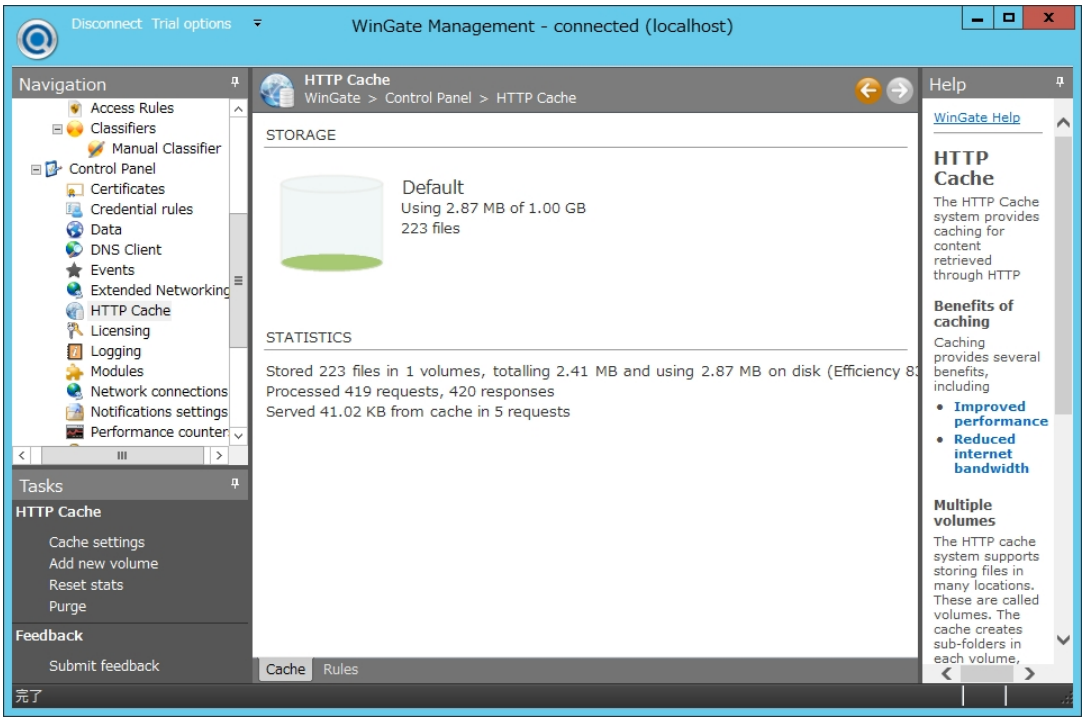



IP ブラックホールでは、特定の IP がお客様のネットワークに侵入する事を禁止する事ができます。

追加ボタンをクリックします。表示されるダイアログで、アクセスを禁止する IP を入力し OK をクリックします。この方法では IP アドレスの範囲による追加を行う事もできます。
注意:ドライバーでこれらの IP がないか確認するために、IP ブラックホールを有効リストボックスがチェックされている事を確認してください。この確認がされていない場合、ブラックホールのリストにある IP が、ネットワークに許可されているかもしれません。

もう一つの方法は WinGate Management（Activity）で禁止することを望む IP を突き止め、その IP を右クリックして、「 Blackhole IP # 」選択する事により、その IP を IP Blackhole タブの禁止されたリストに追加します。
注意:この方法を試用する場合、お客様のネットワーク自身の IP のいずれも禁止しないように注意してください。

### HTTP Cache（HTTP キャッシュ）




HTTP Cache 機能は、WWW Proxy Server で利用される HTTP コンテンツをキャッシュします。これは WinGate8 で大幅に機能変更されました。

HTTP Cache は、Cache と Rules の 2 つのタブから構成されています。

**ご注意：**WinGate6、WinGate7 よりアップグレードした場合、既存のキャッシュ情報、キャッシュボリュームは全て削除されます。

#### Cache タブ

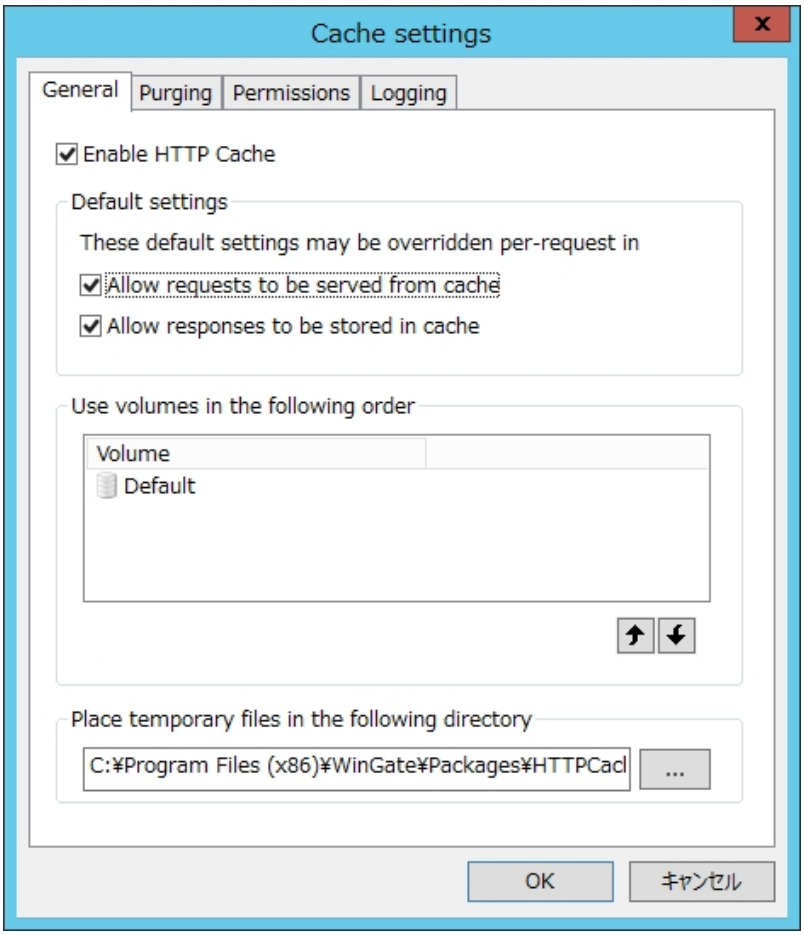
HTTP Cache ウインドウでは HTTP Cache に関する幾つかの情報が表示されます。

STORAGE（ストレージ）には、キャッシュボリュームの現在の状態が表示されています。
表示内容は、ボリューム名、使用量、フォルダー構成となります。
STATISTICS には、キャッシュ状況の統計情報が表示されています。

Tasks では、HTTP Cache に関する設定を行うことができます。

**Cache settings**

**General**（全般）




**Enable HTTP Cache**（HTTP キャッシュを有効）＝チェックをオフにした場合、HTTP Cache 機能は無効になります。

Default Settings

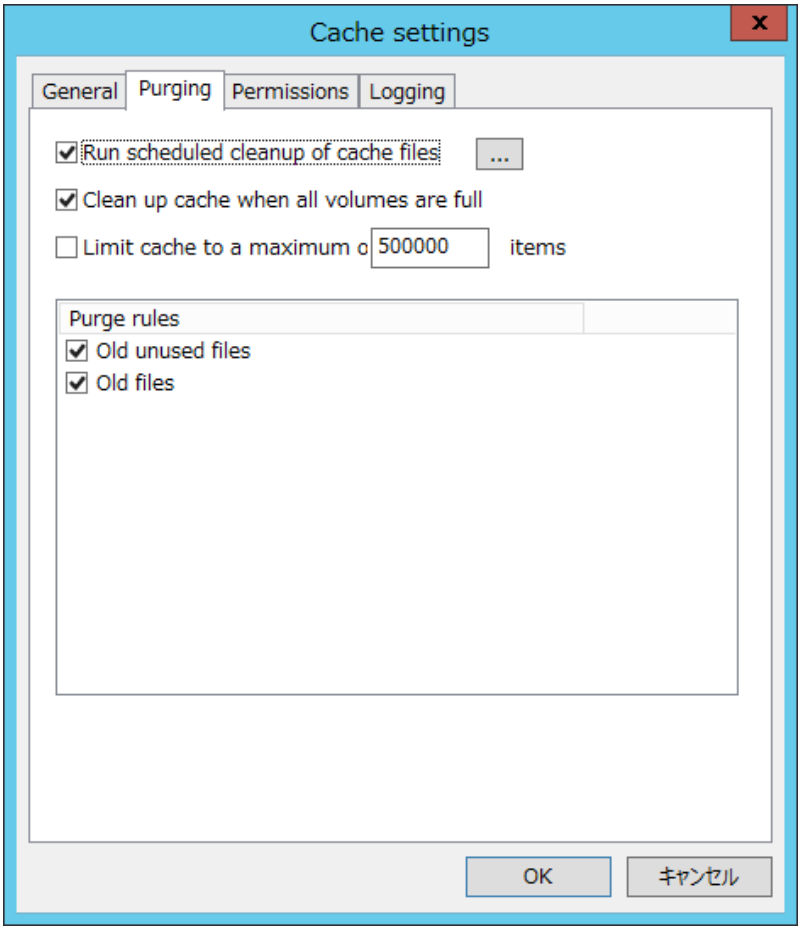
Allow requests to be served from cache（キャッシュへの保存を許可）

Allow responses to be stored cache（保存されたキャッシュからの応答を許可）

Use Volume in the following order では、複数のボリュームを持つ場合に、使用されるボリュームの優先順序を右下の矢印により変更することができます。

Place temporary files in the following directory では、キャッシュにしようされる一時ファイルの場所を変更することができます。

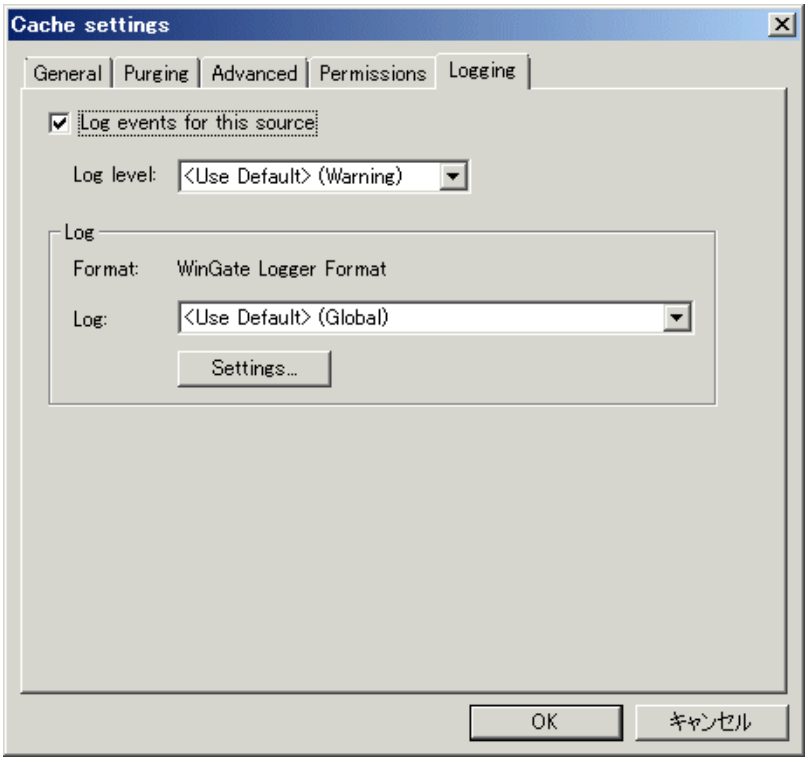
Purging（パージ）




Purging では、どのようにキャッシュのパージ（削除）を行うかを設定することができます。
Run scheduled cleanup of cache files（キャッシュファイルのクリーンアップスケジュールを実行）＝有効にした場合、Scheduled Event で設定されたスケジュールにより、下の Purge Rules の基準に従いキャッシュをパージします。右側のボタンにより、パージするスケジュールを変更することができます。
Clean up cache when full（満杯時にキャッシュをクリーンアップ）＝キャッシュボリュームが一杯になった際にパージします。
Limit cache to a maximum on XXXXXX itemes＝キャッシュファイルの最大数を設定することができます。

Purge Rules（パージ・ルール）では、パージする際の条件を選択できます。
Old unused files（使用されない古いファイル）・Old files（古いファイル）

Logging（ロギング）



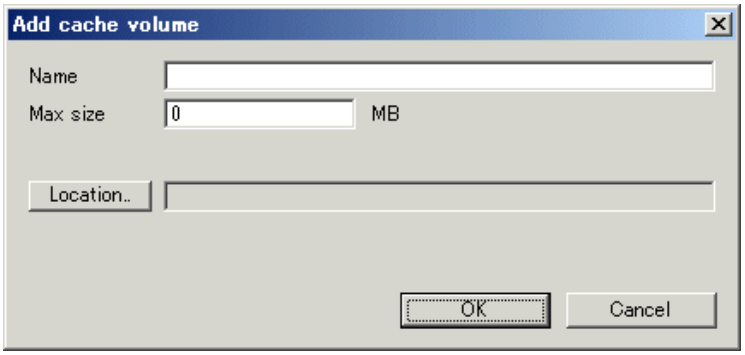

Logging では、HTTP Cache に関するログの取得方法を設定することができます。

**Add new volume**（ボリュームの追加）

Add new volume をクリックすると新しいボリュームを追加することができます。（複数のボリュームを作成するには Enterprise 版が必要です。）

ボリュームを削除した後、新しいボリュームを作成する場合にも使用します。

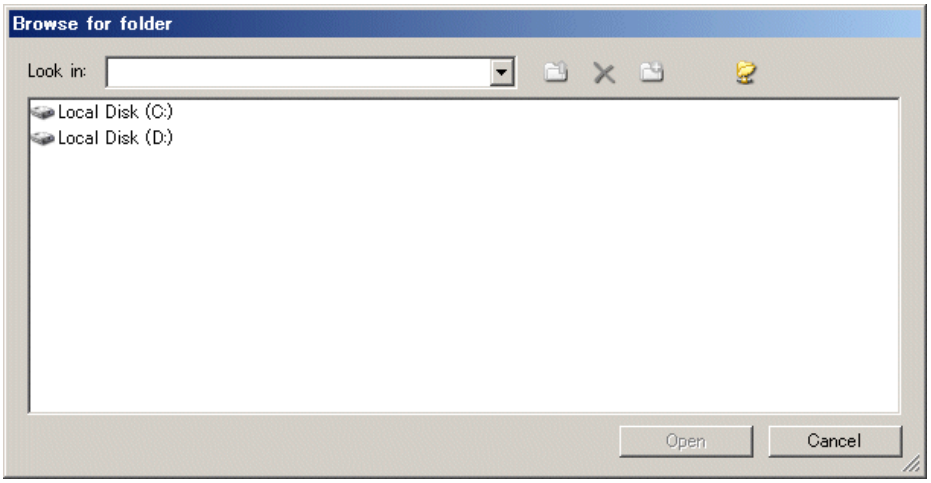
Add new volume をクリックすると Add cache Volume ダイアログが表示されます。




Name へキャッシュボリュームの名前を入力します。

Max size へ作成するボリュームのサイズを入力します。（MB 単位となります。1GB の場合は 1024 となります。）

Location ボタンをクリックしてキャッシュファイルの保存場所を指定します。

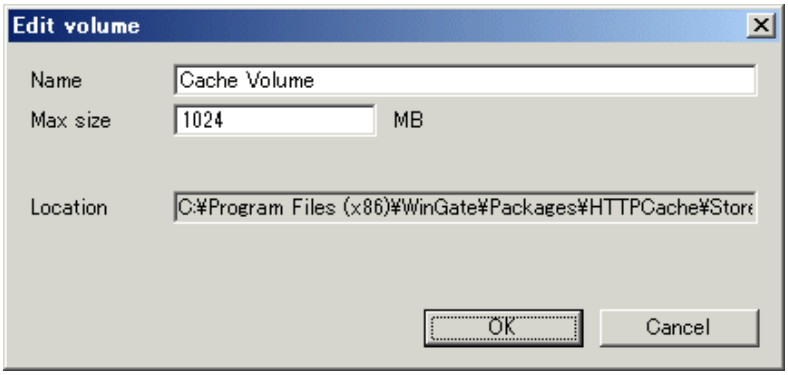



指定が完了いたしましたら OK ボタンで Add cache Volume ダイアログを終了します。
以上でボリュームの作成は終了です。

**Rest statistics**（統計のリセット）
Rest statistics をクリックすると HTTP Cache に記録されている統計情報がリセット（クリア）されます。

**Purge cache**（キャッシュのパージ）
Purge cache をクリックすると Cache settings の Purging ダイアログの条件に従い、キャッシュのパージを実行します。

**Edit volume**（ボリュームの編集）
HTTP Cache ウインドウに表示されているボリュームを選択すると Edit volume メニューが現れ、クリックするとボリュームの設定を変更することができます。




Name では、使用するキャッシュボリュームの名前を変更することができます。
Max size では、使用するキャッシュボリュームのサイズを変更することができます。（MB 単位となります。1GB の場合は 1024 となります。）
Location（ロケーション）には、キャッシュボリュームの場所が表示されます。
※ロケーションを変更する場合には、一度ボリュームを削除し、新たにボリュームを作成する必要があります。

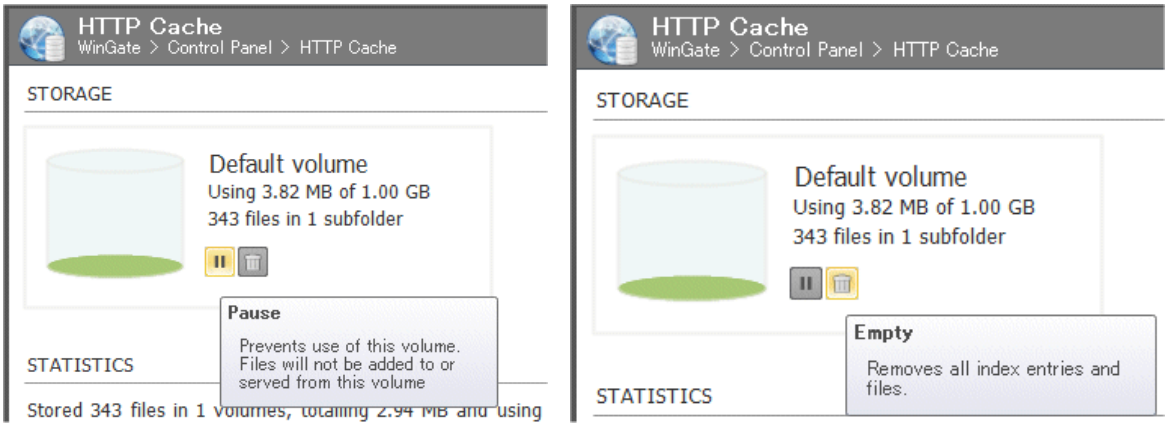
**Delete Volume**（ボリュームの削除）

HTTP Cache ウインドウに表示されているボリュームを選択すると Delete Volume メニューが現れ、クリックするとボリュームを削除することができます。

※ボリューム自体の削除となります。

ボリュームの管理方法

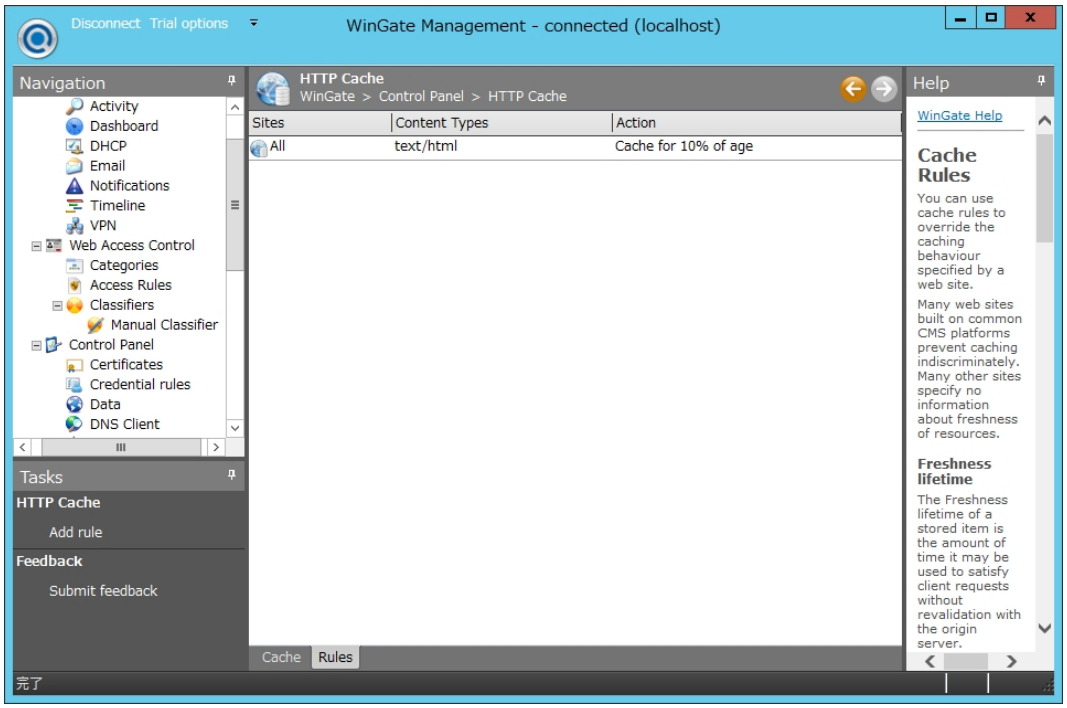
HTTP Cache ウインドウ内に表示されているキャッシュボリューム上にマウスカーソルを移動すると Pause（一時停止）と Empty（空にする）を選択することができます。




Pause をクリックすると、そのボリュームの参照、追加が停止されます。

また、Empty をクリックするとボリューム内のキャッシュファイルが全て削除されます。（データーベースのキャッシュインデックスも削除されます。）

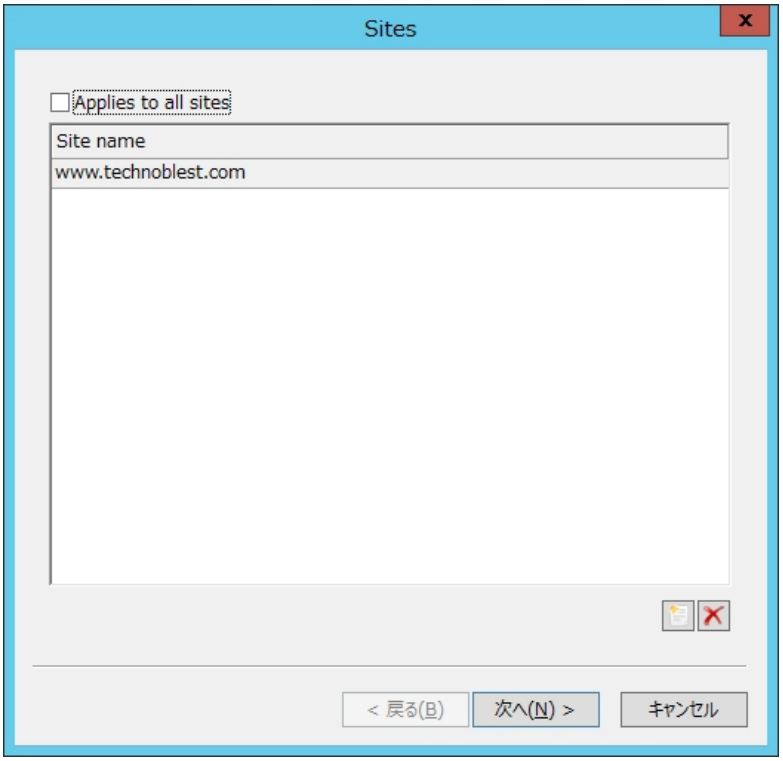
Rules タブ




Rules では、キャッシュするサイト、コンテンツ、ルールの条件、キャッシュしないサイト、コンテンツを設定することができます。

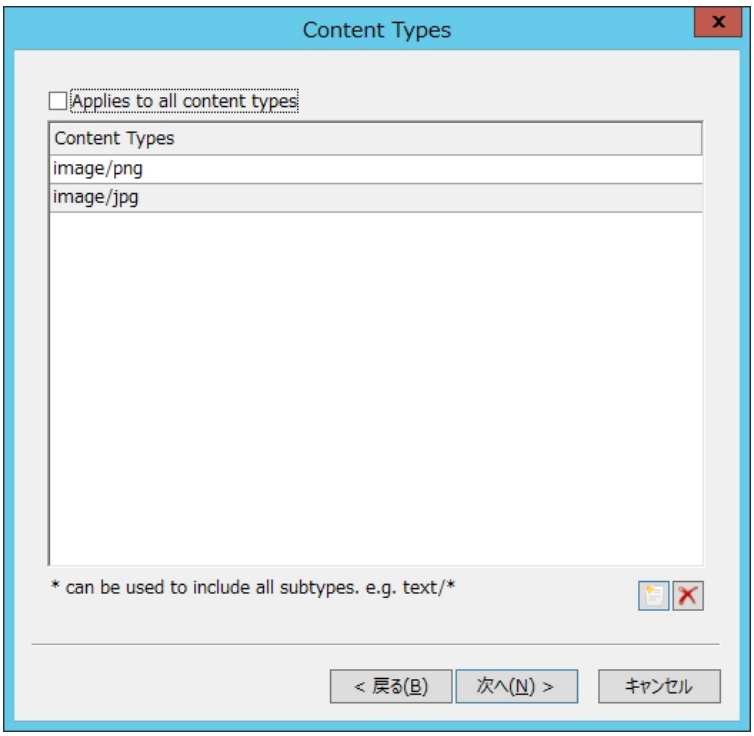
ルールを追加するには、Tasks より Add rule をクリックします。

Site ダイアログ



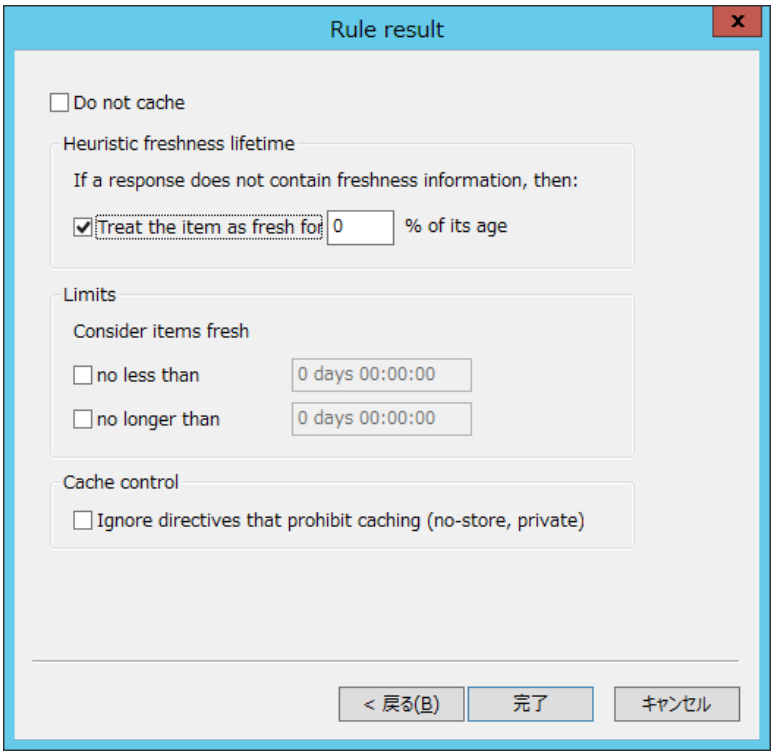

ルールをどのサイトに適用するかを指定します。右下の Add new site ボタンより追加することができます。
Applies to all site をチェックした場合、全てのサイトに対して、このルールが適用されます。
設定が完了いたしましたら次へをクリックします。

Content Types ダイアログ




キャッシュする Content type を指定します。
Applies to all Content types を指定した場合は、全ての Content type をキャッシュします。
設定が完了いたしましたら次へをクリックします。

Rule result ダイアログ




Rule result ダイアログでは、作成するルールの結果を設定します。

- Do not cache
  Do not cache をチェックした場合、指定した Site、Content type をキャッシュしません。これは特定のサイトや特定の Content type をキャッシュさせない場合に有効です。(動画や実行可能ファイルなど大きなファイルをキャッシュすることにより、キャッシュボリュームの使用を削減することもできます。)

- Heuristic Freshness Lifetime
  リソースが、その新しさの期限を(それが、どのくらいの間、キャッシュされて保つことができるか)示す情報が含まれていない場合に、リソースの期限の割合を使用するように選択することができます。

- Limits
  新しいと判断する期限を、一定以上、または最大値を強制することができます。これらの制限は Heuristic Freshness Lifetime を上書きしない場合でも、適用されます。

- Cache control
  このオプションを選択すると、サーバーから送られた応答にいくつかの Cache-Control ヘッダの値を無視します。これは、いくつかの以前にキャッシュ不可コンテンツはその後キャッシュ可能なことがあります。

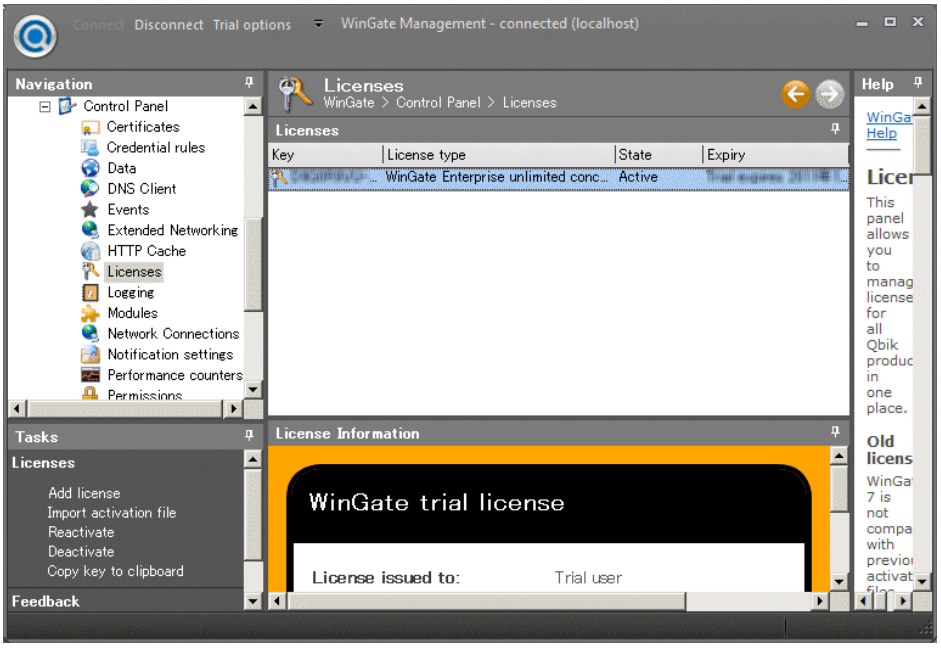
  ご注意:サーバーは通常、データーを非公開にするために、これらの値を設定し、このオプションを変更すると、一人のユーザーのために意図されたリソースがキャッシュの他のユーザーに返されることがありますので注意してください。

**キャッシュ運用のヒント**

WinGate8 のキャッシュシステムでは、キャッシュのインデックスデーターは、指定したボリュームフォルダ内に保存されます。

高速なディスクドライブ、余裕のあるメモリにより、より高速なキャッシュレスポンスが期待できます。また、マシン構成などによる部分もございますが、構成されるボリュームは、より大規模なキャッシュを構築する場合、複数のボリュームを作成いただくことをお勧めいたします。(使用するボリュームのサイズは運用状況などをみながら、環境にあった値としてください。)※作成できるボリューム数は、WinGate の種類により異なります。

## Licensing（ライセンス）




Licensing では、現在登録されている WinGate のライセンスキー情報やアップグレード保証の有効期限の確認、ライセンスキーの登録、各種アクティベーション、試用版の有効期限、オフライン アクティベーションによるファイルのインポートなどを行うことができます。

上部に表示されている登録されたライセンスキー情報を選択すると、下の欄に詳細が表示されます。

**アクティベーションに関係する操作を行った場合には、WinGate の再起動が必要となります。**

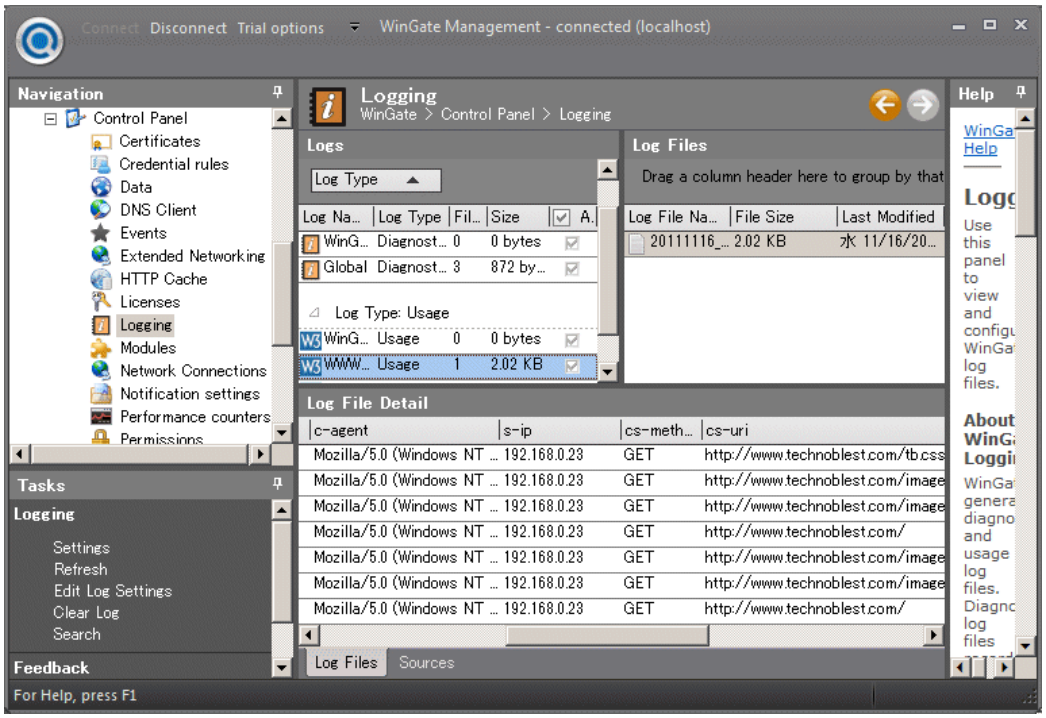
- Add license(ライセンスの追加)
  Kaspersky AntiVirus for WinGate や他のプラグイン、または試用版から正規版へ移行する際など、新たなライセンスを追加する場合に使用します。
- Import activation file(アクティベーションファイルのインポート)
  オフラインアクティベーションで入手したアクティベーションファイルをインポートする場合に使用します。
- Reactivate(再アクティベート)
  アップグレード保証の更新適用など、アクティベーションを再実行する必要がある場合に使用します。
- Deactivate(アクティベート解除)
  アクティベーション情報を解除する場合に使用します。解除後は WinGate の再起動が必要となり、解除した製品は使用できなくなります。
- Copy key to clipboard(クリップボードにキーをコピー)
  クリップボードにキー情報をコピーします。

**Logging（ロギング）**

Logging では、WinGate で保存されているログの参照、および保存されるログの設定変更が行えます。

Logging は、Log file と Sources の 2 つのタブで構成されています。

Log file




Log file タブでは、取得されているログファイルの情報を参照することができます。参照したいログの情報を Logs 内でクリックすると Log File Detail に内容が表示されます。また、Log files で過去のログ情報も参照することができます。

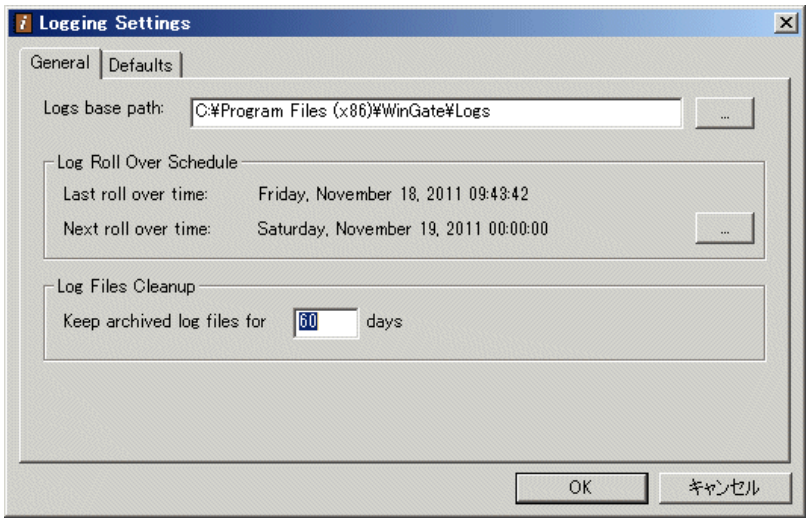
最新のログ情報に更新したい場合は、Tasks の Refresh をクリックすると、最新のログ情報に更新します。

ご注意：Clear log（ログのクリア）をクリックすると Log Files で選択されている日付のログ情報が削除されます。これは、表示だけではなく、ログファイル自体も削除いたしますので操作には十分ご注意ください。

Tasks 内で Search（検索）をクリック、または Log File Detail で右クリックを行い、Search を選択することで、表示されている内容の検索を行うことができます。また、Log File Detail で右クリックを行うことにより、選択したログ情報をクリップボードにコピーすることができます。

Tasks の Settings をクリックすると Log Settings ダイアログが表示されログ全体の設定を行うことができます。

Log Settings は General（全般）と Defaults（デフォルト）の 2 つのタブで構成されています。



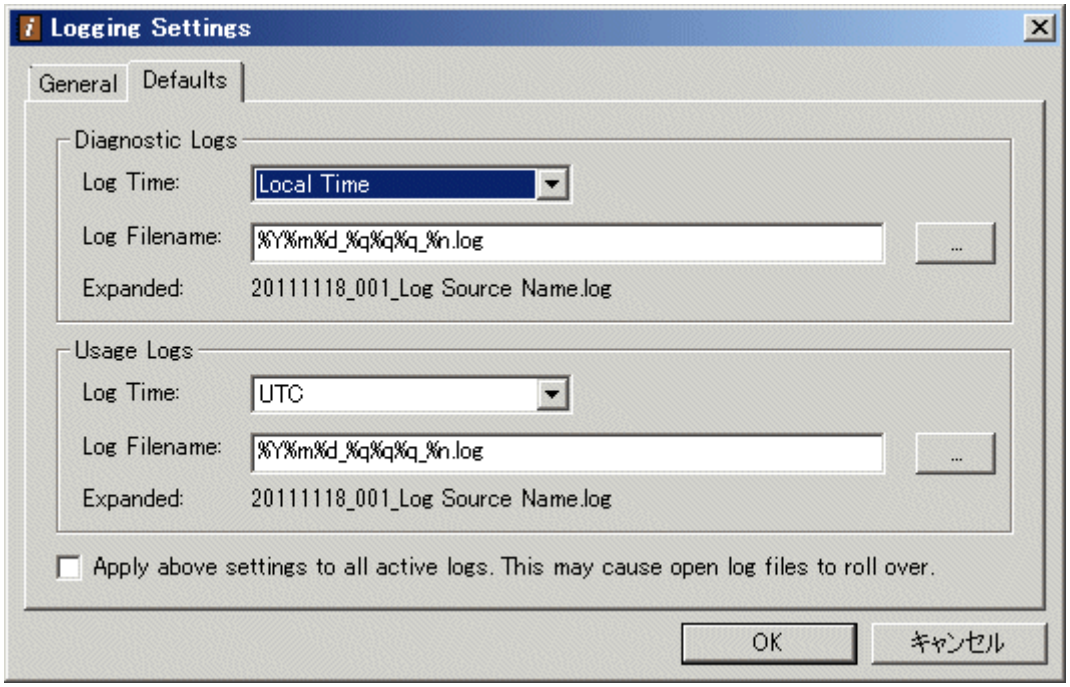

General では、ログファイルのパス、ログローテーションのスケジュール、ログファイルを削除する日数の設定ができます。

Log base path では、ログファイルが保存されるディレクトリのパスを設定することができます。ログファイルの保存場所を変更する場合は、ここでパスを変更してください。右側のボタンをクリックすると Browse for folder ダイアログが表示され、ログフォルダを選択することができます。(変更前のログ情報は自動的に移動されません。)

Log Roll Over Schedule では、ログをローテーションするスケジュールを指定することができます。右側のボタンをクリックすると、スケジュールを変更することができます。デフォルトでは、毎日 0:00 にログをローテーションします。

Log Files Cleanup では、ログファイルを保持する期間を指定することができます。デフォルトでは、60 日間に設定されており、60 日前のログは自動的に削除されます。

**ご注意**:ログ保存期間は、任意に指定する必要があります。(ログを削除しない設定はありません。)最大日数は、32bit の付き整数型の最大値となります。(最大値より少ない任意の期間を指定いただくことをお勧めいたします。)



Defaults では、ログのデフォルト設定として使用される内容を設定することができます。ここで設定された内容が、各ログ情報でデフォルトとして使用されます。

Diagnostic Logs（診断ログ）
Diagnostic Logs は、Sources で Log Type に Diagnostic として表示されている情報の記録方法に関するログとなります。Diagnostic Logs は、主にそのサービスにタイする、エラーや警告を記録します。（変更可能）
Usage Logs は Sources で Log Type に Usage として表示されている情報の記録方法に関するログとなります。Usage Logs は、そのサービスの使用についてのログを記録します。
WWW Proxy Server を例にした場合、エラーや警告は、Diagnostic Logs に記録され、リクエスト内容の詳細は Usage Logs として記録されます。

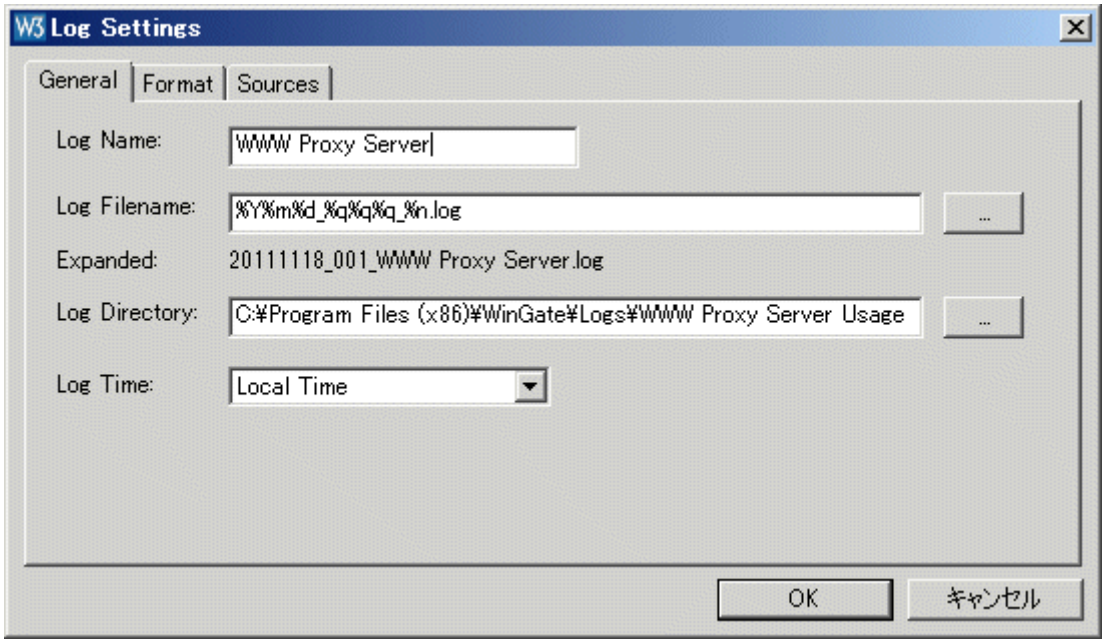
Log Time は記録するログの時刻を変更することができます。選択は、Local Time（ローカル時刻）、UTC（正解標準時）より選択いただけます。
ご注意：Usage Logs はデフォルトで UTC（世界標準時）が設定されています。日本時間でログの時刻を記録したい場合は、Local Time を選択してください。

Log Filename では、保存されるログファイルの先頭に付与される日付時刻のフォーマットを変更することができます。右側のボタンにより、フォーマットを選択することができます。

Apply above settings to all active logs. This may cause open log files to roll over.（設定を全てのアクティブなログに適用する。これは開いているログファイルをロールオーバーします。） ＝ このチェックを有効にして、OK ボタンで大ログを終了すると、変更をすぐに適用します。ログファイルは、ロールオーバー（新たなファイルとして作成されます。）

個々のログ設定の変更
Logs 内に表示されているログ項目をダブルクリックすることにより、個々の内容についてログの取得方法を設定することができます。

WWW Proxy Server の Usage ログを例にいたします。（Diagnostic ログでも共通となります。）



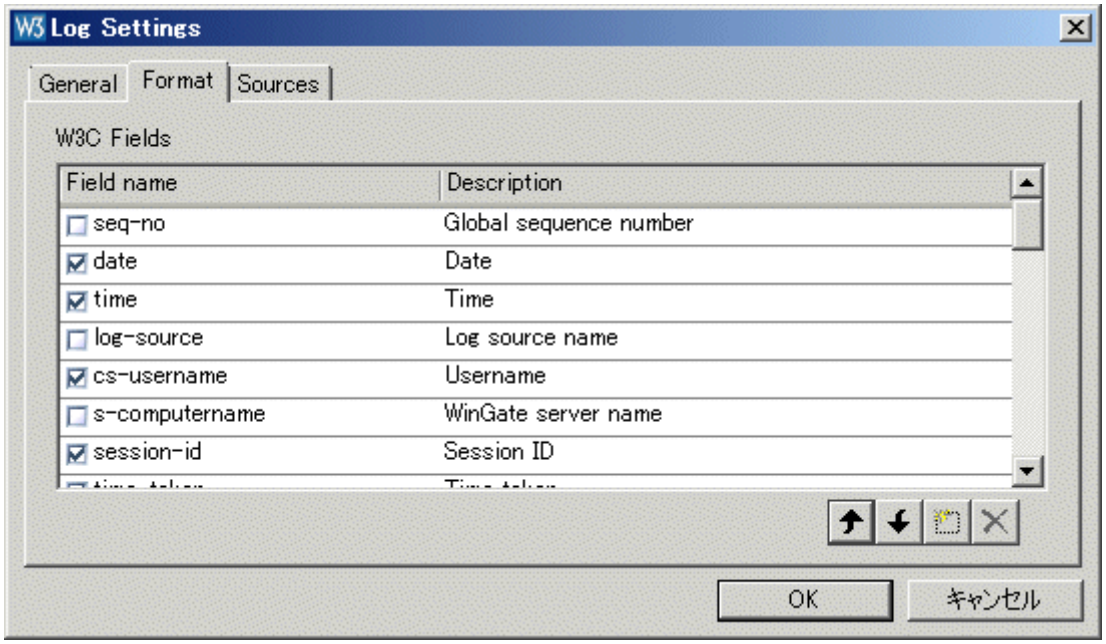

Log Name ＝ ログファイルの名前となります。変更する場合は、任意のログファイル名を入力してください。

Log Filename ＝ ログファイルがローテーションされる際に、ログファイルの先頭に付与される日付とフォーマットを設定することができます。右側のボタンによりフォーマットを選択することができます。

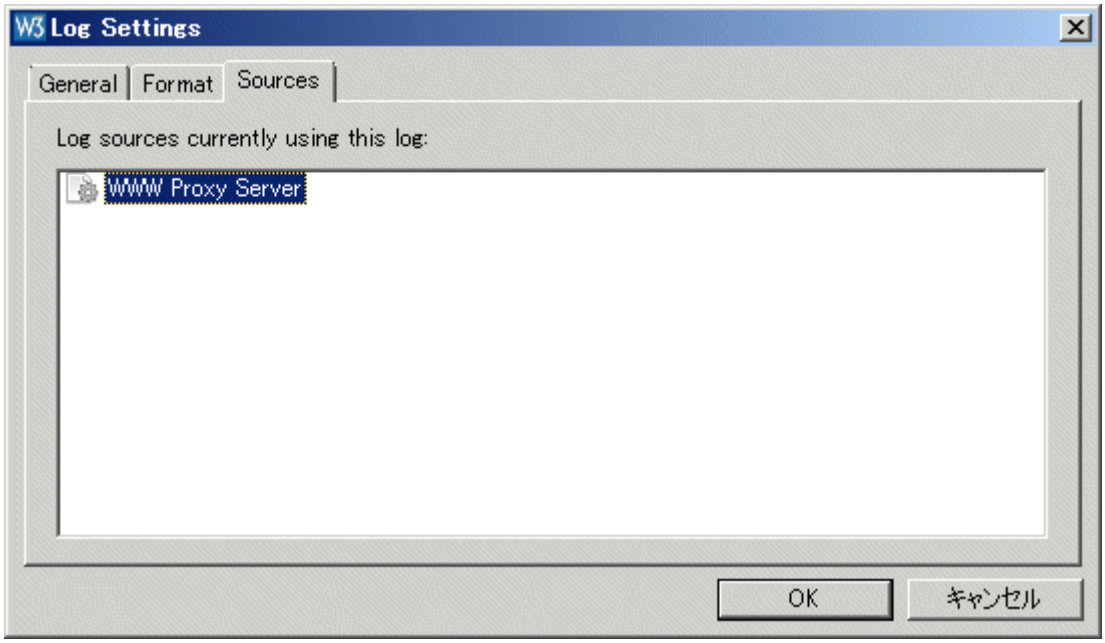
Expanded ＝ 上記で設定した設定のサンプルを表示します。

Log Directory ＝ ログの保存先ディレクトリです。変更する場合、右側のボタンで保存場所を参照することができます。

Log Time ＝ ログに記録される時刻を UTC と Local Time から選択することができます。

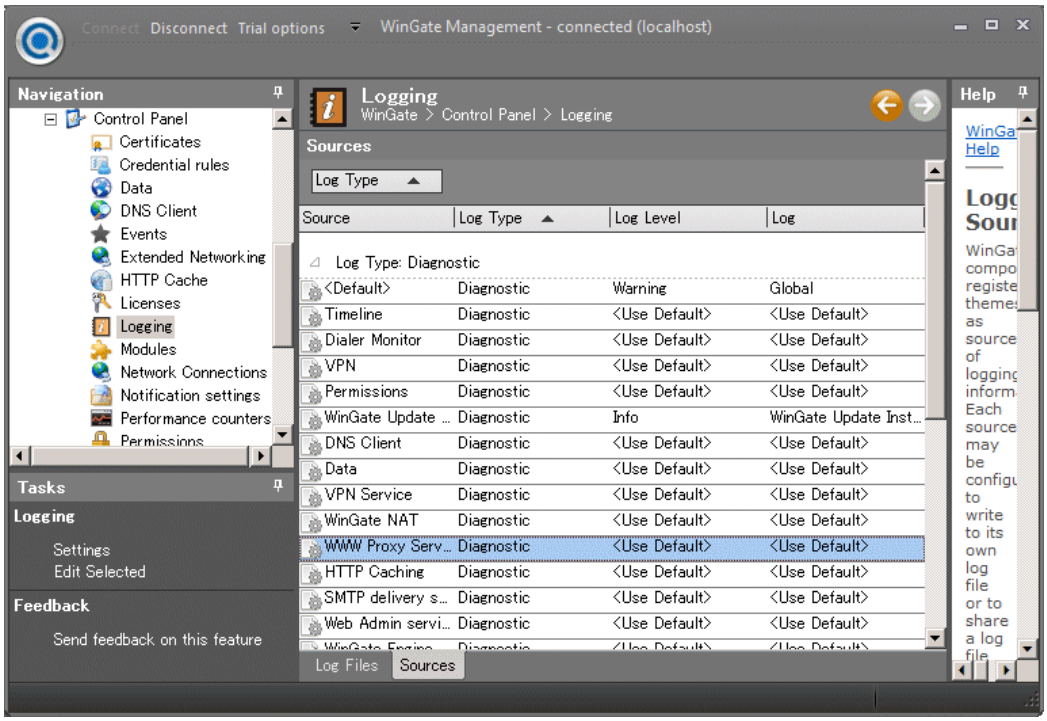



Format タブでは、ログに保存される項目を選択することができます。必要に応じて項目を選択、または解除してください。



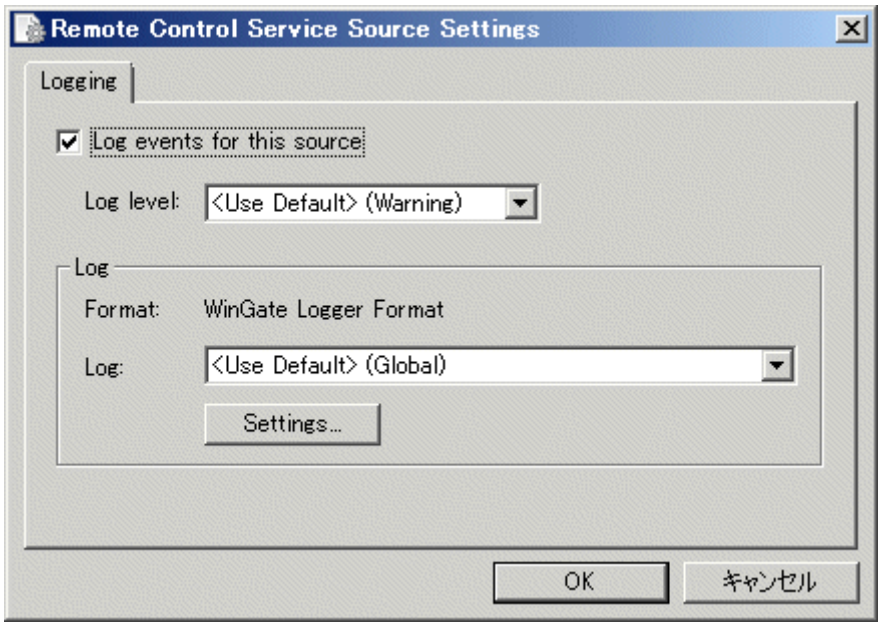

Source には、どのログ情報を保存しているかのソースが表示されます。

Sources（ソース）




Sources では、ログに関する様々な設定を行うことができます。

Sources に表示されているログに取得される項目をダブルクリック、または右クリックで選択し、Edit Selected をクリックすることにより個々の設定変更を行うことができます。




Log events for this source（このソースのイベントをログ）を無効にすると、選択したソースのログを取得いたしません。

Log level（ログレベル）では、取得するログのレベルを選択できます。デフォルトでは Warning（警告）のみがログに保存されます。必要に応じて選択を変更してください。（Debug は、デバッグ用のログとなり取得項目が非常におおくなります。サポートより Debug ログの取得要請があった場合のみご利用ください。）

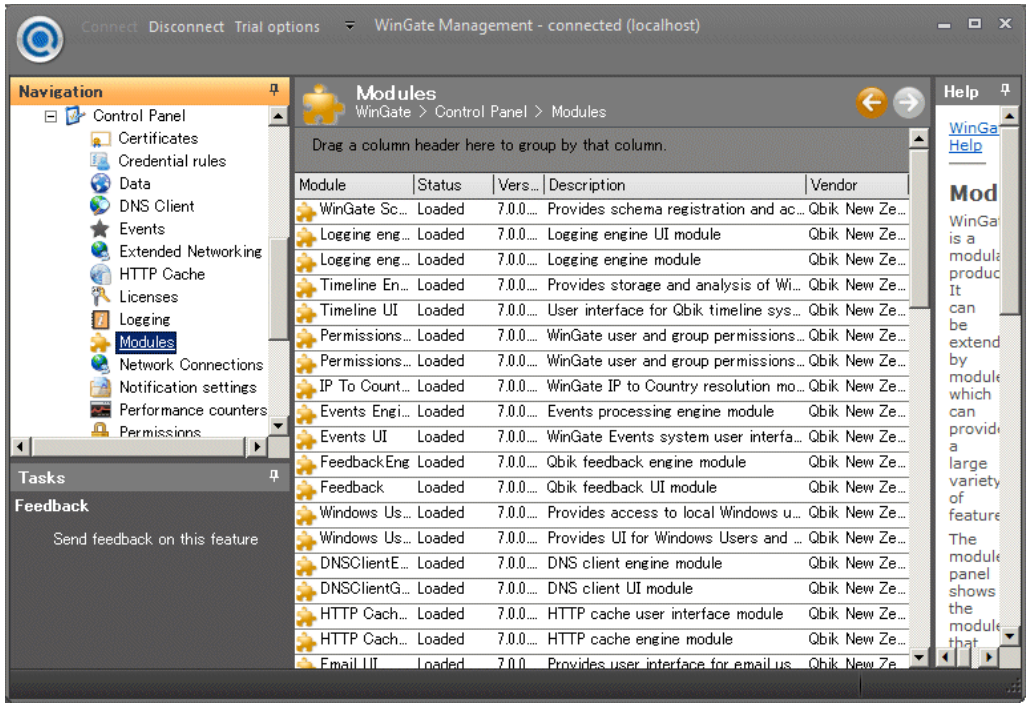
Log では、どのログファイルにログを取得するかを選択することができます。

Log Type が Diagnostic の項目では、デフォルトでエラーや警告を全て Global というログファイルに保存する設定となっています。

個々のログファイルとして、ログ情報を保存したい場合は、Own Log File を選択してください。

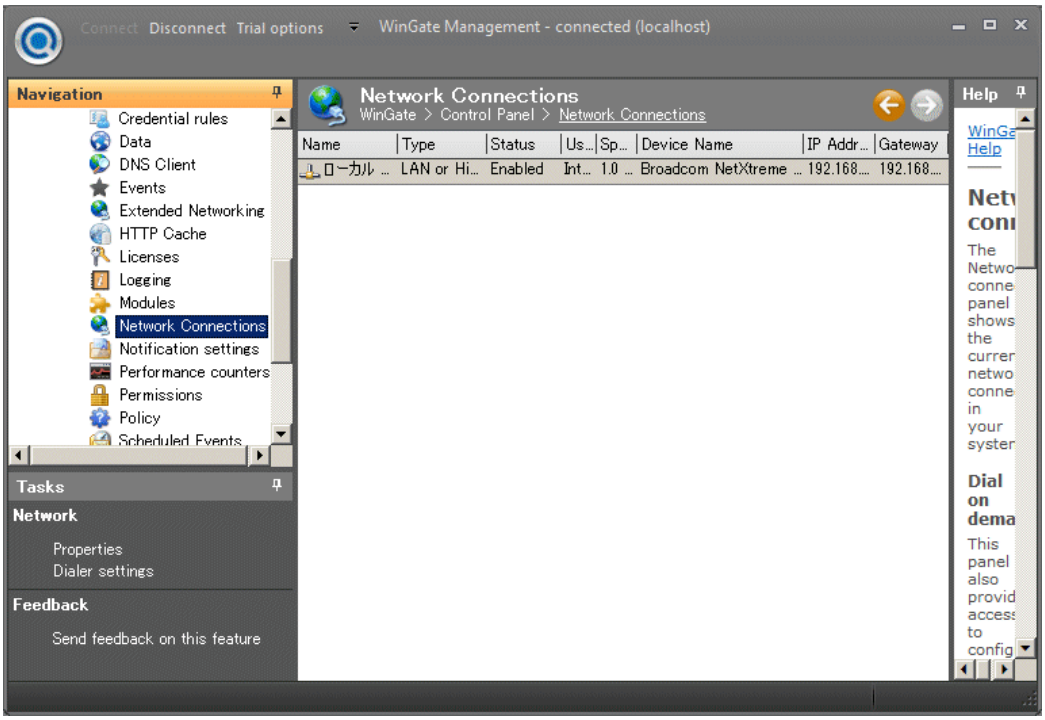
Log Type が Usage の項目では、Log Level、Log の項目を変更することができません。

**Module（モジュール）**



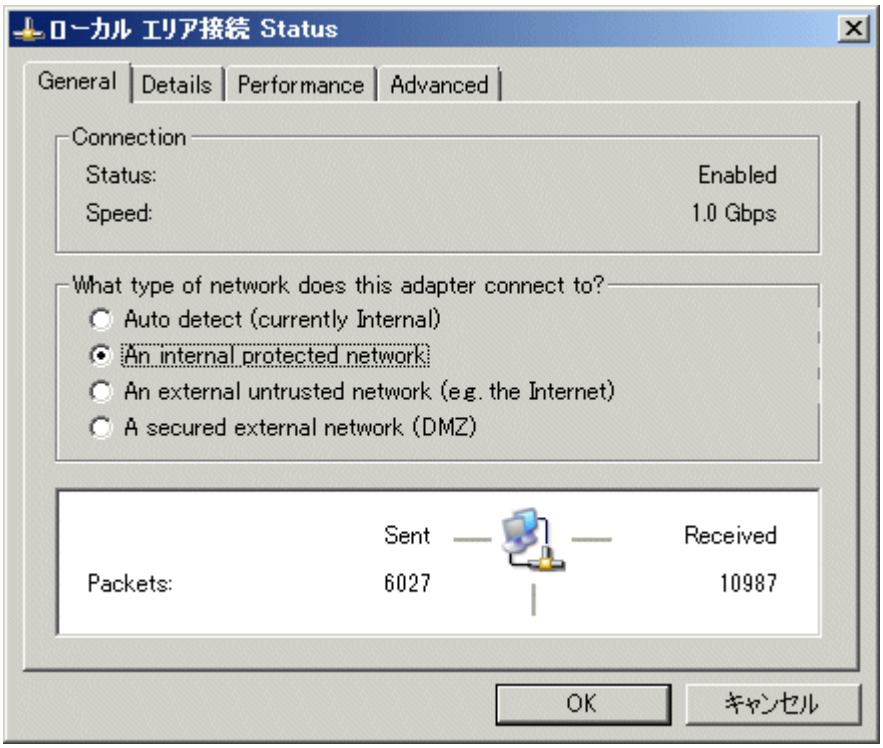
Module では、WinGate が使用するモジュールの確認、制御を行うことができます。
必要がない場合、モジュールの操作を行わないでください。

### Network Connections（ネットワーク接続）




Network Connections では、WinGate がインストールされている PC で構成されている NIC の情報の表示、および WinGate での役割を設定することができます。

設定の確認を行うネットワーク接続をダブルクリックして、そのネットワーク接続のプロパティを表示します。



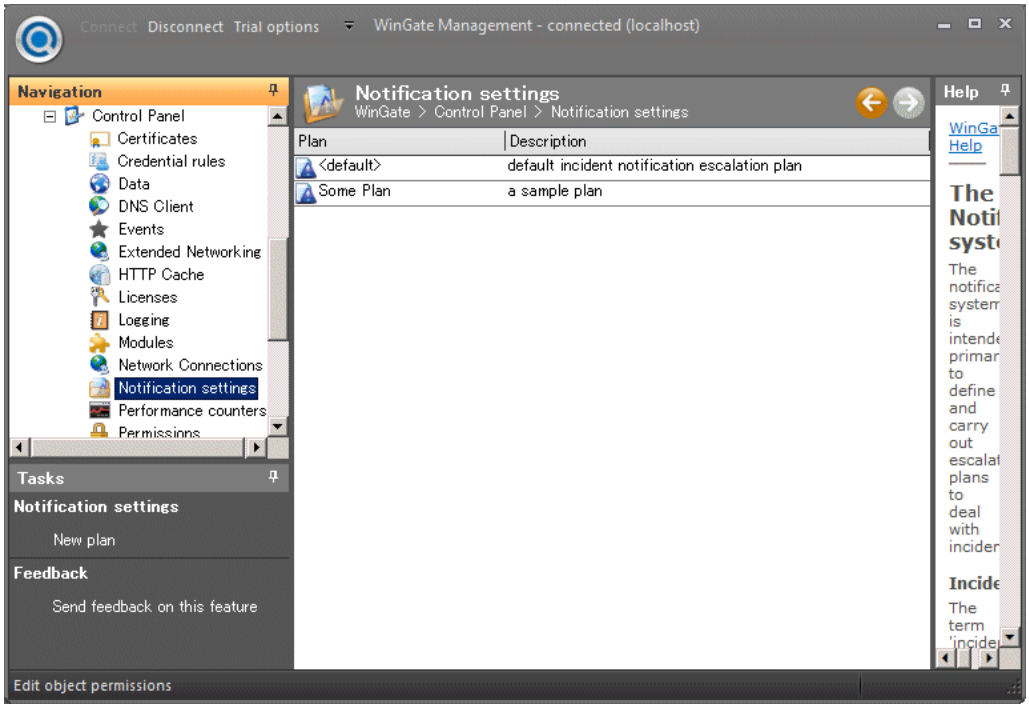

上記の図では Auto detect（自動検知）で currently Internal（現在は内部）と表示されていることから、このネットワーク接続は現在 WinGate では内部の保護されたネットワーク用のインターフェースであると認識されています。

（認識が正しい場合でも手動で設定いただくことをお勧めいたします。）
設定項目の内容は以下の通りです。

- Auto detect
  自動検知　カッコ内には、自動検知での構成が表示されます。currently Internal は内部、currently External は外部用となります。
- An Internal protected network
  内部の保護されたネットワークとなります。WinGate がクライアントから接続をうけるインターフェースは、通常、この設定となります。
- An external untrusted network (e.g. the Internet)
  信頼されない外部ネットワークとなります。NIC2 枚構成で、インターネットへ接続される側のインターフェースは、通常この設定をなります。
- A secured external network(DMZ)
  安全な外部のネットワーク（DMZ）となります。NIC3 枚構成で WinGate により DMZ を構成し、DMZ へ接続されるインターフェースは、通常この設定となります。

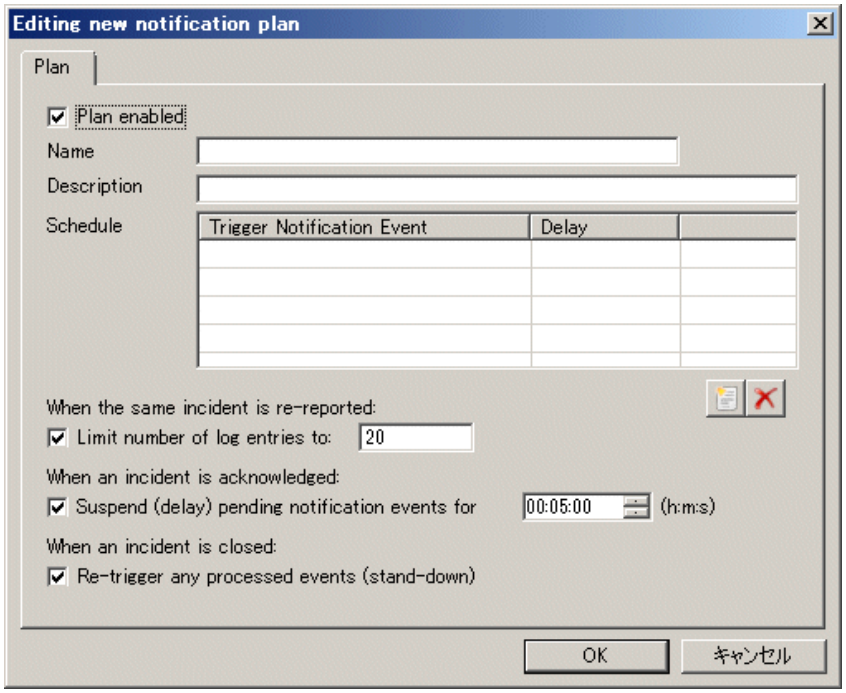
もし自動検知の内容がネットワークの構成に反している場合などは、適切な設定を選択いただくことにより、任意にネットワークインターフェースのタイプを変更することができます。
**※この変更は WinGate の全てのバインド、ファイアウォール構成に影響します。**

### Notifications　Settings（通知設定）

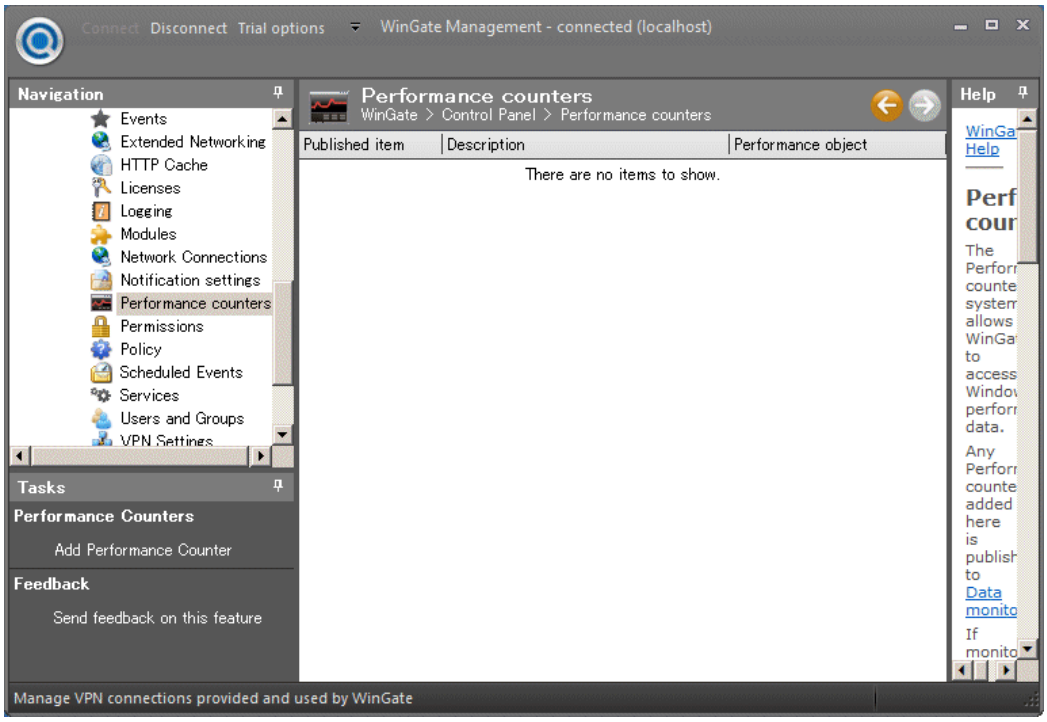



Notifications　Settings では、WinGate で発生したインシデントに基づき通知を行う際のプランの管理、追加を行うことができます。

Tasks の Notification　settings より New　plan（新規プラン）をクリックすることで新しいプランを作成することができます。



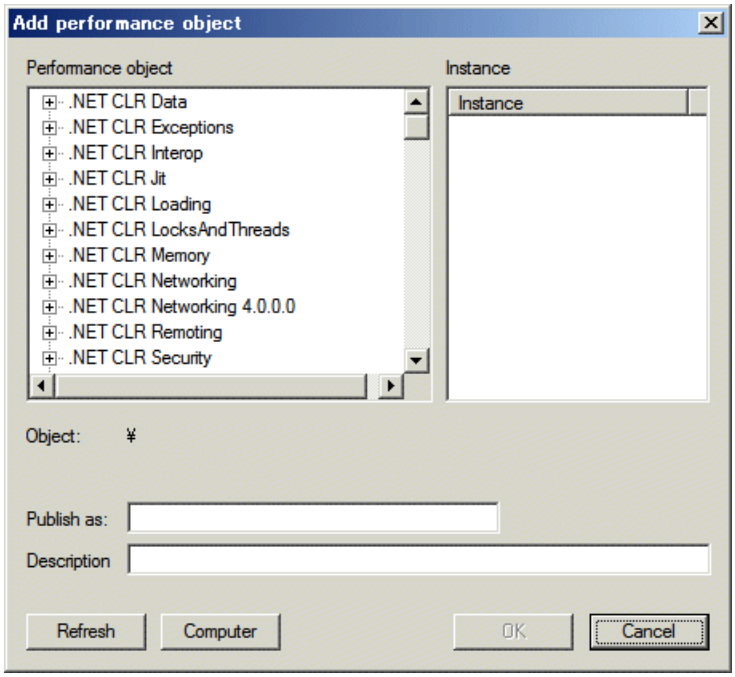

**Performance counters（パフォーマンス・カウンター）**



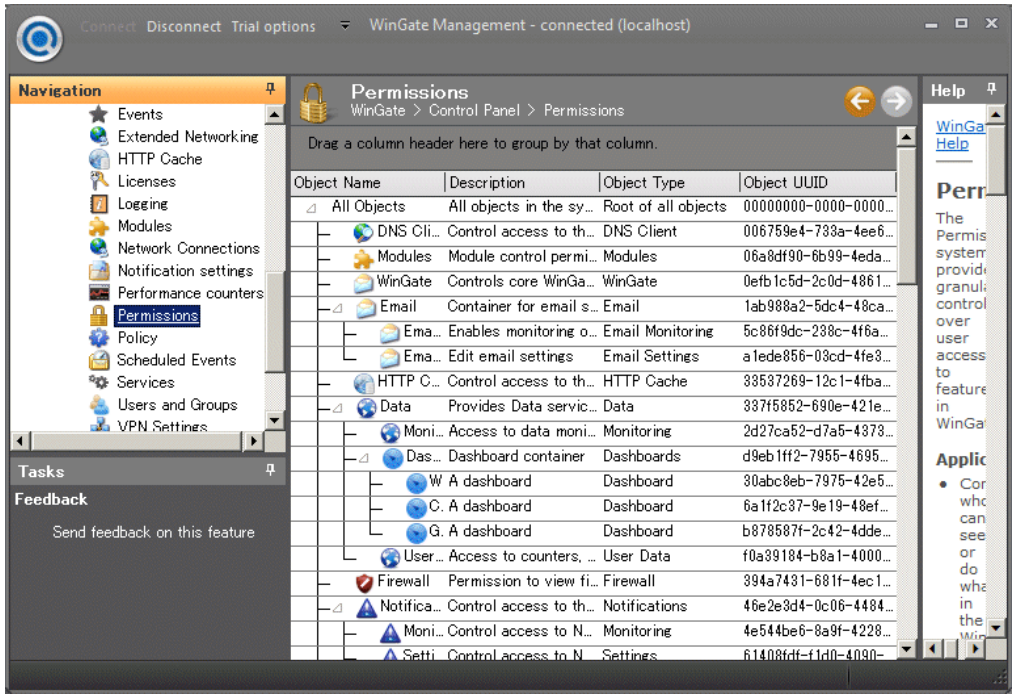

Performance counter は、WinGate  Enterprise ライセンスのみで使用可能です。

Performance  counters では、WinGate マシンで取得可能な情報を使用することができます。それらは Data の Monitoring で使用可能となり、ダッシュボードや Event で利用可能で、管理者へ様々な情報を通知、管理することを可能となります。

Tasks の Performance Counters より Add Performance Counter をクリックすることにより新しい Performance Counter を作成することができます。



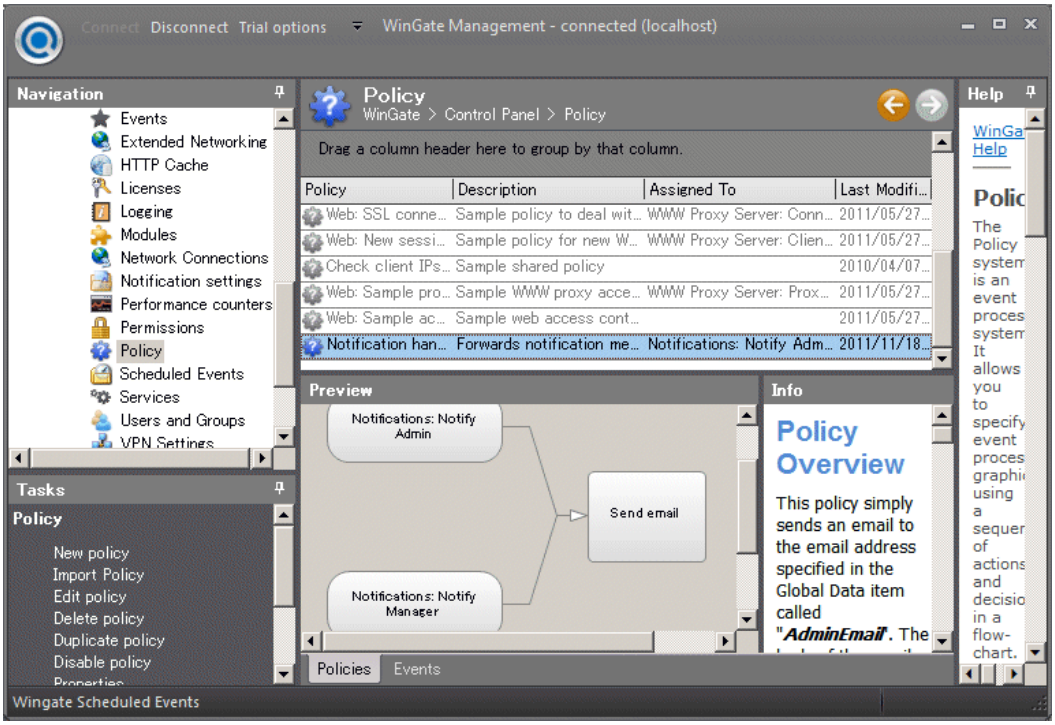

### Permissions（権限）




Permissions には、WinGate の各コンポーネントが表示され、それぞれを制御することができます。アクセスとコントロールの要件によって、それぞれのパーミッション・オブジェクトにユーザーかグループの許可を設定することができます。これは、ユーザーが WinGate Management コンソールにログインするとき、それらのアクセスとコントロールのレベルが特定の機能や使用するのを願うダイアログに設定されたパーミッションによって定義されることを意味します。

ダブルクリックすると、それぞれの権限を設定することができます。

## Policy（ポリシー）




WinGate7 からのポリシー機能は、過去の WinGate から刷新され、大幅に機能の向上を果たしました。新しいポリシー・システムは、WinGate で発生するイベントに対してどのような制限や動作を行わせるかを構成することが可能となります。

また、それは一つのイベントだけに対してではなく、幾つかのイベントに対しても設定することが可能です。

設定は、フローチャート形式によりグラフィカルなインターフェースで容易に設定を行うことができます。

ポリシーでは、それぞれのポリシーの動作を確認するために、ポリシー画面内で、ポリシーに該当したカウント数や割合を確認することもできます。

デフォルトでは、幾つかのサンプルポリシーが用意されております。（イベントが指定されていないため、動作はいたしません。通知イベントのみが管理者電子メールアドレスの警告を表示する場合があります。必要としない場合は、削除してください。）

具体的な設定方法に関しては、後に記述しております「よく使用されるポリシーの設定例」の章をごらんください。

Tasks に表示される Policy での操作内容は移管お通りとなります。

・New policy ＝ クリックすると新しいポリシーを追加することができます。

・Import policy ＝ ポリシーを設定ファイルからインポートする場合インクリックします。

・Edit policy ＝ 選択されたポリシーを編集します。新たに設定ウインドウが表示されます。

・Delete policy ＝ 選択されたポリシーを削除します。

・Duplicate policy ＝ 選択したポリシーの複製を作成します。

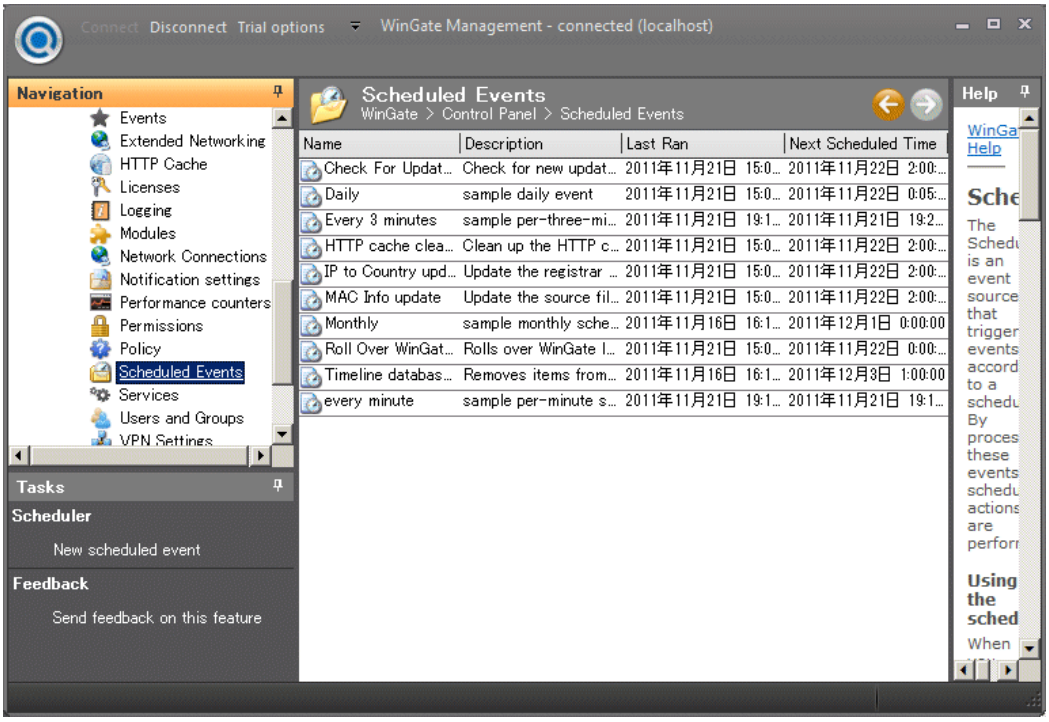
・Enable policy ＝ 無効となっている選択されたポリシーを有効にします。

・Disenable policy ＝有効となっている選択されたポリシーを無効にします。

・Property ＝ 選択されたポリシーのプロパティを表示します。

・Export policy ＝ 選択されたポリシーをインポート可能なファイルへ書き出します。

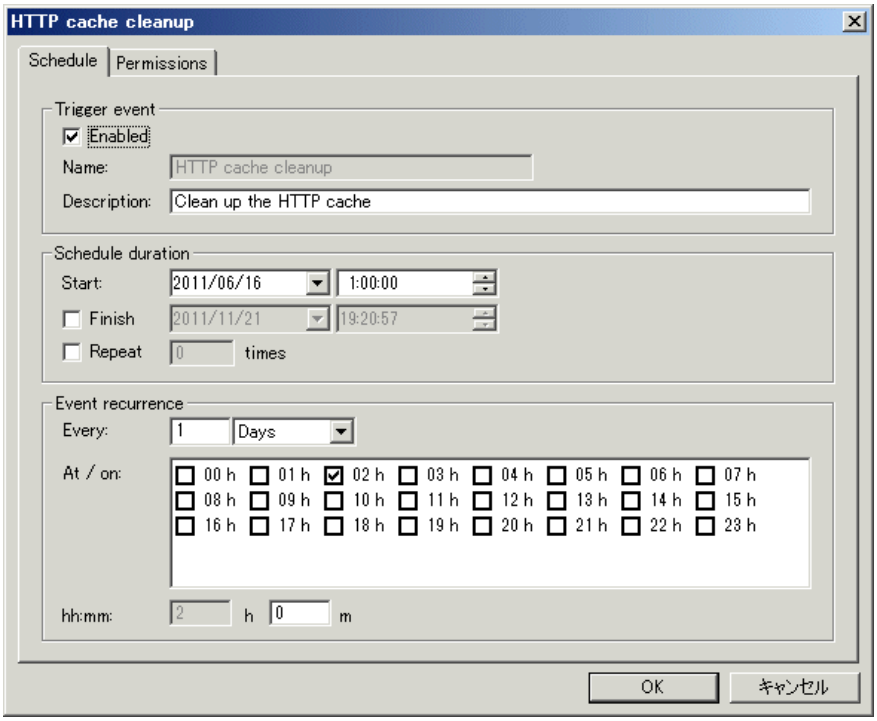
## Scheduled　Events（スケジュール・イベント）




Scheduled　Events では、WinGate が定期的に行うイベントの設定、追加を行うことができます。

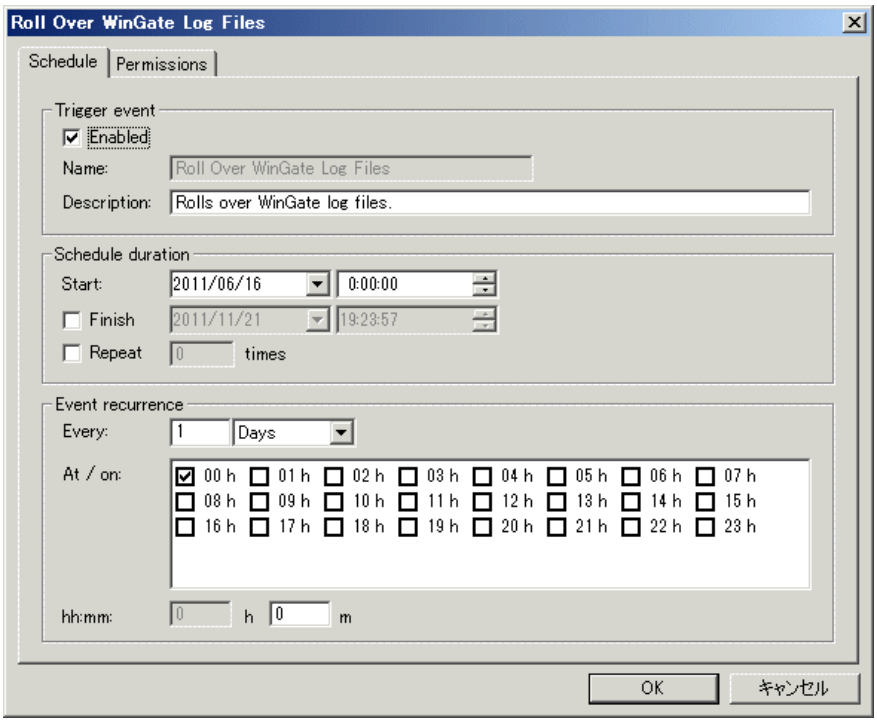
デフォルトでは、WinGate が行う幾つかのスケユールイベントが追加されています。

スケジュール変更を行う場合は、変更を行うイベントをダブルクリックすることで、編集することができます。



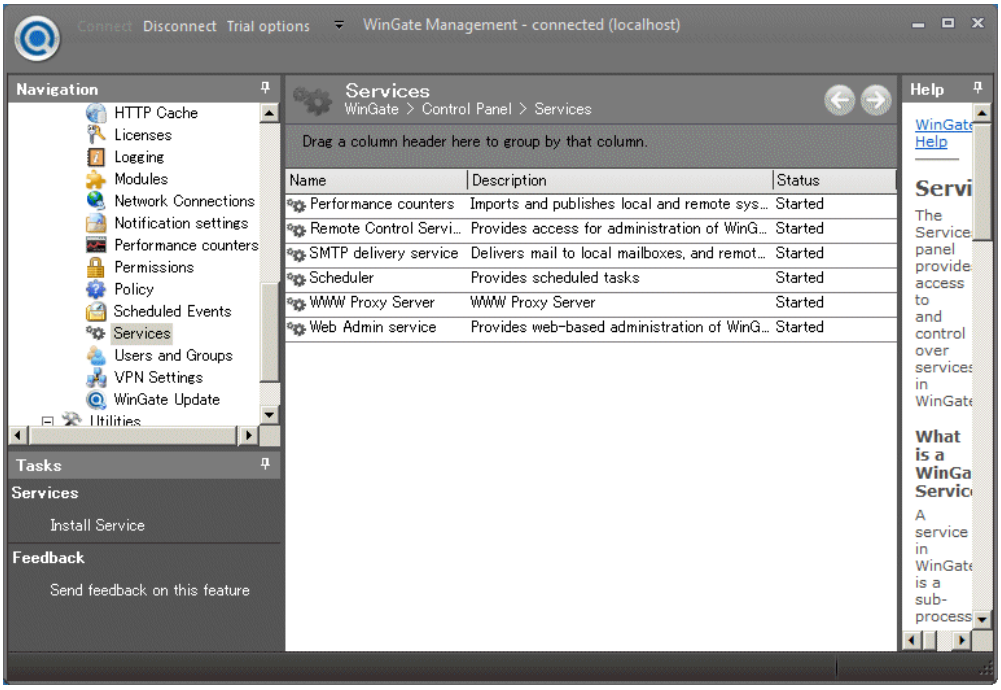

（例）これは、WinGate の HTTP Cache をパージするスケジューリングとなります。デフォルトでは、Every 1 Days 02h 0m に設定されており、これは毎日 2:00 分に、このスケジュールを実施する設定となっております。

また、ログのローテーションは以下のスケジュール・イベントで設定されています。




スケジュールをすぐに実行したい場合は、実行するスケジュールを選択し、Tasks で Run now をクリックすると、スケジュールが実行されます。
また、New Scheduled event をクリックすると新しいスケジュールを追加することができます。
新しいスケジュールを追加すると Events に追加したスケジュールが表示され、どのような動作を行うかを設定することができます。

### Services（サービス）




Services では、WinGate の各プロキシサーバーやサービスなどの、設定、追加、削除を行うことができます。
各サーバー、サービスの詳細は以下の通りとなります。

WinGate がサポートするプロキシサーバー

- WWW Proxy Server（デフォルトインストール、デフォルトポート：80）
  HTTP プロキシサーバーとして動作します。
- POP3 Proxy Server（デフォルトポート：8110）
  POP3 プロキシサーバーとして動作します。
- FTP Proxy Server（デフォルトポート：21）
  FTP プロキシサーバーとして動作します。
- RTSP Proxy Server（デフォルトポート：554）
  メディアストリーム用の RTSP プロキシサーバーとして動作します。
- Telnet Proxy Server（デフォルトポート：23）
  Telnet プロキシサーバーとして動作します。

WinGate がサポートするサービス

- Remote Control Service（デフォルトポート：808　デフォルトインストール　削除不可）
  リモート・コントロールサービスは、WinGate Management が WinGate へ接続するために使用するサービスです。停止した場合、WinGate Management を使用した WinGate の管理、設定ができなくなります。
- SMTP delivery Service（削除不可）
  SMTP デリバリーサービスは、WinGate が通知や SMTP Server でのメール配信を行う際に使用するサービスです。
- Web Admin Service（デフォルトポート：3180　削除不可）
  Web Admin サービスは WinGate の Web ベースでの管理を行うためのサービスです。
- DHCP Service（デフォルトポート：67　ポートの変更はできません。）
  WinGate を DHCP サーバーとして使用する場合に利用します。
- DNS Service（デフォルトポート：53　ポートの変更はできません。）
  WinGate を利用するクライアントへ名前解決のサービスを提供します。WinGate の DNS サービスは DNS サーバーの機能は持ちません。WinGate が持つ DNS サーバーを利用して、クライアントへ名前解決のサービスを提供します。
- GDP Service（デフォルトポート：368　ポートの変更はできません。）
  GDP サービスは、WinGate Internet Client が WinGate サーバーを発見するために使用されるサービスです。
- Winsock Redirector Service（デフォルトポート：2080）
  Winsock リダイレクトサービスは、WinGate Internet Client との接続に使用されるサービスです。
- VPN Service（デフォルトポート：809）
  WinGate VPN を使用する場合に使用するサービスです。
- Socks Service（デフォルトポート：1080）
  Socks プロキシサービスとして動作します。
- POP3 Collection Service
  POP3 収集サービスは、WinGate のメールアカウントへ外部からメールを取得するために使用するサービスです。

- TCP Mapping Service
  TCP マッピングサービスは、TCP 接続を指定した接続先へマッピングする場合に使用されるサービスです。
- UDP Mapping Service
  UDP マッピングサービスは、UDP 接続を指定した接続先へマッピングする場合に使用されるサービスです。

WinGate がサポートするサーバー機能

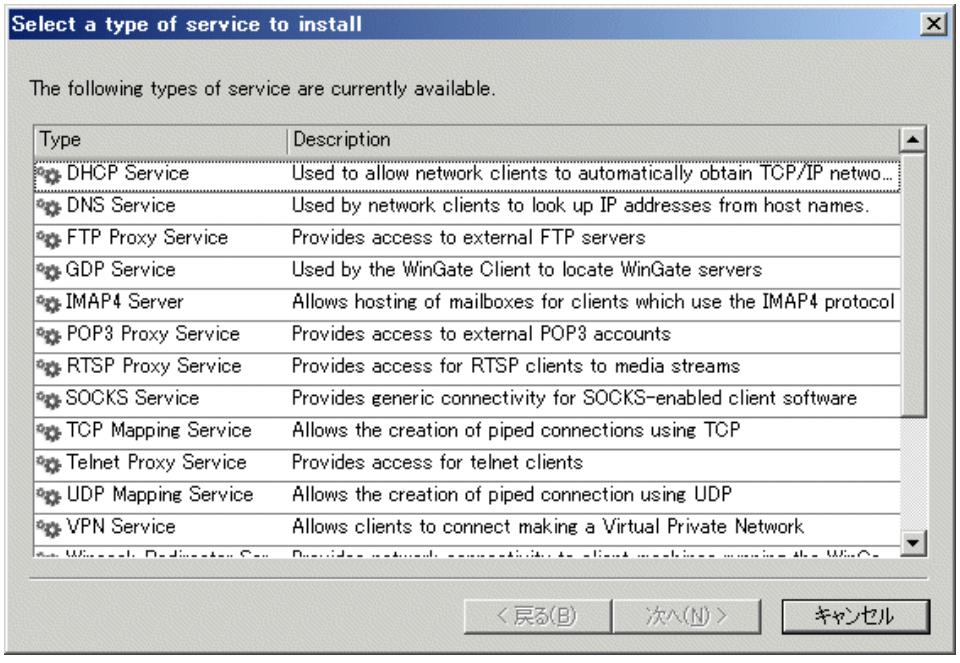
- POP3 Server（デフォルトポート：110）
  POP3 サーバーは、WinGate のメールサーバー機能を使用した場合に、POP3 サーバーとして動作します。
- SMTP Server（デフォルトポート：25）
  SMTP サーバーは、WinGate のメールサーバー機能を使用した場合に、SMTP サーバーとして動作します。
- IMAP4 Server（デフォルトポート：143）
  IMAP4 サーバーは、WinGate のメールサーバー機能を使用した場合に、IMAP4 サーバーとして動作します。

その他の機能

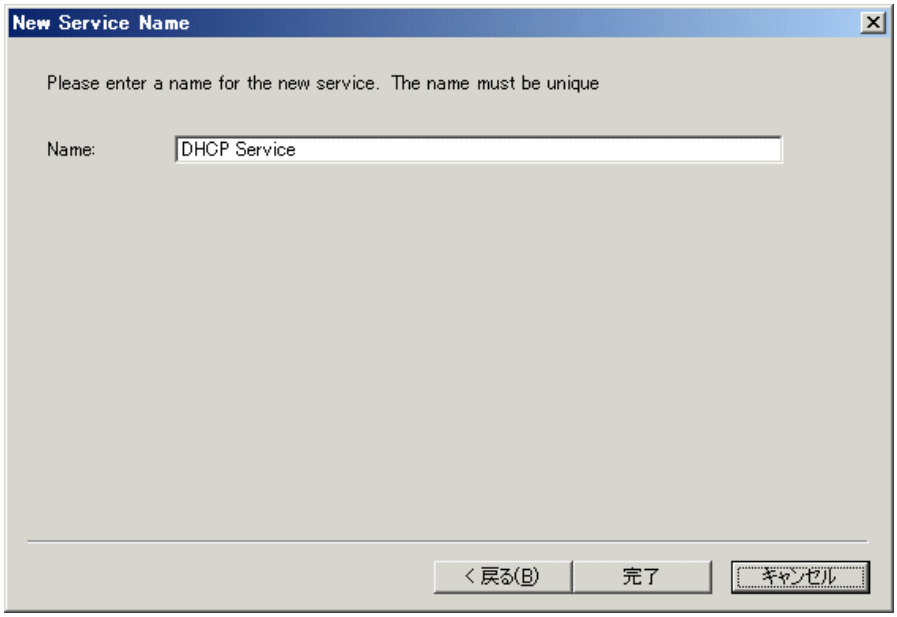
- Performance counters（削除不可）
  パフォーマンス・カウンターは、WinGate のパフォーマンス・カウンターのためのサービスとなります。
- Scheduler（削除不可）
  スケジューラは、WinGate のスケジュール・イベントを実行するためのサービスとなります。

**サービス、サーバーの追加**

Tasks の Services で Install Service（サービスのインストール）を選択することにより、必要なサービスを追加することができます。



必要なサービスを選択して次へボタンをクリックしてください。




必要に応じて、Name 欄でサービス名を変更してください。
完了ボタンをクリックすると、新しいサービスが追加されますので、プロパティを開き設定を行ってください。

**サービスの削除**

削除するサービスを選択して、Tasks の Services Remove クリックすると、選択したサービスを削除することができます。

**サービスの停止**

停止するサービスを選択して Tasks の Services で Stop をクリックすると、選択したサービスを停止することができます。

**サービスの設定変更**

変更するサービスを選択して Tasks の Services で Property をクリックすると、選択したサービスを Property ダイアログが表示され設定を変更することができます。

**サーバー、サービス機能について**

ここでは WinGate の WWW Proxy Server を例に、WinGate のサーバー、サービス機能の設定内容を解説いたします。

- サーバー、サービス機能について

  ここでは WinGate の WWW Proxy Server を例に、WinGate のサーバー、サービス機能の設定内容を解説いたします。

  各サービス、サーバープロパティダイアログは、以下のタブで構成されています。(使用するプサーバー、サービスにより異なります。)

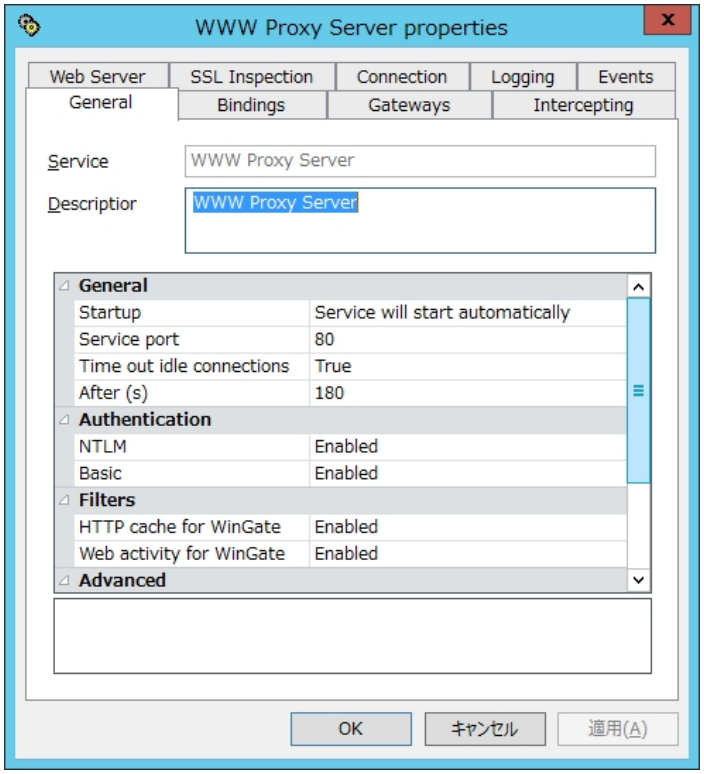
  - General(全般)

    General では、開始オプション、サービスポート、認証方法などの設定を行うことができます。

- Binding（バインド）
  Binding では、プロキシサーバーが接続を受け付けるインターフェースや IP アドレスの設定を行うことができます。
- Gateway（ゲートウェイ）
  Gateway では、プロキシサーバーがインターネット接続に利用するゲートウェイの設定を行うことができます。
- Intercepting（インターセプト）
  Intercepting では、ENS、WinGate Client、Socks 接続をプロキシサーバーにインターセプトする場合の設定を行うことができます。
- Web Server（WEB サーバー）
  WinGate の Web サーバー機能（プロキシリクエスト以外の接続）を、どのように取り扱うかの設定を行うことができます。（WWW Proxy Server のみ）
- SSL Inspection（SSL インスペクション）
  暗号化された内容の検査を行う場合に使用します。この機能を使用する場合、使用する証明書を指定（作成）する必要があります。
- Connection（接続）
  多段プロキシの設定を行うことができます。
- Logging（ロギング）
  ログの取得方法に関する設定を行うことができます。
- Event（イベント）
  プロキシサーバーで取り扱われるイベントの内容を、その設定の変更を行うことができます。

それぞれの詳細は以下の通りとなります。

- General（全般）




General タブでは以下の設定を行うことができます。

Service name（サービス名）は、サービス名を表示します。

Description（説明）は、サービスの説明を入力することができます。（任意に変更することができます。）

**General**

Startup（開始オプション）

Startup は、そのプロキシサーバーが WinGate 開始時にどのような動作とするかを設定することができます。変更するには、Startup をクリックしドロップダウン・メニューから以下のオプションを選択します。

Service will start automatically ＝ サービスを自動的に開始

Service is disabled ＝ サービスは無効

Manual start / stop ＝ 手動開始/停止

Service port（サービスポート）

Service port では、そのプロキシサーバーが、接続を受け付けるポート番号を設定することができます。変更する場合、Service port をクリックし、変更するポート番号を入力してください。

Time out idle connection（使用されていない接続をタイムアウト）

Time out idle connection は、使用されていない接続をタイムアウトするかを設定することができます。変更する場合は、Time out idle connection をクリックしドロップダウン・メニューから選択します。

True は、タイムアウトさせます。False を選択するとタイムアウトしません。

After(s)（何秒後）

Time out idle connection でタイムアウトされる時間を設定することができます。
変更する場合は、After(s)をクリックして、値（秒）を入力してください。

Authentication（認証）
認証が利用可能なプロキシサーバーで認証方法の有効、無効を設定することができます。
NTLM
NTLM 認証を有効、無効にすることができます。変更する場合は、NTLM をクリックしてドロップダウン・メニューから選択します。
Enable は有効、Disable は無効となります。Enable over SSL は、SSL 接続を経由して NTLM 認証を行う場合に選択します。（一部のサーバーのみで使用可）

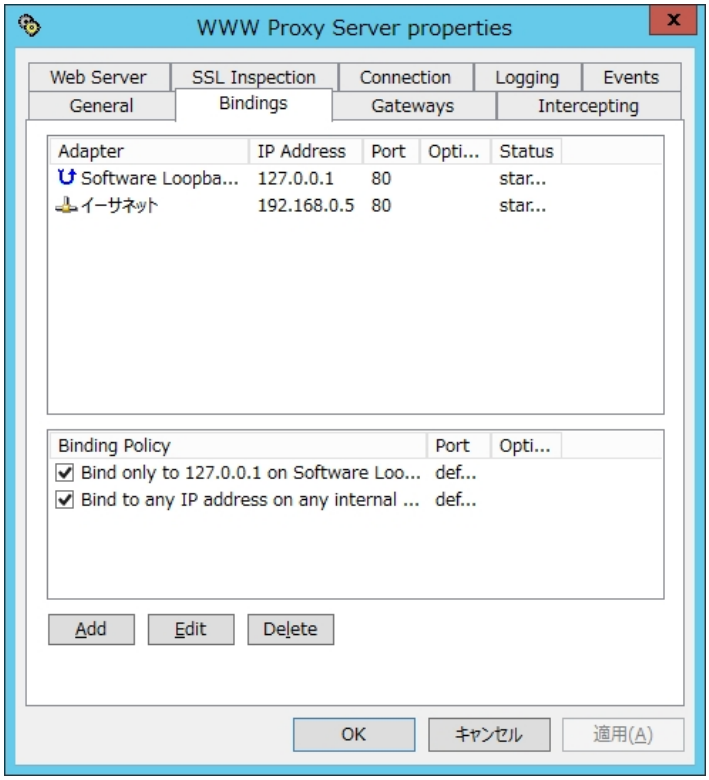
Basic
Basic（ベーシック）認証を無効にすることができます。変更する場合は、Basic をクリックしてドロップダウン・メニューから選択します。
Enable は有効、Disable は無効となります。Enable over SSL は、SSL 接続を経由して NTLM 認証を行う場合に選択します。（一部のサーバーのみで使用可）

Filter（フィルター）
HTTP キャッシュ、Web アクティビティ、Kaspersky AntiVirus などフィルタリング・プラグインを有効、または無効にすることができます。
それぞれのフィルターを有効にする場合は、Enabled を選択、無効とする場合は、Disabled を選択してください。
HTTP cache for WinGate = HTTP キャッシュ機能の有効、無効
Web activity for WinGate = Timeline への記録を有効・無効、Web Access Control の有効・無効
Kaspersky AntiVirus for WinGate = Kaspersky AntiVirus for WinGate によるウイルススキャンの有効、無効（Kaspersky AntiVirus for WinGate インストール時のみ）

Advanced（詳細）
Advanced では、プロキシサービスの最大リクエスト時間、最大接続数のより詳細な設定を行うことができます。

**Bindings**（バインド）

Bindings では、そのプロキシサービスが接続を受け付けるインターフェースと、その方法を設定することができます。



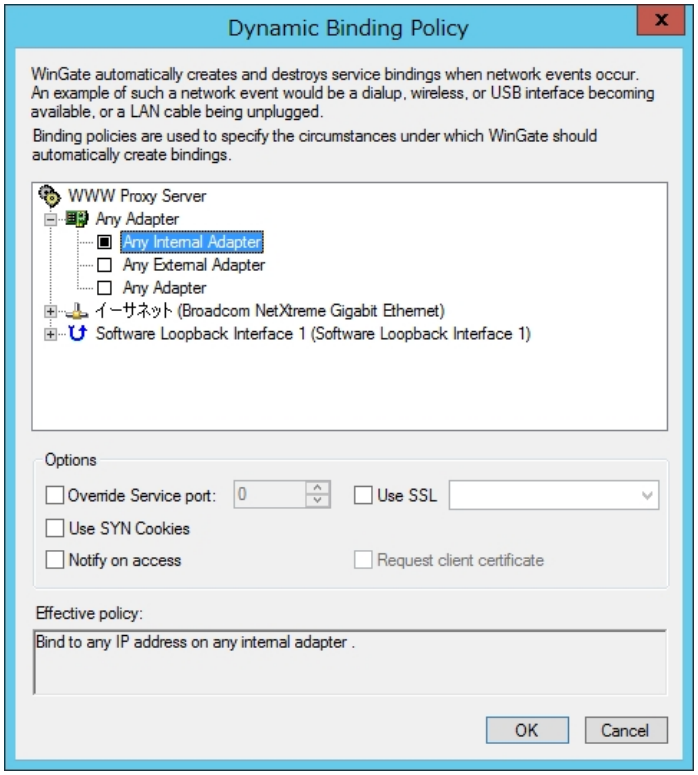

上の段には現在接続を受け付けているインターフェースとその状態が表示されます。

**※Status（状態）欄が Stopped（停止）となっている場合、WinGate の他のサーバー、サービス、または Windows 条で動作する他のサービスとポートの競合などが発生している場合があります。ポートの重複などがないかをご確認ください。**

下の段（Binding Policy）は、どのようにそれらのインターフェースをバインドするかが表示されています。上記のスクリーンショットでは、Binding Policy（バインド・ポリシー）で、ループバックアドレス（127.0.0.1）と Internal adaptation（内部アダプタ）をバインドするポリシーが設定されているため、Software loopback Interface 127.0.0.1 と WinGate の Network Connections で内部（Internal）に指定されているアダプタの IP アドレスで接続を受け付ける状態となっています。

Add（追加）ボタンにより、Binding Policy を追加することができます。既に設定されている Binding Policy を編集する場合は Edit（編集）ボタンをクリック、削除する場合は、Delete ボタンをクリックしてください。

Binding Policy は Dynamic Binding Policy（ダイナミック・バインド・ポリシー）により設定することができます。




ダイナミック・バインド・ポリシーにより、WinGate はネットワークインターフェースの IP アドレス情報などが変化した場合などでも自動的に設定内容に基づきバインド構成をアップデートし、そのインターフェースで接続を受け付けます。

設定は以下の意味を持ちます。(複数選択が可能です。その場合には選択されたポリシーの内容にバインドされます。)

◆ **Any internal Adapter(任意の内部アダプタ)**

Network Connections により、内部と設定されたアダプタにバインドします。

◆ **Any External Adapter(任意の外部アダプタ)**

Network Connections により、外部と設定されたアダプタにバインドします。

◆ **Any Adapter(任意のアダプタ)**

全てのアダプタにバインドします。

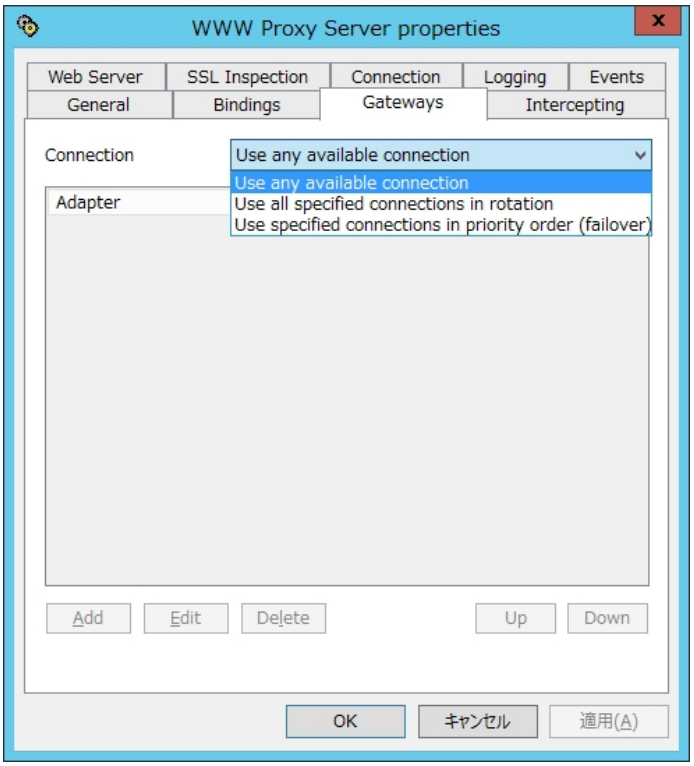
特定の NIC にバインドする場合は、表示されているネットワークインターフェースの Any IP Address(任意の IP アドレス)を選択します。これにより、その NIC2 枚の構成の任意の IP アドレスにバインドします。(NIC の IP アドレスが変更になった場合でも、その NIC へ割り当てられて IP アドレスに自動的にバインドします。)

特定の IP アドレスにバインドする場合は、表示されているネットワークインターフェースで表示されている IP アドレスを選択します。これにより、その IP アドレスにバインドします。(IP アドレスが変更された場合は、対象となる IP アドレスが存在しないため、バインドできません。)

設定変更後は、Bindings で、設定したアダプタが正しく表示されているかご確認ください。

**Gateway**（ゲートウェイ）

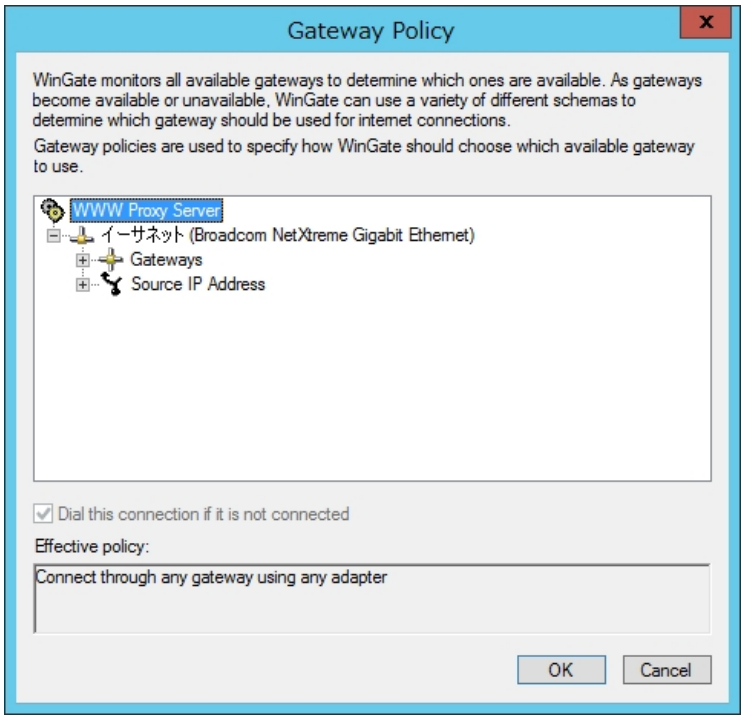
Gateway では、そのサーバーがインターネットへアクセスする際に使用するゲートウェイを設定することができます。




接続スキームは、以下のオプションを持ちます。

- **Use any available connection（任意の利用可能な接続を使用）（デフォルト）**
  WinGate サーバマシンが持つ利用可能なゲートウェイを使用します。PC のゲートウェイが変更された場合でも自動認識します。
- **Use all specified connection rotation（順番指定された全ての接続を使用）**
  追加されたゲートウェイを順番に使用します。
- **Use specified connection in priority order（優先度順に指定された接続を使用）（障害回避）**
  優先度順に指定された接続を使用します。

使用するゲートウェイを指定する場合、Use all specified connection rotation、または Use specified connection in priority order を指定し、追加ボタンをクリックします。
追加ボタンをクリックするとゲートウェイポリシー・ダイアログが表示されます。

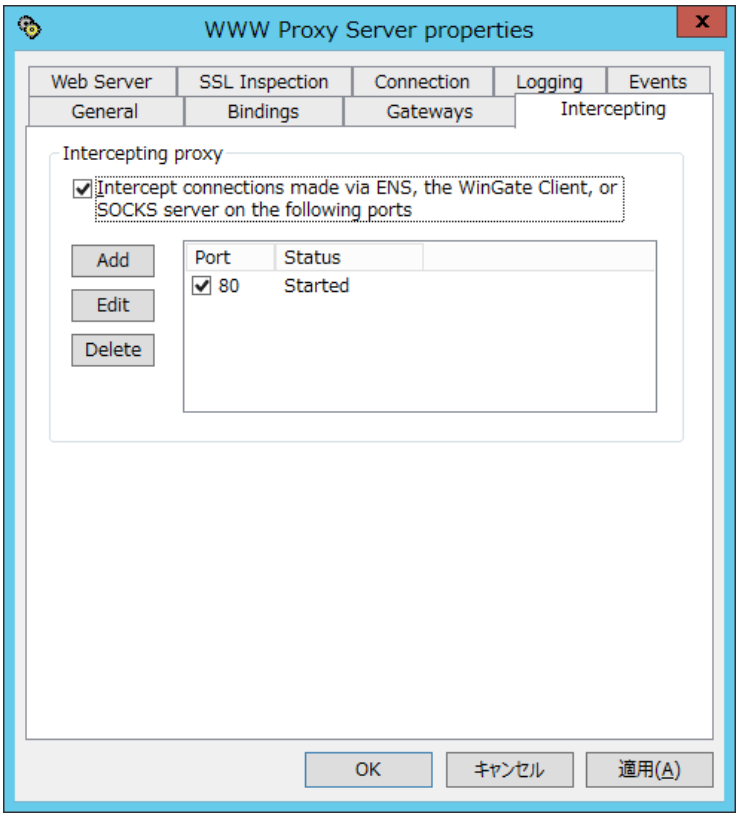



ゲートウェイポリシーには、利用可能なゲートウェイが表示されますので、使用するゲートウェイなどを指定してください。

**ヒント**:WinGate のプロキシサーバーは、バインド、またはポートが重複しなければ複数作成することができます。WWW Proxy Server 1 と WWW Proxy Server 2 で異なるゲートウェイを使用することも可能となります。また、WWW Proxy Server と FTP Proxy Server で異なるゲートウェイを使用することなども可能となります。

追加したゲートウェイの変更を行う場合は Edit(編集)ボタン、削除する場合は Delete(削除)ボタンをクリックしてください。

**Intercepting**（インターセプト）




Intercepting は、NAT、WGIC、Socks サーバーの接続を WinGate 内部で WinGate の各プロキシサーバーがインターセプトする機能です。

この機能により、クライアントマシンは NAT、WGIC を使用して接続を行っていても、WinGate の内部で各プロキシサーバーにリダイレクトされるため、各クライアント PC はプロキシ使用を意識することなく、各プロキシサーバーの機能を使用することができます。

インターセプト・プロキシの利点は NAT、WGIC を使用しているユーザーが意識する事無くプロキシの機能を使用していることです。これにより各プロキシでしか利用できない機能（例：WWW プロキシのキャッシュ機能など）や各プロキシでのポリシーをクライアントマシンに意識させる事なく使用させることができる事です。

NATを使用している場合では、クライアントマシンは、全く意識する事無くWinGateを使用する事ができますが、使用するセッションの内容によっては、必要な WinGate のプロキシにリダイレクトされ、WinGate のプロキシサーバーで設定されている制限事項を適用されている事になります。

また、WinGate のアンチウイルス・プラグインは、各プロキシサービスにプラグインされるため、トランスペアレント・リダイレクションを使用する事により、NAT、WGIC のセッションを各プロキシへリダイレクトされることにより、有効となります。（アンチウイルス・プラグインについては、弊社 Web サイトをご参照ください。）

Intercepting は以下のプロキシサーバーでご使用いただく事ができます。

WWW Proxy（ポート 80）、POP3 Proxy（ポート 8110）、FTP Proxy（ポート 21）、ログファイルサーバ（ポート 8010）、Telnet Proxy（ポート 23） ※ポートは何れもデフォルトで使用されるポートです。

WinGate は、WinGate クライアントコンピュータからのリクエストに対して、それぞれのインターネット・リクエストで使用されるポートによってどのサービスを経由されるべきであるかを決定することができます。つまり、WinGate の WWW プロキシでインターセプト・プロキシが設定されていると、NAT による接続でポート 80 で

のリクエストが行われた場合、WinGate は NAT の接続をインターセプトして、自身の WWW プロキシへリダイレクト（転送）します。

WinGate の NAT を使用している環境での WWW プロキシを例にすると、クライアントマシンは WinGate の NAT を使用することにより、インターネット・アプリケーションではプロキシを使用する設定を行うことなく、Web へのアクセスを行っています。
しかし、WinGate の管理者は Web アクセスへのログ管理（※1）、WWW プロキシでのユーザー制限、多段プロキシ等の WWW プロキシのみでサポートする内容をクライアントマシンに利用させたいと考えています。この場合、以前はクライアントのブラウザでプロキシ設定を行う必要がありました。
トランスペアレント・リダイレクトを設定することにより、NAT のポート 80 を使用する接続は、自動的に WinGate の WWW プロキシへリダイレクトされます。リダイレクトされたセッションは WWW プロキシによって処理がされるため、WWW プロキシの機能（キャッシュ、ポリシー等）やログ情報が全て適用されます。
クライアントマシンはプロキシの使用を一切意識することはありませんが、実際は WinGate のプロキシを使用している事となるのです。

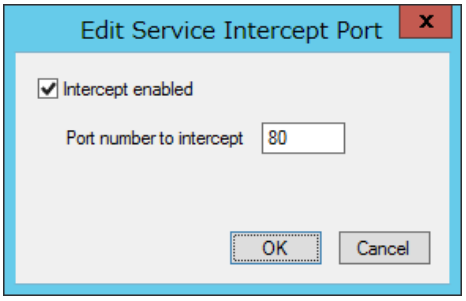
トランスペアレントが設定されていない、またはトランスペアレントの対象とならない接続に関しては、NAT、WGIC、SOCKS によってそのまま処理がされますので、トランスペアレントによる利用できないアプリケーション等の問題は、ほとんど発生することはないでしょう。

※　1 WinGate のログは各サービスのディレクトリに分かれて保存されております。NAT や WGIC のログは全てのセッションを 1 つにまとめられ保存される事となります。トランスペアレントを使用する事により、インターセプトされたプロキシのログにセッションログが保存されますので、ログの管理がしやすくなる利点があります。

**Intercepting の設定**
以下の手順で各プロキシのインターセプトを設定してください。
ここでは WWW プロキシを例にご紹介いたします。

1. WinGate Management の Services でインターセプトを有効にする特定のサービスを開いてください。（WWW プロキシサーバー, POP 3 サーバー, ログファイルサーバ, または Telnet サーバーの何れか）
2. Intercepting タブを開きます。
3. Intercept connection made via ENS, WinGate Client, or SOCKS Server on the following ports（以下のポート上の ENS、WinGate クライアント、SOCKS サーバーを通して作成された接続をインターセプトする）をチェックしてください。

4. Add（追加）ボタンをクリックします。
5. Edit Service Intercept Port（サービスインターセプト・ポートの編集）が表示されます。

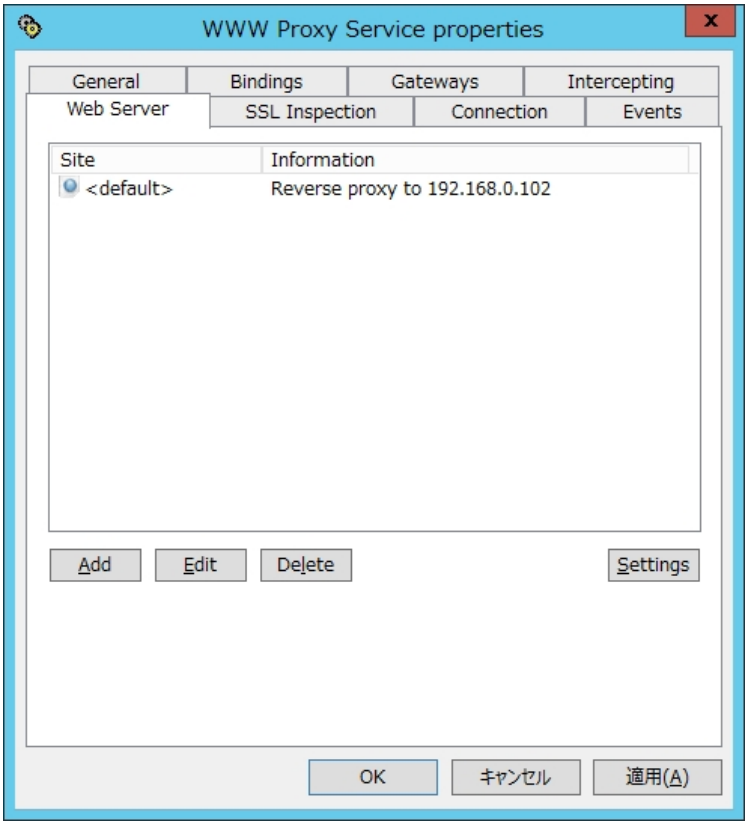



Intercept enabled（インターセプトを有効）チェックボックスがチェックされている事を確認してください。そして、適切なポートが表示されます。（これは通常サービスと同じポートであるでしょう）

6. OK をクリックします。
7. セッション構成に追加したポートが表示されます。
   OK をクリックして、プロキシのプロパティを終了します。

以上で、NAT、WGIC、SOCKS を経由するポート 80 を使用するセッションは WWW プロキシにインターセプトされ、WWW プロキシで処理されます。
他のプロキシサービスについても同様の手順で、インターセプト・プロキシを設定してください。

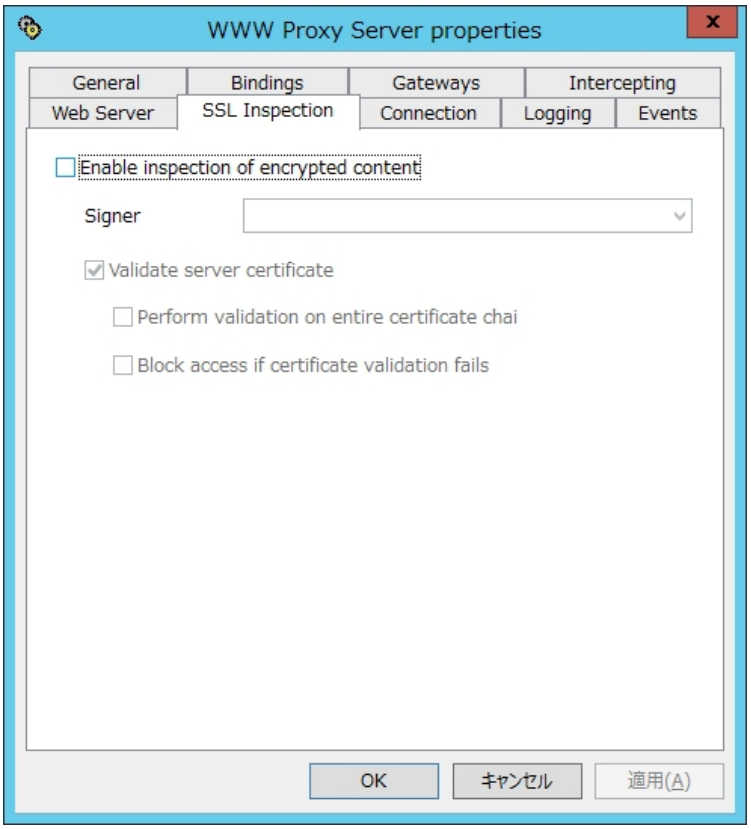
**Web Server**（Web サーバー）WWW Proxy Server のみ




Web Server は、プロキシリクエスト以外の要求（非プロキシリクエスト）が WWW Proxy Server へ送られた場合にどのように、そのリクエストを取り扱うかを設定することができます。
デフォルトでは、Reject request（リクエストを拒否）が設定されており、非プロキシリクエストが送られた場合、WWW Proxy Server は、リクエストを拒否します。
以下のアクションより設定することができます。

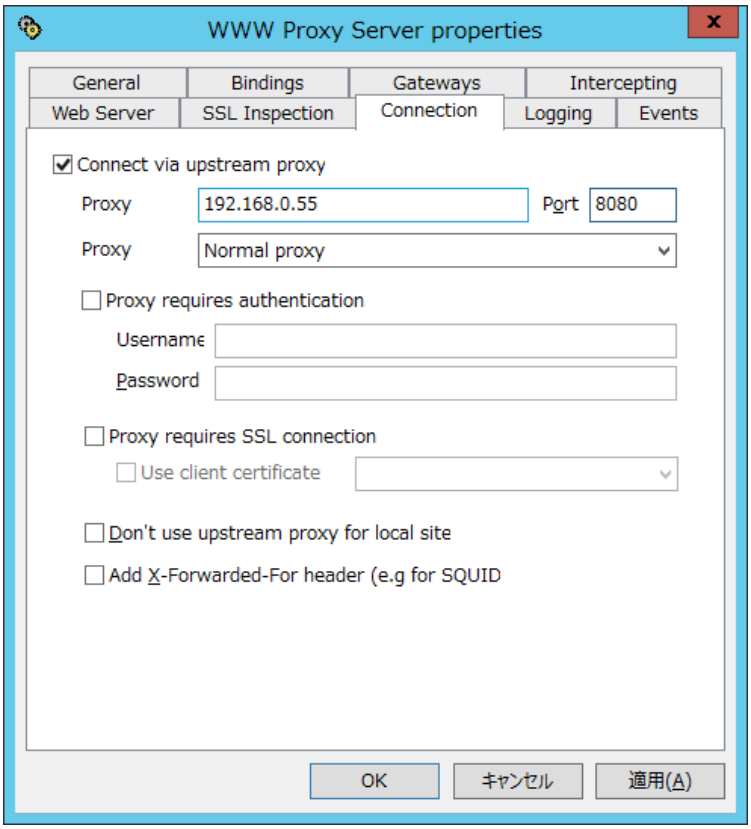
- Reject request
  リクエストを拒否
- Reverse proxy（リバースプロキシ）
  リバースプロキシとして動作させる場合は、このオプションを選択します。このアクションを選択した場合、リバースプロキシとして接続する接続先サーバー、ポートなどのオプションを設定することができます。
- Redirect（リダイレクト）
  指定した URL へ接続を転送する場合は、このアクションを選択します。このアクションを選択すると転送先の URL を設定することができます。
- Serve（サーブ）
  WinGate を Web サーバーとして使用する場合には、このアクションを選択します。このアクションを選択した場合、Web サーバーとして動作させるために root ディレクトリなどの設定を行うことができます。
- Proxy
  非プロキシリクエストに関してもプロキシとして取り扱う場合は、このアクションを選択します。

**SSL Inspection（SSL インスペクション）** WWW Proxy Server のみ



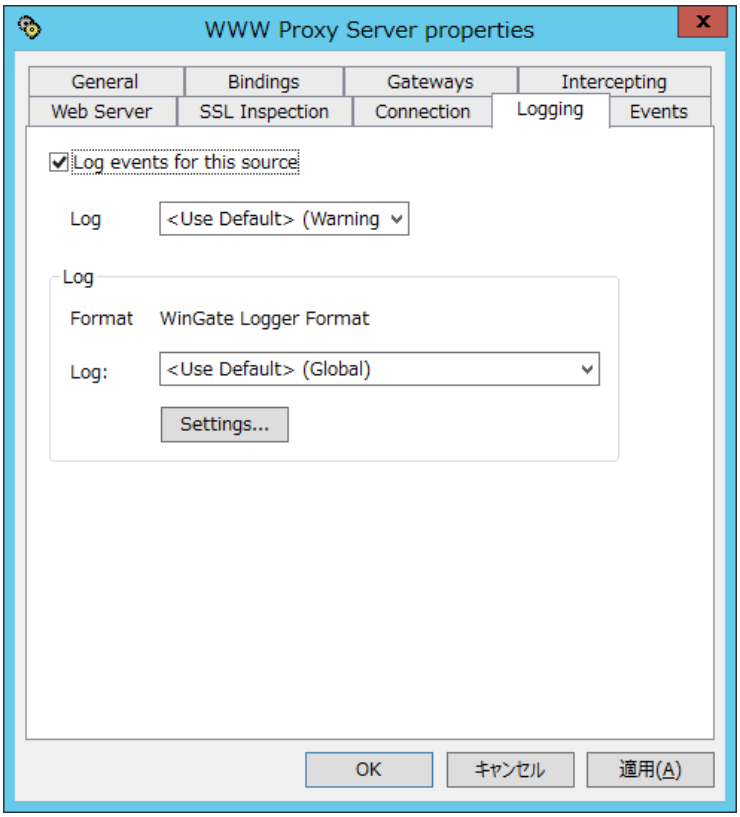

暗号化されたコンテンツを検査する場合に、設定します。この機能を使用することにより、SSL を使用する WWW Proxy リクエストをフィルタリング、キャッシュ、ウイルススキャンすることが可能となります。
この機能を使用するには、クライアントマシンへ中間証明書を配布する必要があります。

**Connection**（接続）




Connection では、多段プロキシの構成を行うことができます。多段プロキシを使用する場合は、Connect via upstream proxy（上位のプロキシを経由）をチェックして、経由するプロキシサーバーとポートを設定してください。Proxy type（プロキシの種類）では、接続するプロキシの種類を選択してください。
接続先のプロキシサーバーが入賞を必要とする場合は、Proxy requires authentication（プロキシは認証が必要）をチェックして認証情報を入力してください。

**Logging**（ロギング）

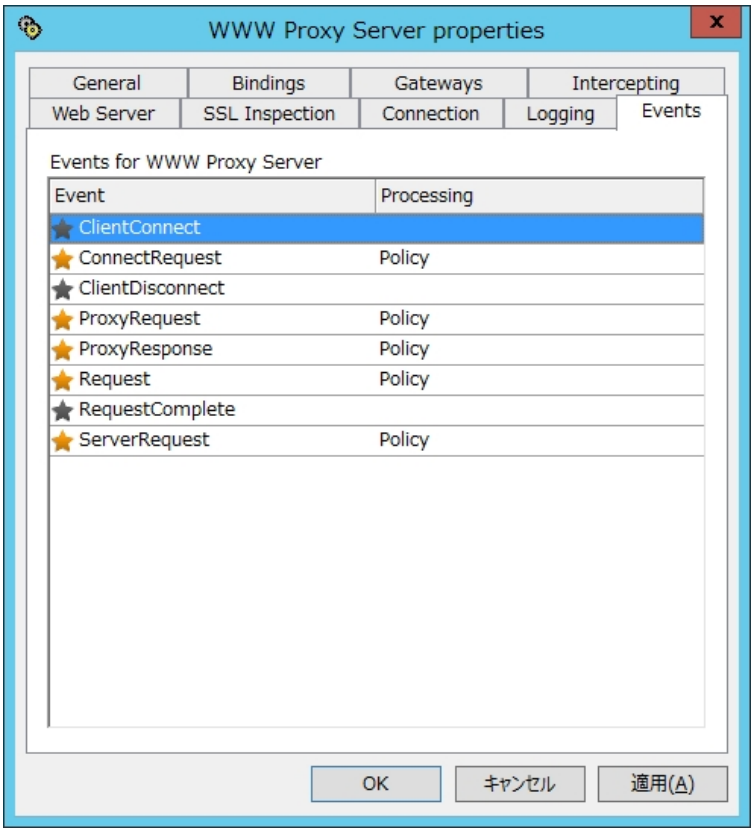



Logging では、そのプロキシサーバーのログ取得の有効、無効、および取得方法を設定することができます。ログ取得を行わない場合は、Log event for this source（このソースのイベントをログ）のチェックを外してください。

**ご注意**：WinGate のログは、Diagnostic（診断）ログと Usage（使用）ログの２種類があります。ここでは、Diagnostic（診断）ログの取得方法についての設定を行うことができます。Usage（使用）ログの変更は Logging で変更する必要があります。
**ご注意**：WinGate のログ設定は、デフォルトで取得するレベルは Warning となっており。警告のみを記録いたします。また、Log 欄にあるように、その Warning のログ内容は、Global ログファイルに全て保存される設定となっております。これを各 Proxy server 毎に保存する場合は、Log のドロップダウン・メニューで Own log file（自身のログファイル）を選択してください。これにより各 Proxy server 毎に警告ログを取得することができます。

Settings ボタンより、ログファイル名やログ保存ディレクトリ、ログのフォーマットを設定することができます。詳しくは Logging をご覧ください。

**Event**（イベント）

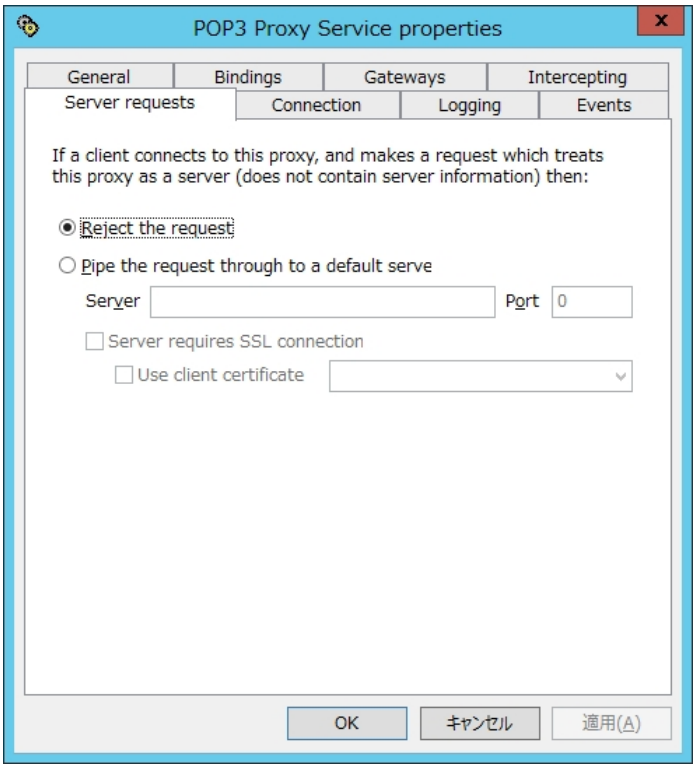



Event では、その Proxy server に対してどのようなイベントが有効で、どのような処理に利用されているかを確認、設定することができます。

**個々のサービス固有の設定**

- **POP3 Proxy Service**

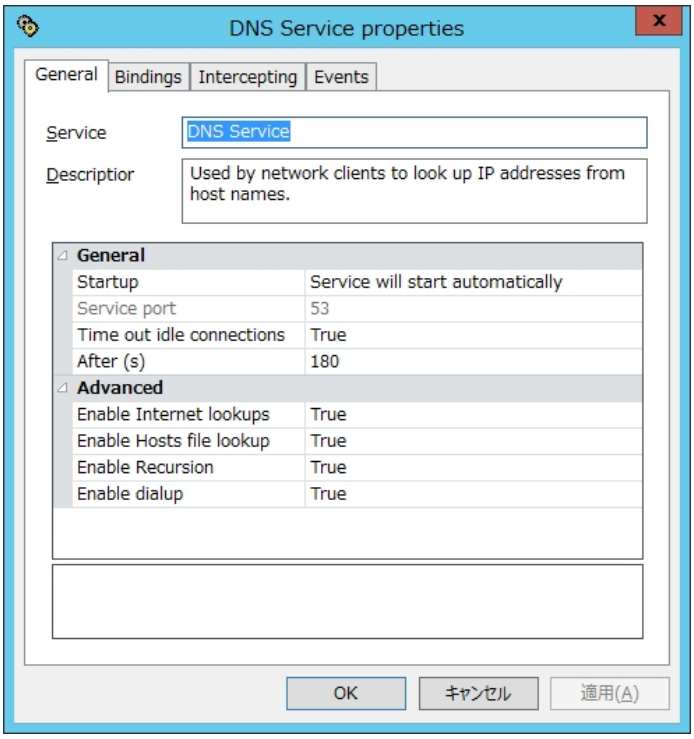
  **Server request**（サーバーリクエスト）タブ




  Server request は、POP3 Proxy Service で利用することができます。POP3 Proxy Service に対して非プロキシリクエストが行われた場合に、どの接続をどのように取り扱うかを設定することができます。
  デフォルトでは、Reject the request が選択されておりリクエストを拒否します。
  指定した接続先へリクエストをパイプする場合は、Pipe the request through to a default server を選択してパイプ先のサーバーとポート番号を入力してください。

- **DNS Service**

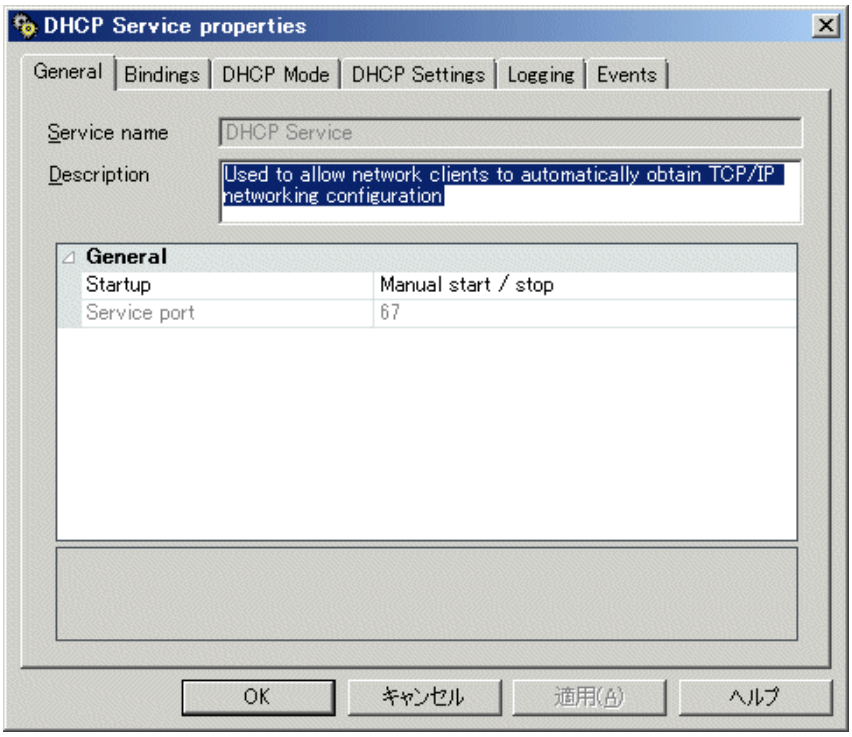
  General タブ




Enable dialup

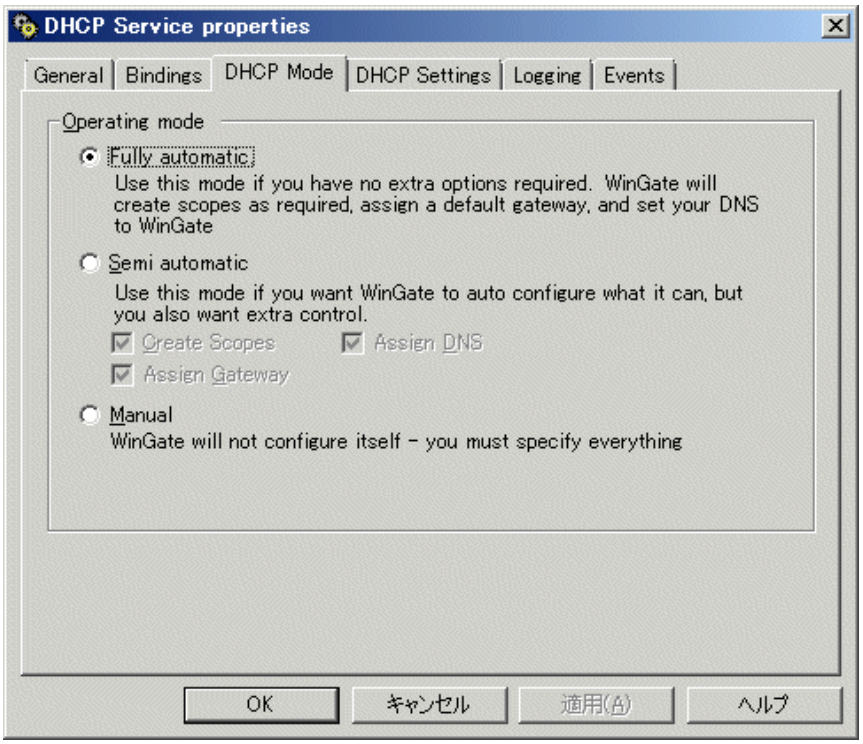
Enable dialup は、WinGate サーバーPC がダイアルアップ接続を持つ場合に、DNS リクエストがダイアルアップの接続を実行するかを設定します。True の場合は有効、False は無効となります。

- **DHCP Service**




DHCP Service は、WinGate を DHCP サーバーとして構成することができます。

DHCP Mode（DHCP モード）タブ




DHCP Mode タブでは、WinGate の DHCP サービスが、どのように運用されるかを選択します。

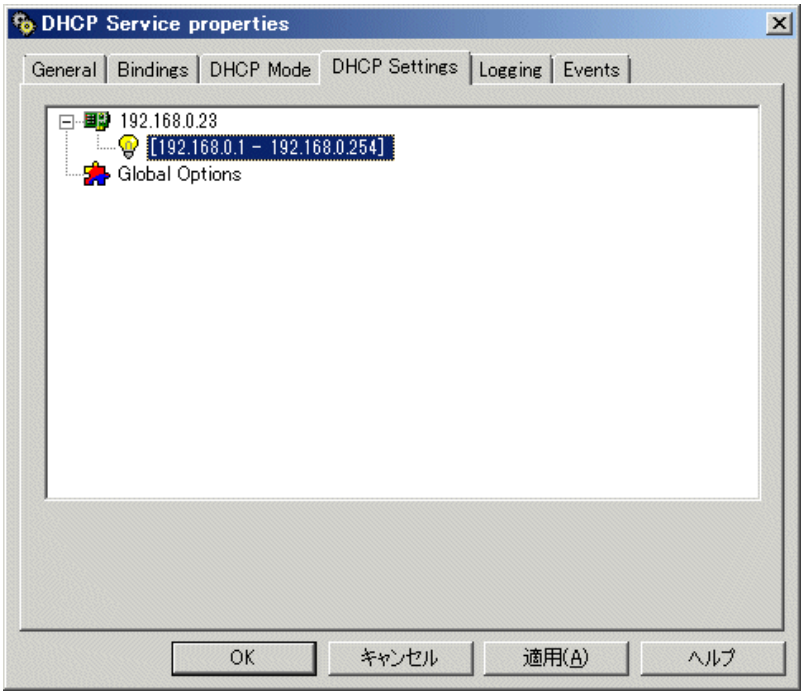
Fully automatic（フルオートマティック）を選択した場合、デフォルトゲートウェイ、DNS サーバーを WinGate マシンに設定してアドレスを割り当てます。

Semi automatic（セミオートマティック）では、どれを WinGate マシンにするかを選択することができます。

マニュアルでは、全て手動で設定することができます。

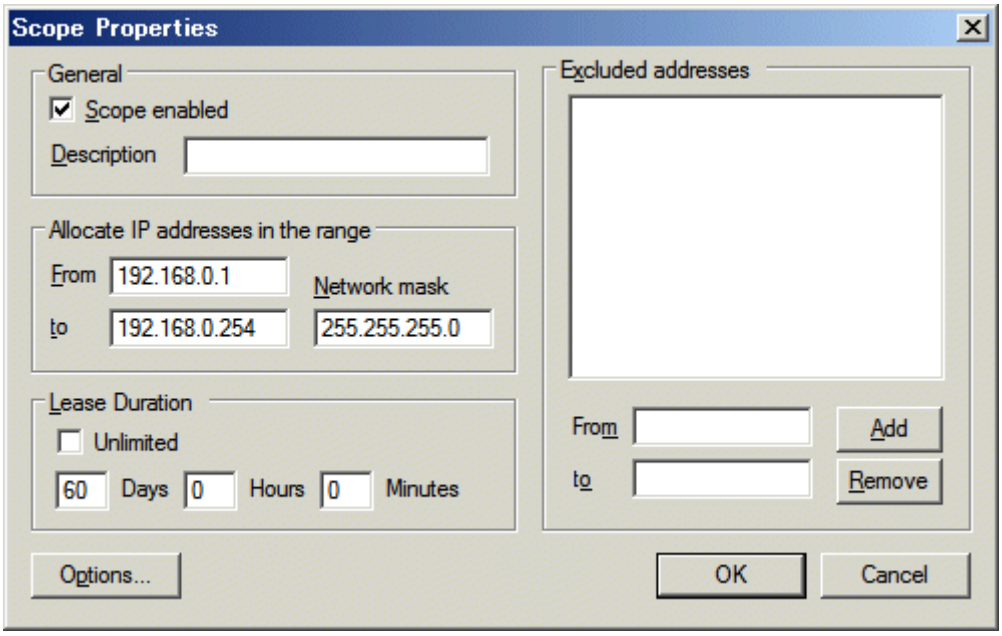
Manual（手動）では、全てを手動で設定する必要があります。

DHCP Settings（DHCP 設定）タブ



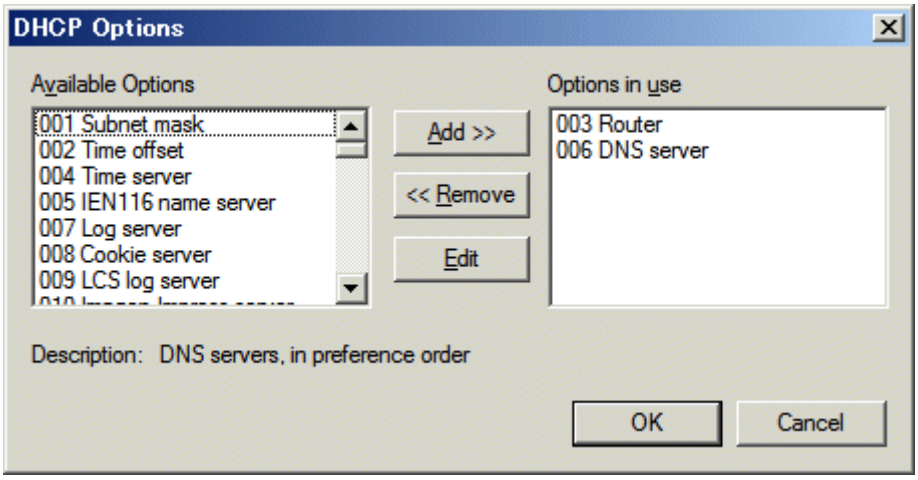

DHCP Settings タブでは、DHCP 設定の詳細を設定、確認することができます。

設定されているスコープをダブルクリックすることにより「スコープのプロパティ」ダイアログを表示することができます。（スコープが追加されていない場合、右クリックにより New scope（スコープの新規作成）を選択してください。）

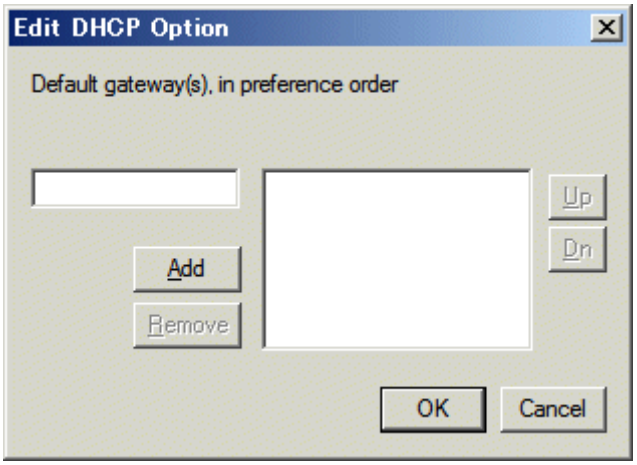



スコープのプロパティでは、Scope enable（スコープの有効・無効）、Allocate IP addresses in the range（IP アドレスの割り当て範囲）、Lease Duration（リース期間）、Excluded addresses（除外アドレス）を設定することができます。

Options（オプション）ボタンにより、このスコープで使用されるDHCPオプションを設定することができます。



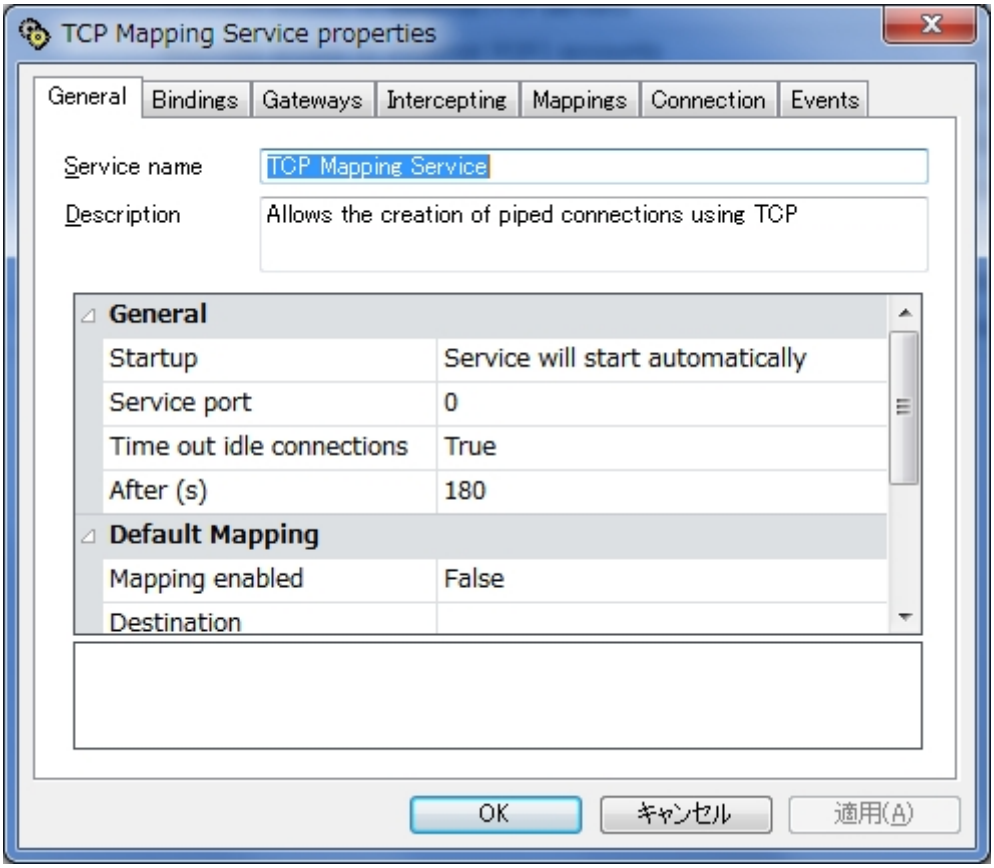

使用中のいずれか項目を選択した状態で編集ボタンをクリックすると、設定可能な内容が表示されます。




- **TCP/UDP Mapping Service**

  TCP/UDP Mapping Service は、TCP/UDP の接続を指定したサーバーのポートへマッピングすることができます。

  これは外部の SMTP サーバーを使用する場合や決められたサーバーへの TCP 接続を行う場合に使用することができます。




主な設定項目

**Service Port** = TCP Mapping で接続を受け付けるポートを指定します。TCP Mapping Service は、ここで指定されたポートと Bindings で開始された IP アドレスで接続を受け付けます。

**Default Mapping**

**Mapping enabled** = 設定したデフォルトマッピングの有効・無効を設定します。False は無効状態、True は有効の状態となります。

**Destination** = デフォルトマッピングのディスティネーション（目的地）を指定します。（マッピング先の

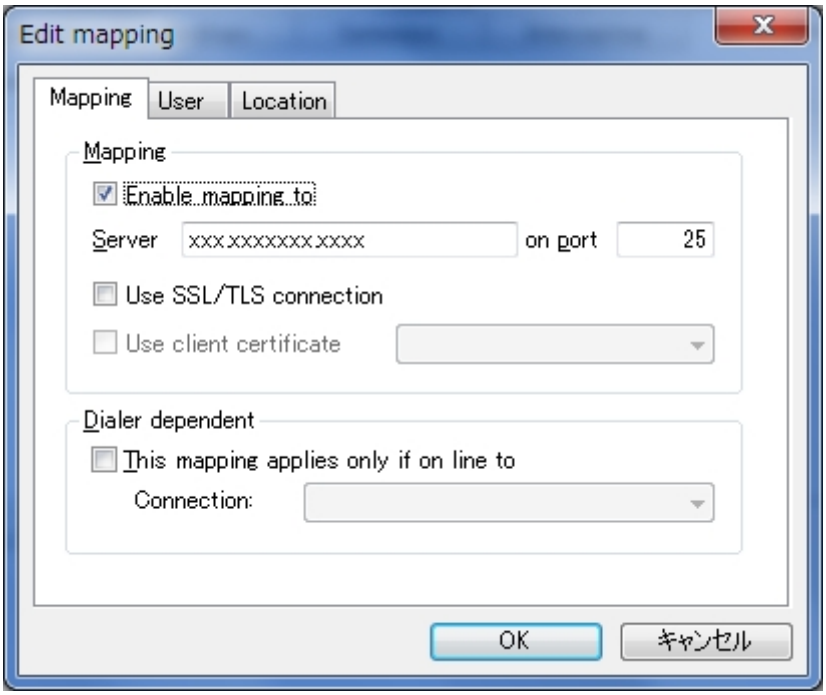
サーバー）指定は、IP アドレス、または名前解決可能なホスト名となります。

**Destination Port** = ディスティネーションのポート番号となります。

例：外部の SMTP サーバーを指定する場合、Destination で smtp.xxxxx.co.jp，Destination Port で 25 を指定します。また、Service port は、25 を指定します。

**Mappings タブ**

Default Mapping とは別に条件に合わせてマッピング先を指定することができます。

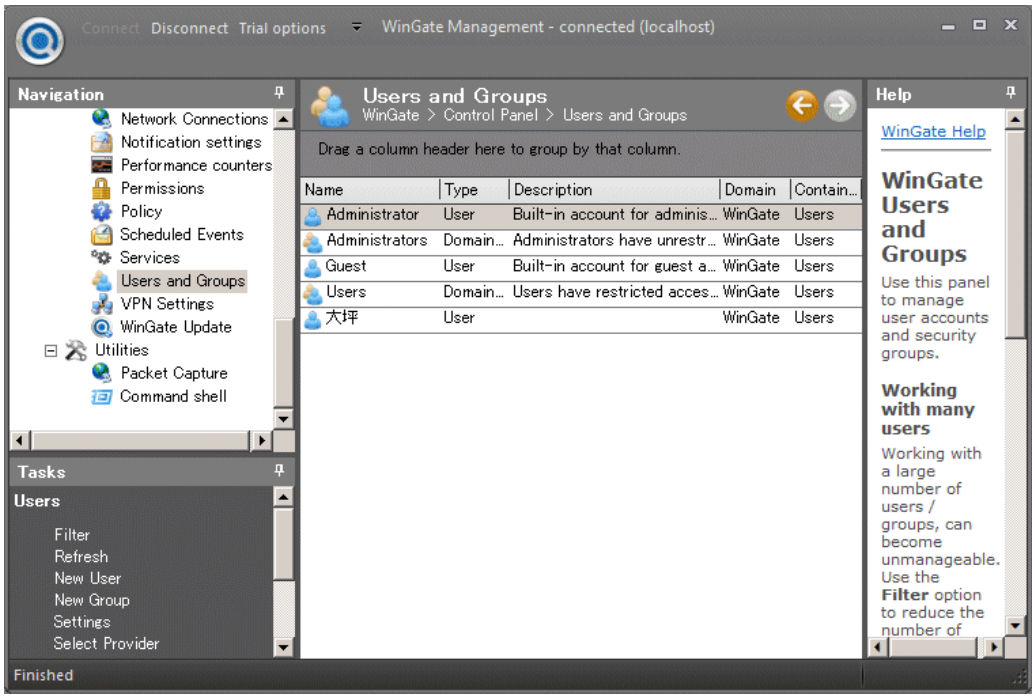



このマッピングを使用できるユーザーや、ユーザーのロケーションを指定することができます。

ユーザーやロケーションに一致しない場合は、デフォルトマッピングで指定した内容が使用されます。

デフォルトマッピングが無効である場合は、接続が拒否されエラーとなります。

### User and Groups（ユーザーとグループ）

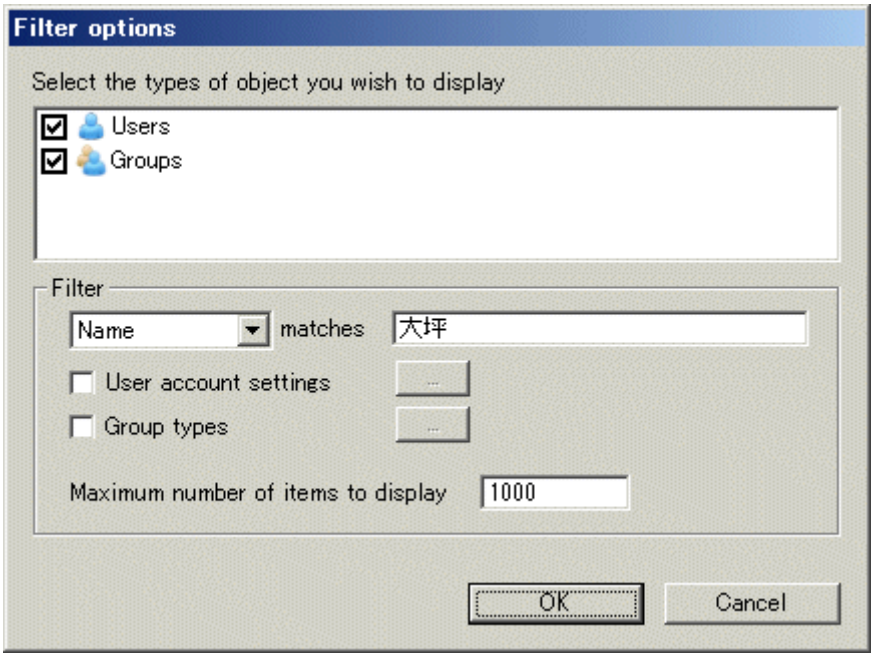



User and Groups では、WinGate で使用するユーザーとグループの構成することができます。

**ご注意**:インストール時に Active Directly Connector、Windows Users and Groups Connector を選択した場合、ユーザー管理はそれぞれのユーザー・データーベース（Active Directly、Windows ユーザー・データーベース）で行う必要があります。

Tasks の Users からは、以下の動作を実行できます。

- Filter（フィルター）

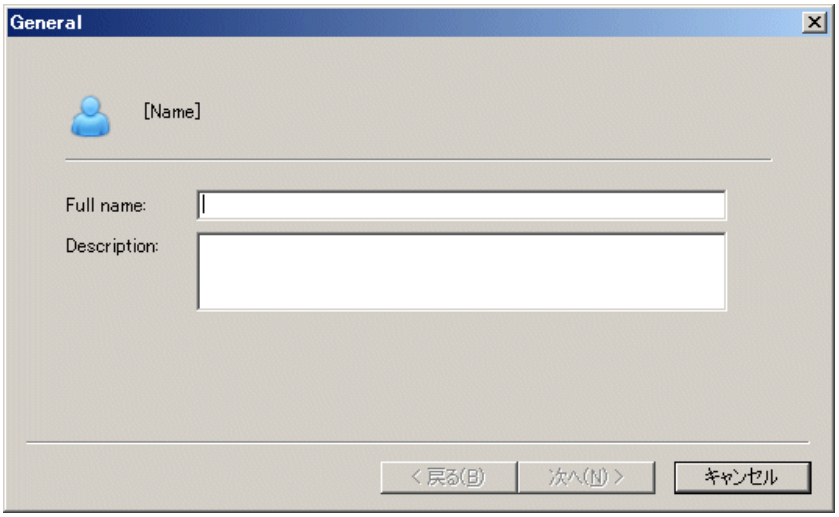



多くのユーザーが構成されている場合、Filter タブより条件を指定して、ユーザーの絞り込みを行うことができます。一旦 Filter 条件を指定すると指定した条件で、ユーザーやグループを表示します。

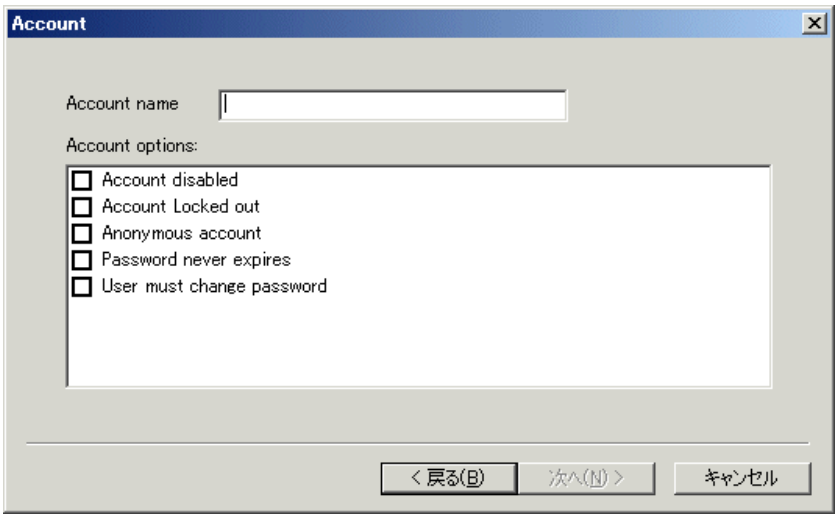
ユーザー、グループ欄の表示を元に戻す場合は、Filter 条件をクリアしてください。

- Refresh（更新）
  Refresh を実行すると、表示内容を最新の情報に更新します。

- New User（新規ユーザー）
  新しくユーザーを作成する場合、New User をクリックすると新しいユーザーを作成するためのウィザードが開始されます。



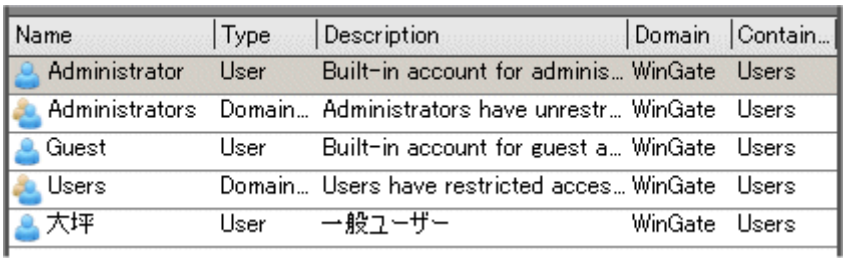

Full name（フルネーム）にユーザーの名前を入力します。Description（説明）には、そのユーザーの説明を入力します。（任意）




Account name（アカウント名）には、そのユーザーのアカウント名を入力します。
Account options は、以下の内容を意味します。必要に応じてチェックしてください。
Account disabled ＝ アカウントは無効
Account Locked out ＝ アカウントをロックアウト
Anonymous account ＝ 匿名アカウント
Password never expires ＝ ポスワード期限切れなし
User must change password ＝ ユーザーはパスワード変更が必要

Password には、そのユーザーのパスワード、Confirm にはパスワード確認のため同じパスワードを入力してください。

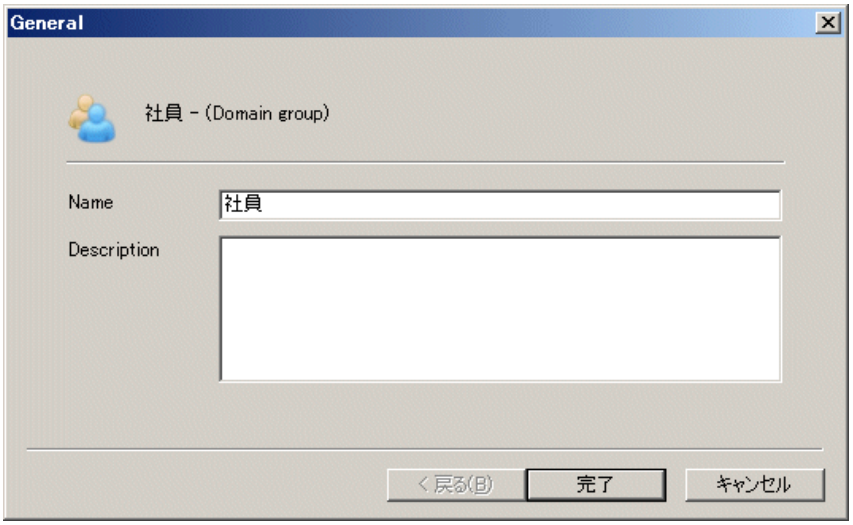
全ての内容が完了するとユーザーが、ユーザー欄に追加されます。



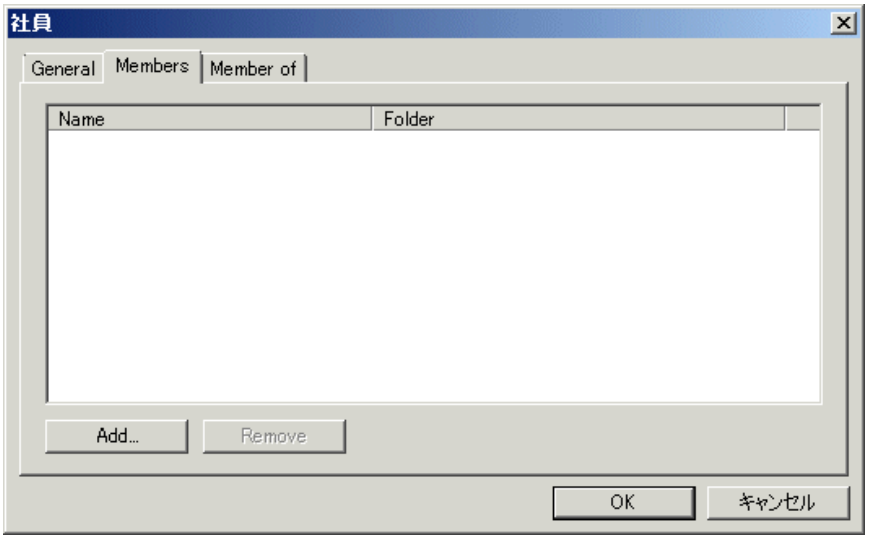
| Name | Type | Description | Domain | Contain... |
|---|---|---|---|---|
| Administrator | User | Built-in account for adminis... | WinGate | Users |
| Administrators | Domain... | Administrators have unrestr... | WinGate | Users |
| Guest | User | Built-in account for guest a... | WinGate | Users |
| Users | Domain... | Users have restricted acces... | WinGate | Users |
| 大坪 | User | 一般ユーザー | WinGate | Users |

- New Group（新規グループ）

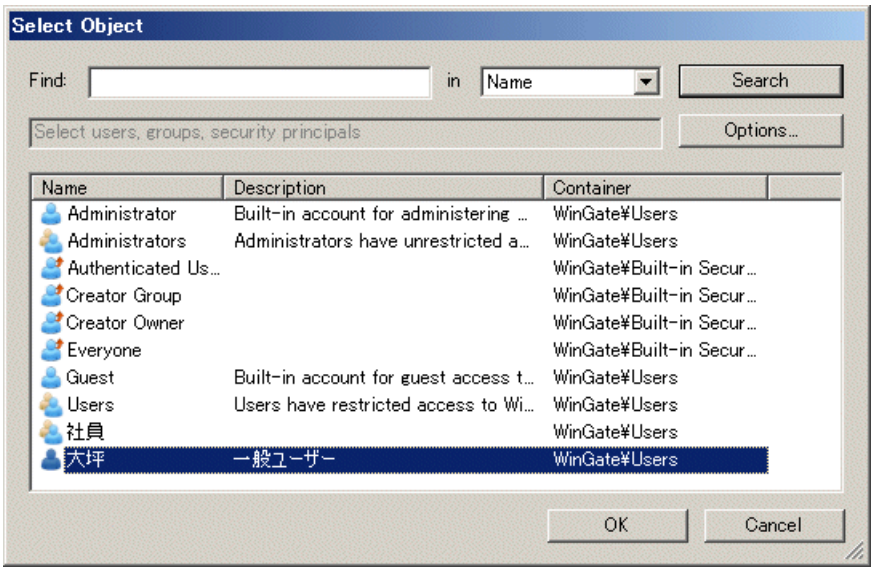
  新しくグループを作成する場合、New Group をクリックすると新しいグループを作成するためのダイアログが開始されます。



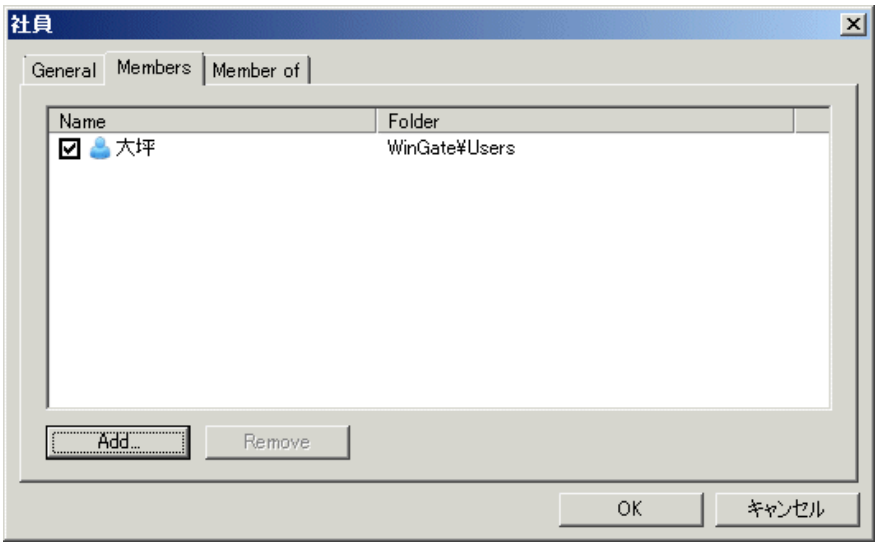

Name（名前）欄にグループ名を入力、Description（説明）に、そのグループの説明を入力してください。
完了ボタンでグループが追加されます。
グループのメンバーの設定を行うには、追加したグループをダブルクリック、または編集を行うグループを選択して、Tasks の Users から Edit（編集）ボタンをクリックしてください。




Members タブで、グループのメンバーを追加することができます。
メンバーを追加するには Add（追加）ボタンをクリックしてください。

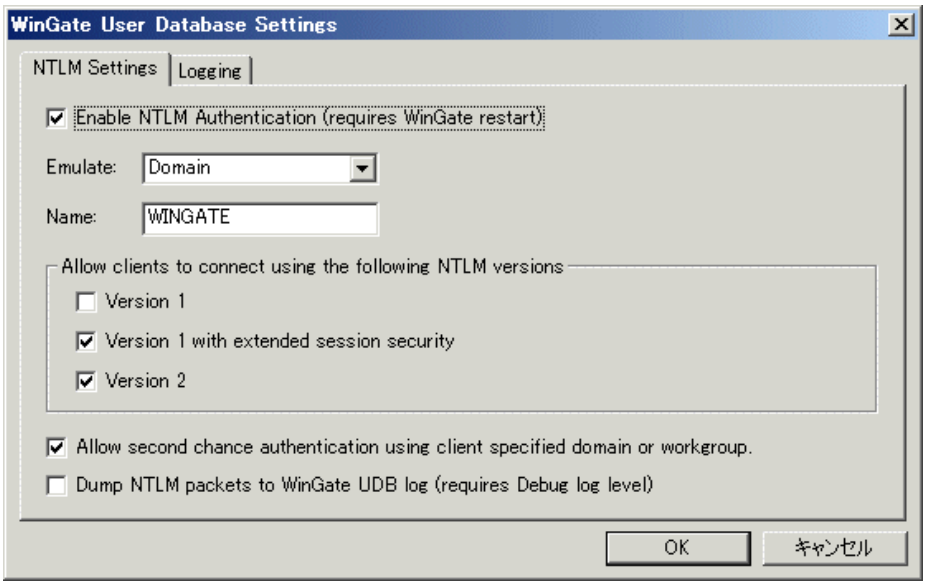



Select Object（オブジェクトの選択）ダイアログが表示されますので、検索条件をFindに入力しSearchボタンをクリックしてください。（全てのユーザーを表示する場合は、検索条件を入力する必要はありません。）
表示されたユーザーからグループに追加するユーザーを選択して OK ボタンをクリックしてください。




Member タブにユーザーが追加されます。
メンバーを削除するには、グループから削除するユーザーを選択して Remove（削除）ボタンをクリックしてください。

- Settings（設定）
  Settings では、使用しているユーザー・データーベースに関する設定を行うことができます。
  WinGate ユーザー・データーベースを使用している場合は、以下のダイアログが表示されます。

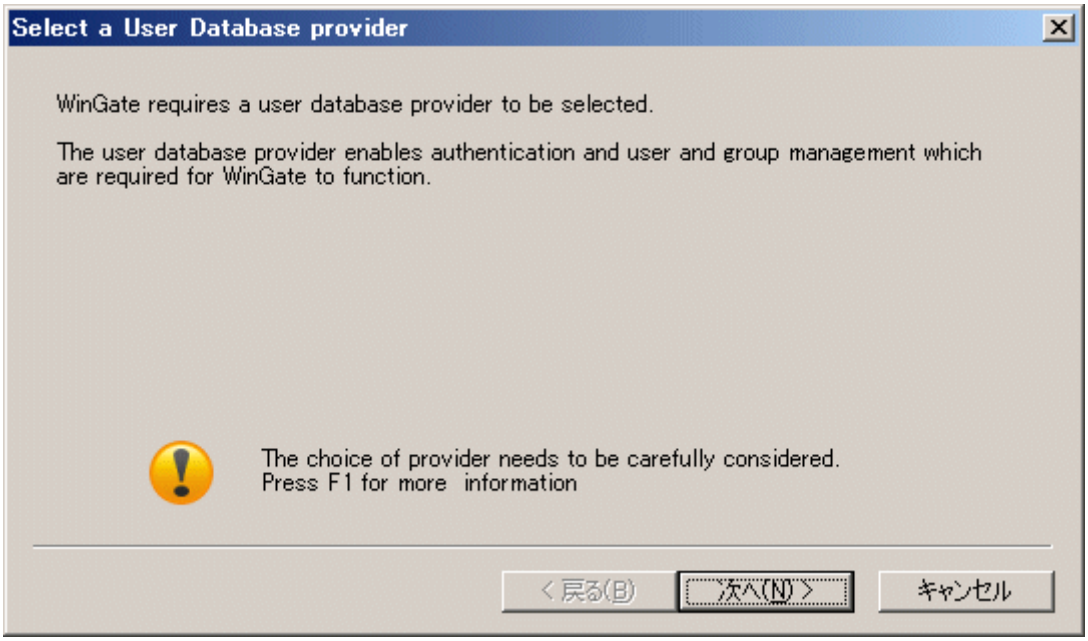



NTLM Settings（NTLM 設定）

Enable NTLM Authentication（NTLM 認証を有効）＝NTLM 認証を有効にする場合は、チェックをしてください。
必要に応じて NTLM 認証の Emulate（エミュレート）と Name（名前）設定してください。
また、NTLM もバージョンを選択してください。

- Select Provider（プロバイダの選択）
  Select Provider をクリックすると WinGate で使用されるユーザー・データーベースの種類を変更することができます。

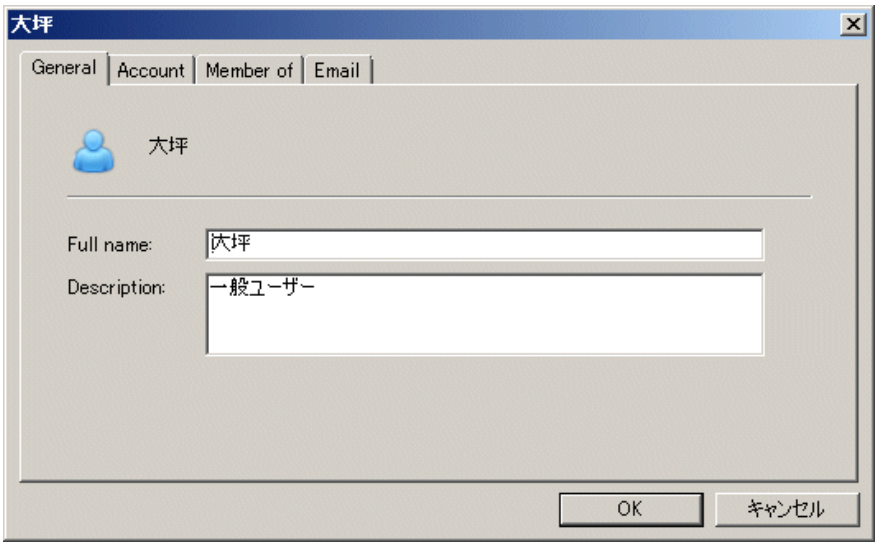
ウィザードに従いユーザー・データーベースの種類を変更してください。



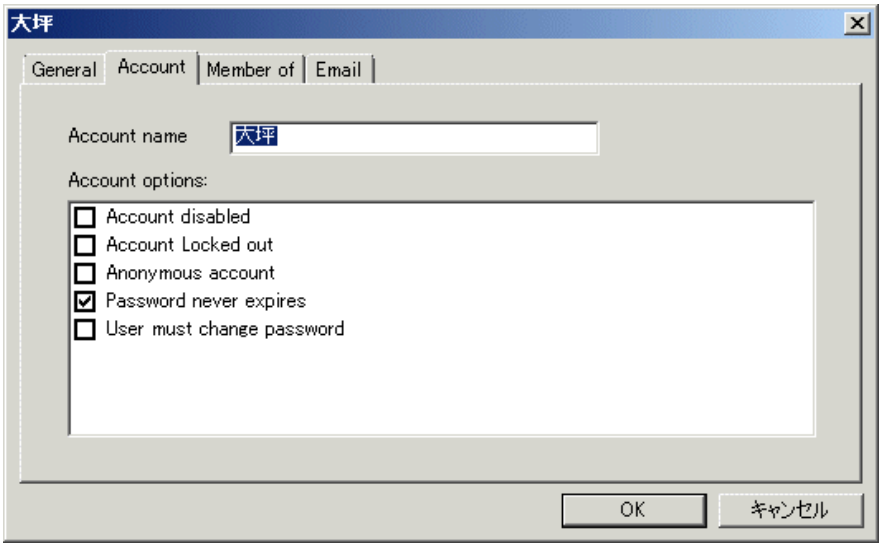

変更後は、新しいユーザー・データーベースを認識するために WinGate が再起動されます。

- Edit（編集）
  ユーザーやグループを選択して Edit ボタンをクリックすると、設定されたユーザーやグループを変更することができます。

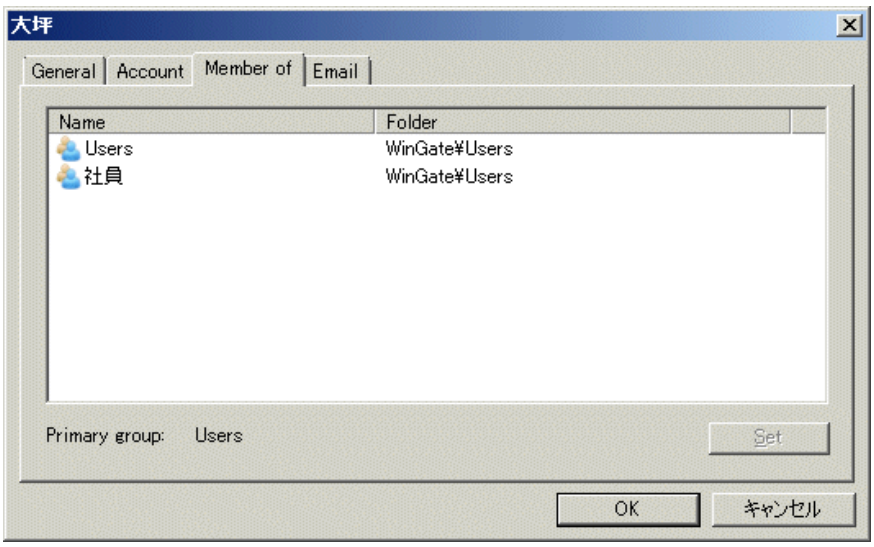
ユーザーの編集



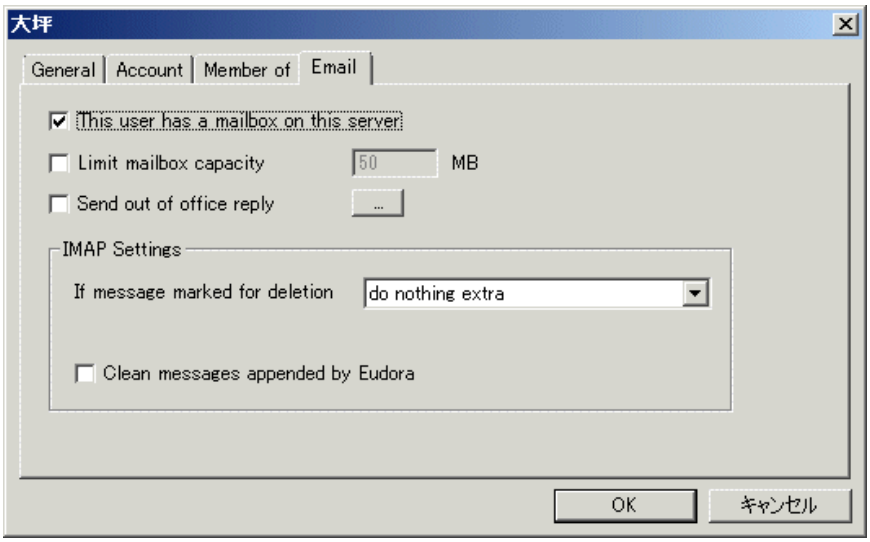

General（全般）タブでは、設定されている、ユーザーの Full name（フルネーム）、Description（説明）を編集する事ができます。




Account(アカウント)タブでは、ユーザーの Account name(アカウント名)と Account options(アカウントオプション)を設定することができます。




Member of(メンバー)には、どのユーザーが属しているグループが表示されます。複数のユーザーに属している場合、優先させるグループを選択して Set ボタンをクリックすると Primary group(プライマリ・グループ)として設定することができます。




Email（メール）タブでは、そのアカウントが WinGate の電子メールサーバー機能で、どのような電子メールアカウント設定とするかを設定することができます。

各項目の内容は以下の通りです。

This user has a mailbox on this server（このユーザーは、このサーバーでメールボックスを持つ）

WinGate のメールサーバー機能が使用されていない場合やユーザーがメールボックスを持つ必要がない場合は、このチェックを外してください。

Limit mailbox capacity（メールボックス容量を制限）

メールボックスの容量を制限する場合は、このチェックを有効にして制限するサイズを入力してください。

Send out of office reply（外出時の返信を送信）

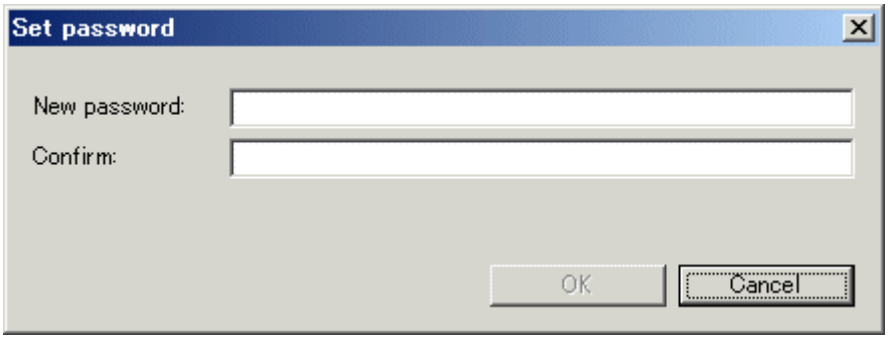
メールを見られない場合などに自動応答のメッセージを返信する場合は、このチェックを有効にして返信するメッセージを右側のボタンから表示されるダイアログで入力してください。

IMAP Settings（IMAP 設定）

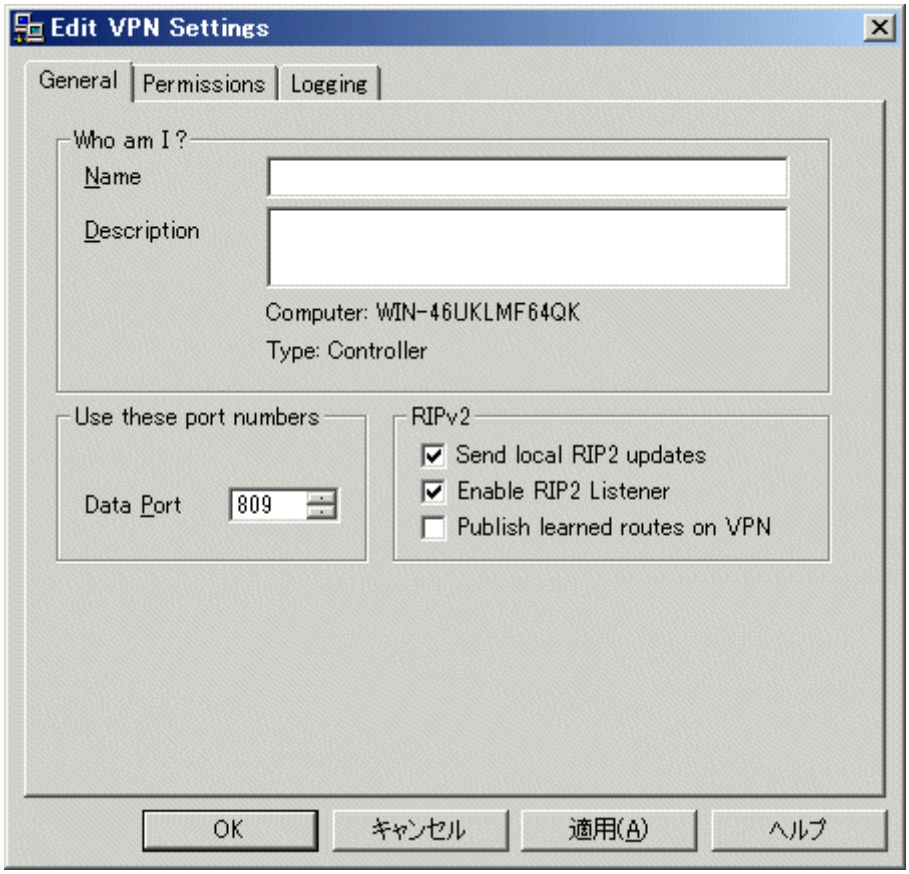
IMAP のメッセージ削除の関する設定を行うことができます。

- Set password（パスワードの設定）

  新しくパスワードを設定する場合や既存のパスワードを変更する場合、設定するユーザーを選択して、Set password をクリックしてください。

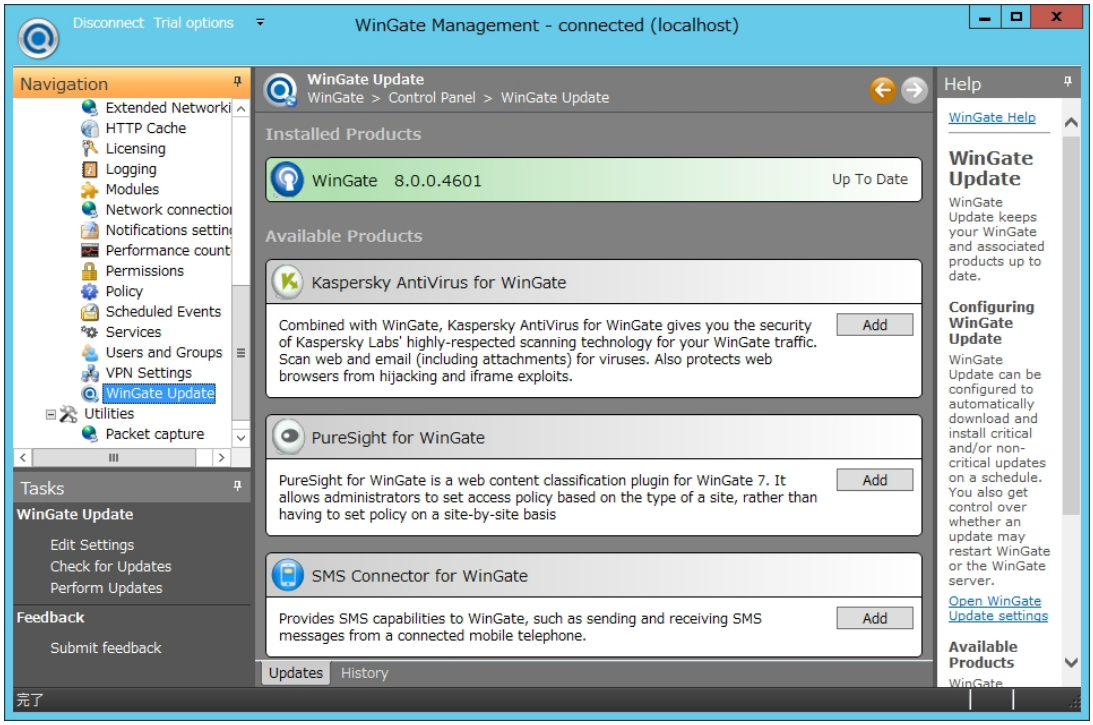


### VPN Settings（VPN 設定）




VPN Settings は、WinGate の VPN 機能を使用する場合に、VPN 機能の内容を設定するために使用されます。詳細な WinGate VPN のガイドをご参照ください。

### WinGate Update（WinGate アップデート）

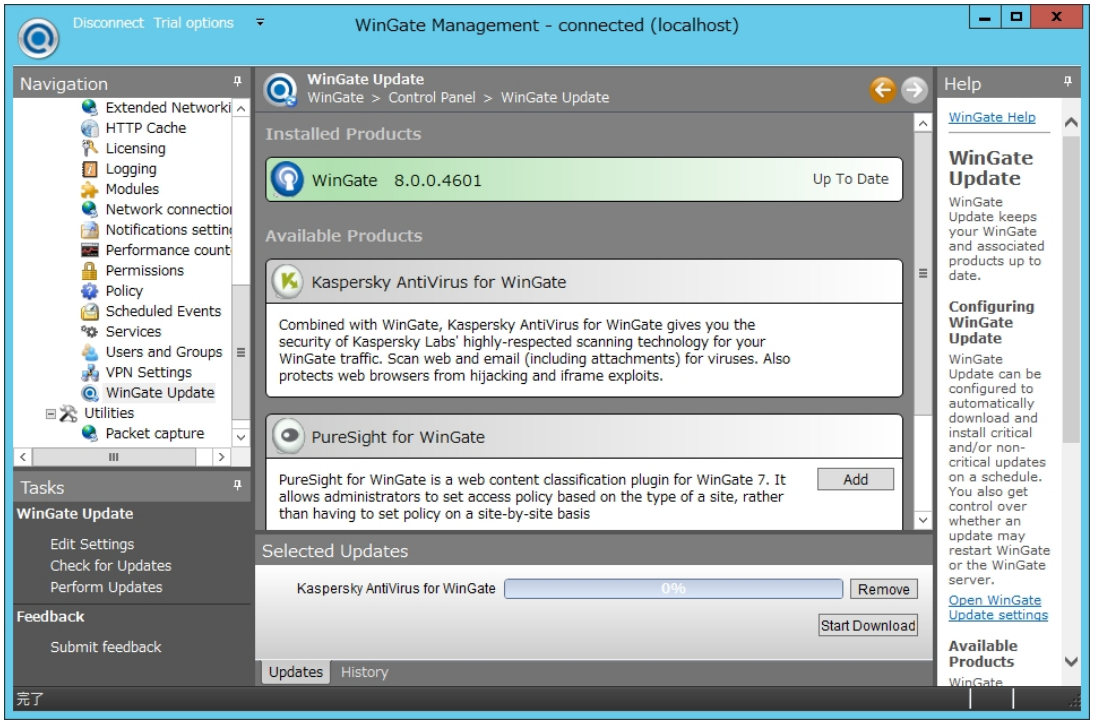



WinGate Update では、現在インストールされている WinGate やプラグインのバージョン情報や最新バージョンの確認、インストール方法などを設定することができます。

Installed Products（インストールされている製品）には、現在インストールされている WinGate のバージョンと

Kaspersky AntiVirus for WinGate などのプラグインのバージョン、および追加可能な製品が表示されます。Available Products（利用可能な製品）には、現在インストールされていない利用可能なプラグインが表示されます。

プラグインを追加する場合は、その製品の Add ボタンをクリックすると、下の欄に選択した製品のダウンロードウインドウが表示されます。




Start Download（ダウンロード開始）をクリックするとダウンロードが開始されます。ダウンロード完了後は、Install ボタンをクリックして、ダウンロードした製品のインストールを行ってください。（ダウンロードした製品のインストーラーが開始されます。）

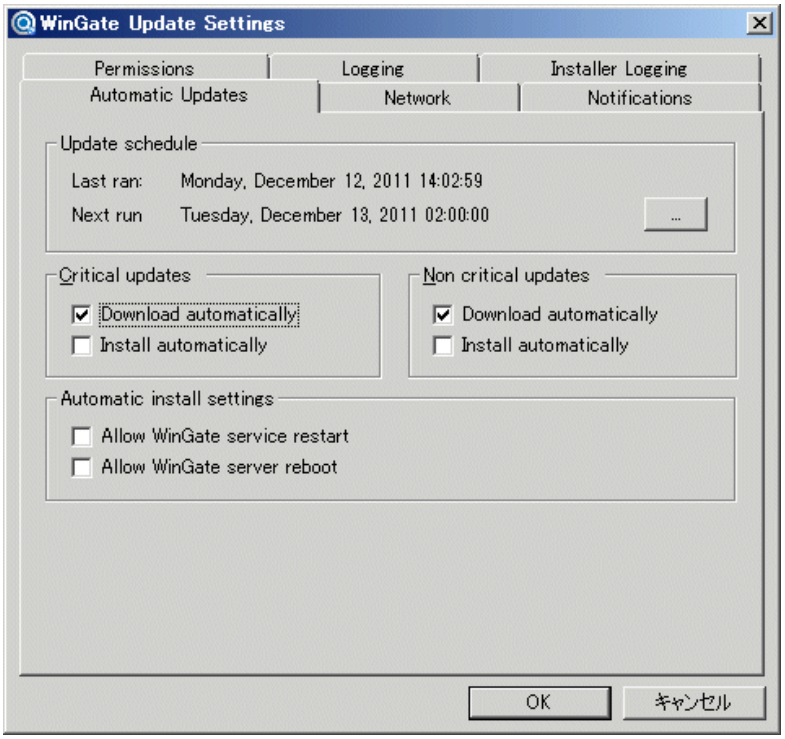
**ご注意**：インストーラーが開始されると製品をインストールするために WinGate エンジンは自動的に停止されます。

Tasks の WinGate Update では、以下の操作を行うことができます。

- Edit Settings（設定の編集）

  Edit Settings では、WinGate の更新に関する情報の確認、および更新の適用方法に関する設定を行うことができます。

  Automatic Update（自動更新）タブ



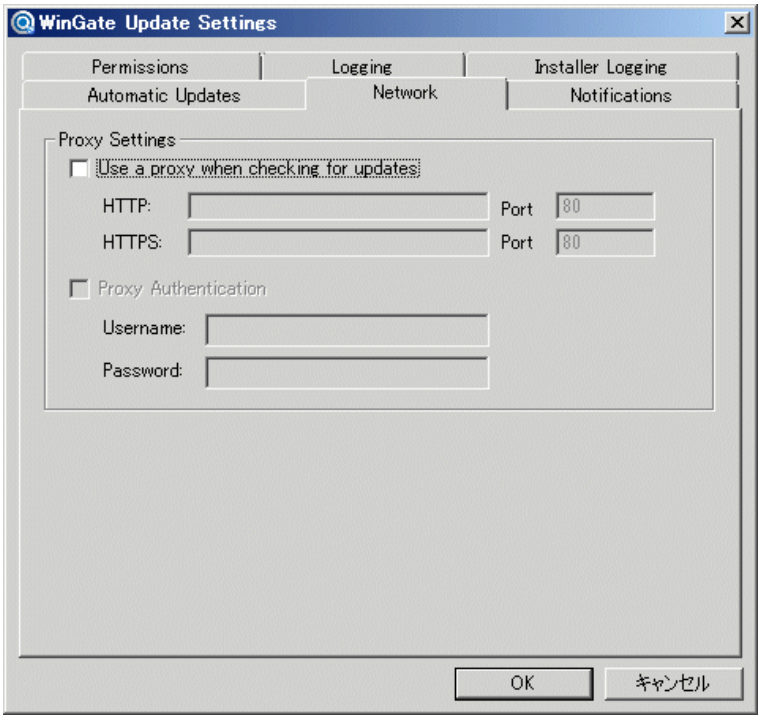

Update schedule（更新スケジュール）には、更新を確認するためのスケジュールの実行状況が表示されています。Last ran（前回の実行日時）Next run（次回の実行日時）が表示されています。右側のボタンをクリックするとスケジュールダイアログが表示されスケジュールの設定を変更することができます。

Critical updates（重要な更新）では、リリースされた重要な WinGate の更新があった場合の動作を設定することができます。
Download automatically をチェックした場合、ダウンロードを自動的に行います。
Install automatically をチェックした場合、ダウンロード完了後に自動的にインストールを開始します。

Non critical updates（重要ではない更新）では、重要な更新を持たない WinGate があった場合の動作を設定することができます。
Download automatically をチェックした場合、ダウンロードを自動的に行います。
Install automatically をチェックした場合、ダウンロード完了後に自動的にインストールを開始します。

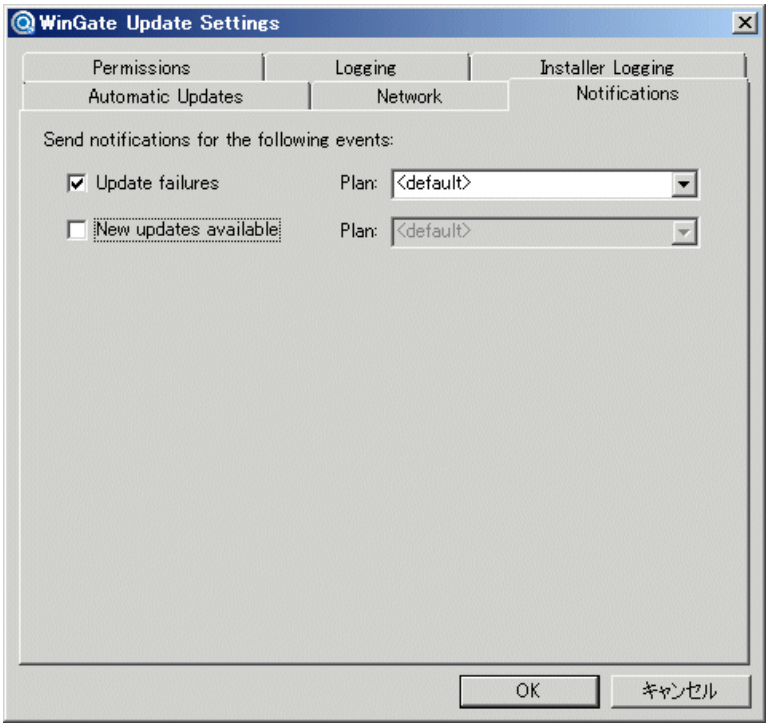
Automatic install settings（自動インストールの設定）では、Install automatically がチェックされた場合のインストール時の WinGate の状態を設定することができます。
Allow WinGate service restart（WinGate サービスの再起動を許可）をチェックした場合、インストール後に WinGate サービスを自動的に再起動します。
Allow WinGate server reboot（WinGate サーバーの再起動を許可）をチェックした場合、インストール完了後に WinGate サーバーを再起動します。

Network（ネットワーク）タブ




Network タブでは、更新の確認を行う際にプロキシサーバーを使用する設定を行うことができます。インターネット接続に上位のプロキシサーバーを使用する必要がある場合は、このタブで設定を行ってください。

Notifications（通知）タブ

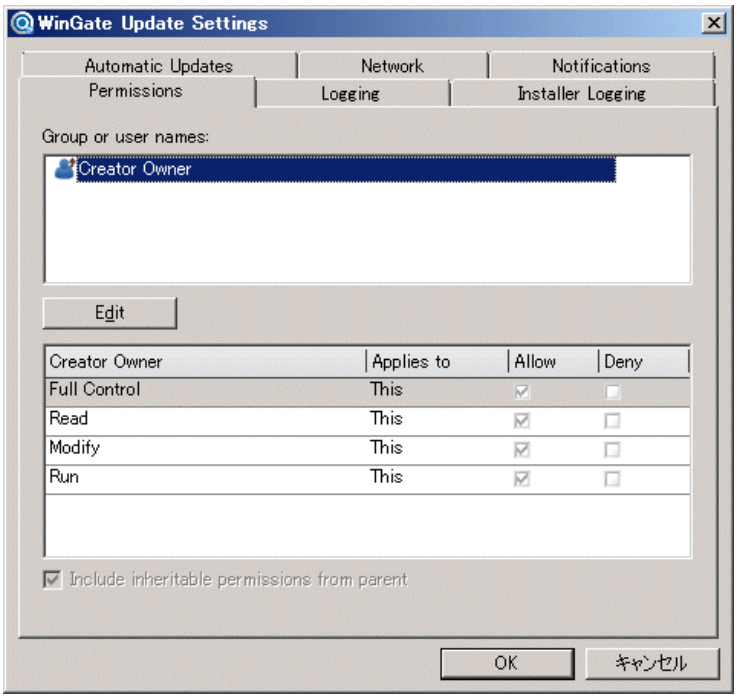



Notifications タブでは、WinGate Update で更新の失敗が発生した場合、および新しい更新があった場合に WinGate の Notification 機能でどのプランを適用するかを設置絵することができます。

Update failures（更新失敗）がチェックされた場合、更新に失敗した際に、選択された Plan（プラン）に基づき通知されます。

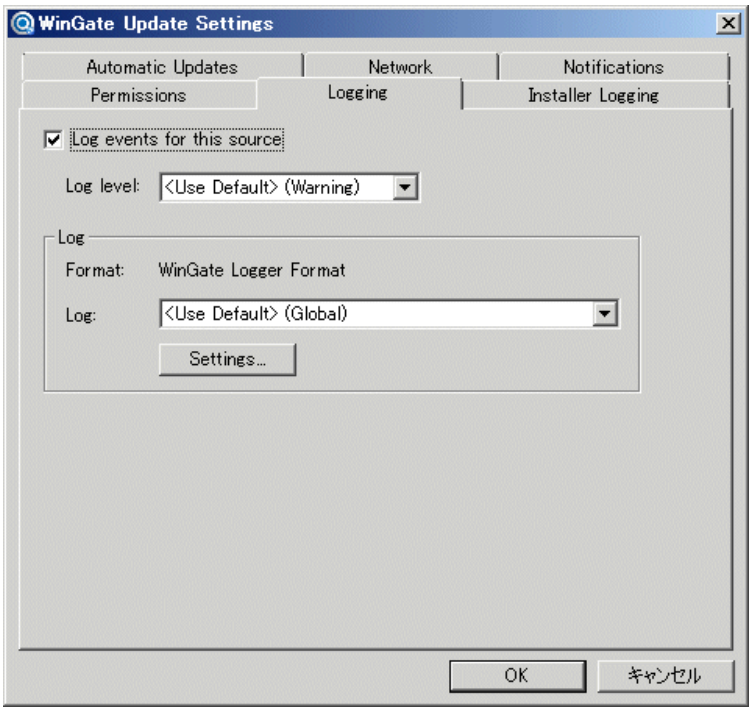
New update available（新しい更新が利用可能）がチェックされた場合、新しい更新がある場合に、選択された Plan（プラン）に基づき通知されます。

Permission（権限）タブ



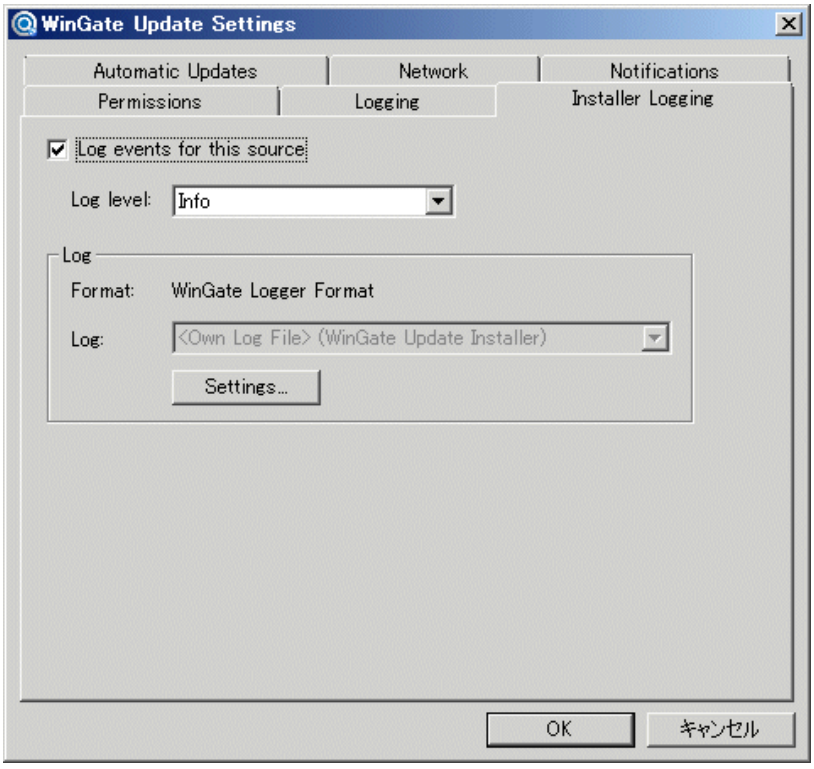

Permission タブでは、WinGate Update の権限を設定することができます。

Logging（ロギング）タブ




Logging タブでは、WinGate Update のログ取得方法について、設定することができます。
必要に応じて設定を変更してください。

Install Logging（インストールログ）タブ

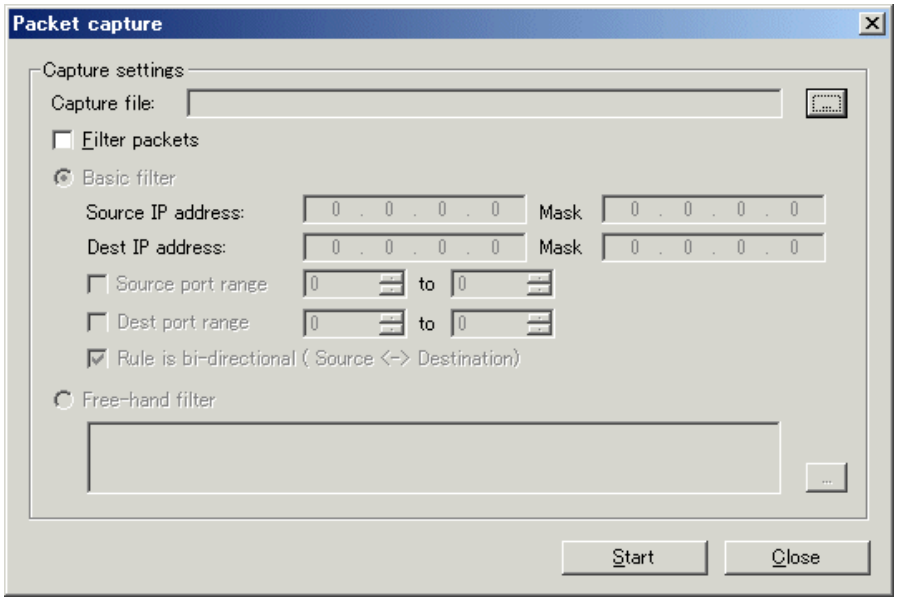



Install Logging タブでは、WinGate 更新のインストールに関するログ取得の設定を行うことができます。
必要に応じて設定を行ってください。

**Utilities（ユーティリティ）**

Utilities では、WinGate で発生した問題の解決やメンテナンスに必要なツールを使用する事ができます。

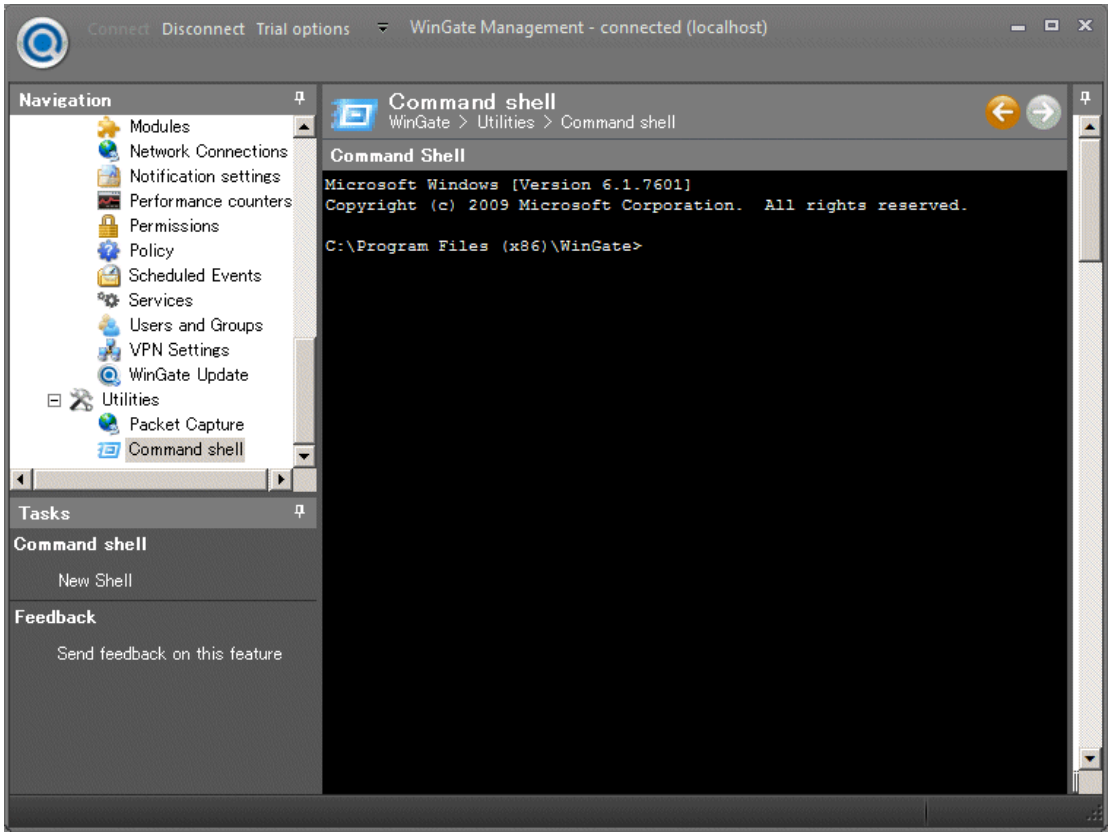
Packet Capture（パケットキャプチャー）




Packet Capture では、WinGate マシンのパケットをキャプチャする機能を使用することができます。
通常、この機能はサポートからの指示がない場合には、使用しないでください。

Command shell（コマンドシェル）

コマンドシェルを使用すると、WinGate Management 内でコマンドプロンプトを利用することができます。




## WinGate 設定例

この章では、基本的な設定をご照会しております。詳細な設定については、各機能の説明ページをご参照ください。

### クライアント PC から WWW Proxy Server を使用して Web サイトを参照

クライアント PC のブラウザでプロキシサーバーの設定を行い、WinGate の WWW Proxy Server をプロキシサーバーとして使用する場合の例となります。

この構成は NIC が 1 枚、または 2 枚でも利用できます。

1. WinGate をインストールします。

   **ご注意：WinGate の NAT 機能、ファイアウォール機能を使用しない場合は、インストール時に WinGate Network Driver をインストールしないでください。**

   インストール時には、最低限 WinGate services、および WinGate Management が選択されている必要があります。

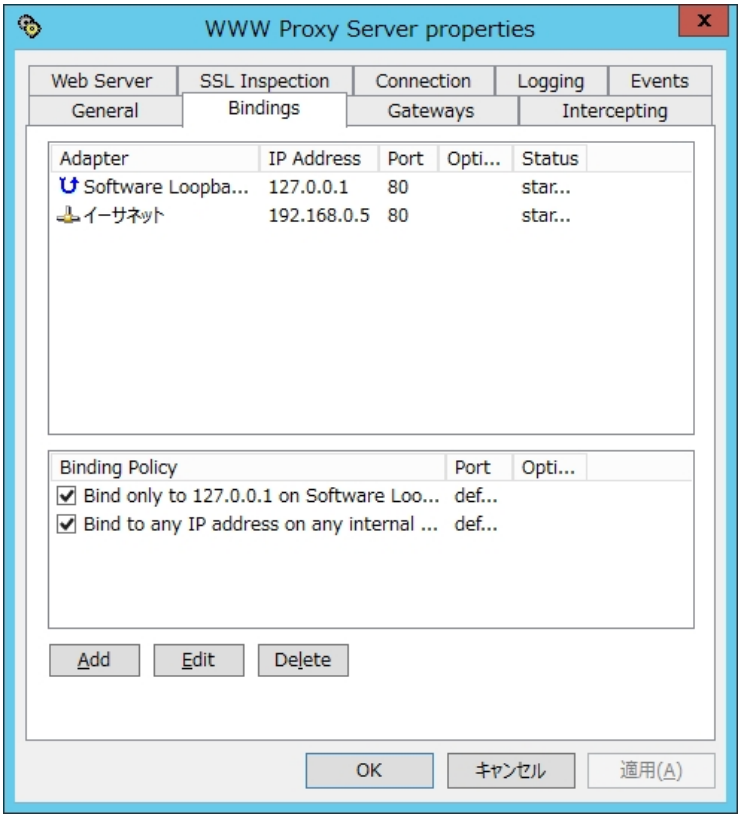
2. インストール完了後に、WinGate Management へログインします。

   必要に応じて、ログや通知の設定を変更してください。

3. WinGate Management の Navigation から Network Connections 開き、NIC の構成が WinGate の使用目的に合っているか確認してください。

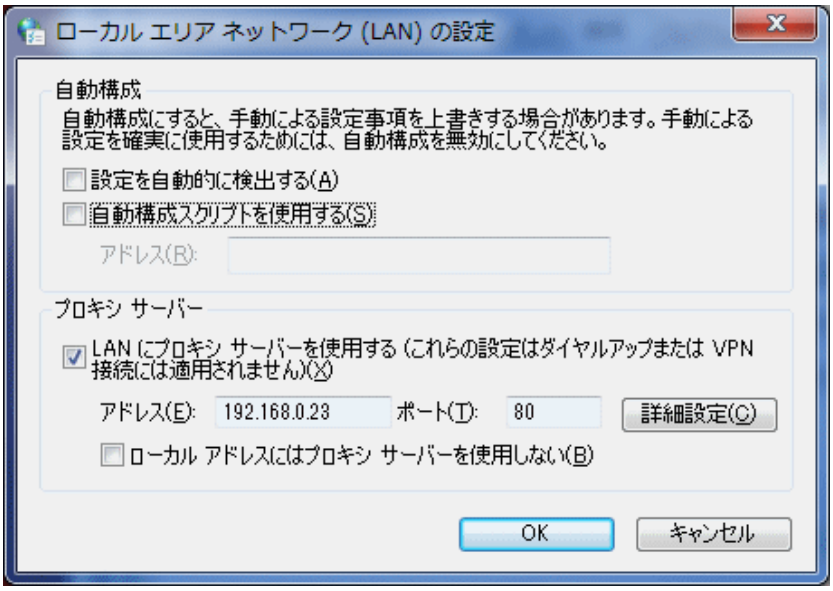
必要に応じて、Network Connections で NIC を Internal（内部）、External（外部）を選択してください。

4. WinGate Management の Navigation から Services を選択し、WWW Proxy Server をダブルクリックし WWW Proxy Server property ダイアログを開き、Binding タブを選択します。




上記の欄に表示されているインターフェースが接続を受け付けるインターフェースとなります。
接続を受け付けるインターフェースが正しいかをご確認ください。
変更する場合は、Binding Policy を必要に応じて変更してください。

5. クライアント PC のブラウザでプロキシサーバーを使用する設定を行ってください。
Windows の場合、コントロール・パネル、インターネットオプション、接続タブ、LAN の設定ボタンより表示されるローカルエリア ネットワーク（LAN）の設定ダイアログよりプロキシサーバーの設定を行うことができます。




6. クライアント PC のブラウザを起動し、Web ページの参照が行えるかを確認します。

ブラウザでの Web ページが表示できない場合の原因調査の方法については、本書のトラブルシューティングの章をご確認ください。

**WinGate のプロキシ機能を使用してメールの送受信を行う（POP3 Proxy、TCP Mapping）**

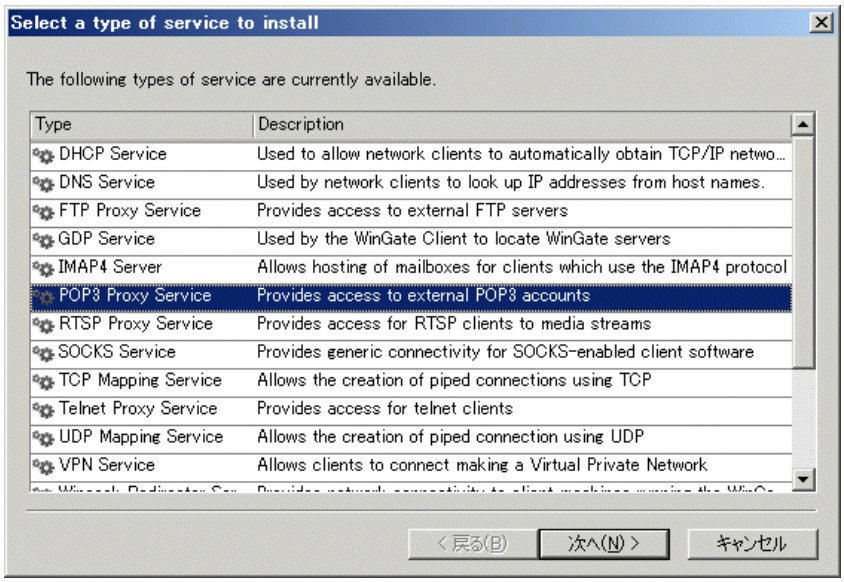
**ご注意**：WinGate が持つ SMTP Server、POP3 Server 機能は、メールサーバー機能となります。これらの Server 機能は、プロキシ、マッピングサービス機能とは異なります。SMTP Server では、WinGate が SMTP Server として動作し直接メールの配信・受信を行いますのでご注意ください。

WinGate のプロキシサービスを利用してメールの送受信を行う場合、WinGate の POP3 Proxy Service と TCP Mapping Service を使用します。

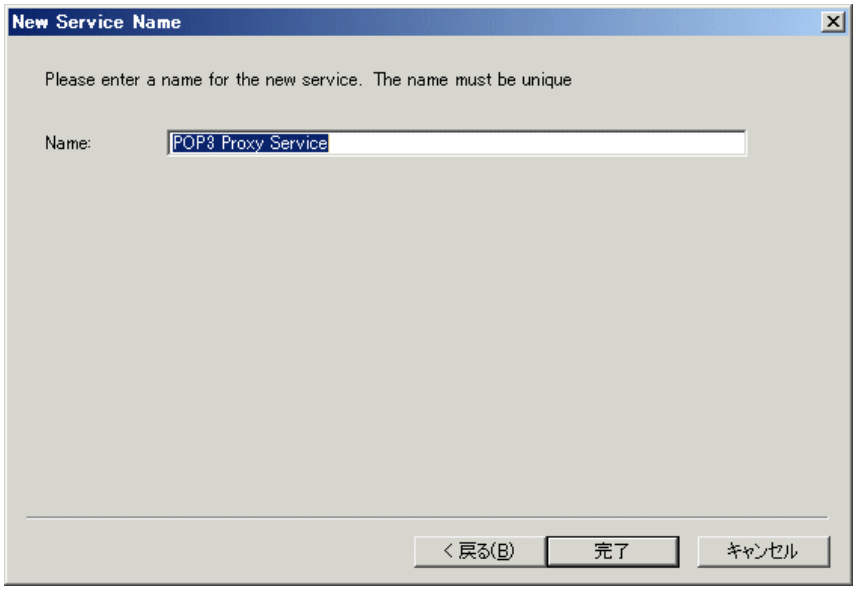
メールの受信には POP3 Proxy Service を使用します。

POP3 Proxy Service は、デフォルトでは追加されていないため WinGate Management の Navigation、

Services の Tasks から Install Service を選択して Select a type of services to install（インストールするサービスのシュルを選択）らか POP3 Proxy Service を選択します。



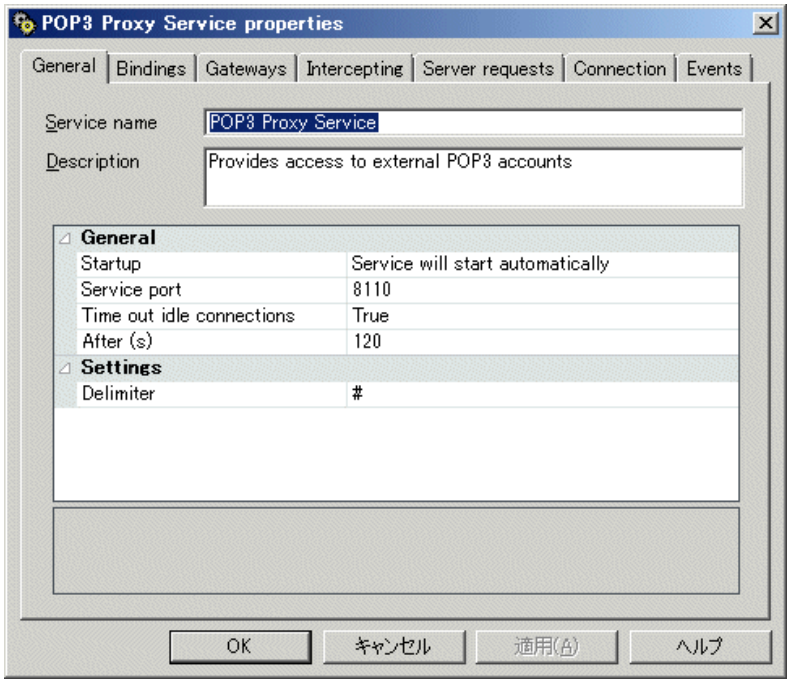

次へボタンをクリックします。




必要に応じて Name（名前）変更してください。

完了ボタンで終了します。

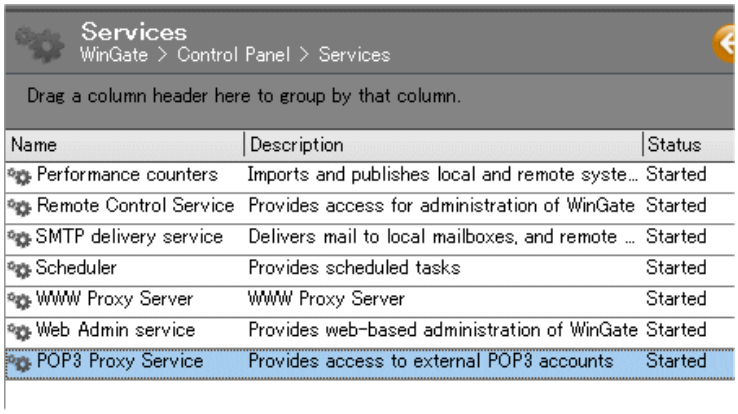
POP3 Proxy Service property ダイアログが表示されますので、必要な設定を確認します。




デフォルトでは Service port に 8110 が割り当てられていますので、必要に応じて変更してください。(一般的には POP3 のポートとして 110 が使用されます。)

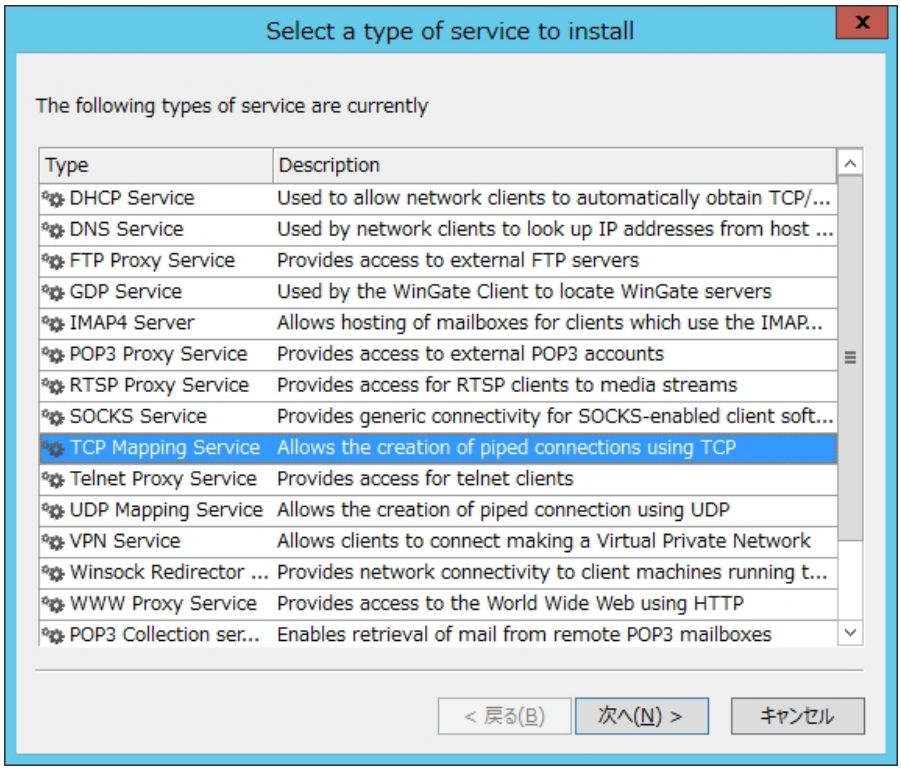
また、Binding タブで接続を受け付けるインターフェースの確認を行ってください。

OK ボタンで終了すると Services に POP3 Proxy Service が追加されます。

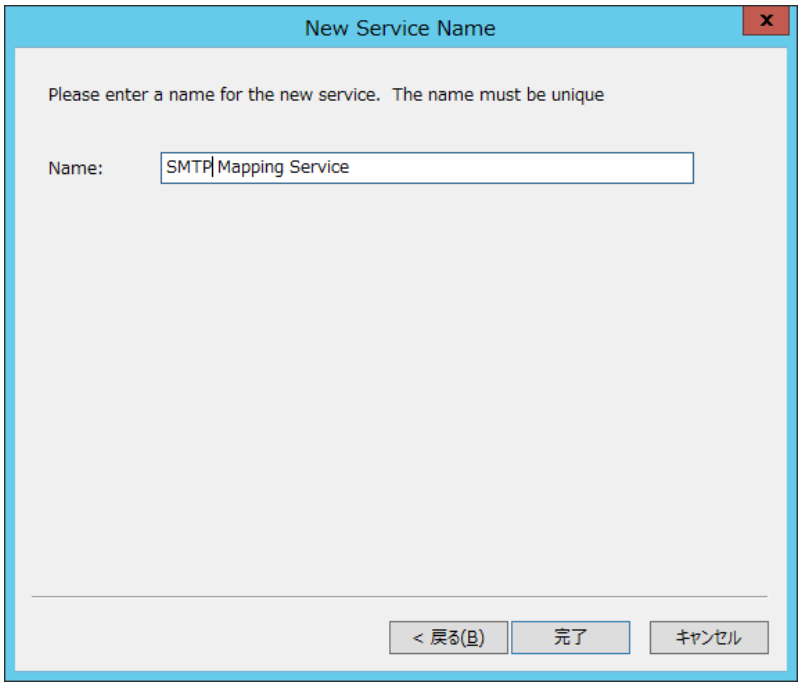



メール送信に使用する TCP Mapping Service の追加を行います。

WinGate Management の Navigation、Services の Tasks から Install Service を選択して Select a type of services to install(インストールするサービスのシュルを選択)らか TCP Mapping Service を選択します。

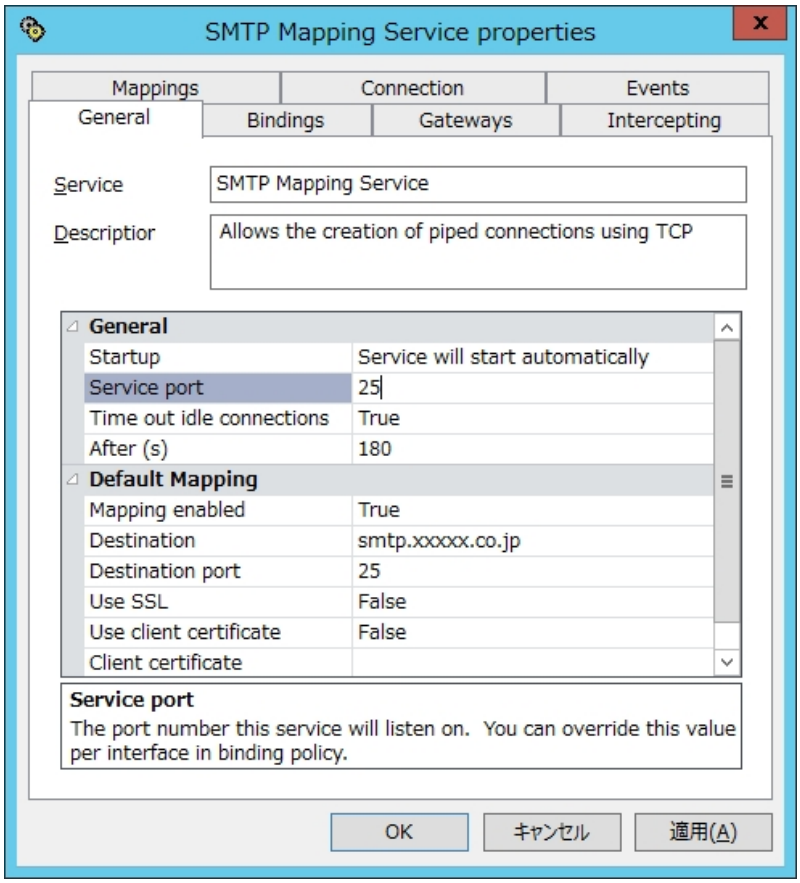



「次へ」をクリックします。




Name（名前）をわかりやすいように、SMTP Mapping Service などに変更し、完了ボタンをクリックします。

SMTP Mapping Service ダイアログが表示されます。




SMTP に使用するサービスとなるため、WinGate で接続を受け付けるポートを Service port で指定します。一般的に SMTP には 25 ポートが使用されます。

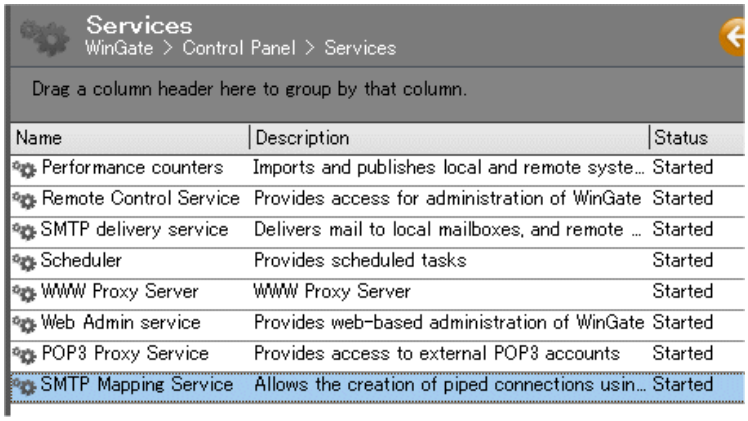
メール配信に利用する外部の SMTP サーバーを Destination（ディストネーション）欄に入力します。

また、その配信に使用する外部 SMTP サーバーが接続を受け付けるポートを Description port 欄で指定します。

一般的にこれは 25、または 587（サブミッションポート）かもしれません。

このサーバーへのマッピングを行うために Mapping enabled のドロップダウン・メニューTrue を選択します。

OK ボタンで終了すると Services に SMTP Mapping Service が追加されます。




以上で WinGate の設定は完了となります。

メールクライアントで、これらのサービスを使用したメール送受信を行うための設定をします。

Outlook Express の設定は以下の通りとなります。

1.ツールメニューの「ツール」から「アカウント」を選択し、インターネットアカウントダイアログを開きます。

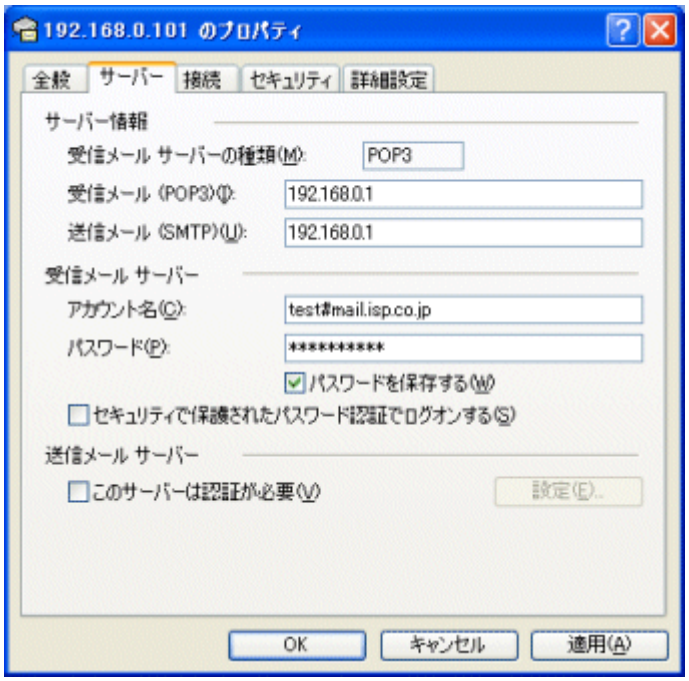
2.「メール」タブを開きます。ここで既にアカウントが作成されている場合、アカウントを選択して、「プロパティ」ボタンをクリックします。まだ設定していなければ、「追加」ボタンのメニューから「メール」を選択します。

3.プロパティ画面の「サーバー」タブで以下の設定を行います。

「送信メール」欄、「受信メール」欄には、WinGate サーバーの接続を受け付けている IP アドレス(192.168.0.1 等)を入力します。

「受信メールサーバー」欄では「次のアカウントとパスワードでログオンする」を選択し、「アカウント名」欄には「(プロバイダのアカウント)#(プロバイダのメールサーバー名)」、「パスワード」欄はプロバイダから受けたパスワードを記入します。

以下のスクリーンショットをご参照ください。




受信メール、送信メールサーバーに WinGate の IP アドレス、受信メールサーバーのアカウント名をアカウント名#メールサーバー(user#mail.isp.co.jp)と設定する事に注意してください。

4.OK ボタンでダイアログを終了します。

以上で、WinGate の POP3 プロキシ、SMTP マッピングを使用する構成は完了となります。

その他のアプリケーションのプロキシ設定に関しては、各ソフトウェア開発元にご確認ください。

メール送信に認証(SMTP 認証)を必要とする場合、メールクライアントにて認証の設定を行ってください。WinGate は、メールクライアントの認証情報を持ちません。

設定完了後は、利用するメールクライアントよりメールの送受信を行い、動作をご確認ください。送受信が正しく行えない場合は、送信のみ、受信のみを行い、どちらが正しく行えていないかをご確認ください。

**Extended Networking（拡張ネットワーク）の NAT を使用する方法**

NAT を使用するクライアントの構成は非常に簡単です。クライアントマシンの TCP/IP 設定でデフォルトゲートウェイに WinGate の内部側 NIC の IP アドレスが指定されている場合に利用可能でしょう。

NAT は、ほとんどのアプリケーションとの互換性をもっており、クライアントマシンで特に設定変更を行うことなくインターネット・アプリケーションをご使用いただく事ができます。

クライアントマシンのインターネット・アプリケーションではインターネットへ直接接続する設定がされていれば、ご使用いただく事ができます。

クライアントマシンの構成では先に記述いたしました DHCP、ゲートウェイの設定にご注意ください。

また、管理者は NAT のセッションを WinGate 各プロキシサービスのインターセプト機能を使用して、WinGate 内部のプロキシサーバーにリダイレクトすることができます。

※NAT 機能を使用するには、Extended Networking がインストールされていて、NIC2 枚構成が必要となります。

インターセプトの設定に関しては、本書のインターセプトの設定の章をご参照ください。

**WinGate インターネットクライアント（WGIC）を使用するクライアントの構成**

**WGIC とは**

WGIC をクライアントマシンにインストールする事により、クライアントマシンでは、プロキシの設定などを行うことなく、インターネット・アプリケーションを使用することができます。

これはプロキシに対応していないアプリケーションでも WGCI を使用することにより、利用できることを意味します。

クライアントマシンはインターネットへ直接接続しているような感覚で、インターネット・アプリケーションをご使用いただく事ができます。

WGIC は WinGate の Winsock Redirector Service（Winsock リダイレクトサービス）を使用して、この機能を提供します。また、クライアントマシンが WinGate サーバーを発見するために GDP Service が必要となります。

WinGate Management の Service でこれらのサービスをインストールしてください。

また、管理者は WGIC のセッションを WinGate のトランスペアレント機能を使用して、WinGate 内部のプロキシサーバーにリダイレクトすることができます。

トランスペアレントの設定に関しては、本書のトランスペアレントの設定の章をご参照ください。

**WGIC のインストール**

**ご注意**：WinGate インターネット・クライアントは Windows 専用となります。MacOS や Linux 等の他の OS では使用する事はできません。また、インストールを行う際、管理者権限が必要となります。

**ご注意**：WinGate インターネット・クライアントは Windows Vista,2008、7、8、2010 および 64bitOS には対応しておりません。これらの OS に関しては他の方法をご検討ください。

WGIC のインストールプログラムは、WinGate サーバマシンの WinGate インストールディレクトリ内の Client ディレクトリ内にある WGIC.msi ファイルとなります。

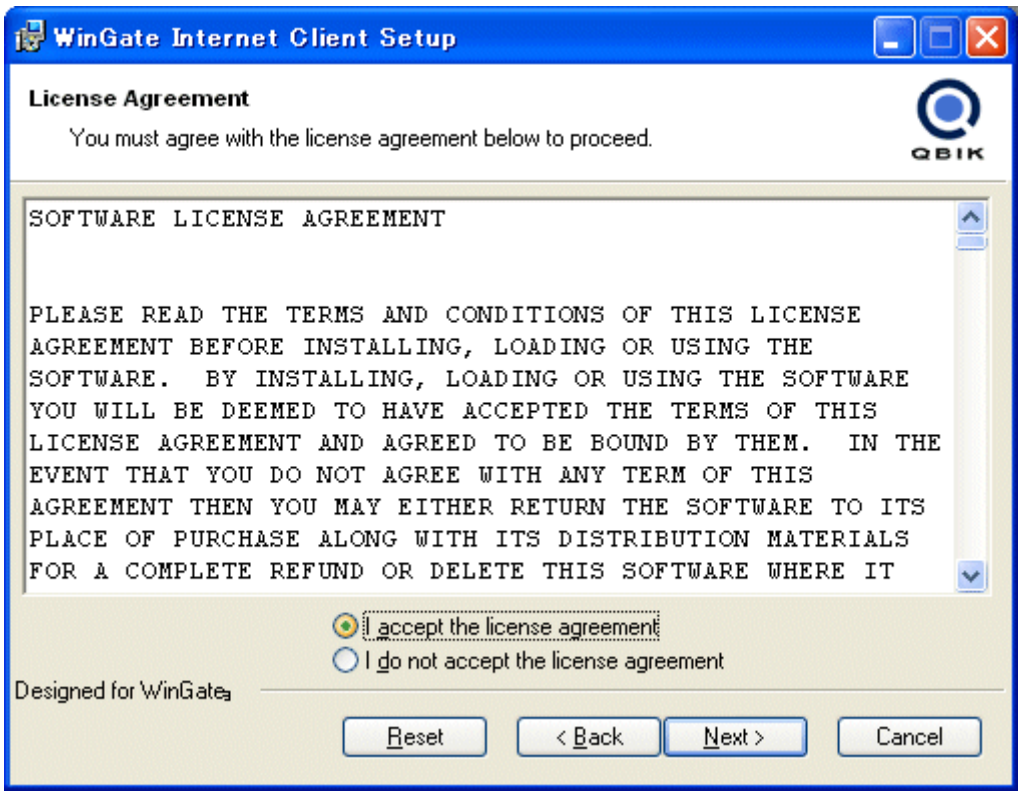
管理者はこのインストールファイルをディスクや、ファイル共有によって、クライアントに配布することができます。

**WGIC のインストールの開始**

インストールプログラム（WGIC.msi）を実行します。

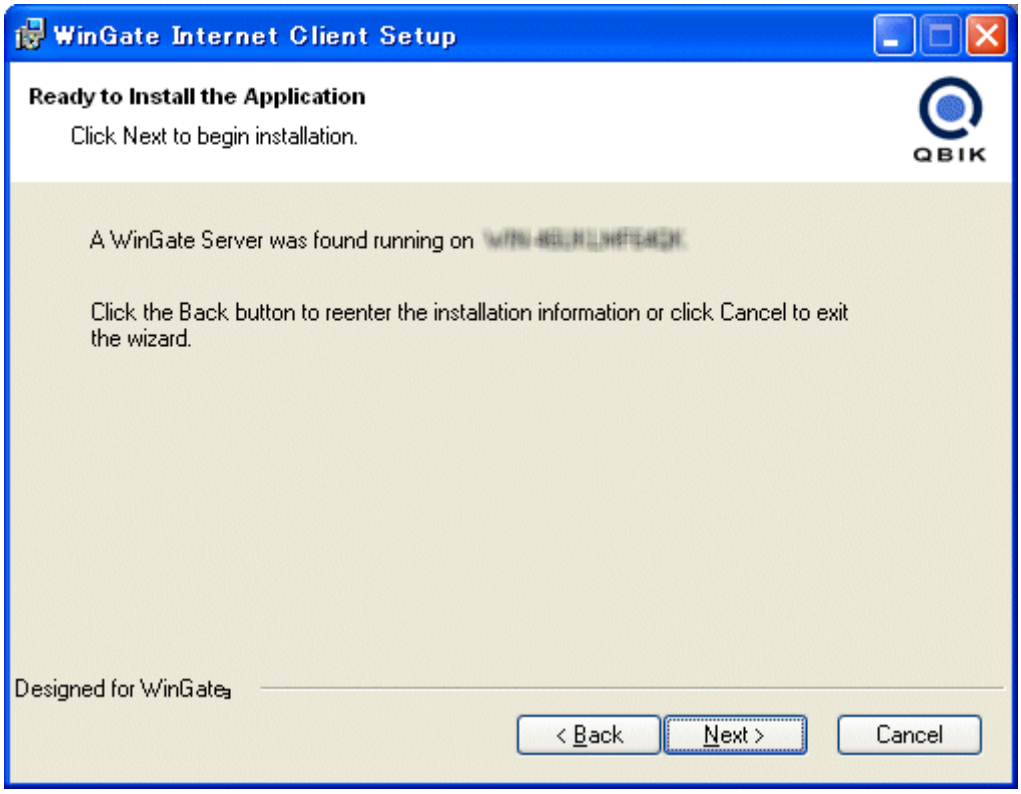
Next ボタンで次へ進みます。

エンドユーザーライセンス契約書が表示されます。



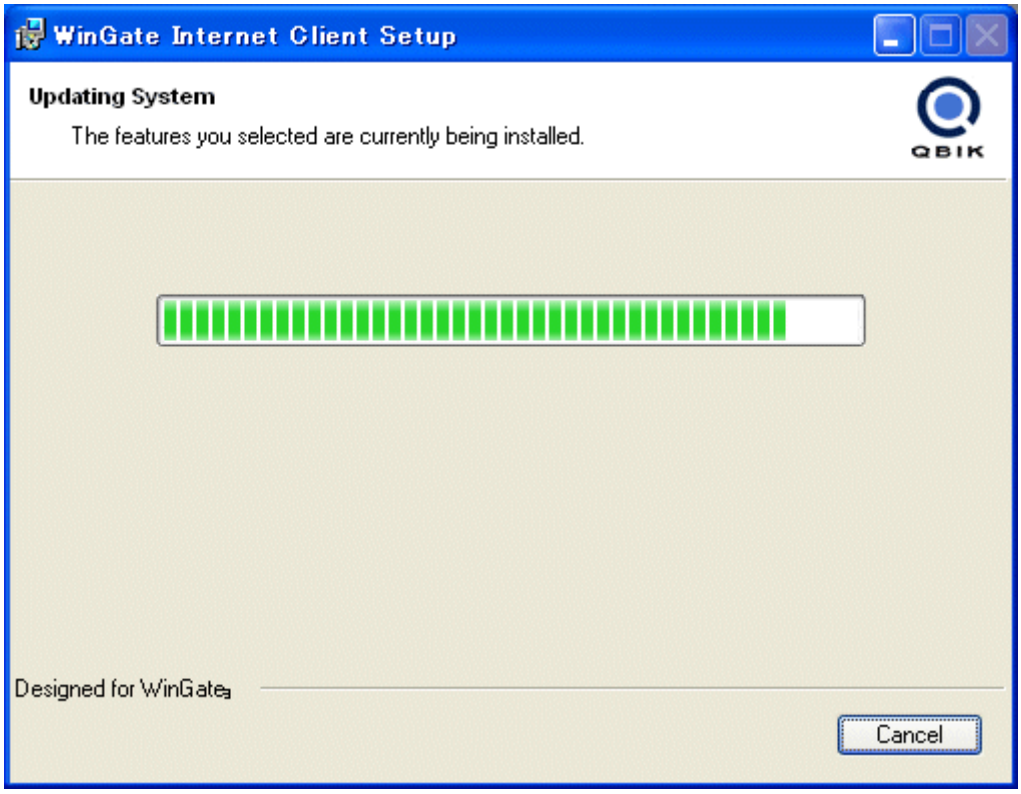

I accept the license agreement（ライセンス許諾に同意します。）を選択して Next ボタンで次へ進みます。

WinGate サーバーを発見します。




WinGate のインストーラーはネットワーク内に他の WinGate サーバーが存在するかを調査し、WinGate サーバーが発見された場合、自動的に「このコンピュータを WinGate サーバーとして構成する」を選択します。WinGate サーバーの発見には、WinGate の GDP サービスが利用されます。
利用可能な WinGate サーバーがネットワーク内に存在し、クライアントマシンで、自動的にこの選択がされない場合、WinGate サーバーの構成が正しく行われていないか、クライアントマシンが WinGate サーバーへ接続できない状態であることが考えられます。
自動的にクライアントとしての構成が選択されない場合、手動で「このコンピュータを WinGate サーバーとして構成する」を選択してください。
Next をクリックします。

インストールが開始されます。




WGIC のインストールディレクトリは変更することはできません。

インストール完了

「完了」ボタンをクリックして、インストーラーを終了してください。

インストール完了後は、念のため PC を再起動いただくことをお勧めいたします。

### クライアントマシンでのアプリケーションの実行

WGIC は Winsock を利用しようとするネットワーク要求を常に監視し、アプリケーションがインターネットへアクセスしようとしているのを検知すると、その要求を捕捉して WinGate サーバーの Winsock リダイレクション・サービスに転送します。Winsock リダイレクション・サービスは、クライアント・アプリケーションに代わって、その要求を WinGate サーバー上で実行します。

WinGate サーバーがどこにあるかは、WGIC が自動的に発見します。複数の WinGate サーバーがネットワーク内に存在する場合、そのうちのどれかを自動的に選択します。

WGIC を利用するアプリケーションが開始すると、デフォルトでは WinGate ダイアルアップ・モニタが起動します。

WinGate ダイアルアップ・モニタ

WinGate ダイアルアップ・モニタでは利用している WinGate サーバーや接続時間などの情報が表示されます。

デフォルトでは、暫くすると WinGate ダイアルアップ・モニタはタスクトレイに格納されます。

タスクトレイに格納された WinGate ダイアルアップ・モニタ・アイコンをダブルクリックすると、WinGate ダイアルアップ・モニタを表示することができます。

WinGate インターネット・クライアントはデフォルト状態で動作するでしょう。多くの場合、設定変更の必要ないことが考えられます。

### WinGate インターネット・クライアントの構成

WinGate インターネット・クライアントの構成は WinGate インターネット・クライアント・アプレットから行うことができます。

WinGate インターネット・クライアントアプレットは、以下の場所から表示することができます。

Windows のコントロール・パネル

Windows のスタートメニュー、「すべてのプログラム」、WinGate Internet Client、WinGate Internet Client Applet を選択

WinGate インターネット・クライアントアプレットが表示されます。

WinGate インターネット・クライアント・アプレットでは、WGIC の有効・無効、ダイアルアップ・モニターの起動などをはじめとする、WGIC の機能に関する設定や、使用する WinGate サーバーの選択、アプリケーションごとのアクセスモードなどを設定することができます。

**クライアント PC の FTP クライアントソフトウェアから FTP を行う**

FTP クライアントから WinGate を経由して FTP を行う場合、以下の方法があります。

- Extended Network Service（ENS）の NAT 機能を使用する
- FTP Proxy service を使用する

ENS の NAT 機能を使用する場合、WinGate では特に設定を行う必要はございません。FTP クライアントでも、特にプロキシ用の設定などを行うことなく、FTP を使用できます。（※FTP クライアントで PASV モードを使用する必要があります。

FTP Proxy server を使用する場合、WinGate Management の Services で FTP Proxy service を追加いただく必要があります。

FTP Proxy service を追加いただきました後、WWW Proxy server などと同様に、Service port（サービスポート）の設定や Bindings 設定をご確認いただき、WinGate の FTP Proxy service がクライアントから接続可能な状態であるかをご確認ください。

FTP クライアントソフトウェアでは、FTP Proxy service を使用するために、以下の接続設定を行う必要があります。

- **FTP サーバー** :

WinGate の FTP Proxy service で接続を受け付けているインターフェースの IP アドレスを指定してください。

- **FTP サーバー ポート**:

WinGate の FTP Proxy service で接続を受け付けているインターフェースのポート番号を設定してください。

- **ユーザー名**:

FTP Proxy service を使用するために user_name@ftp_server というような設定が必要になります。
user_name は、接続をする FTP サーバーのユーザー名、ftp_server は、接続をする FTP ホストとなります。

- **パスワード**:

パスワードは、接続をする FTP サーバーのアカウントで使用されるパスワードとなります。

FTP Proxy service をクライアント PC から使用する場合、FTP クライアントソフトウェアでは、PASV（パッシブモード）を使用する必要があります。
PASV モードの設定や FTP クライアントが PASV モードをサポートしているかについては、ご利用をいただいております FTP クライアントソフトウェアの開発元へご確認ください。

**WinGate メールサーバー機能**

WinGate はプロキシサーバー機能とは、ことなるアカウント構成可能なメールサーバー機能を持ちます。メールサーバー機能では、WinGate で使用されるユーザー・データーベースを使用したメールアカウントの構成やリレーサーバとして WinGate メールサーバーを構成いただくことも可能となります。

これらは、WinGate の POP3、SMTP、IMAP4 サーバー機能を使用いたします。

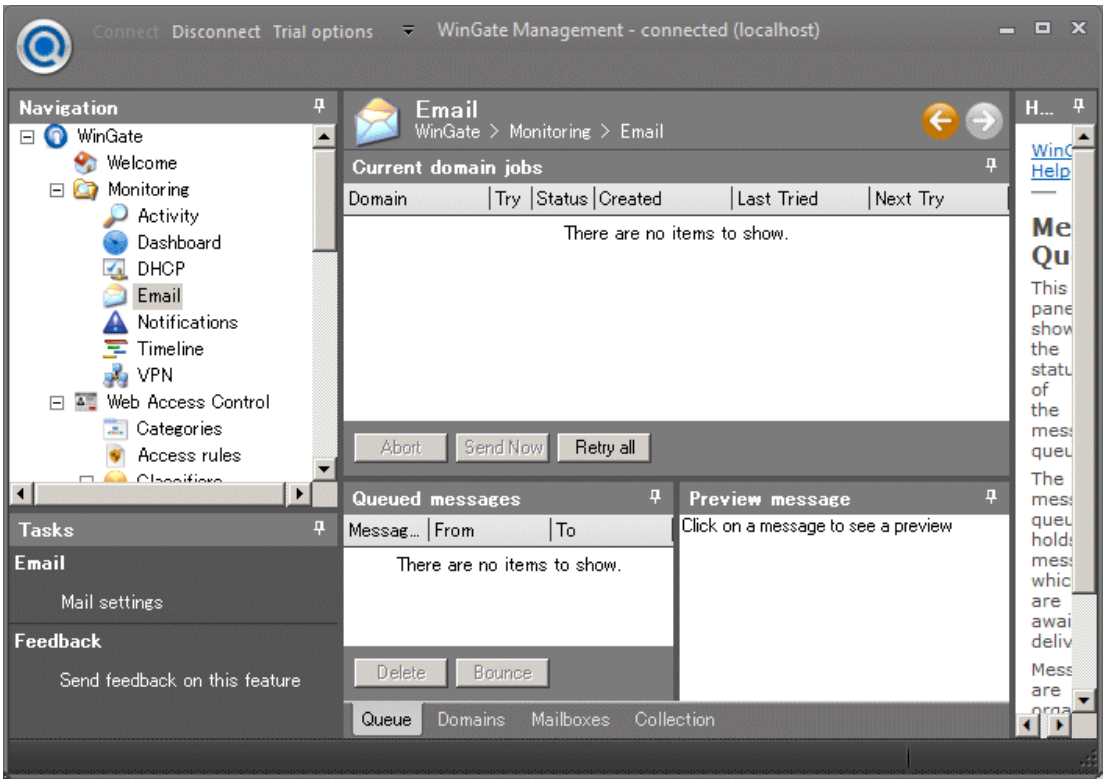
E メールの各種設定を行っても、POP3、SMTP、IMAP4 サーバーが停止されている場合、メールサーバーは正しく動作いたしません。

**プロキシ機能とは異なります事にご注意ください。**

**メールサーバーの設定**

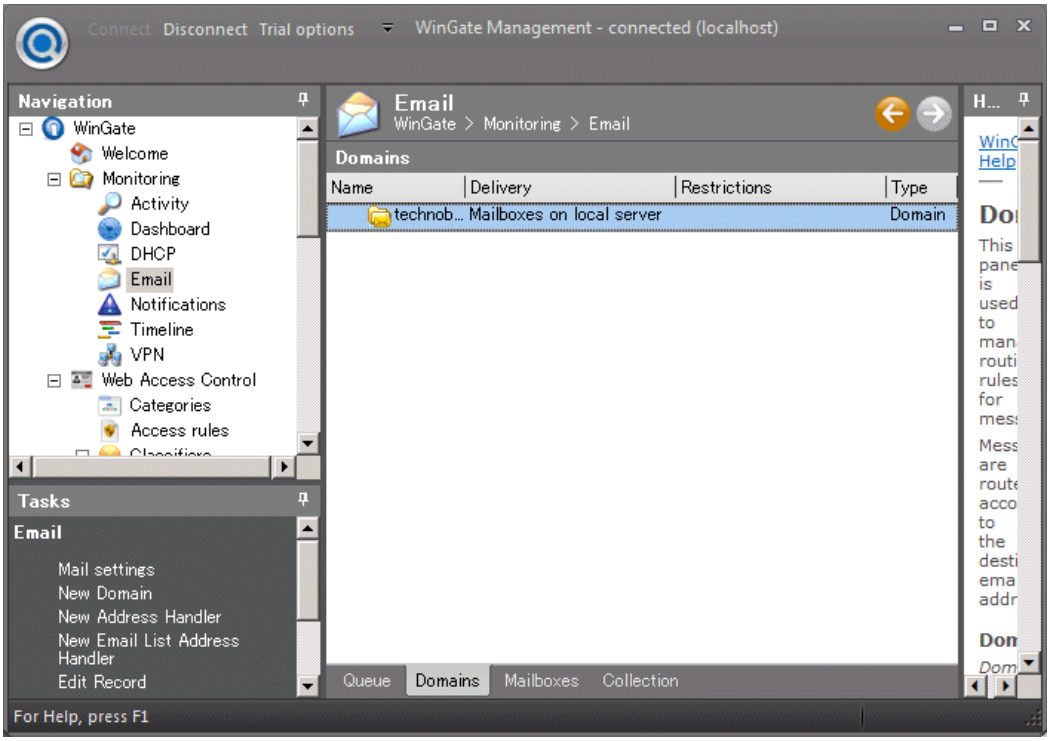
メールサーバーの設定を行うには、WinGate Management の Navigation の Email をクリックします。

◆ Queue（キュー）




Queue には、WinGate のメール配信状況やキューにあるメールを参照することができます。

◆ **ドメイン**



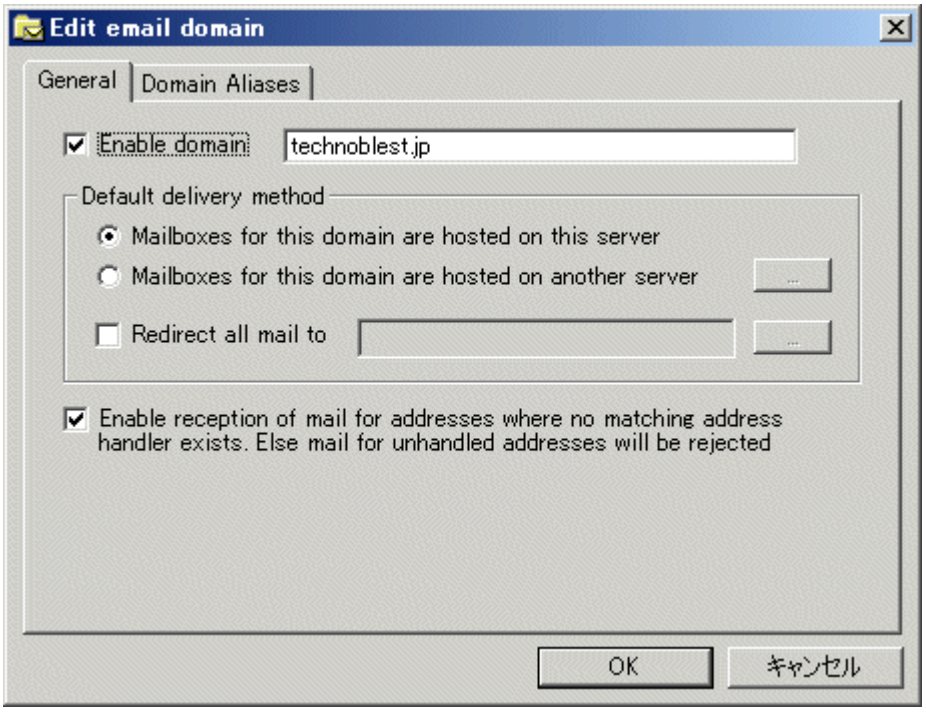

ドメインでは、WinGate 上でホストするドメインと、そのドメインに関する設定を行うことができます。

新たにドメインを追加する場合は、New Domain（新規ドメイン）をクリックしてください。

Delete Record（削除）ボタンは、追加されたドメインを削除します。既に追加されているドメインを編集する場合は Edit Record（編集）ボタンをクリックしてください。

E メール・ドメインの編集

- **General**（全般）タブ




ドメインに関する基本的な内容を設定します。

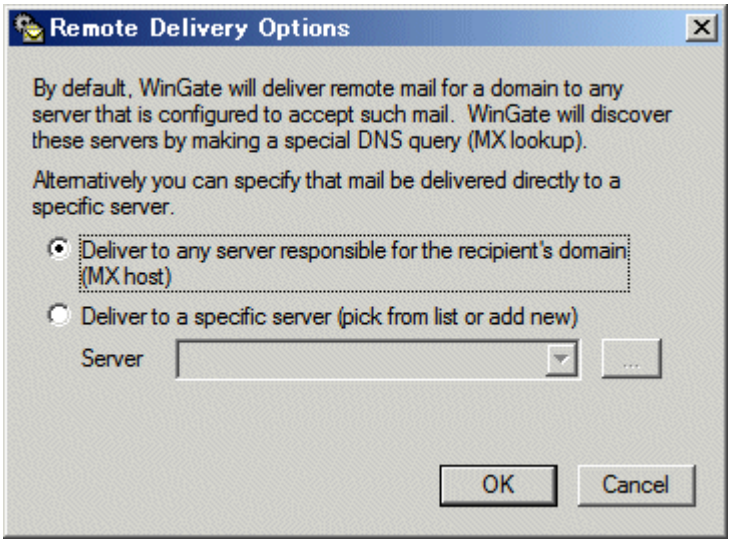
**Enable domain（ドメインを有効）** ： ドメインの有効、無効を切り替えます。

この欄に使用されるドメイン名を入力してください。ここで設定されたドメイン名が使用されます。ドメイ

ン名は通常 DNS サーバーで名前解決される必要があるでしょう。(WinGate の DNS サービスとは異なります。)

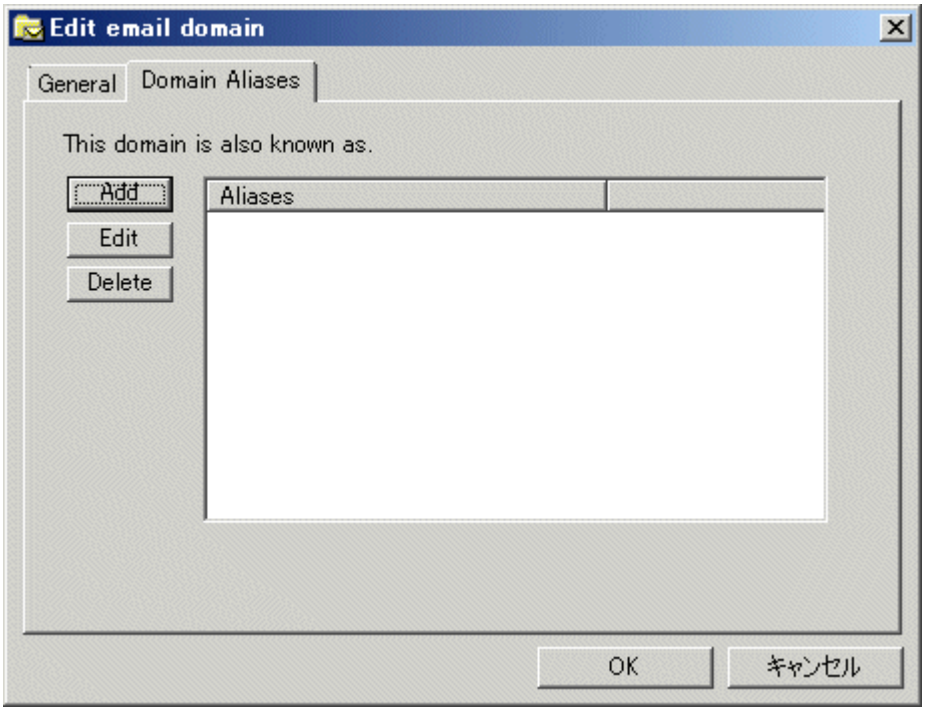
**デフォルトの配信方法**: このドメインのメールをどのように取り扱うかを決定します。

- **Mailboxes for this domain are hosted on this server(このドメインのメールボックスは、このサーバー上でホストされる )**
  これはドメインのメールボックスを WinGate が持つ事を意味します。
- **Mailboxes for this domain are hosted on another server(このドメインのメールボックスは他のサーバー上でホストされる)**
  これはドメインのメールボックスが他のサーバーにあり、WinGate はメールをそのサーバーへ配信することを意味します。
  右側のボタンにより配信先のサーバーを設定することができます。



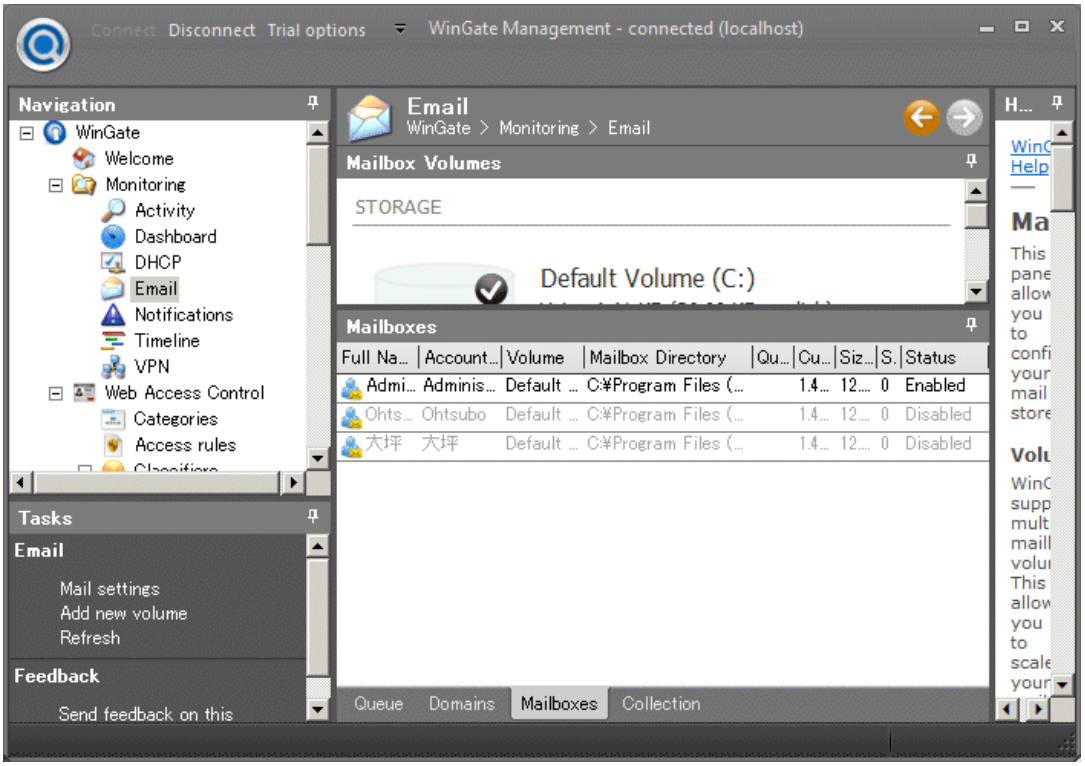

- **Redirect all mail to(全てのメールを転送)**
  有効とした場合、このドメインに届くメッセージは、ドロップダウンで選択されたユーザーへ全て転送されます。

➢ **Domain Aliases(ドメインエイリアス)**



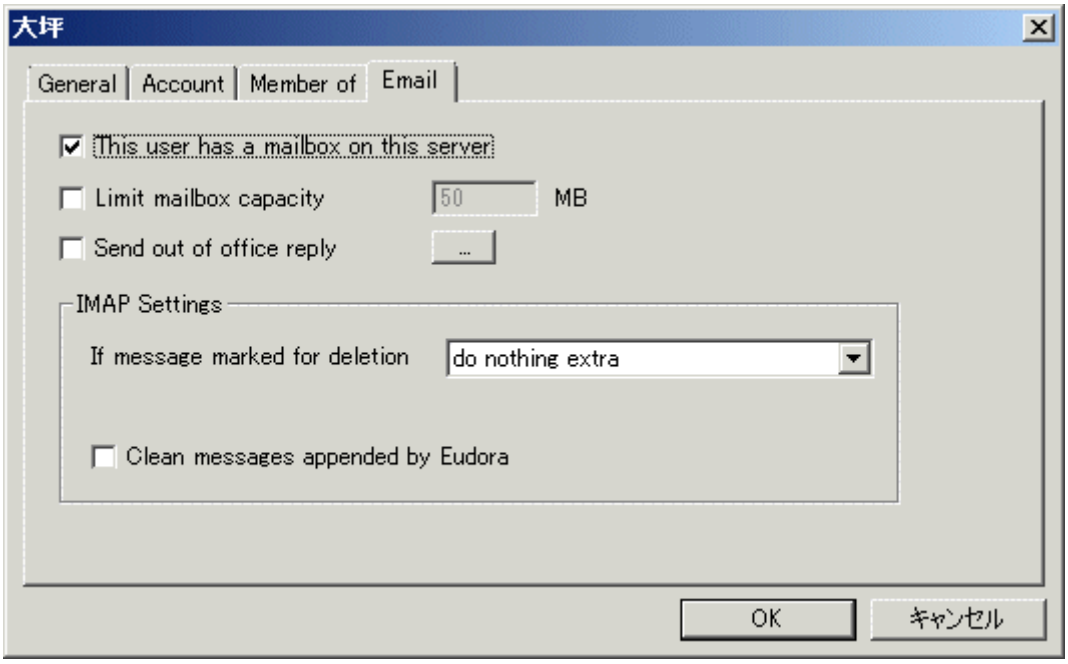

ドメインエイリアスでは、ドメインのエイリアスを設定することができます。

◆ **メールボックス**

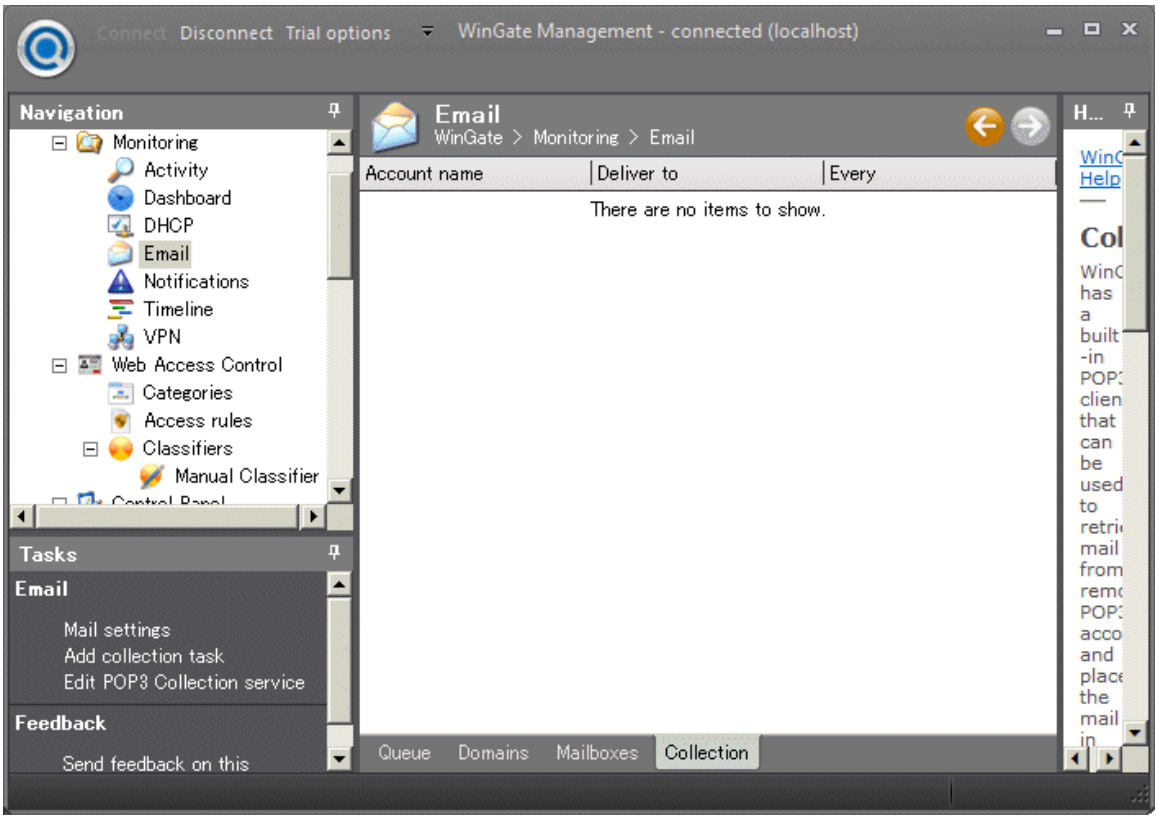



メールボックスでは、メールサーバーが持つアカウントの状況を確認することができます。

ユーザーをダブルクリックすることで、ユーザーのアカウントプロパティダイアログが表示されます。



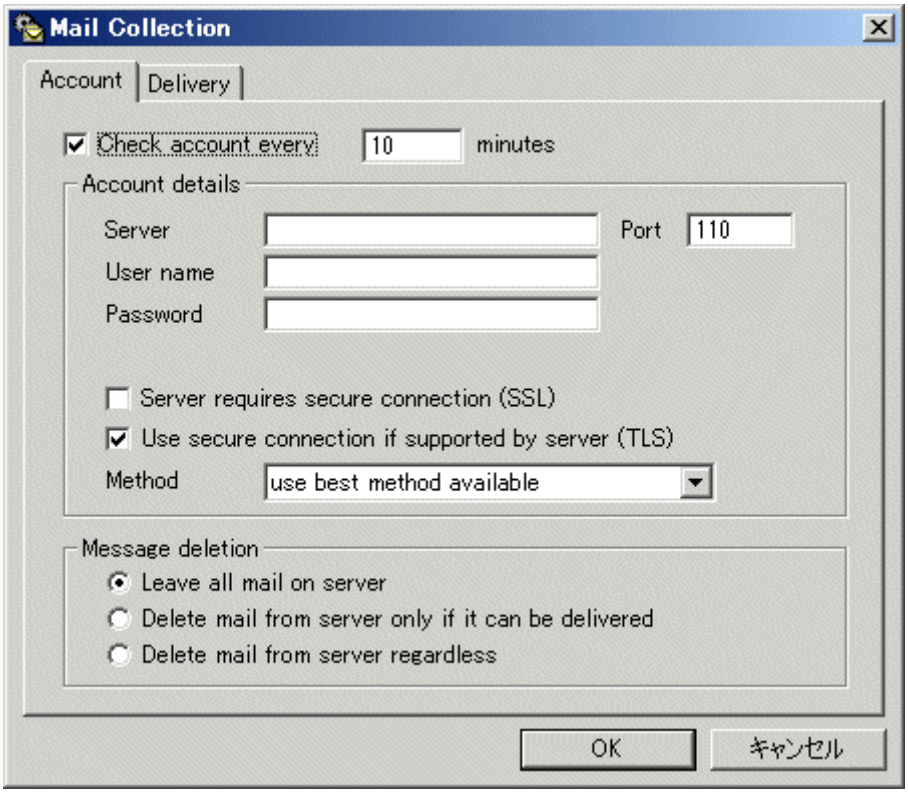

◆ **Collection（収集）**




Collection では、外部メールサーバーからのメール受信をサポートします。

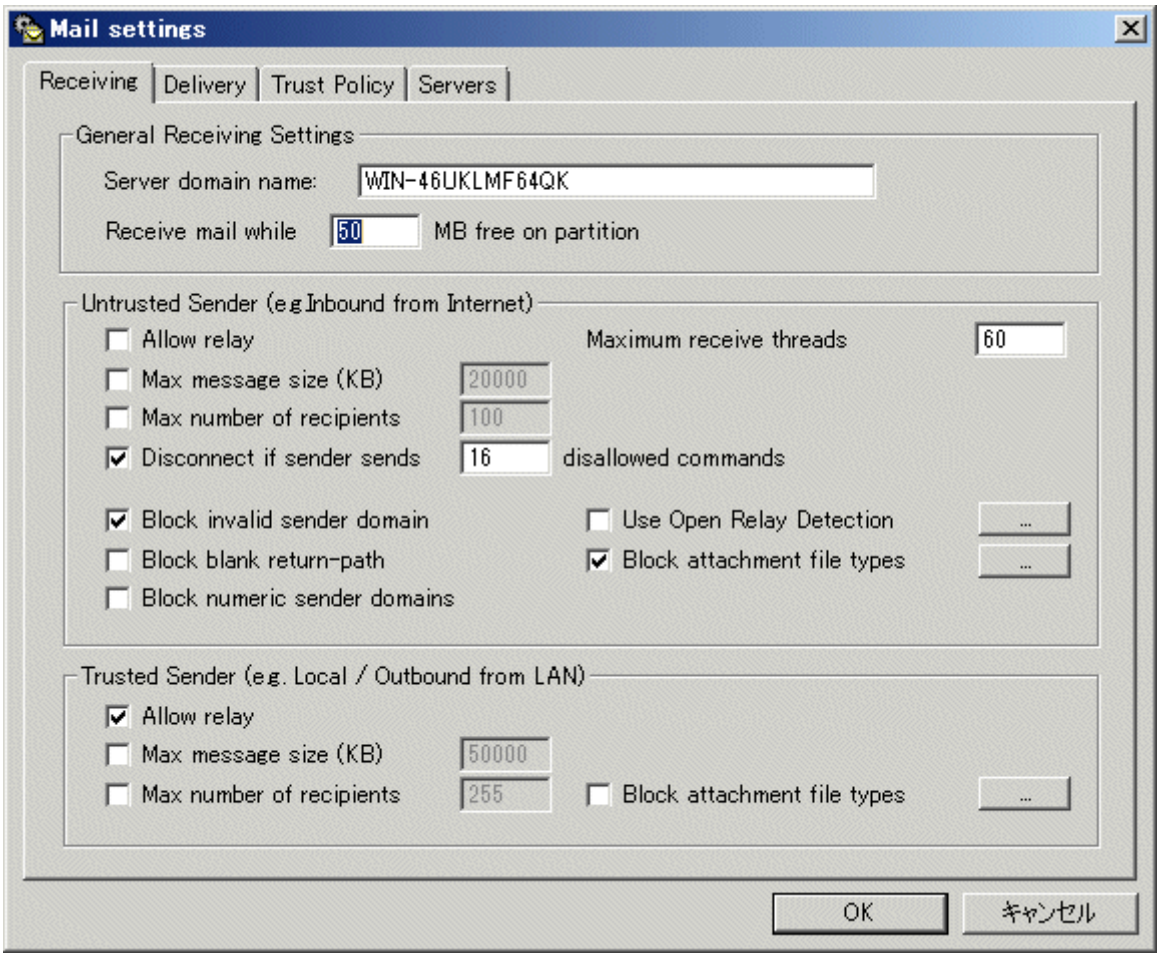
使用するには、Services で POP3 Collection service がインストールされている必要があります。

追加するには、Add collection task をクリックします。




収集に利用するサーバーやアカウント情報、配信先などを設定することができます。

◆ **Mail settings　Receiving（受信）**

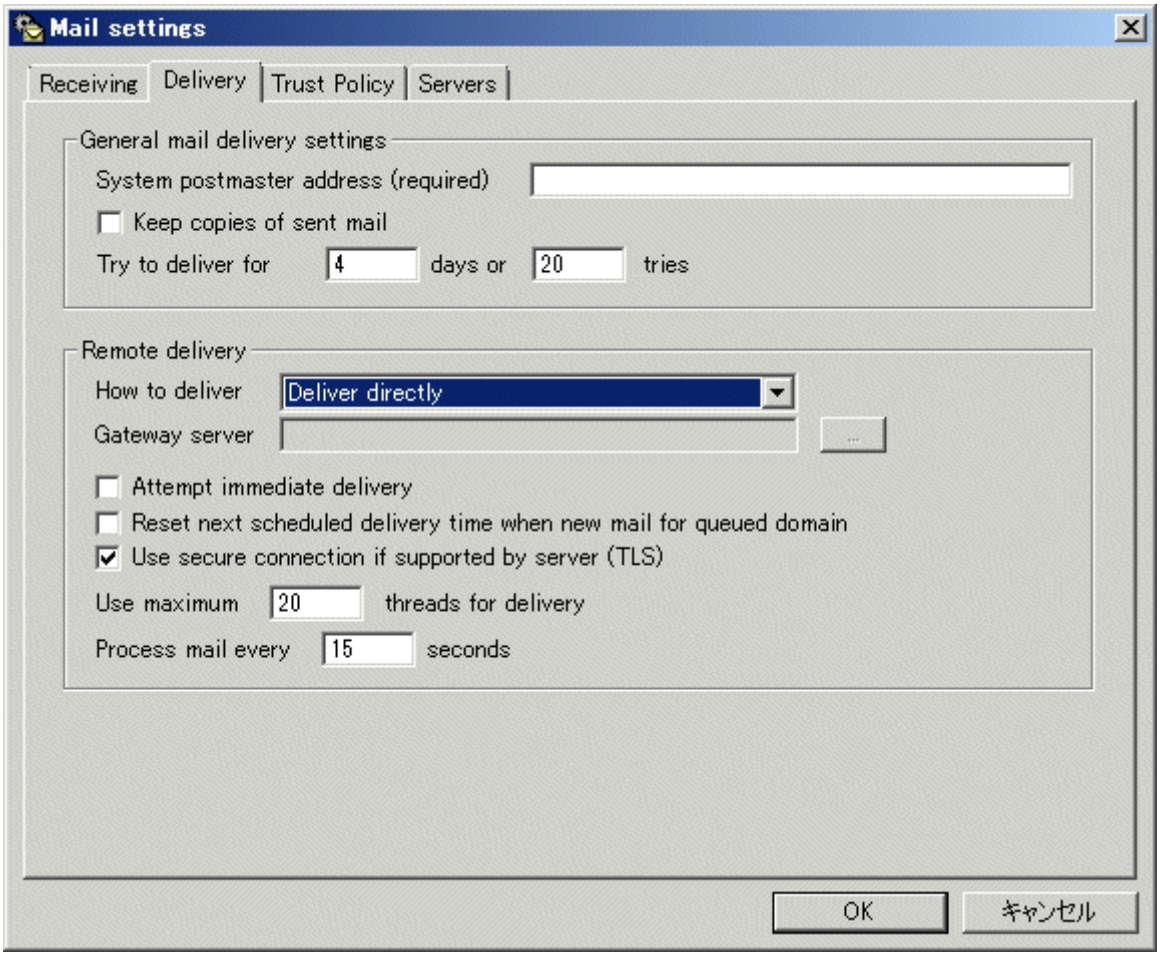



受信では WinGate メールサーバーでの、メール受信（配信受付）方法を設定します。

必要に応じて各設定を行ってください。
添付ファイル形式でのブロックやメッセージサイズを制限することができます。
信頼できる送信者は、信頼ポリシーで許可された送信者となります。

**ご注意**:信頼できない送信者の欄のリレーを許可した場合、オープリレーサーバとして構成されることとなります。信頼できない送信者からの「リレーを許可する」を有効とする場合、その危険性を認識した上で設定してください。

**Mail settings　Delivery(配信)**

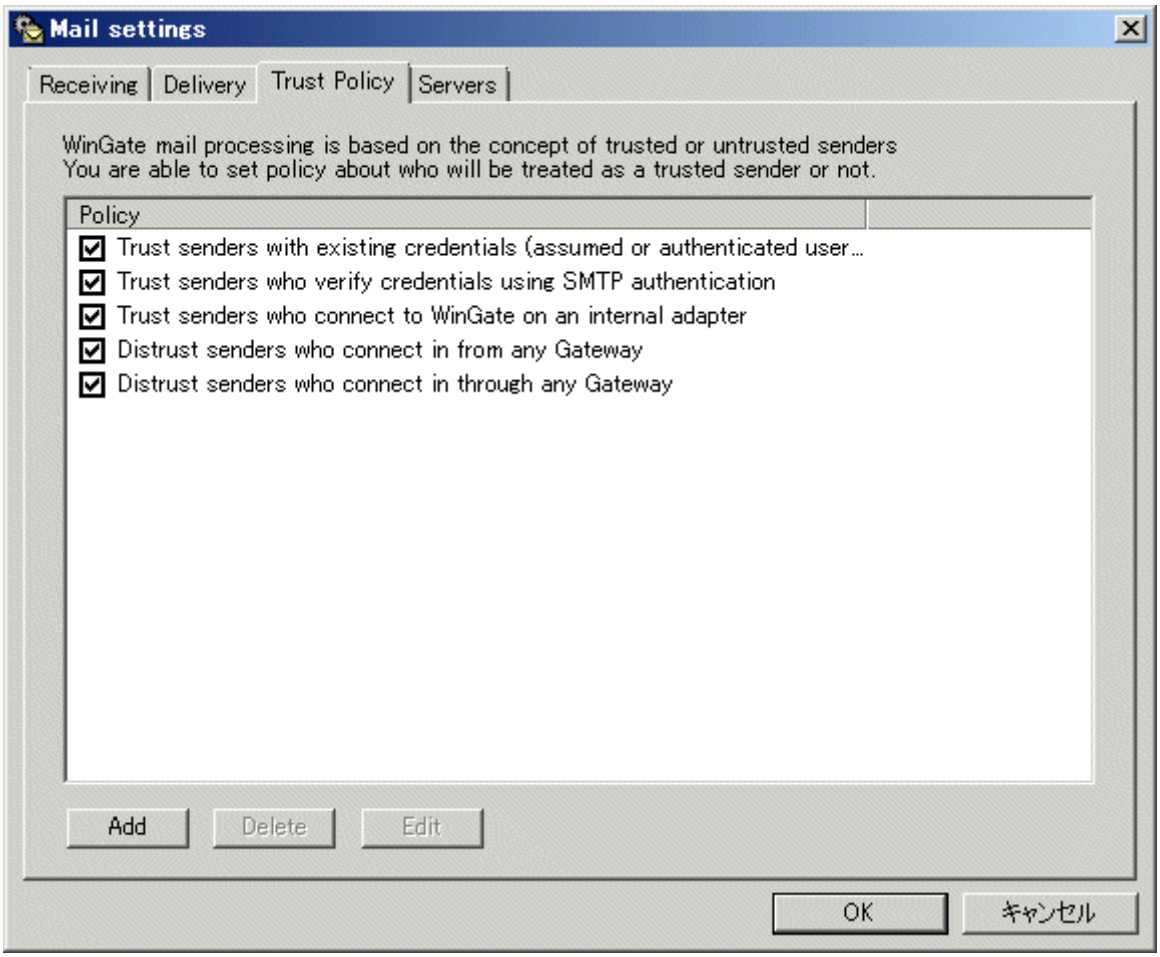



配信では、WinGate メールサーバーが、どのようにメールを配信するかを設定することができます。
幾つかの配信設定を選択することができます。

- **Delivery directly(直接配信)**
  WinGate サーバーが直接メールを配信します。
- **Use gateway(ゲートウェイを使用)**
  メールはゲートウェイサーバを使用して配信されます。
- **Use gateway for undelivery mail(配信不可メールにゲートウェイを使用)**
  直接配信でエラーとなった場合にゲートウェイを使用します。

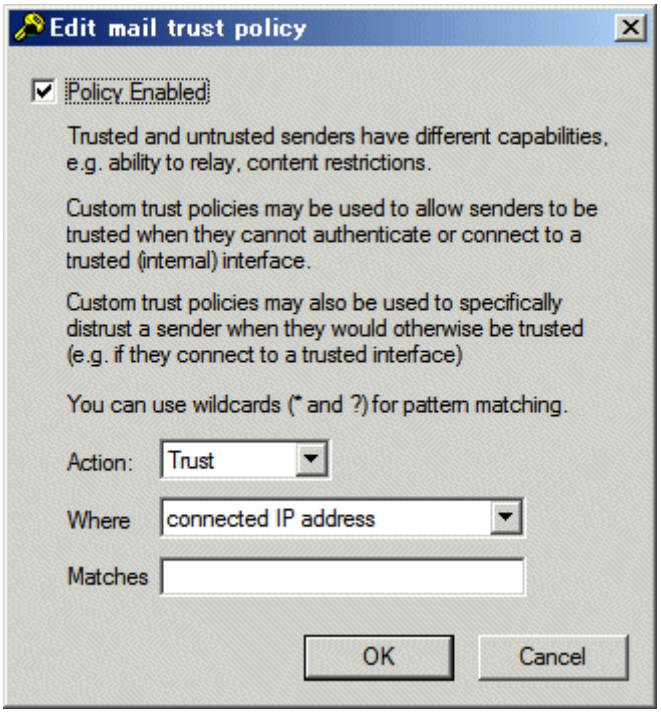
ゲートウェイを使用する場合、ゲートウェイサーバ欄にゲートウェイサーバを入力してください。右側のボタンによりゲートウェイサーバの詳細を設定することができます。
その他、必要に応じて設定を行ってください。

◆ **Trust Policy（信頼するポリシー）**

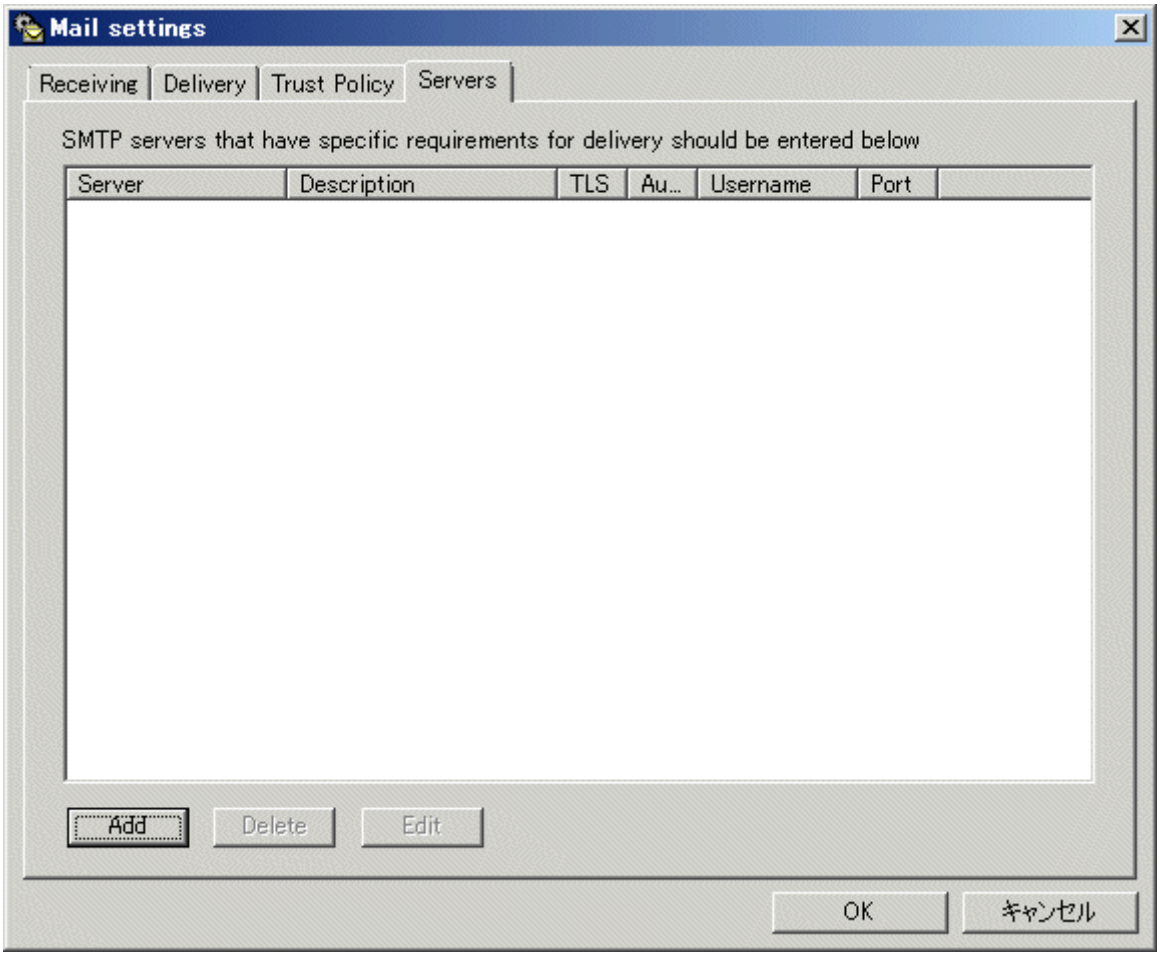



使用する認証方式を設定することができます。

Add（追加）ボタンによりポリシーを追加することができます。

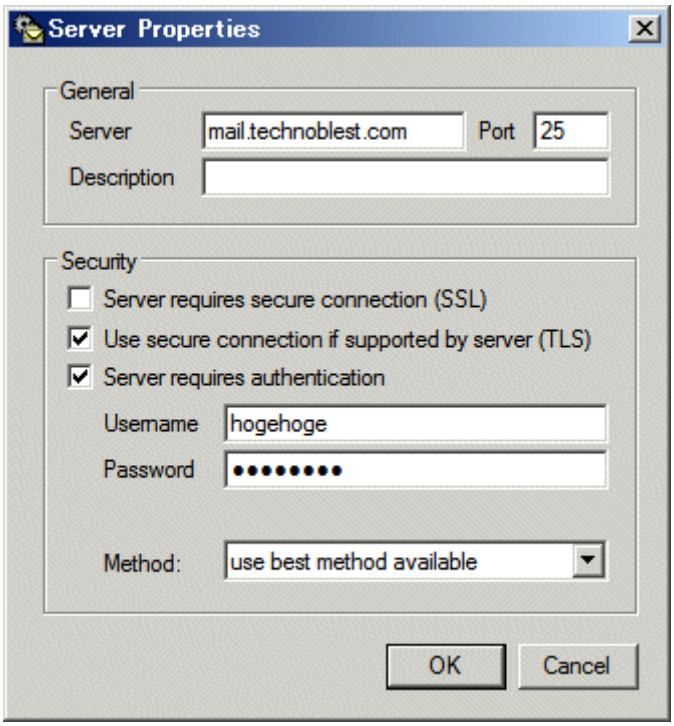



◆ **Servers（サーバー）**




WinGate が配信に利用する外部サーバーを追加、管理することができます。

Add（追加）ボタンにより、配信に使用するサーバーを追加することができます。



## WinGate でよく利用される設定の事例

この章では一般的に多く使用される WinGate の設定例をご紹介しております。
**※WinGate の種類などにより使用できない場合もございます。**
**※設定後は、必ず動作確認を行い、設定した内容が正しく動作しているかをご確認ください。**

### ご注意：ポリシーに関して

Policy（ポリシー）は、接続のイベントタイプを元に動作いたします。
WWW Proxy server を例にした場合、WinGate の WWW Proxy server がクライアントから利用される際は、HTTP リクエストでは、Event Type：ProxyRequest、HTTPS リクエストでは、Event Type：ConnectRequest がクライアントから要求され、WinGate のポリシーも、この Event Type に基づき処理されます。
これは、ProxyRequest に対するポリシーが設定されている場合でも、ConnectRequest により処理される HTTPS サイト（SSL 接続）では、ProxyRequest に対するポリシーが働かず制限が適用できないことを意味します。
ポリシーを追加いただく場合、その追加いただくポリシーが、どのソース（Source Tyape）の、どのイベント（Event Type）に対して適用されるものであるかをご確認ください。
ソースとイベントの種類により、ポリシーで使用できるアイテム（Items）やシンボル（Symbol）は異なります。

また、例えば WWW Proxy server でポリシーを設定する場合、ポリシーは、WinGate の WWW Proxy server（名前の異なる複数の同一サービスがある場合、ポリシーで追加されたサービス名のサービスに対して）への要求にのみ対応いたします。

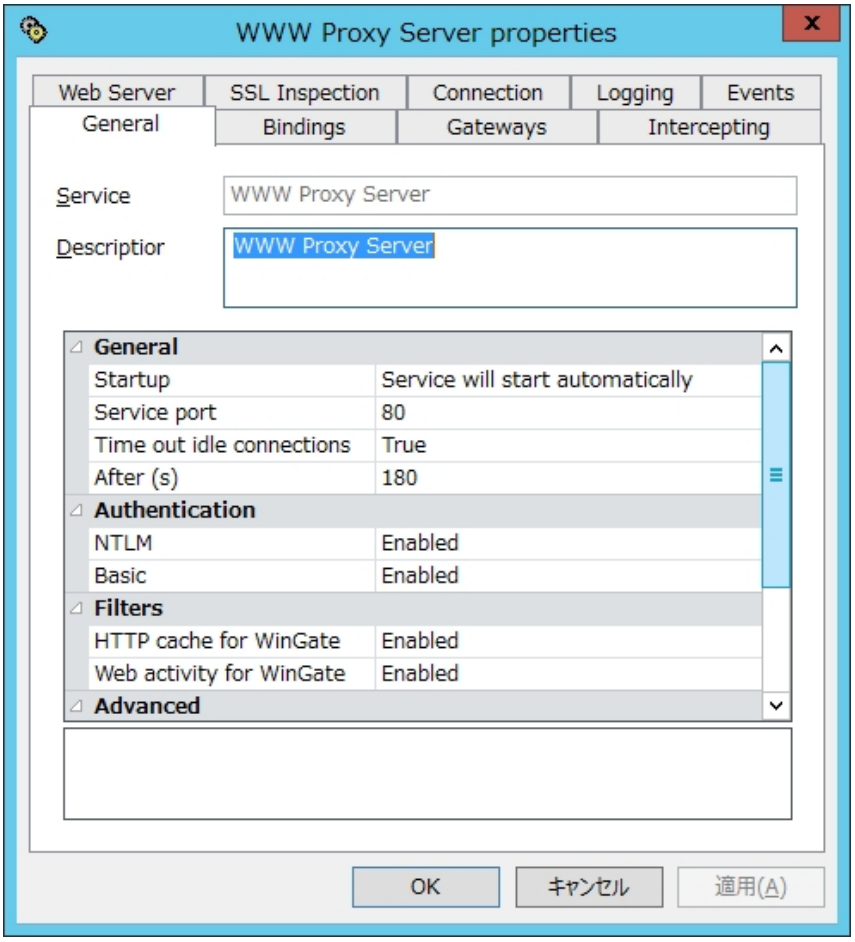
WinGate の NAT や WinGate インターネット・クライアントを使用している場合、HTTPS リクエストは、インターセプトされずインターセプト先となるプロキシサービス（WWW Proxy Server 等）を経由しないため、SSL サイトへの接続では、各プロキシサービスでの制限を利用できません。このような場合、WinGate の NAT や WinGate インターネット・クライアントを使用せず、HTTPS リクエストに関してもクライアントで直接、プロキシサーバーを指定する必要があることにご注意ください。

以下でご紹介しております設定事例では、一部 HTTP 接続（ProxyRequest）のみをご紹介している場合がございます。HTTPS サイトに対しても同様の制限を行う場合、Source Type（ソースタイプ）で Any HTTPProxy を選択、Event Type で ConnectRequest を選択し、同様のポリシーを作成していただく必要がございます。

### WWW Proxy Server でユーザー認証を行う

WinGate の WWW Proxy Server を使用する際に認証ダイアログを表示し、ユーザー名、パスワードの入力がない場合に Web ページの参照を拒否します。

認証についてのご注意
WinGate は、認証方法に NTLM、および Basic 認証をサポートします。
WWW Proxy Server では、デフォルトで両方の認証方法が有効になっております。




この場合 NTLM 認証が優先されて使用されます。

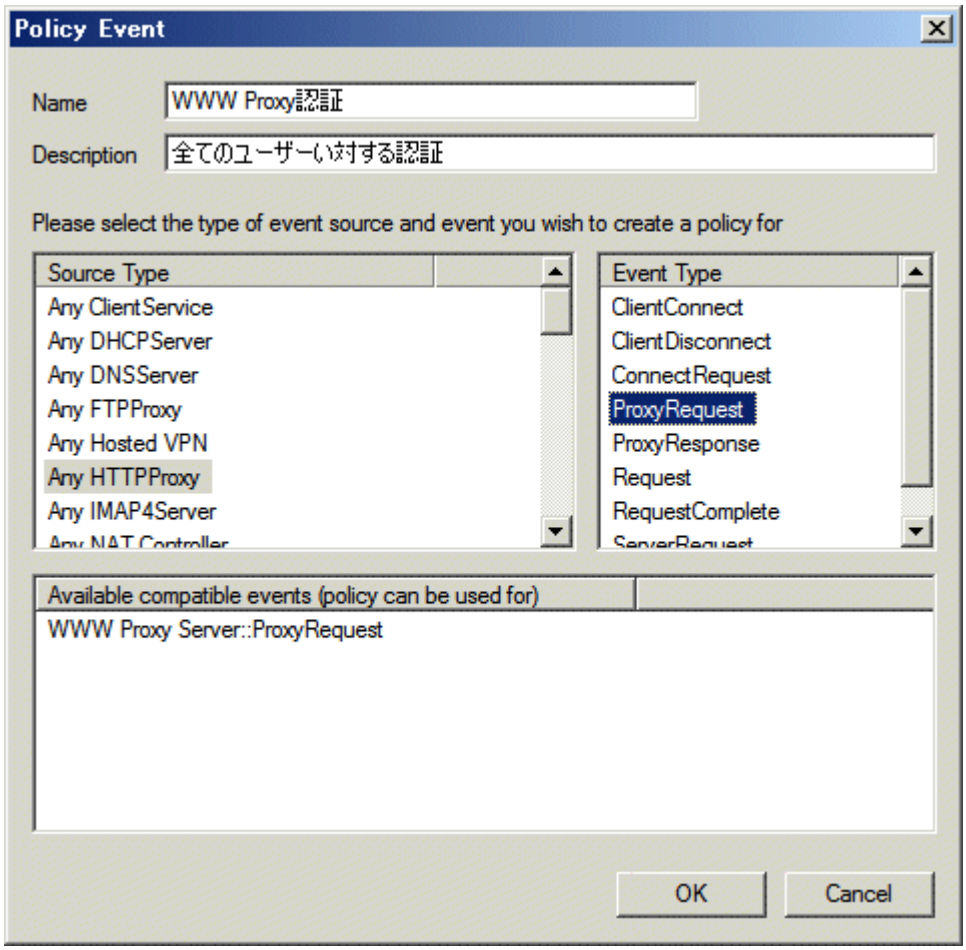
NTLM 認証では、パスワードは暗号化して送信されますが、Basic 認証は、パスワード情報を暗号化しません。
また、NTLM 認証を使用した場合、Internet Explorer や Firefox は、使用している Windows のアカウント情報を自動的に認証情報に使用するため、ユーザー名、パスワードの入力を促す NTLM 認証ダイアログを表示いたしません。
しかしながら実際は、ブラウザにより認証情報が送られているため、WinGate では認証されたユーザーとして扱われます。
同様に WinGate のユーザー・データーベースに、Windows ユーザー・データーベース、Active Directly が使用されている場合も、NTLM 認証を使用する場合は、ブラウザの種類によっては、NTLM 認証ダイアログが表示されない場合があります。
お客様の環境や使用目的に合わせて、NTLM 認証、Basic 認証、両方の認証を使用するかを決定してください。

一旦認証されたユーザーは、認証が有効になっている間、ページを参照することができます。
また、認証をされる事によりユーザー名が WinGate のログ情報に記録されます。

全てのユーザーに対して認証を必要とする場合は、以下の手順で設定することができます。

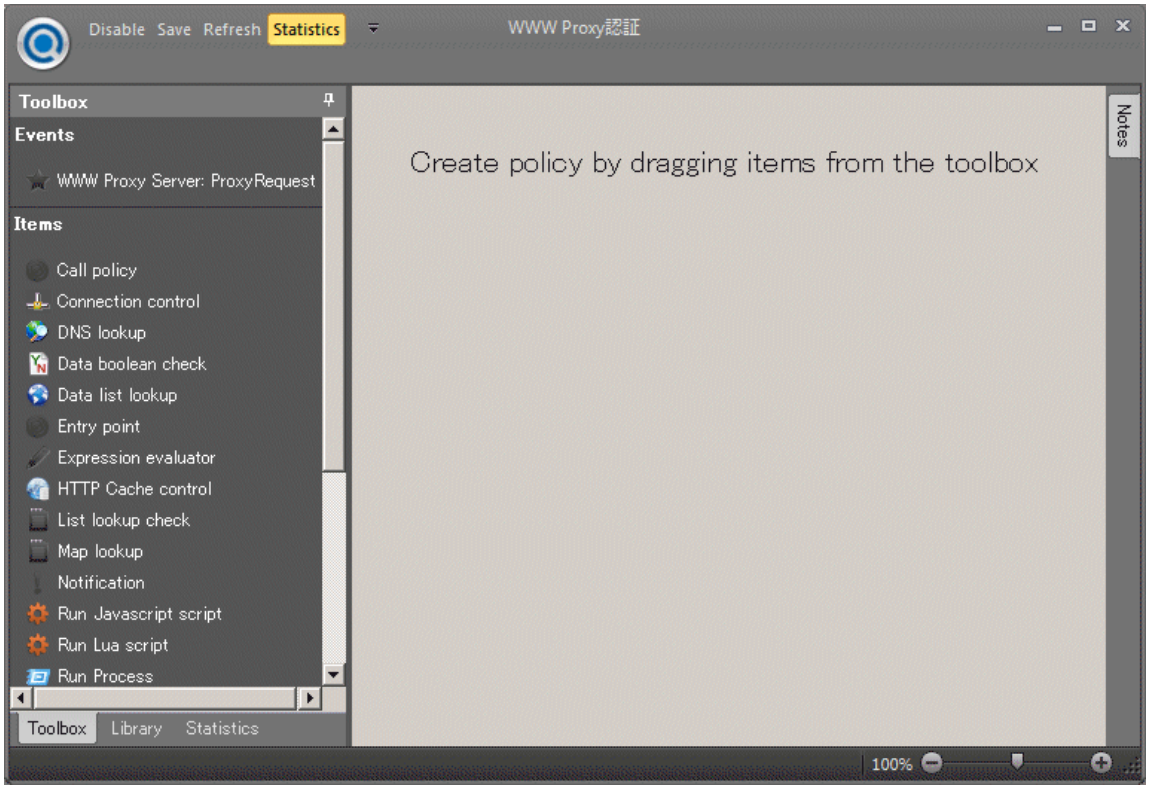
1. ユーザー・データーベースに WinGate ユーザー・データーベースを使用している場合は、ユーザーを作成します。
   また、Windows ユーザー・データーベース、Active Directly を使用している場合は、それぞれのユーザー・データーベースでユーザー管理を行ってください。

2. WinGate Management の Navigation より Policy（ポリシー）を選択し、Tasks より New Policy をクリックします。

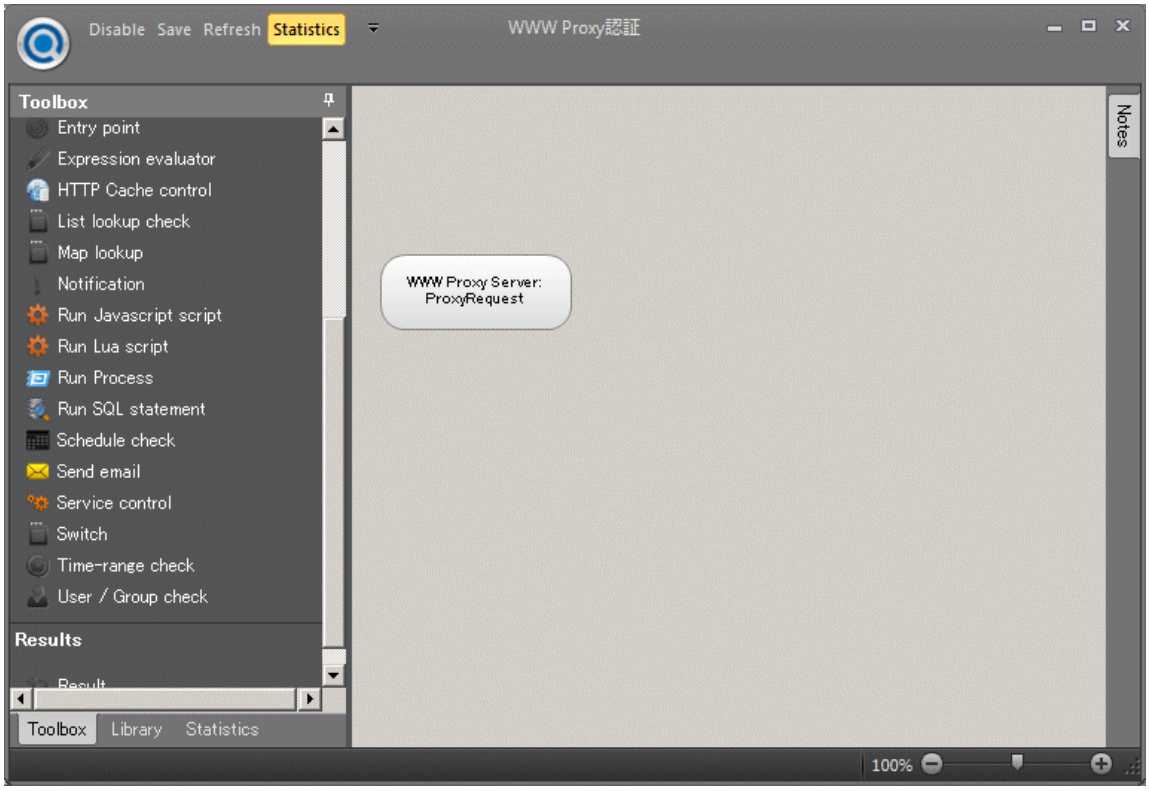



Name（名前）欄に、この制限の名前を入力します。
Description（説明）欄には、この制限の簡単な説明を入力します。（任意）
Source Type（ソースタイプ）で Any HTTPProxy を選択、Event Type で ProxyRequest を選択し、OK ボタンをクリックします。

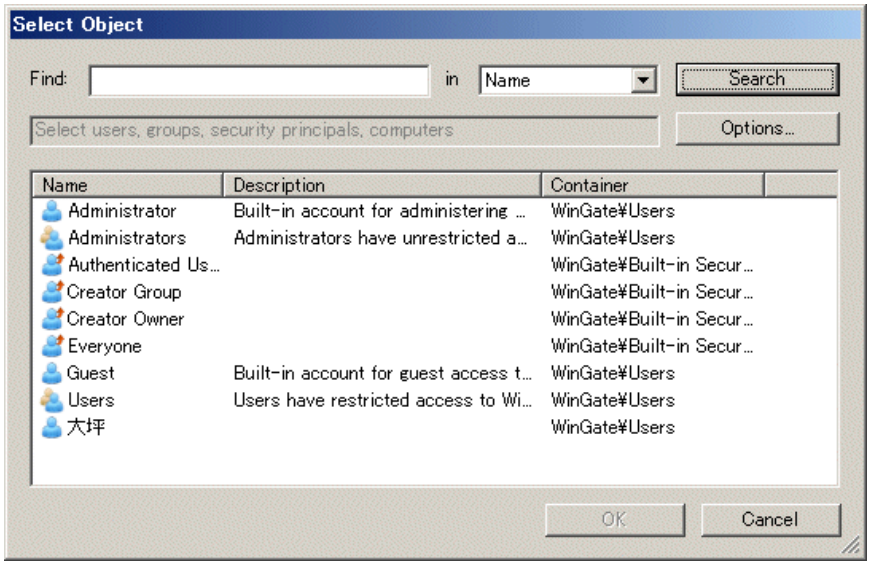
3. Policy（ポリシー）ウインドウが表示されます。




4. Policy ウインドウで、Event にある、WWW Proxy Server: ProxyRequest を右側の欄にマウスでドラッグします。

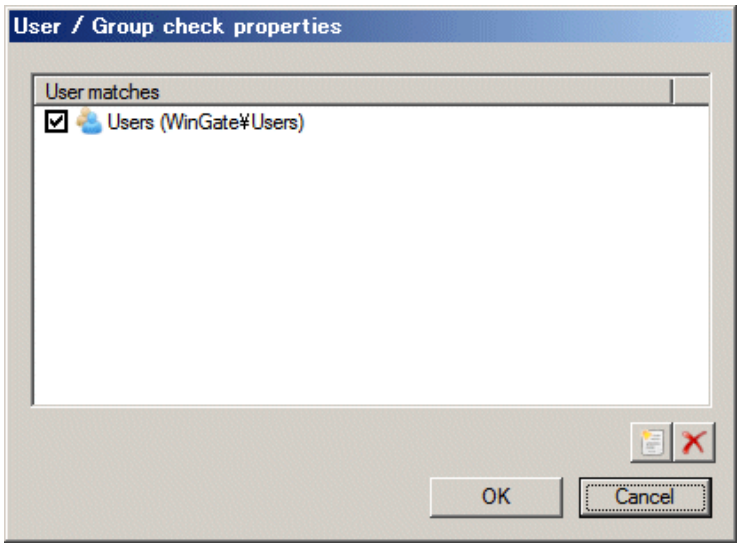



5. 続いて Items より User / Group check をドラッグします。




Select Object ダイアログが表示されますので、Search ボタンをクリックして認証を必要とするユーザー、またはグループを選択し、OK ボタンをクリックします。

全てのユーザーに対して認証を行う場合は、グループ選択を行うことが便利です。



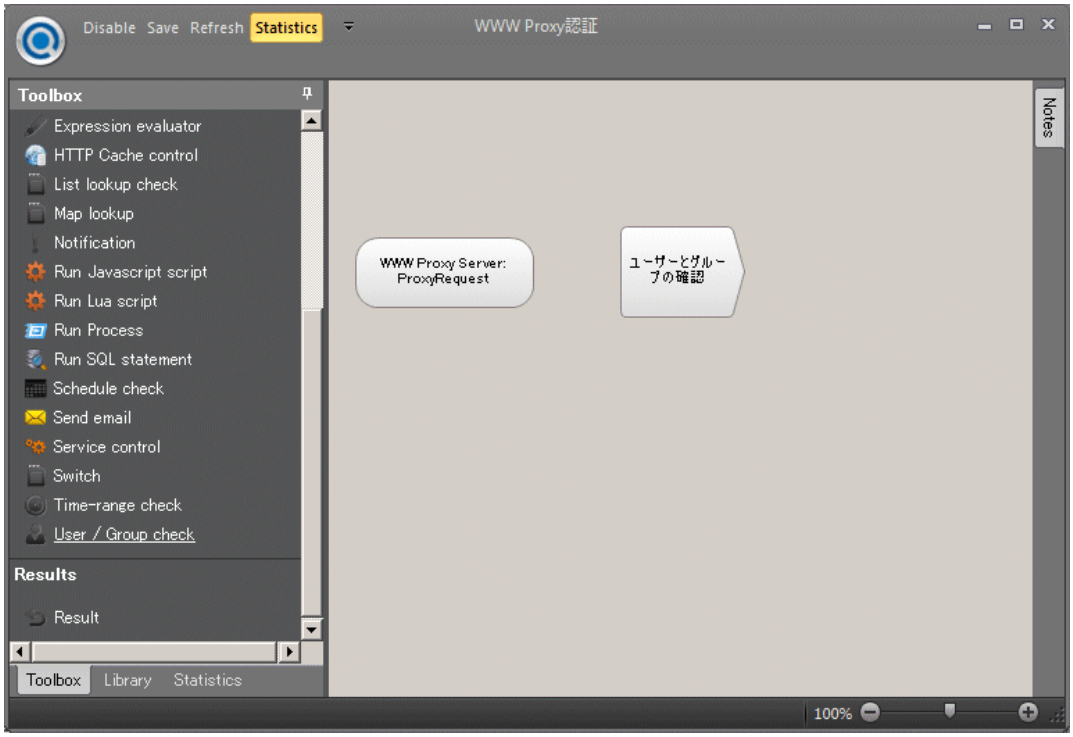

選択が完了すると User / Group check properties ダイアログに選択したユーザーやグループが表示されます。

Cancel（キャンセル）ボタン上の新規ボタンをクリックすると、Select Object ダイアログが表示されますので、複数のユーザーを追加する必要がある場合は、この操作を繰り返してください。

「×」ボタンをクリックすると削除することができます。

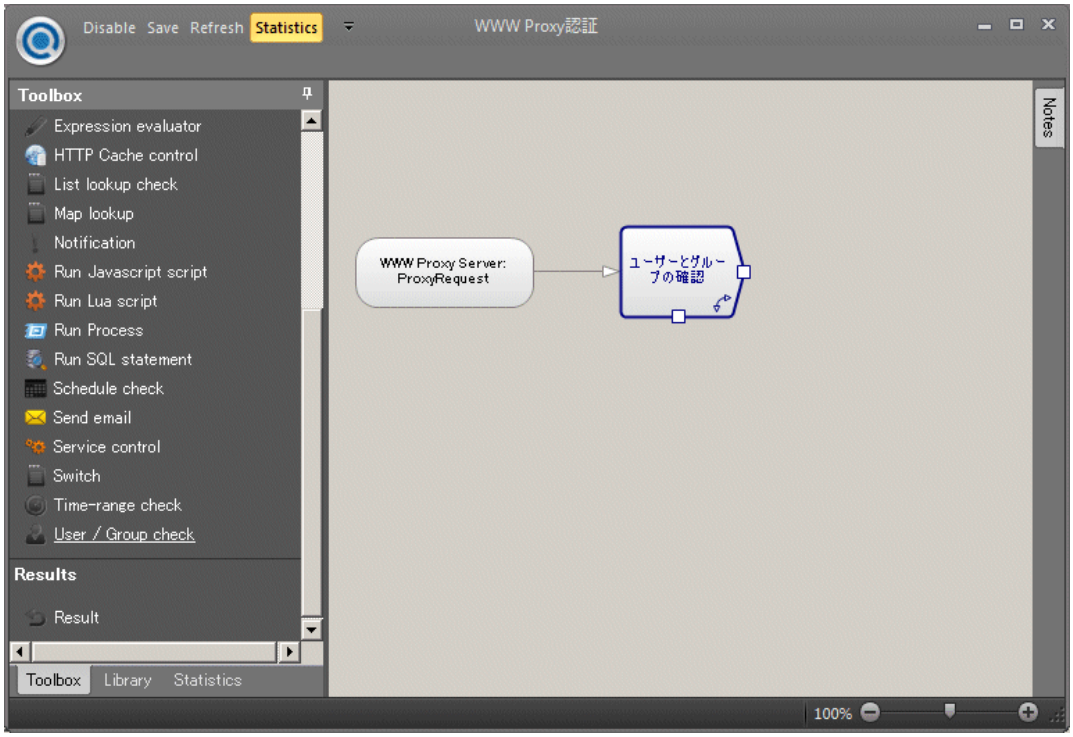
ユーザー、グループの選択が完了いたしましたら、OK ボタンで User / Group check properties を終了してください。

6. Policy ウインドウに戻ります

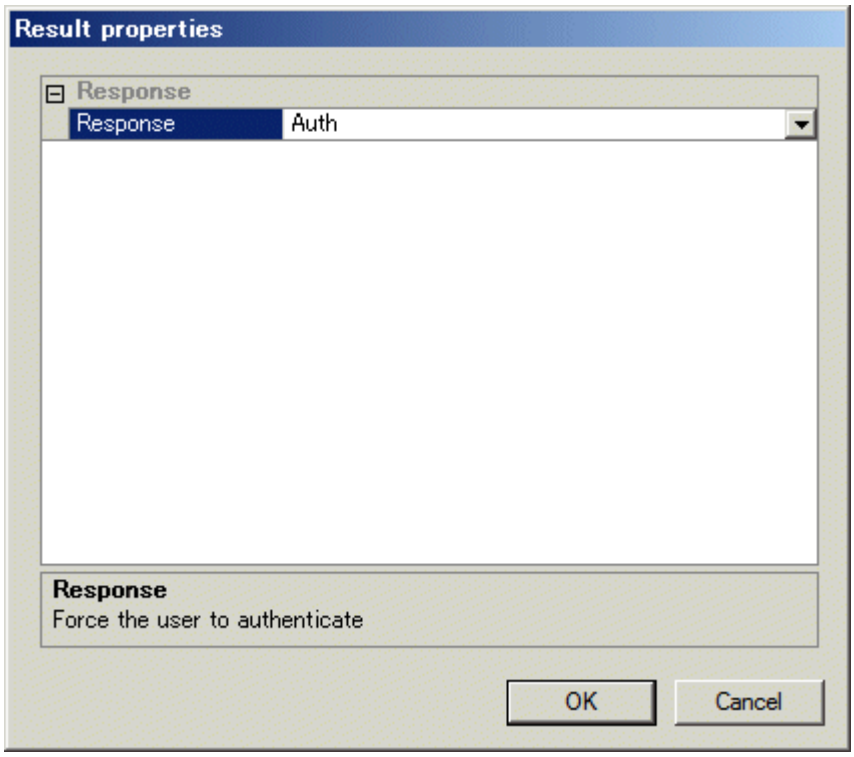



作成した User / Group check アイテムに任意の名前を入力します。

7. WWW Proxy Server: ProxyRequest が User / Group check を行うように WWW Proxy Server: ProxyRequest から作成した User / Group check へ向けてマウスをドラッグし、フローチャートの順序が WWW Proxy Server: ProxyRequest → User / Group check になるようにします。

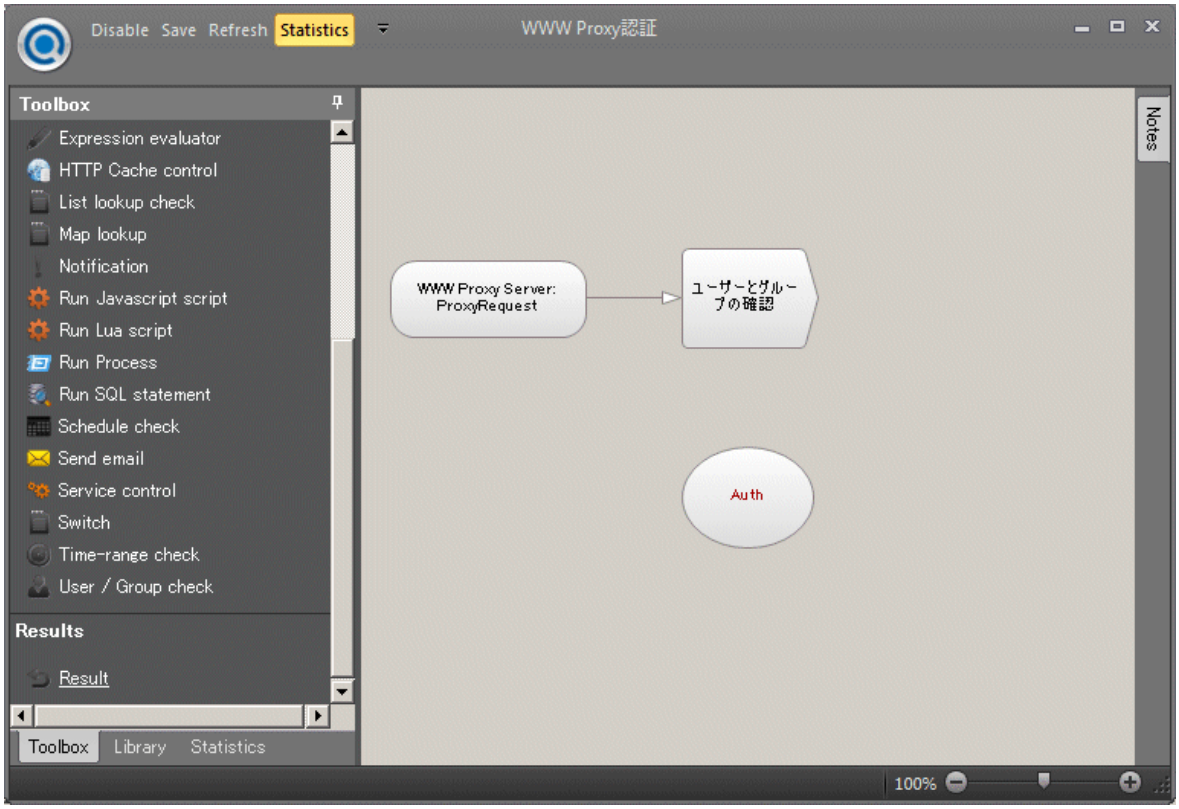



8. 認証を行うように Results から Result を選択して、右側にドラッグします。

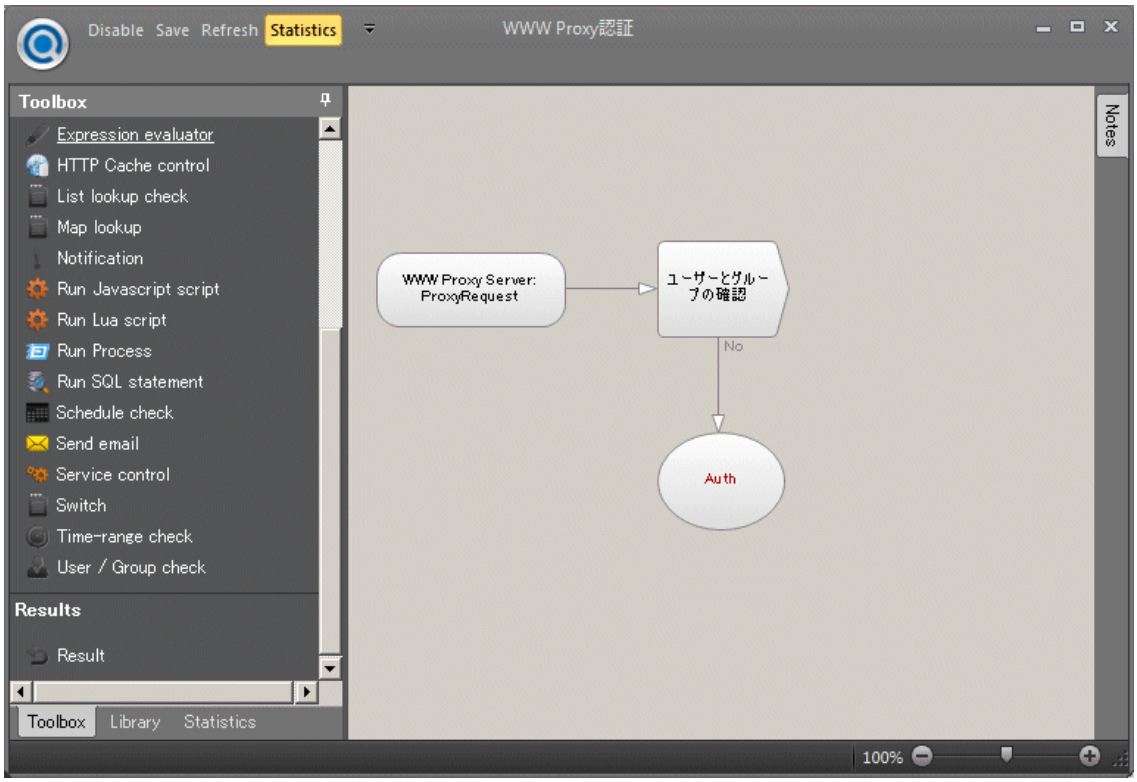



Result Response ダイアログが表示されますので、Response ドロップダウン・メニューから Auth（認証）を選択し、OK ボタンをクリックします。

以下の状態になります。

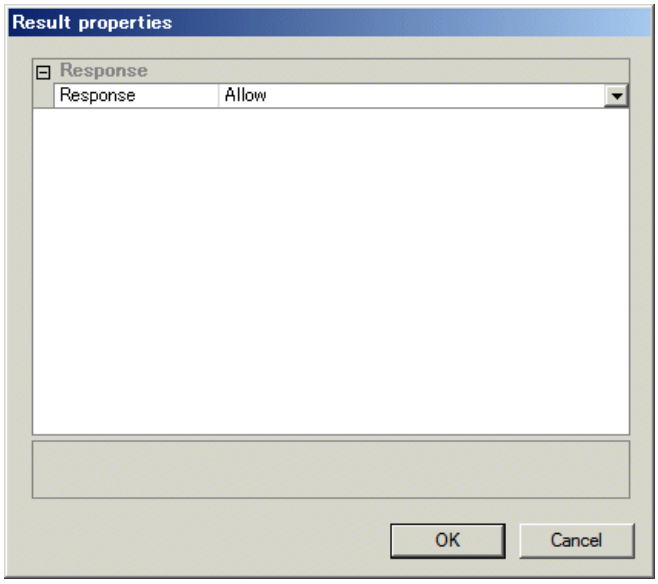



User / Group check から作成した Auth に向けてマウスをドラッグして、以下の状態とします。



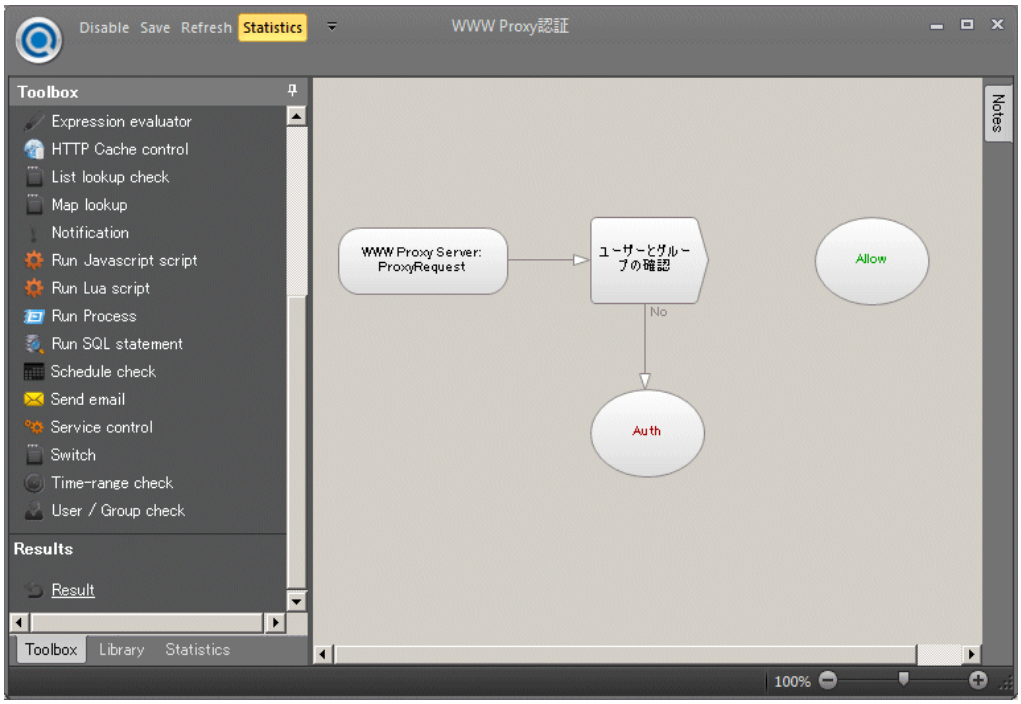

この時、No が Auth へ向けられるようにすることにご注意ください。

9. 認証されたユーザーを許可するため Results から Result を選択して、右側にドラッグします。

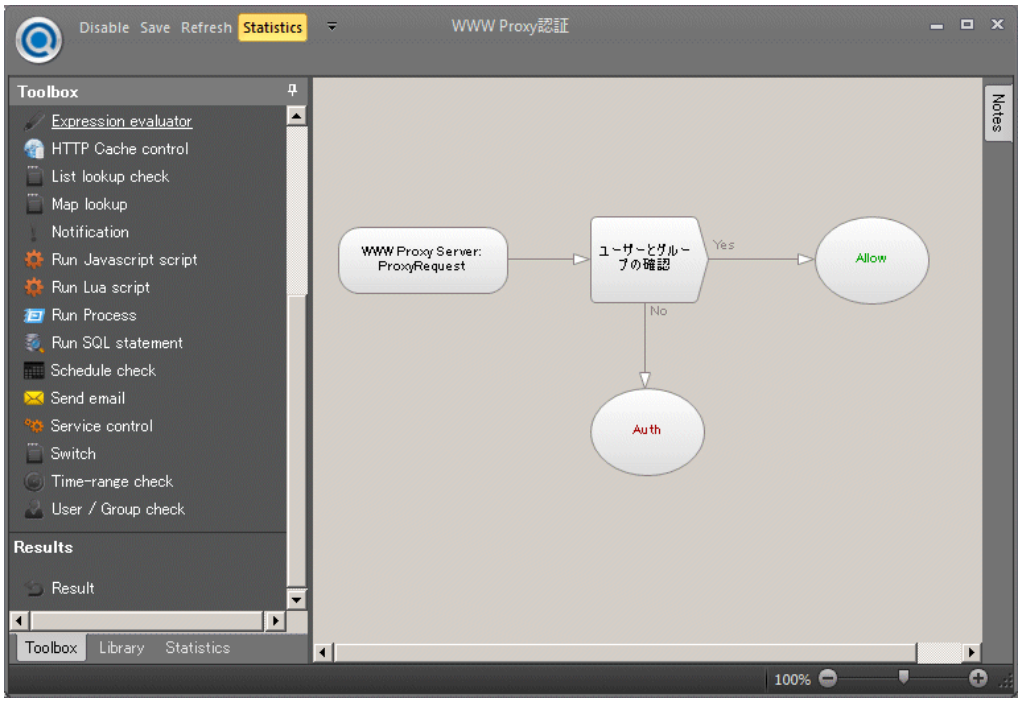



Result Response ダイアログが表示されますので、Response ドロップダウン・メニューから Allow（許可）を選択し、OK ボタンをクリックします。

以下の状態になります。




User / Group check から作成した Allow に向けてマウスをドラッグして、以下の状態とします。




10. Policy ウインドウの Save（保存）をクリックして、現在の状態を保存します。
    保存が完了いたしましたら、ウインドウ右上の「閉じる」をクリックして Policy ウインドウを終了します。

11. 作成した Policy が追加されます。

以上で、WWW Proxy Server でのユーザー認証設定は完了となります。

**（重要）ご注意：**

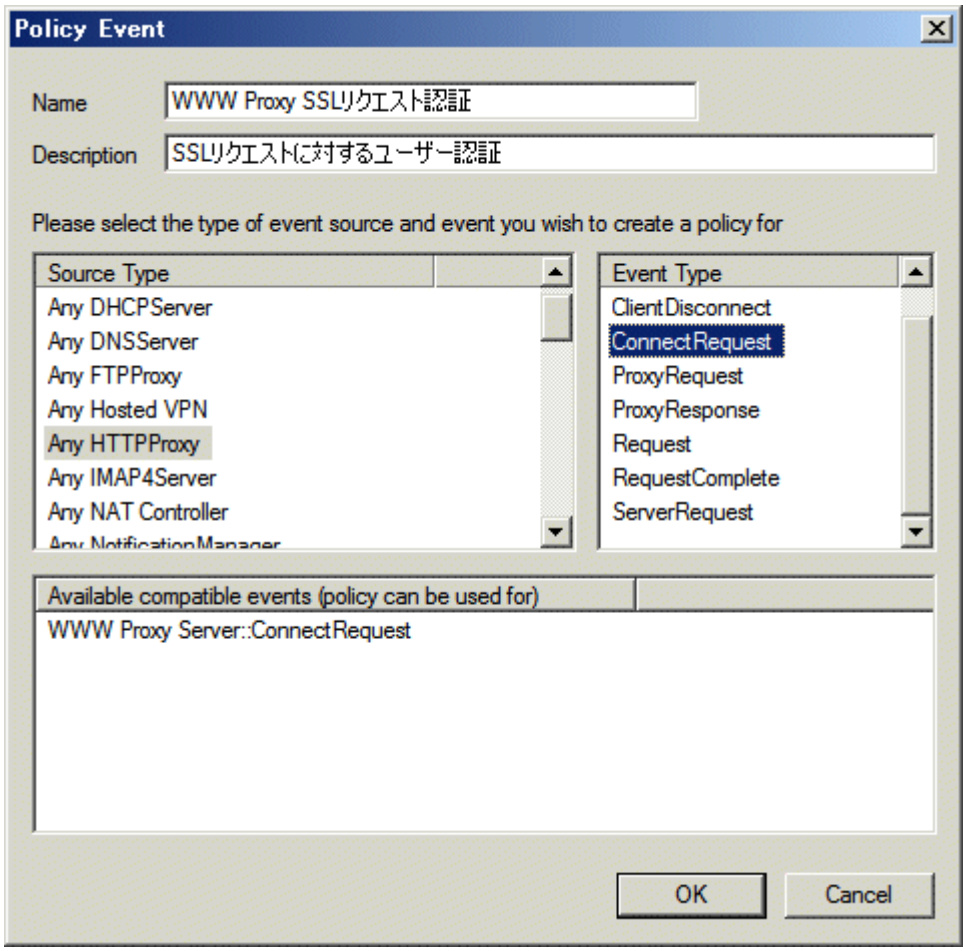
**ブラウザで最初に SSL サイトを参照するような場合、上記の設定では、認証を行わずに SSL サイトを表示することができます。**（例　ブラウザのホームページで　https://　で開始する　URL　が指定されている場合や認証が切れた後に https://　で開始する URL を参照する場合など）

これは、ブラウザでプロキシサーバーを使用する構成となっている場合に送られる SSL 要求が CONNECT 要求により行われるため、先程作成した ProxyRequest では識別できない為に発生します。

また、WinGate　の　NAT　や　WinGate　インターネット・クライアントを使用している場合、SSL　要求は、WWW　Proxy Server を経由して取り扱うことができません。よってインターセプト・プロキシを使用する場合は、SSL サイトへの接続では、WWW Proxy Server による認証を行えません。

このような SSL サイトの参照に対しても、認証を必要とする場合には、以下のポリシーを作成します。

1. WinGate Management の Navigation より Policy（ポリシー）を選択し、Tasks より New Policy をクリックします。

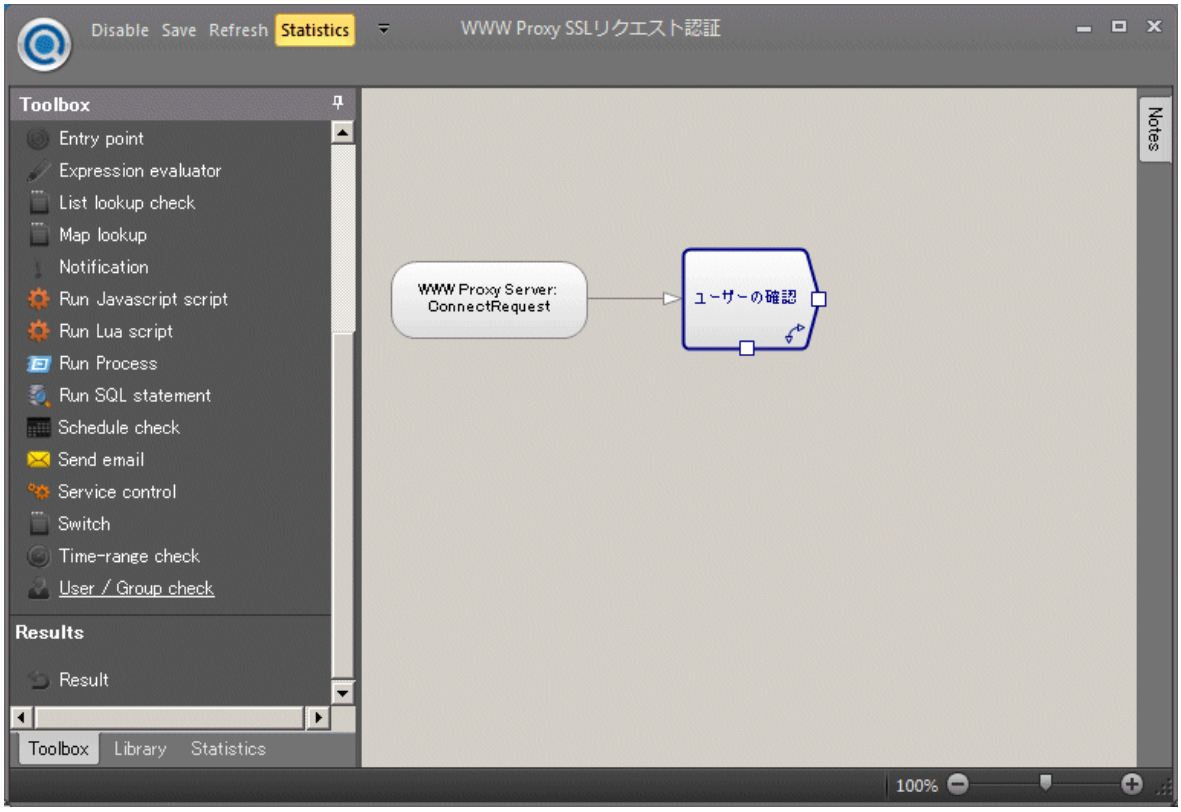



Name（名前）欄に、この制限の名前を入力します。

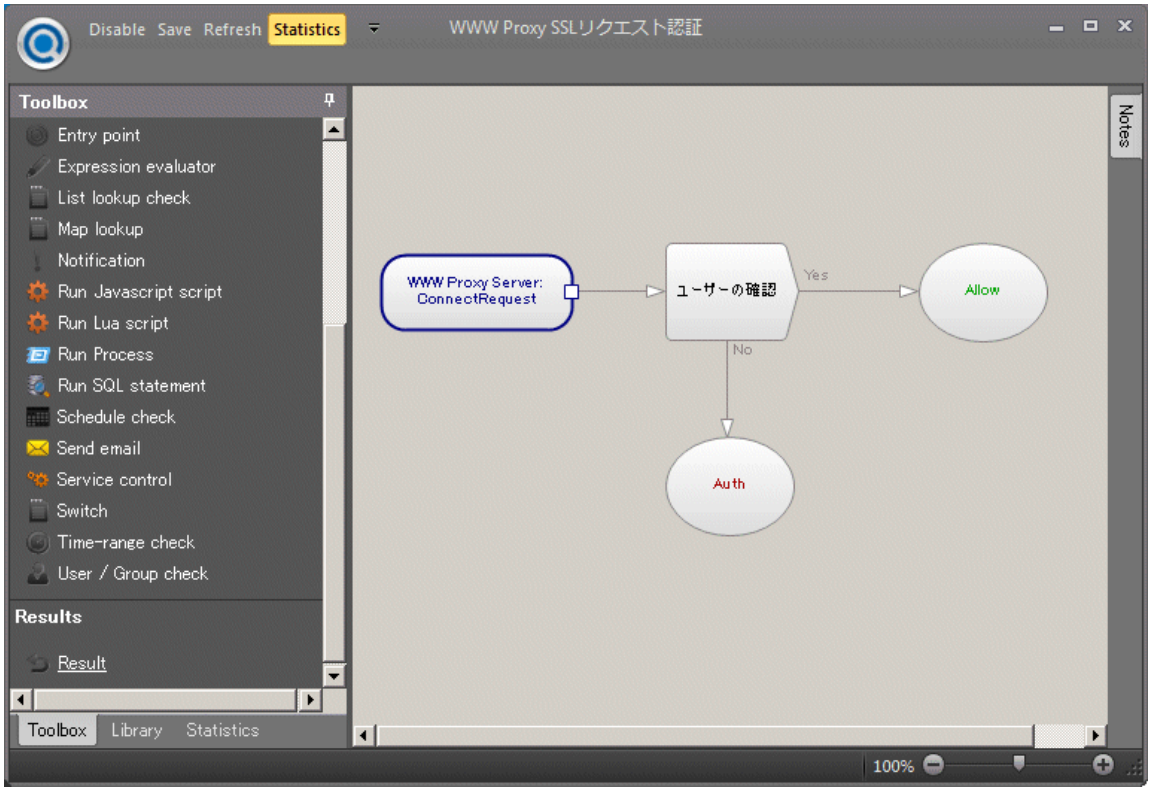
Description（説明）欄には、この制限の簡単な説明を入力します。（任意）

Source Type（ソースタイプ）で Any HTTPProxy を選択、Event Type で ConnectRequest を選択し、OK ボタンをクリックします。

2. ProxyRequest の Policy と同様に WWW Proxy Server:ConnectRequest をドラッグ、Items より User / Group check をドラッグして認証を必要とするユーザーを選択します。



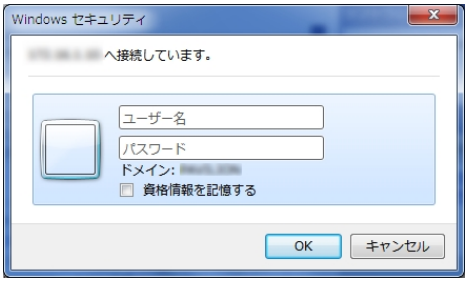

3. 後の手順は、先の ProxyRequest の Policy と同じになります。
最終的に以下の状態としてください。



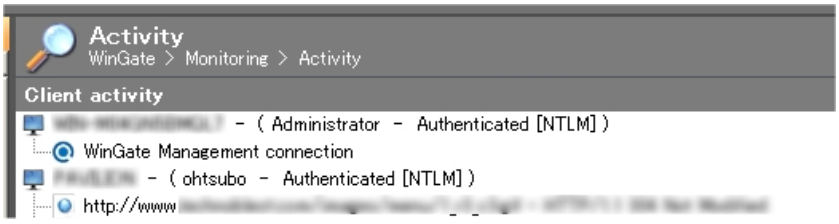

これらの設定により、WWW Proxy Server への接続があった場合は、認証を行う構成となります。

クライアントのブラウザからアクセスした場合に、ユーザー認証が行われているかをご確認ください。
WinGate ユーザー・データーベースを使用している場合、以下の認証ダイアログが表示されます。(以下は、Internet

Explore で表示される認証ダイアログとなります。NTLM、Basic 認証かによりダイアログの内容は異なります。また、使用するブラウザの種類によっても認証ダイアログは異なります。）

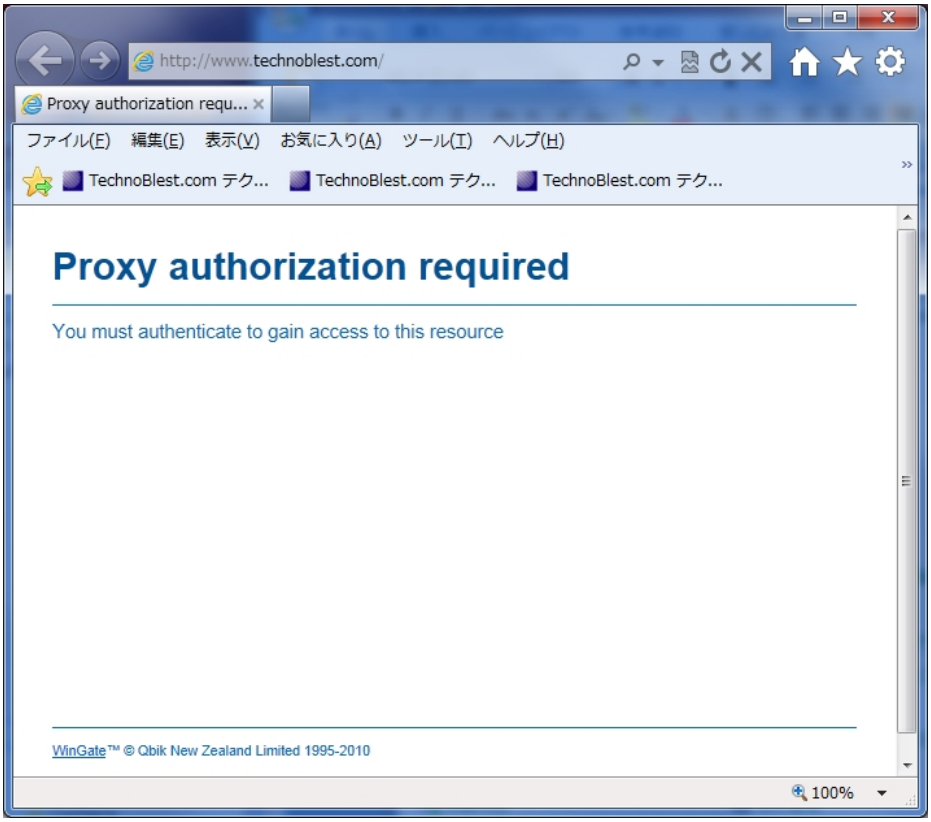



Active Directory ユーザー・データーベースや Windows ユーザー・データーベースを使用している場合は、クライアントの Windows から自動的に資格情報が送られるため、認証ダイアログが表示されない場合があります。
認証済みユーザーは、WinGate Management の Activity スクリーンで以下のように表示されます。




クライアントアクティビティにユーザー名、Authenticated（認証済み）、 [ ] 内に認証方式が表示されます。

認証に失敗した場合、以下のメッセージがブラウザに表示されます。また、WinGate の Diagnostic ログには、認証に失敗したことを示す Authentication failed to WWW Proxy server が記録されます。

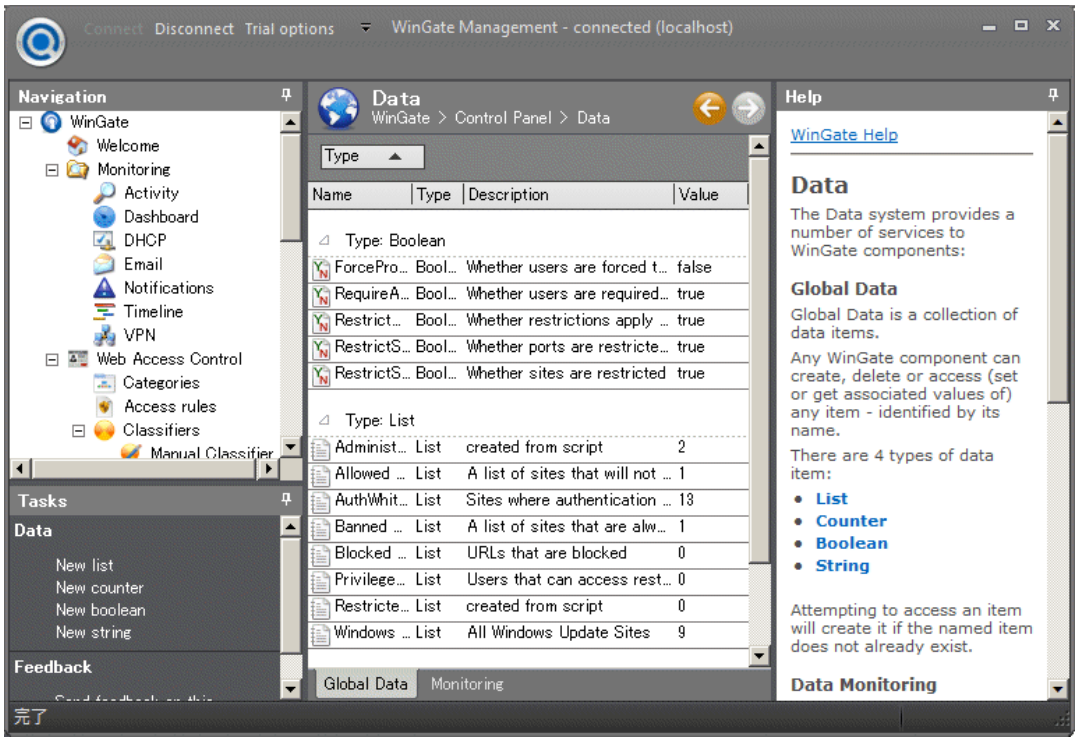



※ブラウザが要求したページのキャッシュを持っている場合、このメッセージが表示されずキャッシュされた情報が表示される場合がございます。

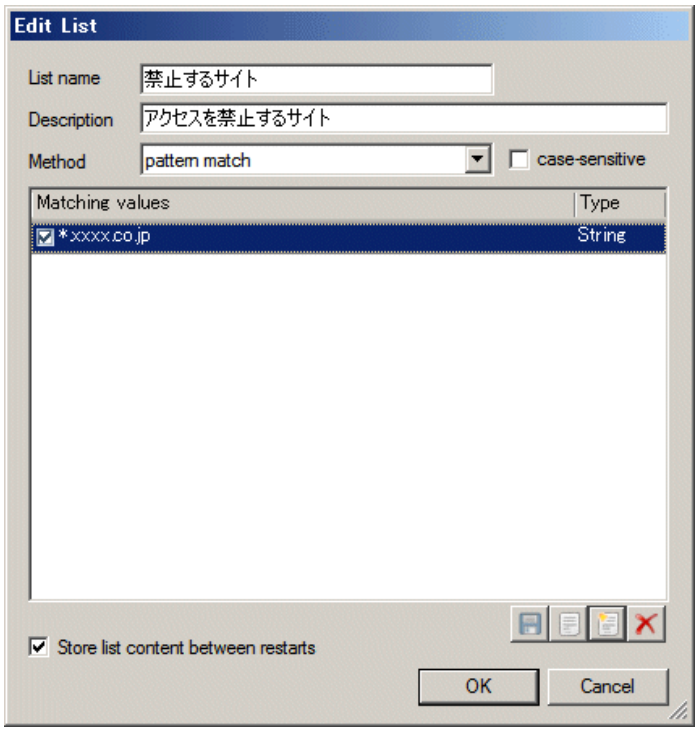
**ユーザーに特定の Web サイトのみの表示を認める、または特定の Web サイトの表示を許可しない。**

WinGate の Web Access Control 機能を使用して、特定のサイトのみの表示を許可、または特定の Web サイトの表示を許可しない設定を行います。

1. アクセスを禁止するサイト、または URL のリストを作成します。
   WinGate Management の Navigation より Data を選択し、Global Data タブを開きます。




2. Tasks の Data より New list（新規リスト）をクリックします。

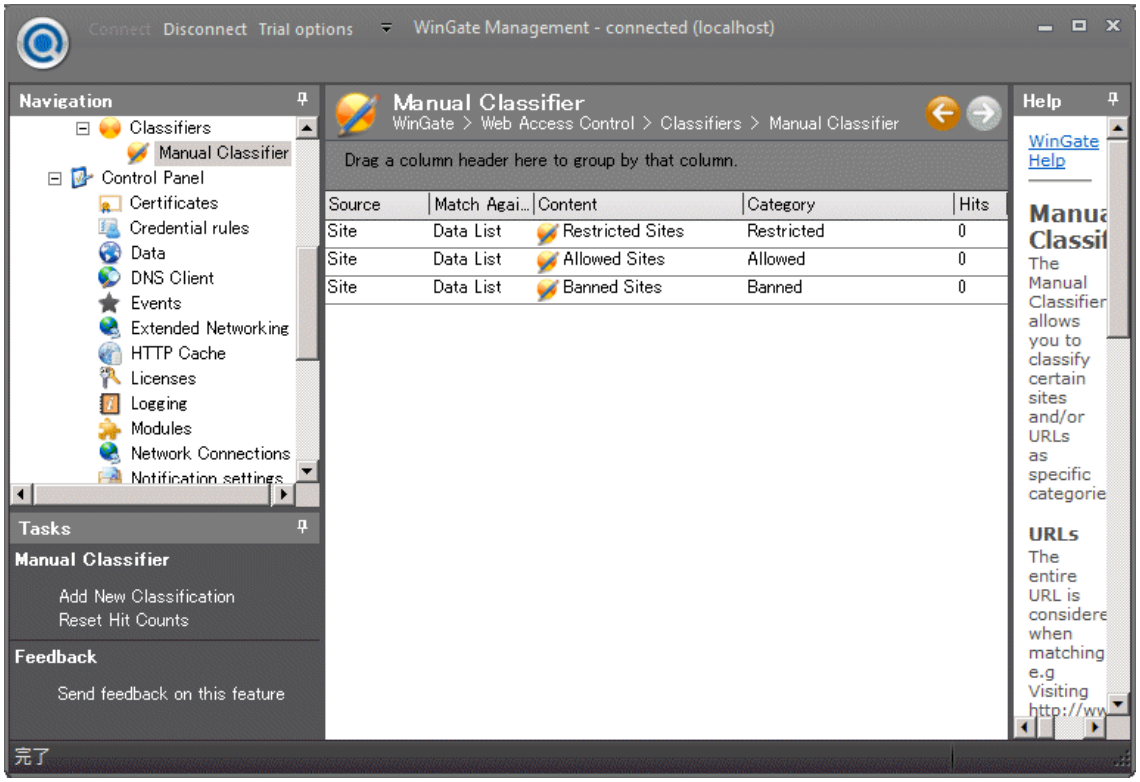



   Edit List ダイアログが表示されますので以下の項目を入力します。

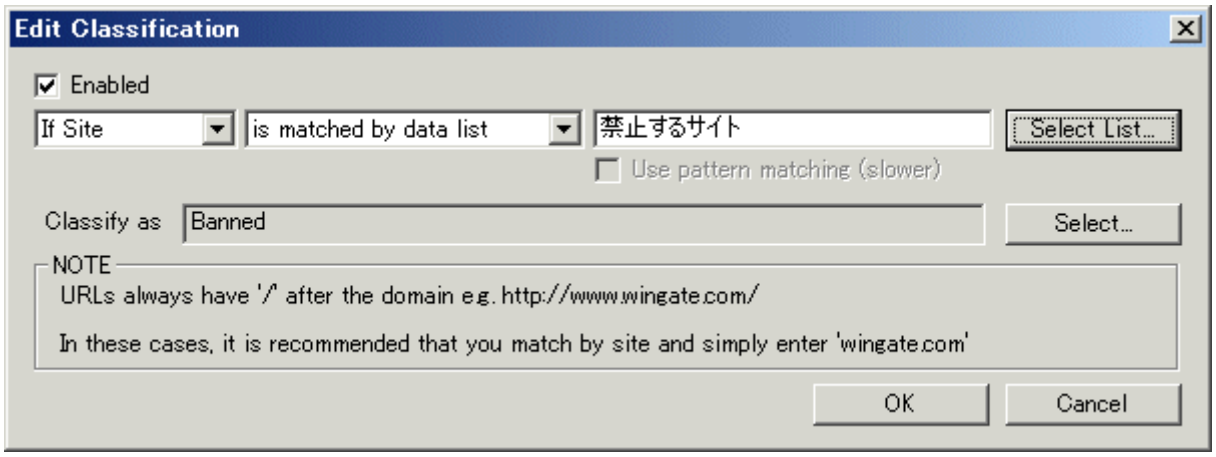
List name ＝ このリストの名前を入力します。
Description ＝ このリストの説明を入力します。(任意)
Method ＝ ドロップダウン・メニューより Pattern match(パターンマッチ)を選択します。
Matching values ＝ 右下のボタンより、右から 2 番目の新規ボタンをクリックして、アクセスを禁止するサイトまたは URL を入力します。
幾つかのサイト、URL を追加する場合は同じ動作を行ってください。
※ご注意
URL による禁止を行う場合は http://www.xxxxxx.com/ のように先頭に http:// を持ち、最後が / (スラッシュ)で終わるようにしてください。
サイトによる禁止を行う場合は、www.xxxx.com または xxxx.com のように設定してください。( * によるワイルドカードが使用できます。

OK ボタンでダイアログを終了し、Type List 欄に新しくリストが作成されていることを確認してください。

3. WinGate Management の Navigation より Web Access Control、Manual Classifier を選択します。




Tasks の Manual Classifier より Add New Classifier(新規分類の追加)を選択します。



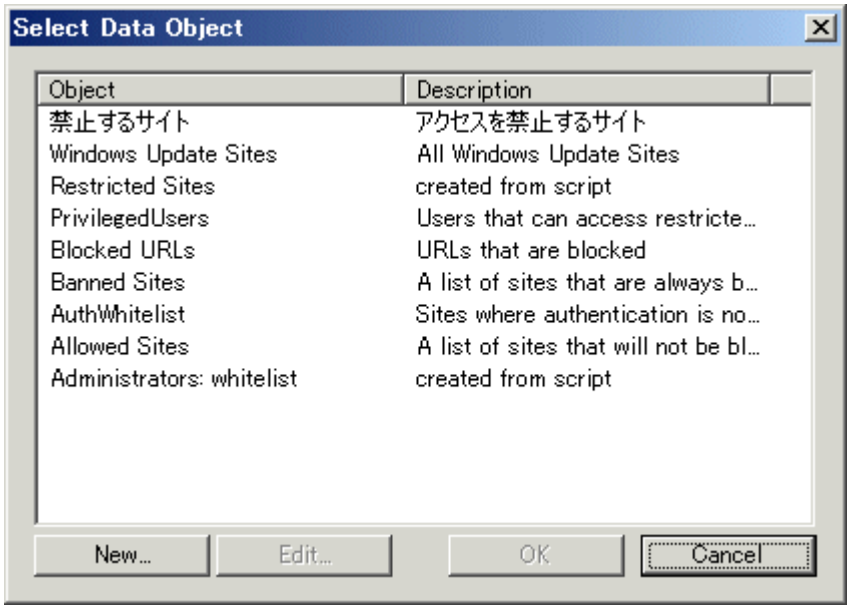

Edit Classification（分類の編集）ダイアログが表示されますので、上記のダイアログのように設定します。

Enable（有効）をチェック

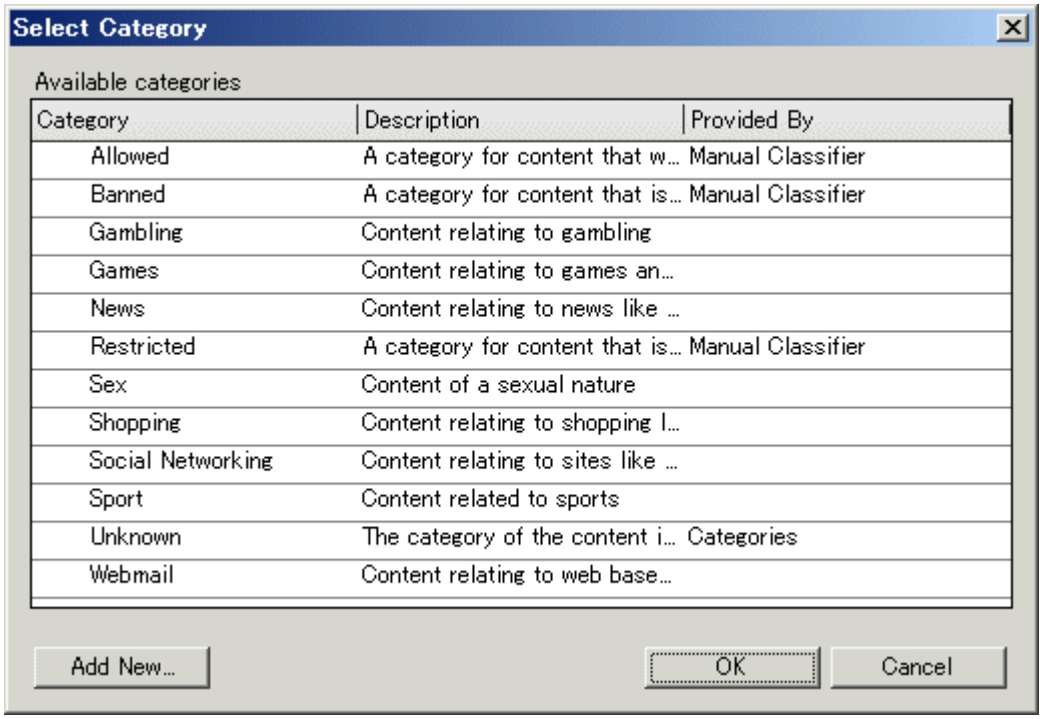
サイトによる禁止リストを作成した場合は、先頭のドロップダウン・メニューで If Site を選択、URL による禁止リストを作成した場合は、ドロップダウン・メニューで If URL を選択します。

中央のドロップダウン・メニューでは、is matched by data list　を選択します。

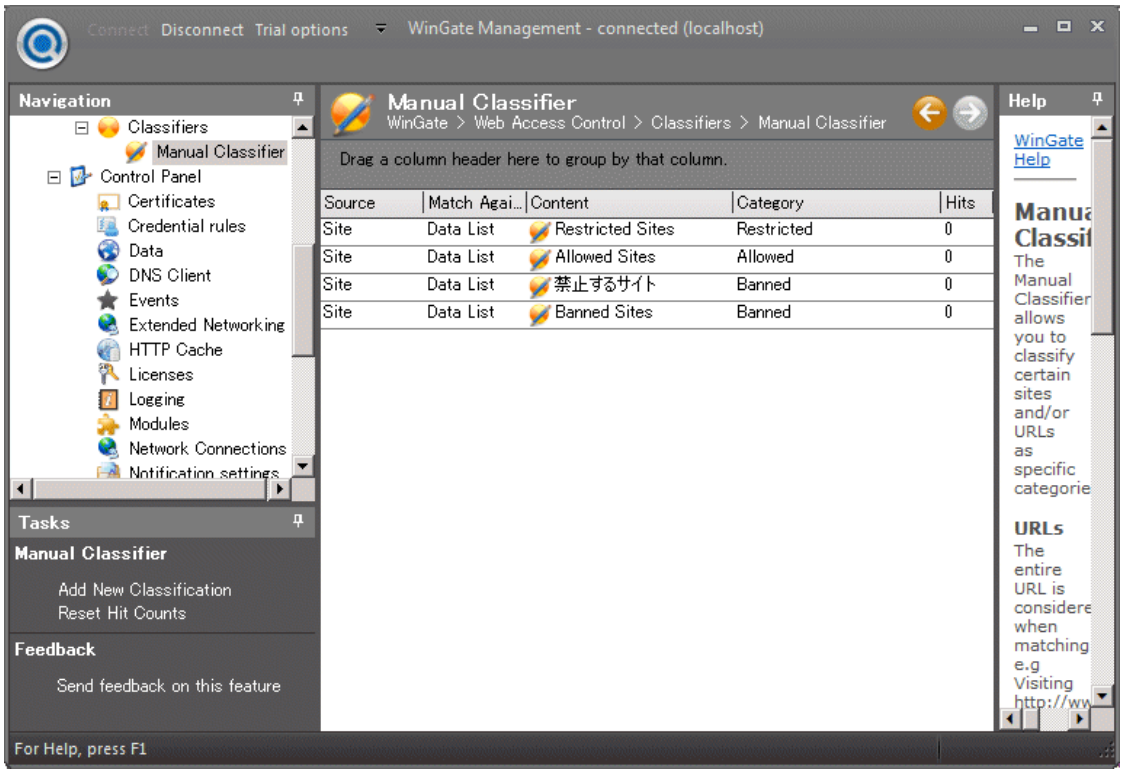
右側の Select List ボタンをクリックし、Select Data Object ダイアログで、最初に作成したデータリストを選択し、OK ボタンをクリックします。




Classify　as では、右側の Select ボタンで表示される Select　Category ダイアログから Banned（禁止された）を選択し、OK ボタンをクリックします。




全ての選択が完了いたしましたら、OK ボタンで Edit Classification を終了します。

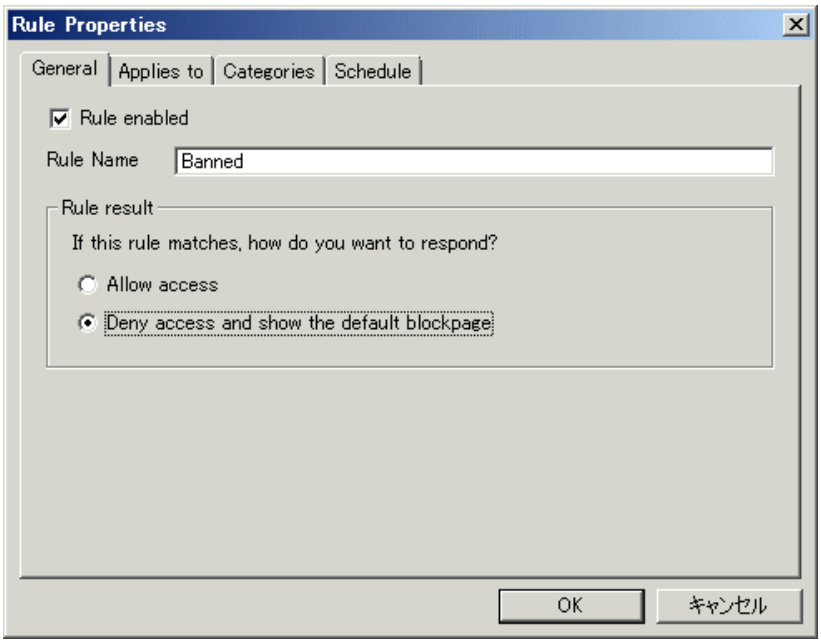



上記のように分類が追加されます。

以上で、全てのユーザーに対してリストで作成したサイト、URL をブロックする事ができます。

また特定のユーザーに対してのみ、ルールを適用する事も可能となります。
その場合は、Access rules の Applies to タブより適用するユーザーを選択します。
ご注意：Access rules の Applies to タブでユーザーやグループを指定した場合、WinGate はユーザーを判断する必要があるため、ユーザー認証が自動的に有効になります。

ユーザー認証を使用しない方法としては、Credential rules で IP アドレスとユーザーを関連付ける事により、WinGate はユーザーを認識できるため、認証を行わずにユーザー毎に制限を適用する事ができます。



**決められた IP アドレスからの接続を許可する（または許可しない）①（ポリシー）**

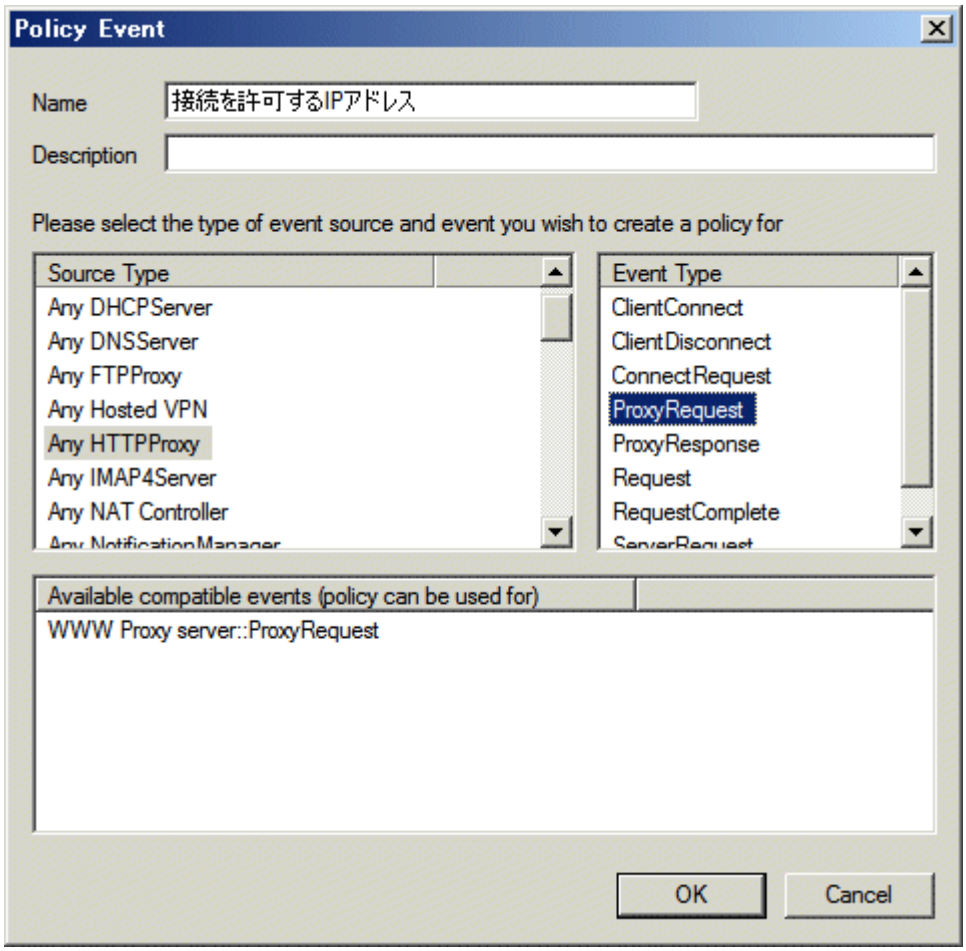
WinGate の WWW Proxy Server へのアクセス（HTTP リクエスト）で特定の IP アドレスからの接続を許可する設定となります。（HTTPS サイトを制限する場合、別途 Any HTTPProxy の ConnectRequest でポリシーを作成する必要があります。）

WWW Proxy Server で特定の IP アドレスからの利用のみを許可したい場合に有効なポリシー設定となります。

※他のポリシーアイテムと組み合わせて利用する場合、このポリシーによる設定をお勧めいたします。より容易に、指定した IP アドレスを禁止したい場合には、②の Web Access Control を使用する方法をご利用ください。

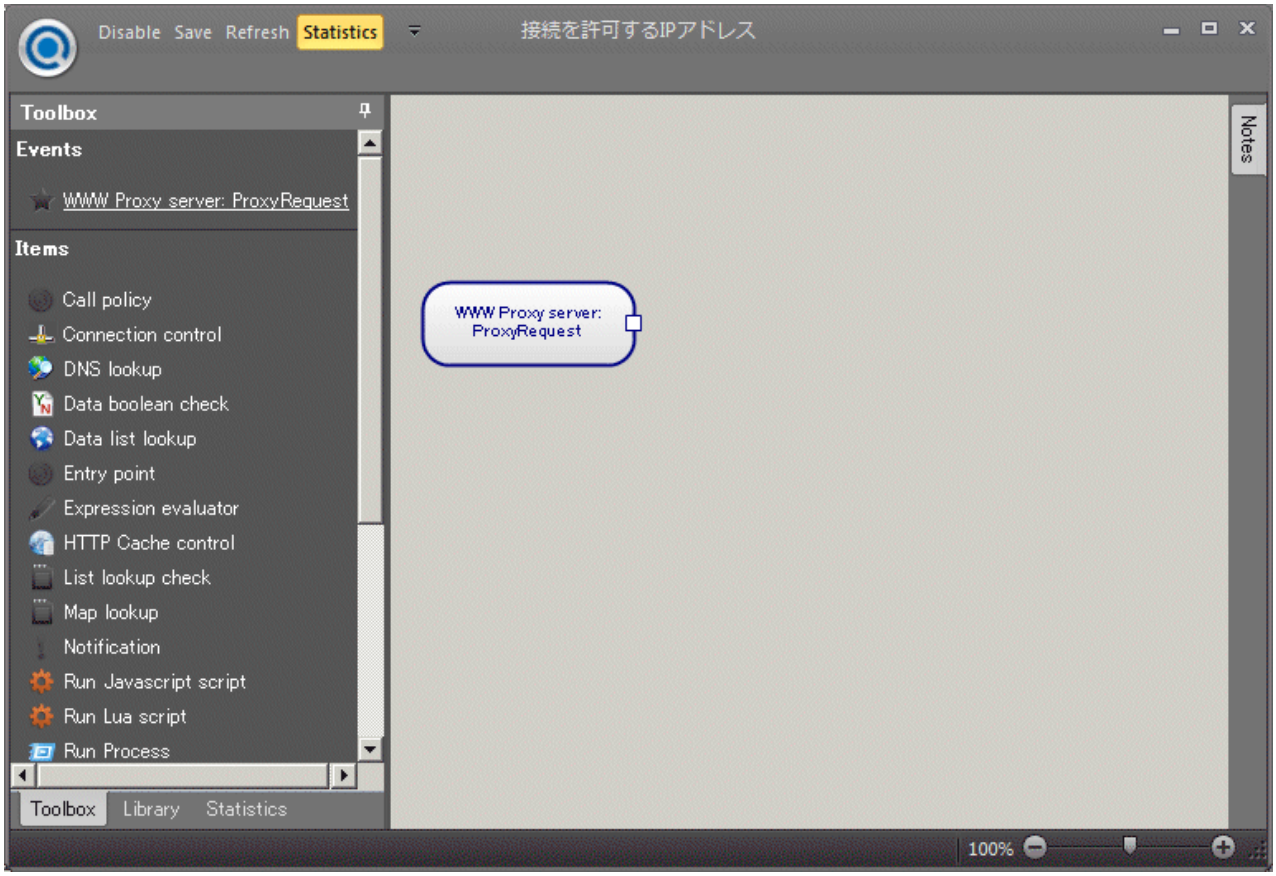
※他の Proxy サービスなどでもご利用いただける設定となります。

1. WinGate Management の Navigation より Policy（ポリシー）を選択します。
   Tasks より New Policy を選択します。



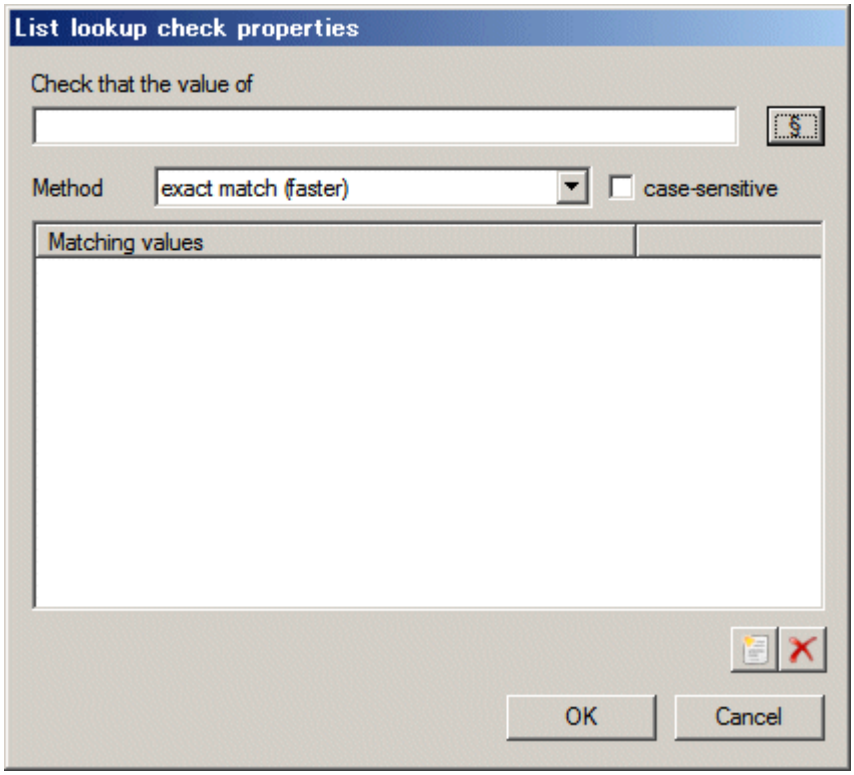

   Name 欄に作成するポリシーの名前を入力します。
   Source Type では、Any HTTPProxy を選択、Event Type で ProxyRequest を選択します。
   Available compatible event には、このポリシーで制限可能なサービスが表示されます。
   OK ボタンクリックします。

2. Policy ダイアログが表示されます。

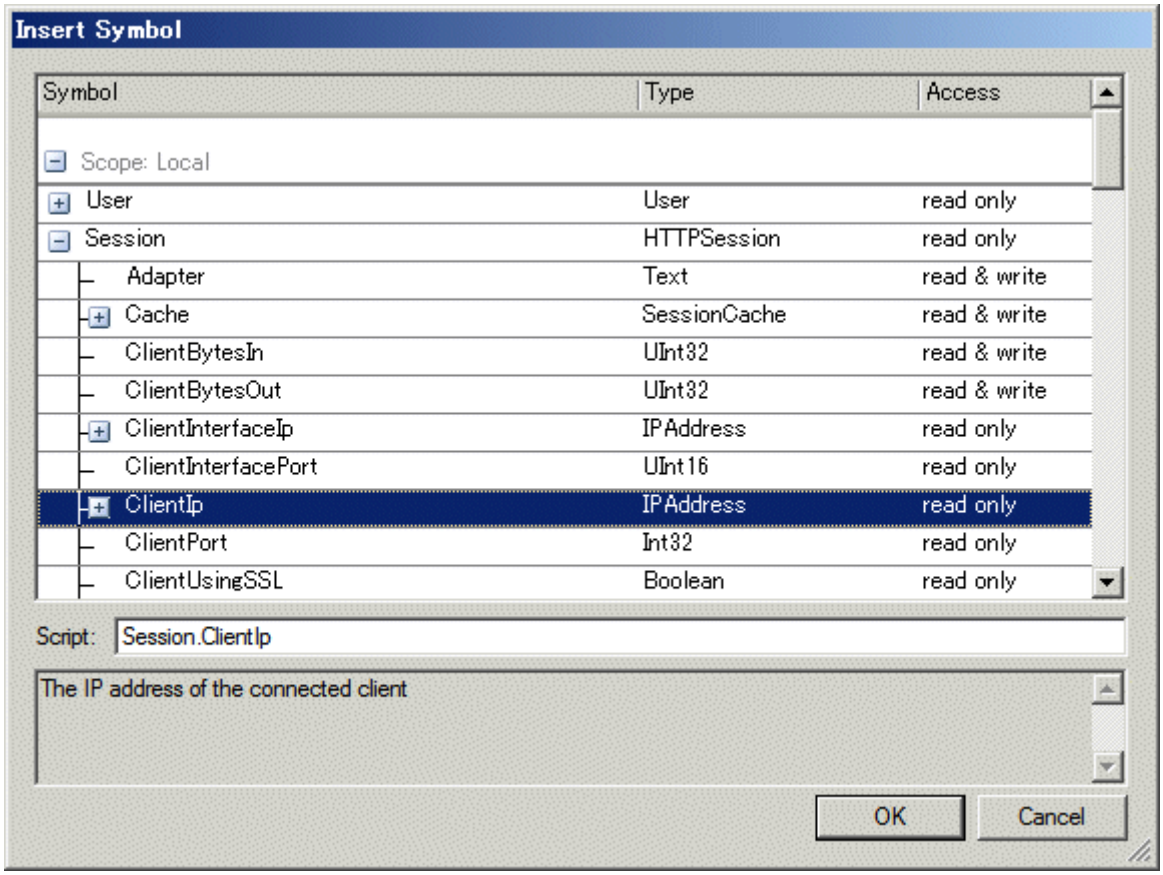



Event より WWW Proxy Server: ProxyRequest をマウスで選択しドラッグします。

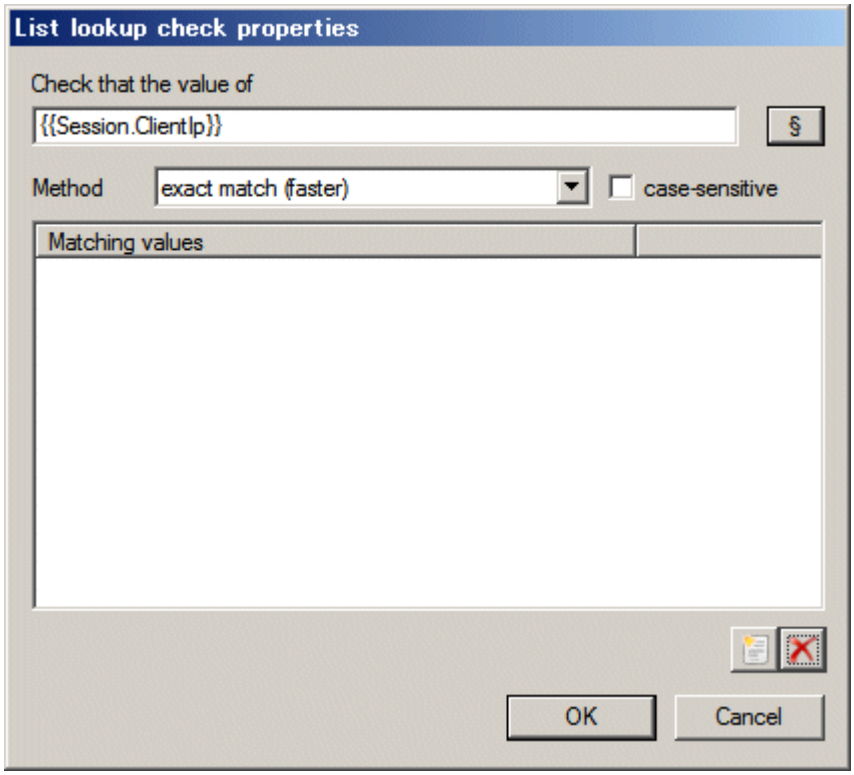
3. Items より List lookup check を選択して右側の欄にドラッグします。
   すると List lookup check properties ダイアログが表示されます。




Check that the value of 欄の右側にある Insert Symbol ボタンをクリックします。



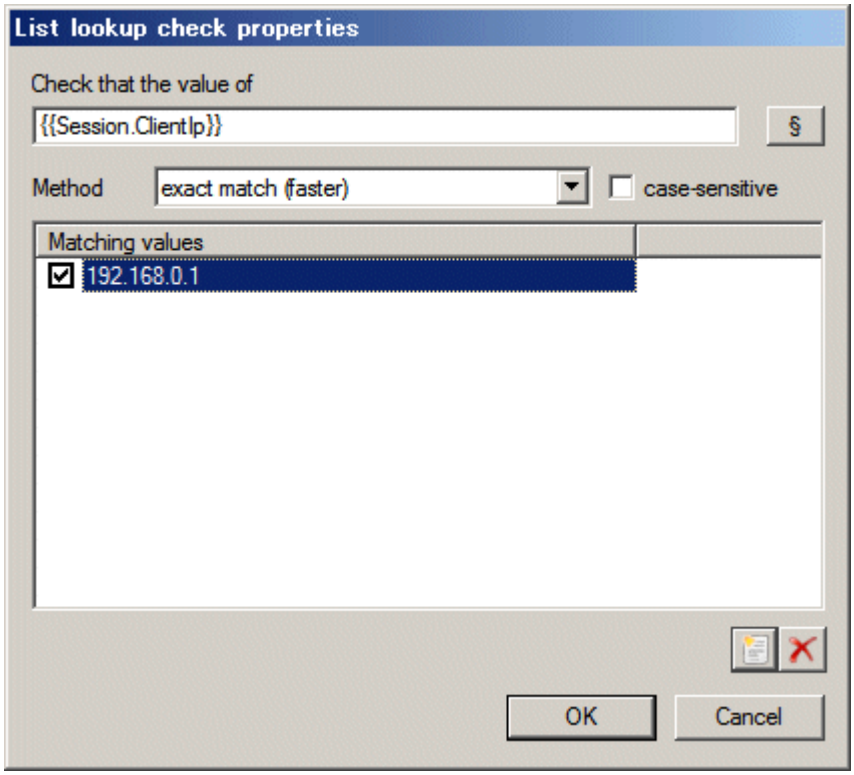

Insert Symbol ダイアログが表示されますので、Session より ClientIp を選択し OK ボタンをクリックします。




List lookup check properties ダイアログに {{Session.ClientIp}} が追加されます。

Method では、exact match(faster) （完全一致）を選択します。

続いて、右下の Add a new policy decision ボタンをクリックして、接続を許可する IP アドレスを設定します。




複数のアドレスを追加する場合は、この操作を繰り返し行います。

また、192.168.0.* のようなワイルドカードを使用する場合は、Method で Pattern mutch を選択してください。

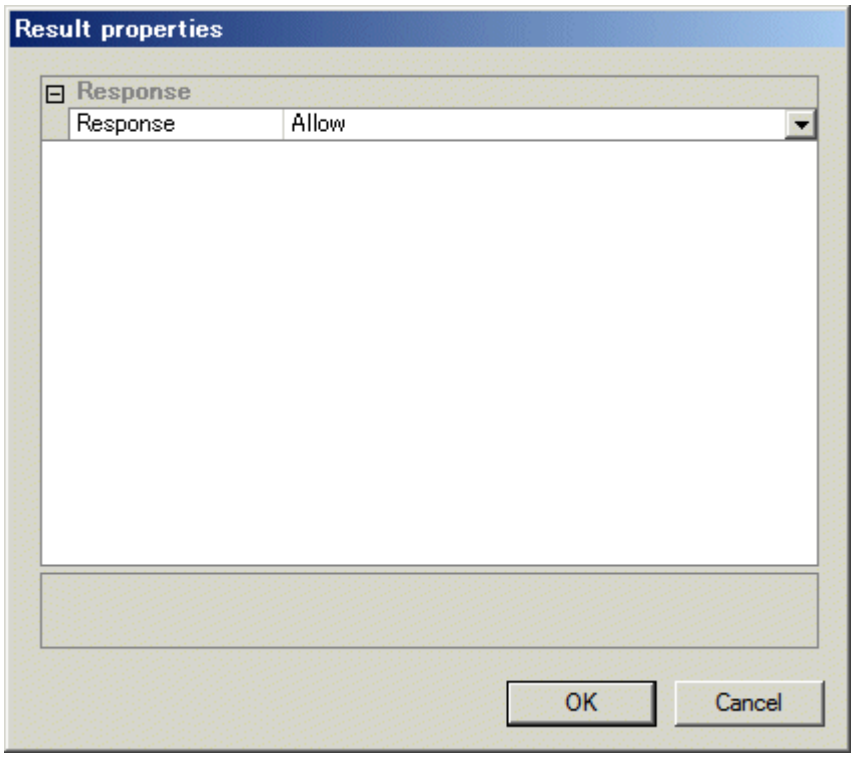
アドレスの追加が完了いたしましたら、OK ボタンで List lookup check properties ダイアログを終了します。

4. 作成した List lookup check に名前を入力します。

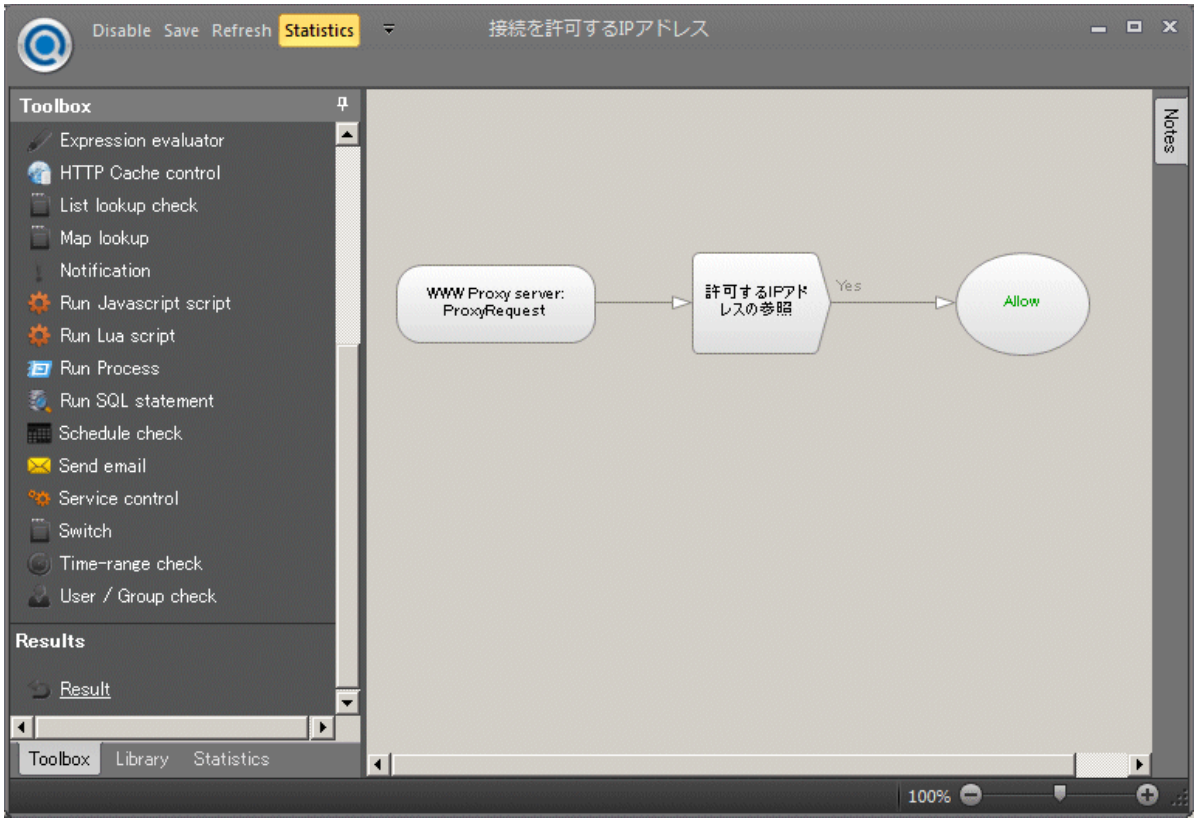
5. WWW Proxy Server: ProxyRequest から作成した List lookup check にマウスをドラッグして以下の状態としま

す。

6. Result 欄から Result を右側の欄にドラッグします。

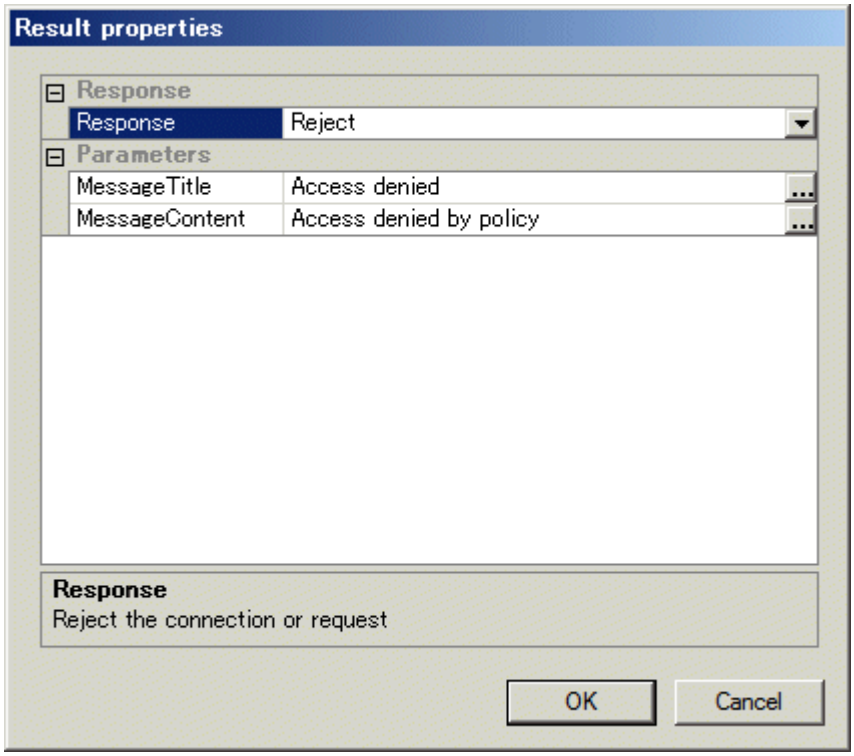



一致した IP アドレスを許可するために、Result properties ダイアログが表示されますので、Allow を選択して、OK ボタンをクリックします。

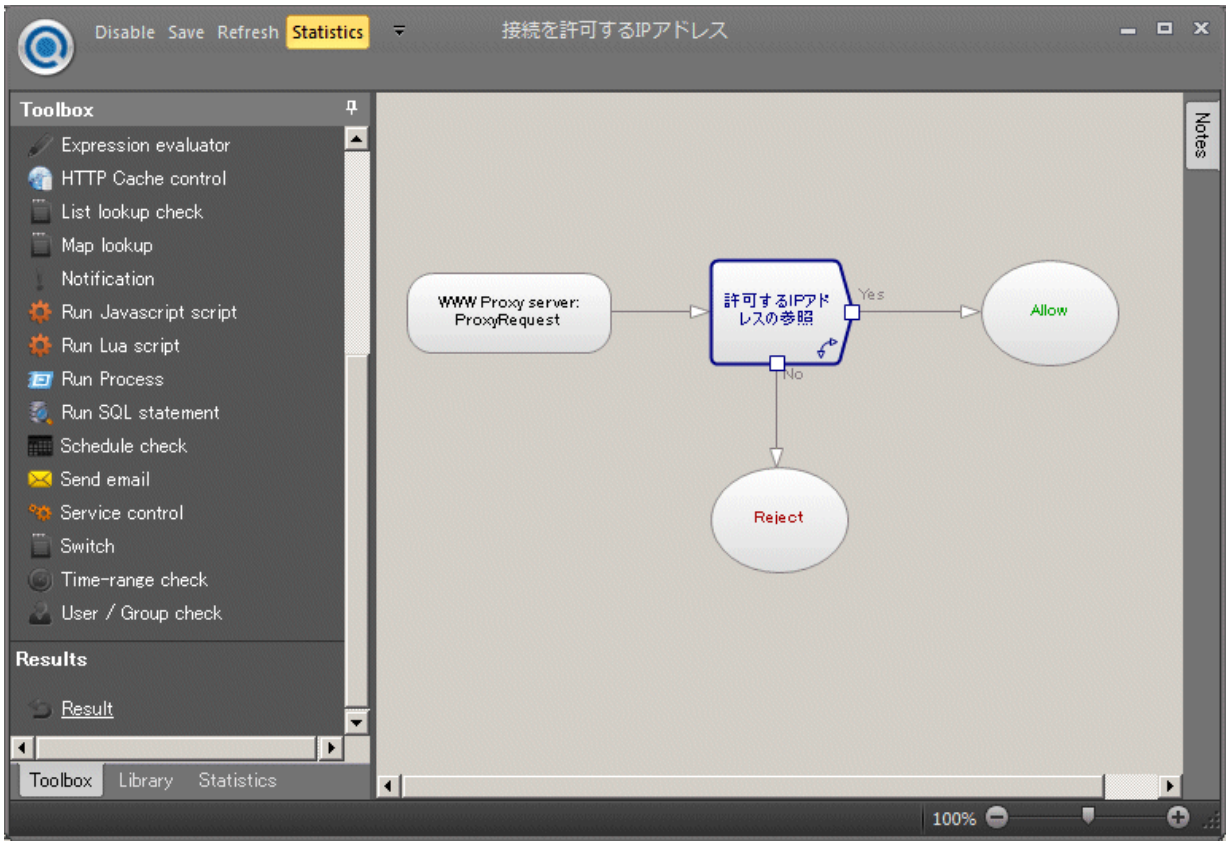



追加された Result Allow に List lookup check からマウスをドラッグして上記の状態とします。

7. Result 欄から Result を右側の欄にドラッグします。

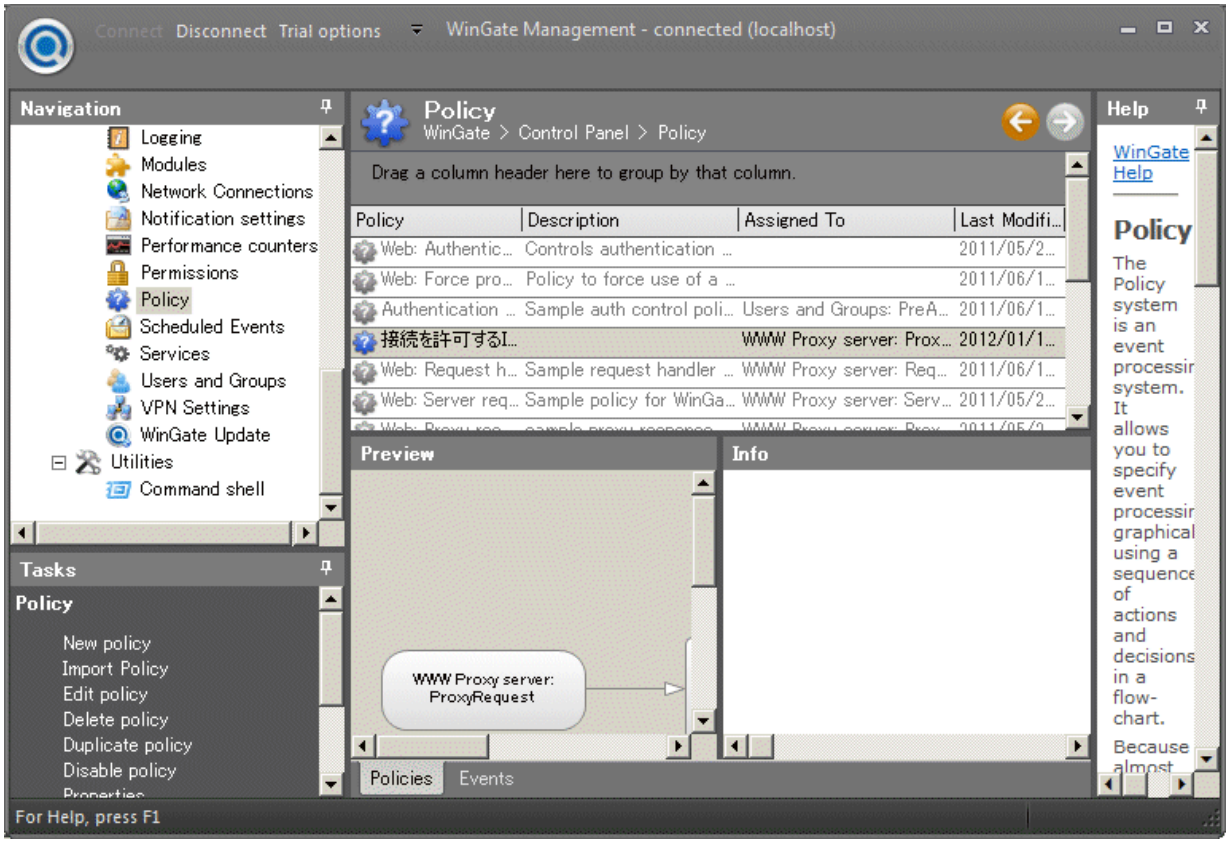



一致しない IP アドレスを拒否するために、表示された Result properties ダイアログで、Reject（拒否）を選択して、OK ボタンをクリックします。（表示されるメッセージを変更する場合は、Parameters 欄を変更してください。日本語の設定も可能となります。※一部のブラウザでは、文字化けが発生する場合があります。）




追加された Result Reject に List lookup check からマウスをドラッグして上記の状態とします。
Save ボタンで設定内容を保存して右上の閉じるボタン(×)でダイアログを終了します。

8. 作成されたポリシーが追加されます。

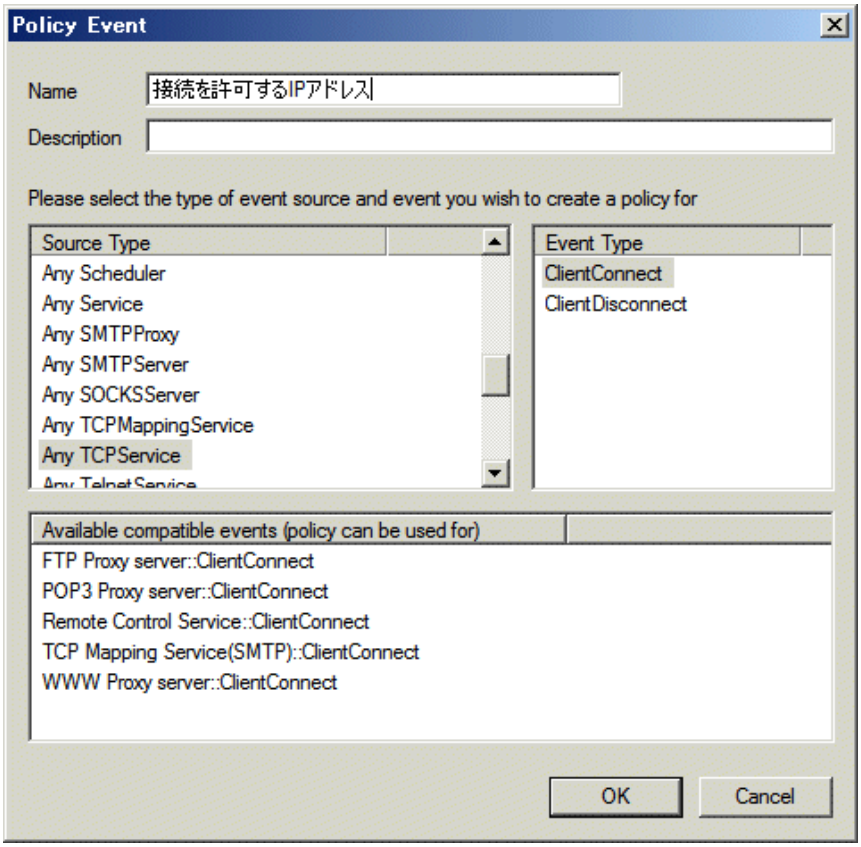


以上で接続を許可する IP アドレスの設定は完了となります。
設定完了後は、実際にクライアント PC より接続を行い、動作をご確認ください。
接続を許可しない IP アドレスを設定する場合は、手順 6～7 で Allow と Reject を逆に設定してください。

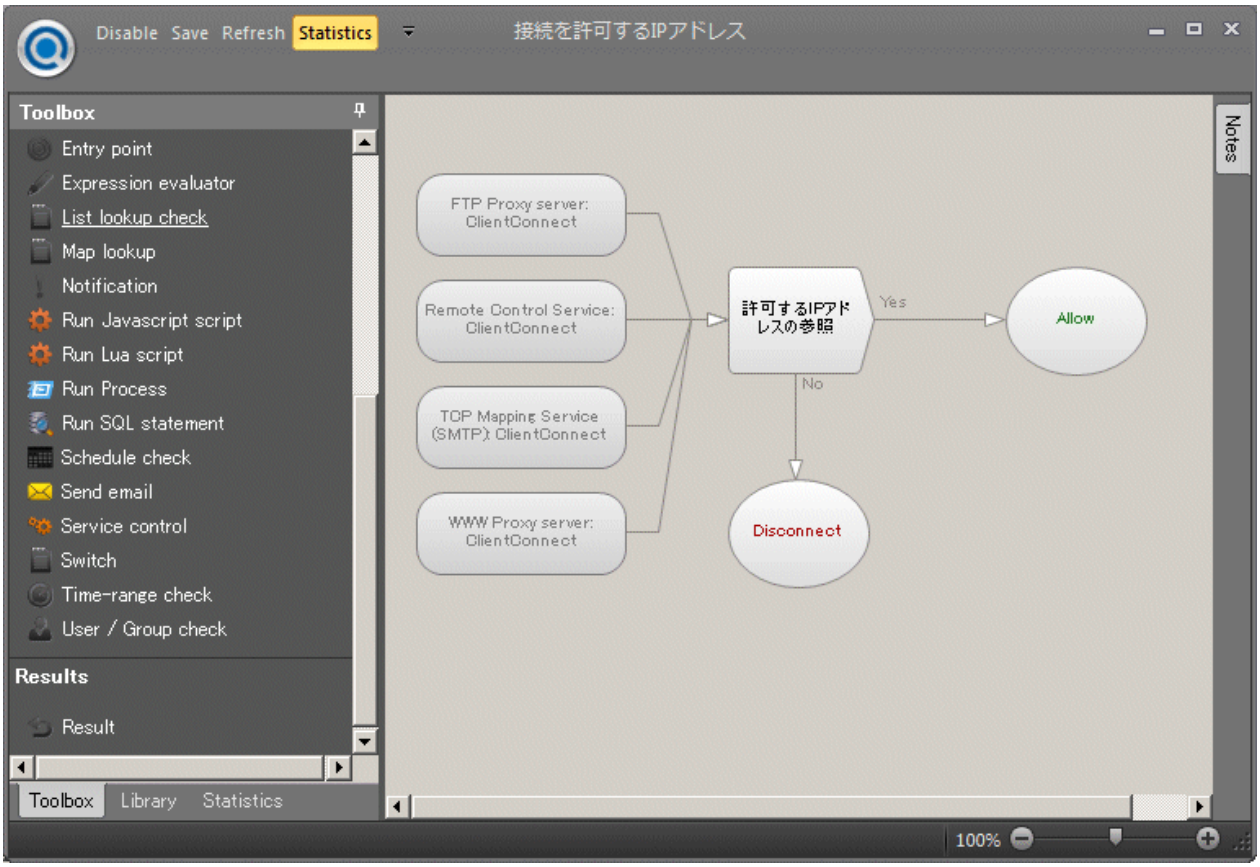
**ご注意：**

**ブラウザで SSL サイトを参照するような場合、上記の設定では SSL サイトを表示することができます。**（例 ブラウザのホームページで https:// で開始する URL が指定されている場合や認証が切れた後に https:// で開始する URL を参照する場合など）
これは、ブラウザでプロキシサーバーを使用する構成となっている場合に送られる SSL 要求が CONNECT 要求により行われるため、先程作成した ProxyRequest では識別できない為に発生します。
また、WinGate の NAT や WinGate インターネット・クライアントを使用している場合、SSL 要求は、WWW Proxy Server を経由して取り扱うことができません。よってインターセプト・プロキシを使用する場合は、SSL サイトへの接続では、WWW Proxy Server による認証を行えません。
本設定では、HTTP 接続のみが制限の対象となりますので、HTTPS サイトに対しても同様の制限を行う場合、Source Type（ソースタイプ）で Any HTTPProxy を選択、Event Type で ConnectRequest を選択し、同様のポリシーを作成してください。

WWW Proxy Server 以外のサービスで IP アドレスによる接続を許可する（しない）設定を行う場合、手順 1 の Policy Event ダイアログで Source Type で制限するサービスを選択して、Event Type に ClientConnect を選択することにより設定することができます。
また、下のスクリーンショットのように Source Type に Any TCPService を選択することにより、TCP 接続を使用するサービスをまとめて制限することもできます。（WinGate の全ての TCP サービスで同じ IP アドレスによる制限を行う場合は、この設定が便利です。）




設定後のポリシーウインドウは以下のようになります。




**ご注意**:Event Type で ClientConnect を選択した場合、リストに一致しない場合の処理として、Disconnect(切断)のみが選択可能となります。

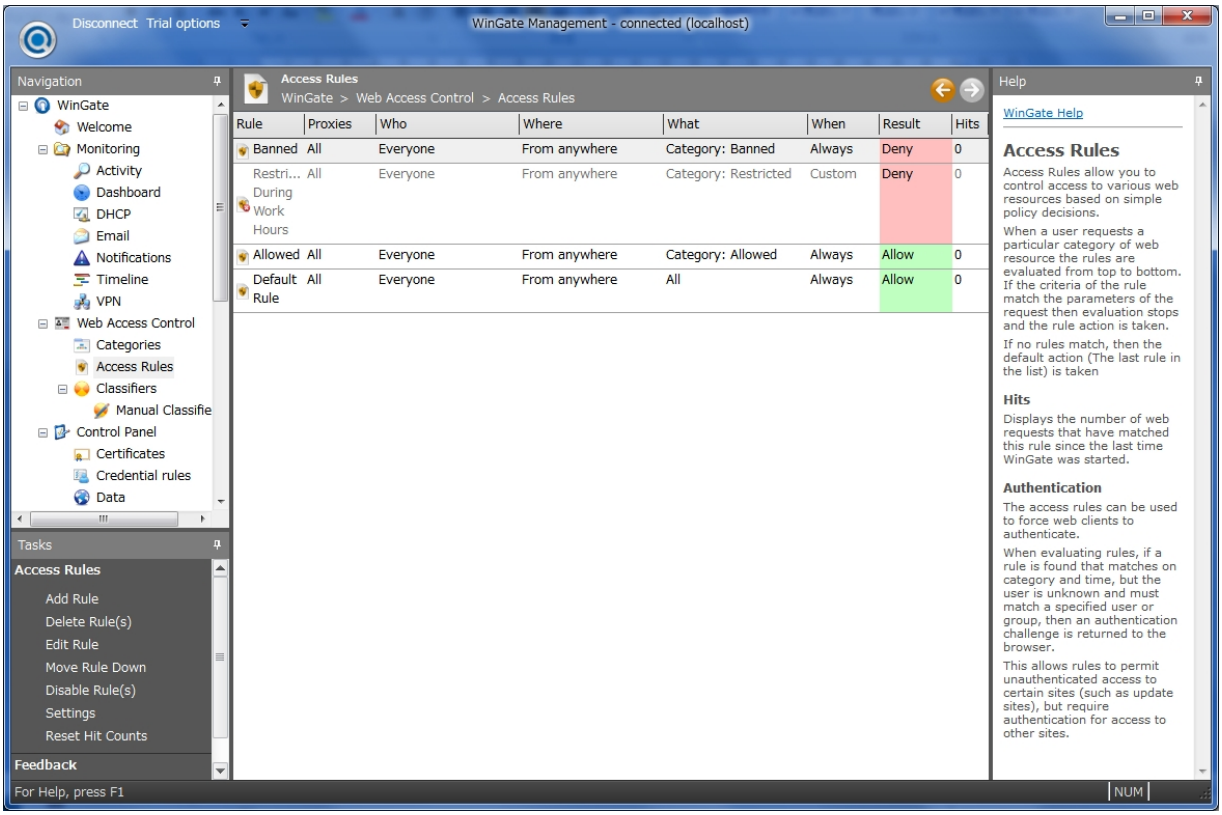
WWW Proxy Server を利用するブラウザで、接続を許可されない IP アドレスが接続された場合、ブラウザでは接続エラーのメッセージが表示され Reject(拒否)の場合にようにブラウザへメッセージを表示させることはできません。

**決められた IP アドレスからの接続を許可する（または許可しない）②（Web アクセスコントール）**

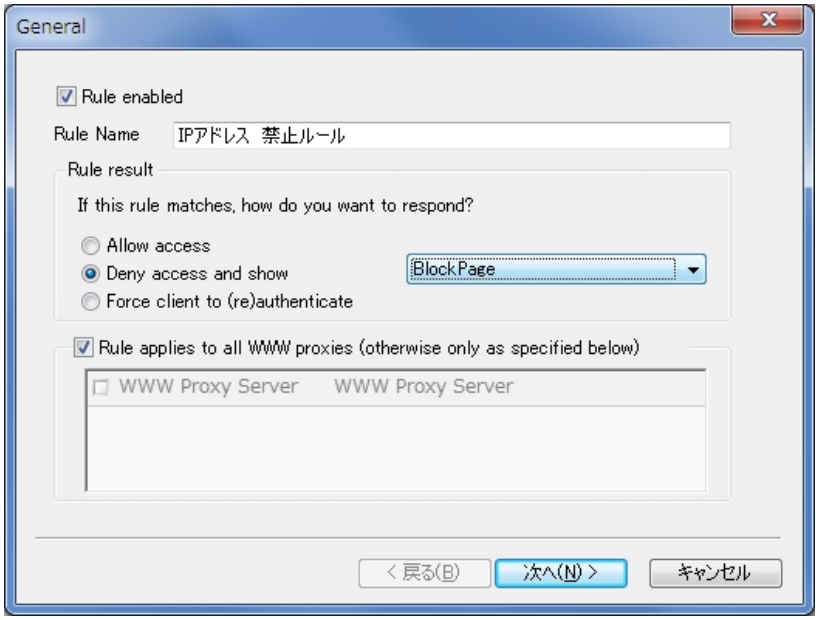
WinGate の Web Access Control 機能を使用して、特定の IP アドレスのみ許可、または許可しない設定を行います。

※容易に指定した IP アドレスを禁止したい場合、この設定をお勧めいたします。他のポリシーアイテムと組み合わせて利用する場合には、①のポリシーを使用する方法をご利用ください。

1. WinGate Management で Web Access Control、Access Rules を開きます。




2. Tasks より Add Rule をクリックします。

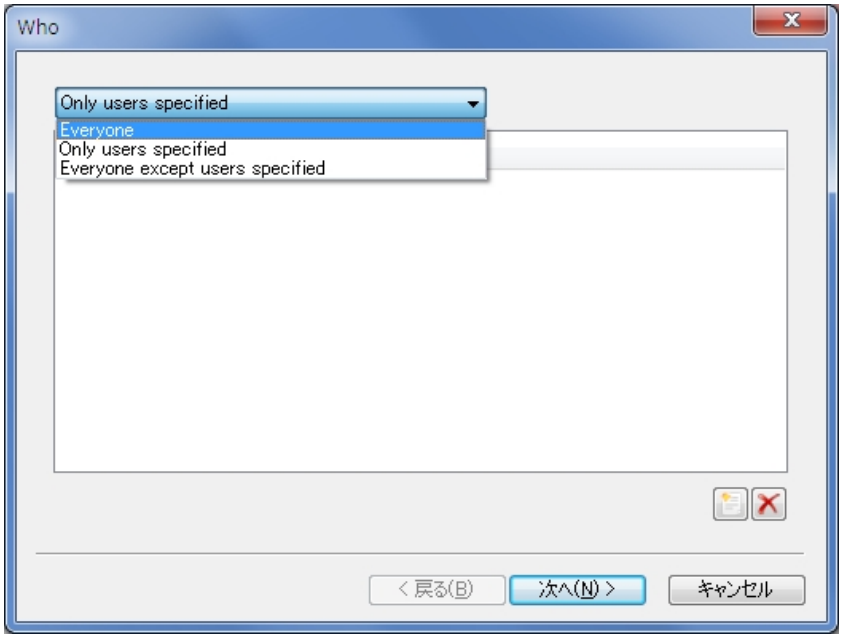



General ダイアログが表示されますので、Rule Name に任意のルール名を入力します。

指定した IP アドレスから WWW Proxy server の利用を禁止（または、許可）する場合には、Deny access and show を選択します。

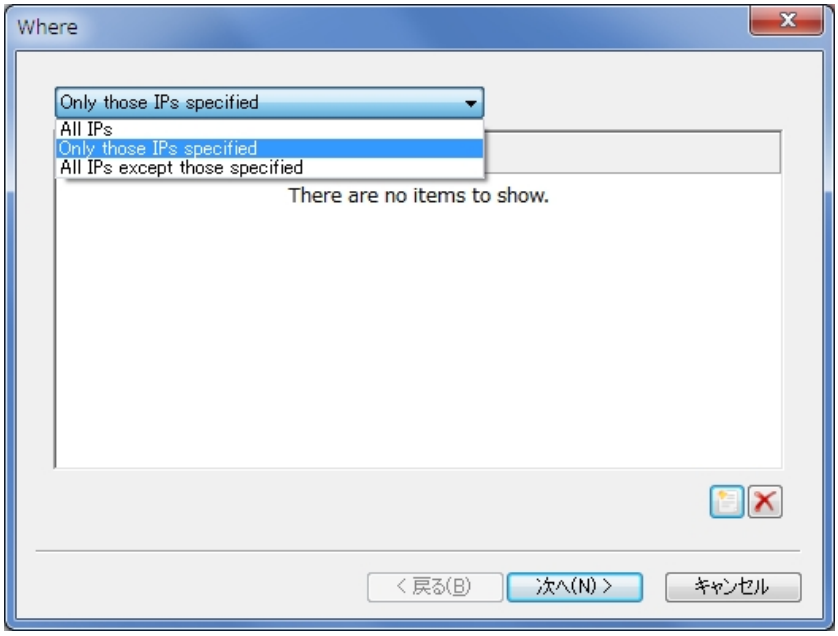
複数の WWW Proxy server を構成しており、このルールを適用する WWW Proxy server を指定する場合は、Rule applies to all WWW proxies のチェックを外し、適用する WWW Proxy server を選択してください。

3. Who ダイアログが表示されます。

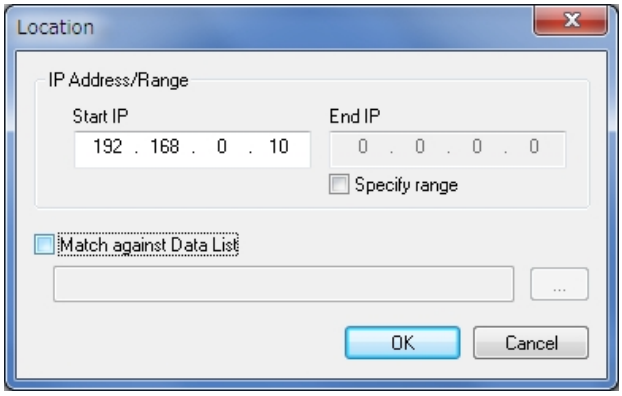



この制限を全てのユーザーに適用する場合、Everyone を選択してください。(ユーザーを指定する場合、Only users specified を選択します。この場合、ユーザー認証などによりユーザーが特定できる必要があります。)
次へボタンをクリックします。

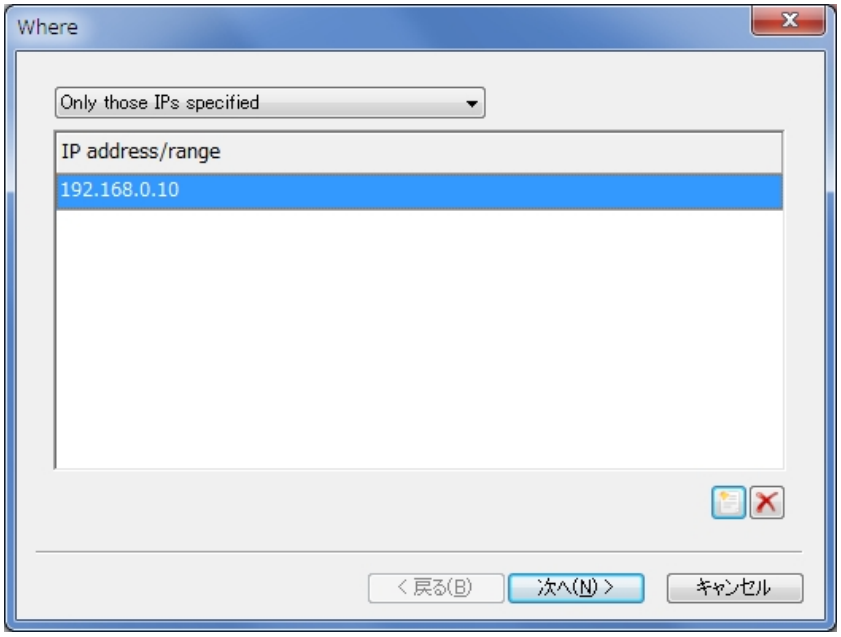
4. Where ダイアログが表示されます。




指定した IP アドレスを禁止する場合には、Only those IPs specified を選択します。(逆に選択した以外の IP を禁止する場合には、All IPs except those specified を選択します。)
ダイアログ右下にある Add Rule ボタンをクリックします。

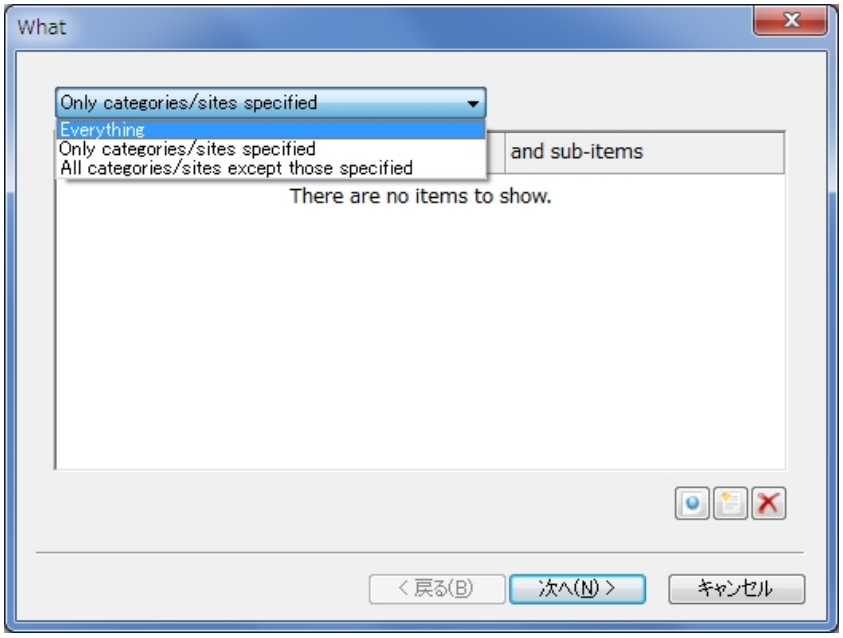



Location ダイアログが表示されますので、禁止する(または、許可する)IP アドレスを指定します。
IP アドレスの範囲で禁止する場合、Specify range をチェックして IP の範囲をしてしてください。
また、Match against Data List を選択した場合、Data で作成したリストから IP アドレス参照することができます。
指定が完了いたしましたら OK ボタンでダイアログを終了します。



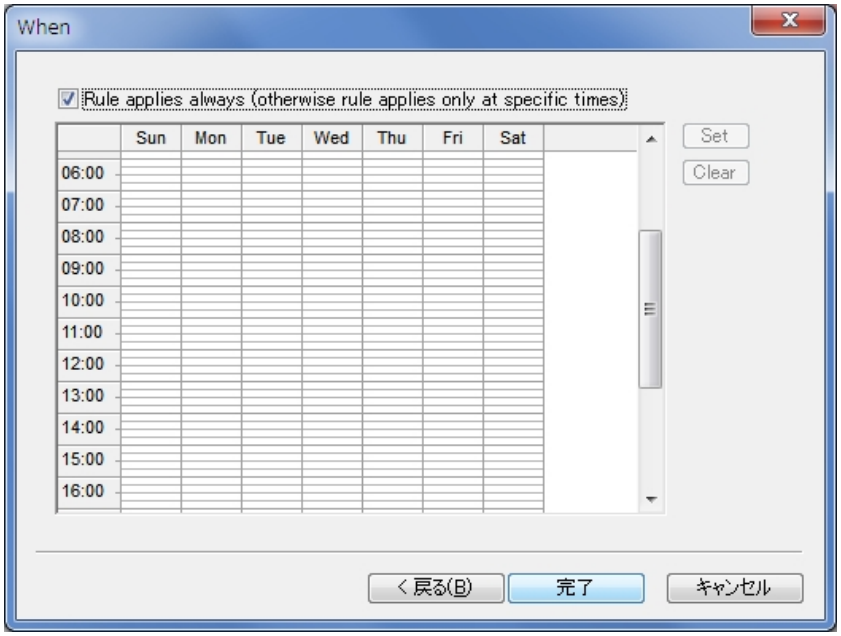

Where ダイアログに指定した内容が表示されます。
次へボタンをクリックします。

5. What ダイアログが表示されます。



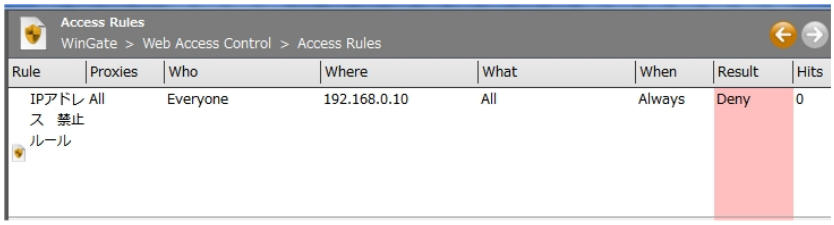

ここでは、適用するカテゴリーを選択します。
全ての内容に対して制限を行う場合、Everything を選択してください。
次へボタンをクリックします。

6. When ダイアログが表示されます。




このルールを適用する時間を指定することができます。
デフォルトでは、Rule applies always が選択され全ての時間でこのルールが適用されます。
完了ボタンをクリックします。

7. 作成したルールが追加されます。




以上でルールの作成は完了となります。
クライアントから WWW Proxy server を使用して、ルールが適切に動作しているかをご確認ください。
ページがブロックされた場合、HTTP サイトでは、WinGate のブロックメッセージが、HTTPS サイトではブラウザのエラーページが表示されます。(使用するブラウザによりメッセージが異なります。)
Web Access Control を使用した場合、HTTP、HTTPS ともに一つのルールで動作させることができます。

作成したルールに該当した接続は、Access Rules の Hits でカウントされます。(Hits のカウントがカウントアップしない場合、ルールに該当していない状態となりますので、設定をご確認ください。

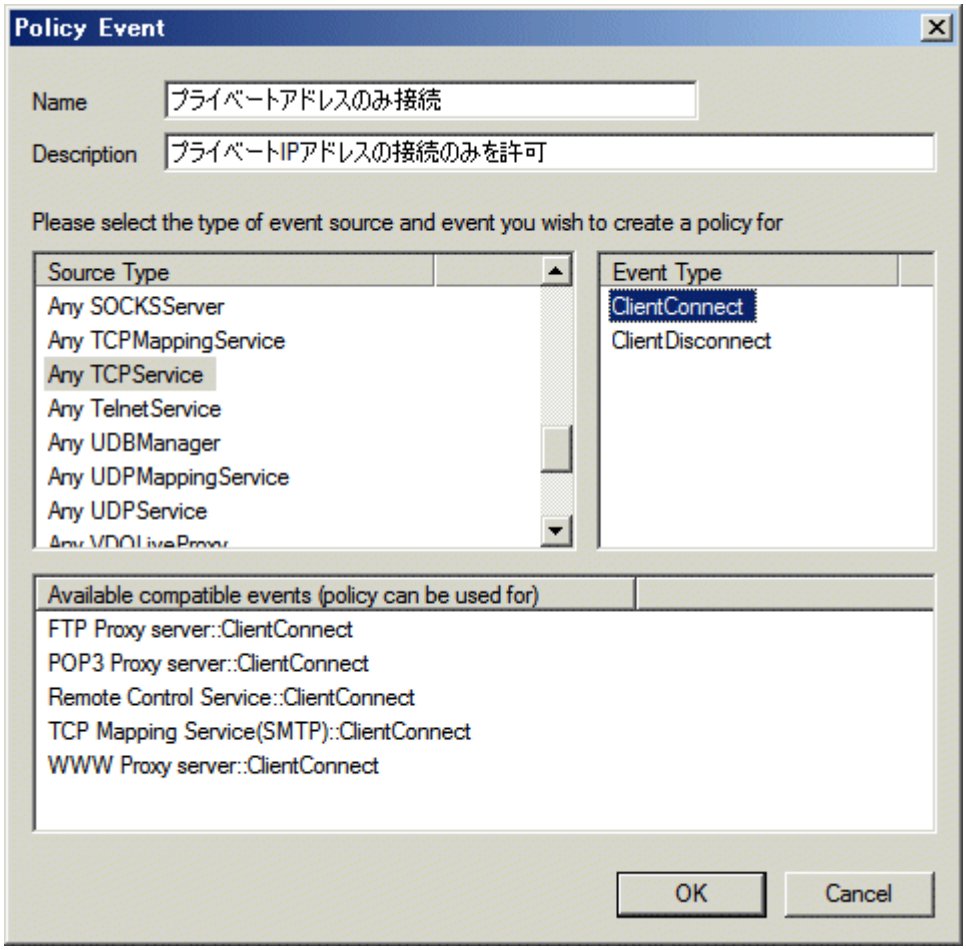
また、ユーザー認証や URL の禁止(許可)と組み合わせて利用する事も可能となります。

**プライベートアドレスの接続のみを許可する**

プライベート IP アドレスのみの接続を許可する場合に有効なポリシー設定となります。

WinGate がグローバル IP アドレスを持っている場合に、グローバル IP アドレスからの接続を拒否するため、セキュリティ面で有効な設定となります。

1. WinGate の TCP サービスに対してプライベート IP アドレスの接続のみを許可するポリシーを設定します。
   WinGate Management の Navigation より Policy（ポリシー）を選択します。
   Tasks より New Policy を選択します。

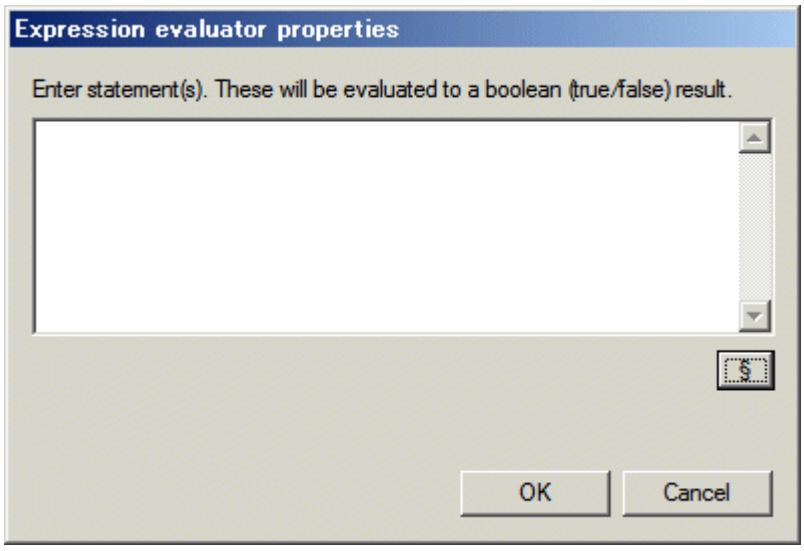



   Name に追加するポリシーの名前を入力します。
   Source Type では、Any TCPService を選択し、Event Type で ClinetConnect を選択します。
   Available compatible event に制限可能なサービスが表示されます。
   OK ボタンをクリックします。

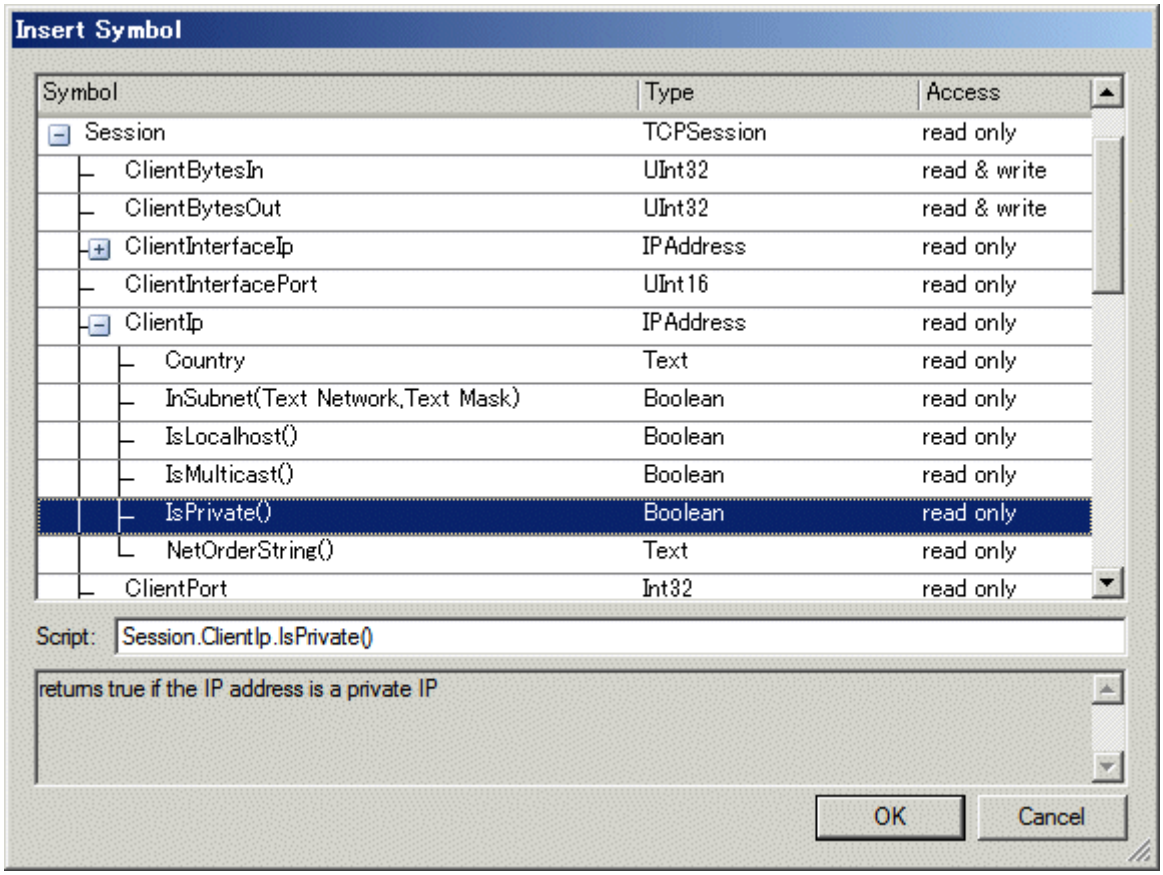
2. Policy ダイアログが表示されます。

Event 欄から制限を適用するサービスを右側の欄にドラッグします。

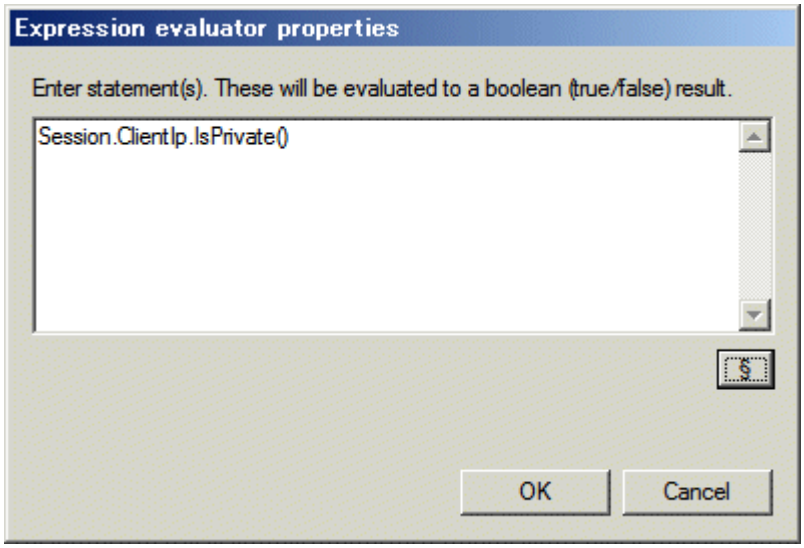
3. Items より Expression evaluator を選択して右側にドラッグします。




Expression evaluator properties ダイアログが表示されますので、右下の Insert Symbol ボタンをクリックします。




Insert Symbol ダイアログで Session より ClientIp 、IsPrivate()を選択して OK ボタンをクリックします。

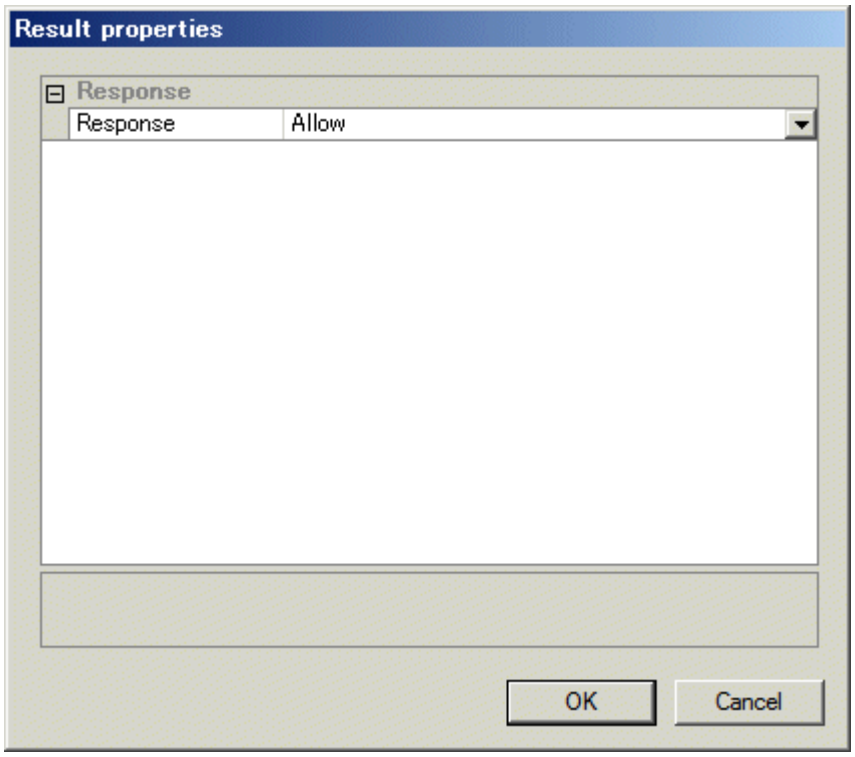



Expression evaluator properties ダイアログに Session.ClientIp.IsPrivate() が追加されます。
OK ボタンでダイアログを終了します。

4. ポリシーウインドウに追加された Expression evaluator に名前を入力します。

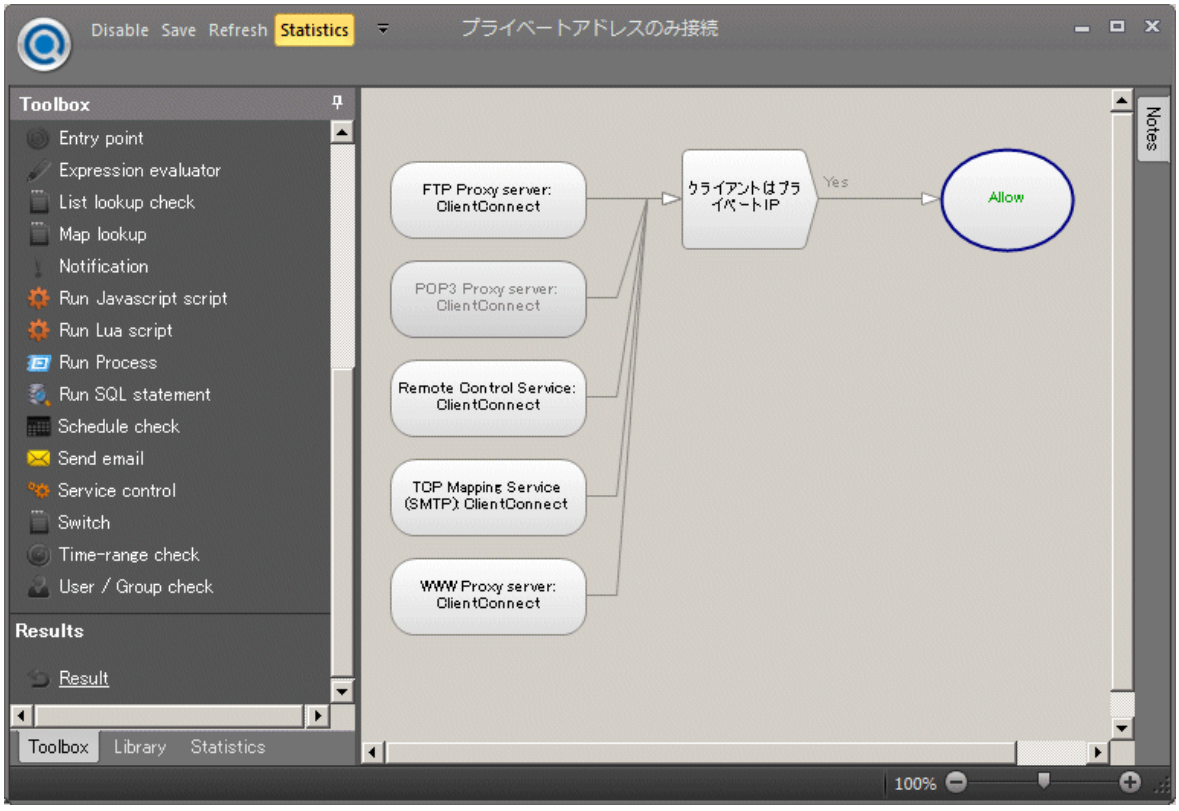
5. サービスから Expression evaluator へマウスカーソルをドラッグして以下の状態とします。

6. Result 欄から Result を右側の欄へドラッグします。

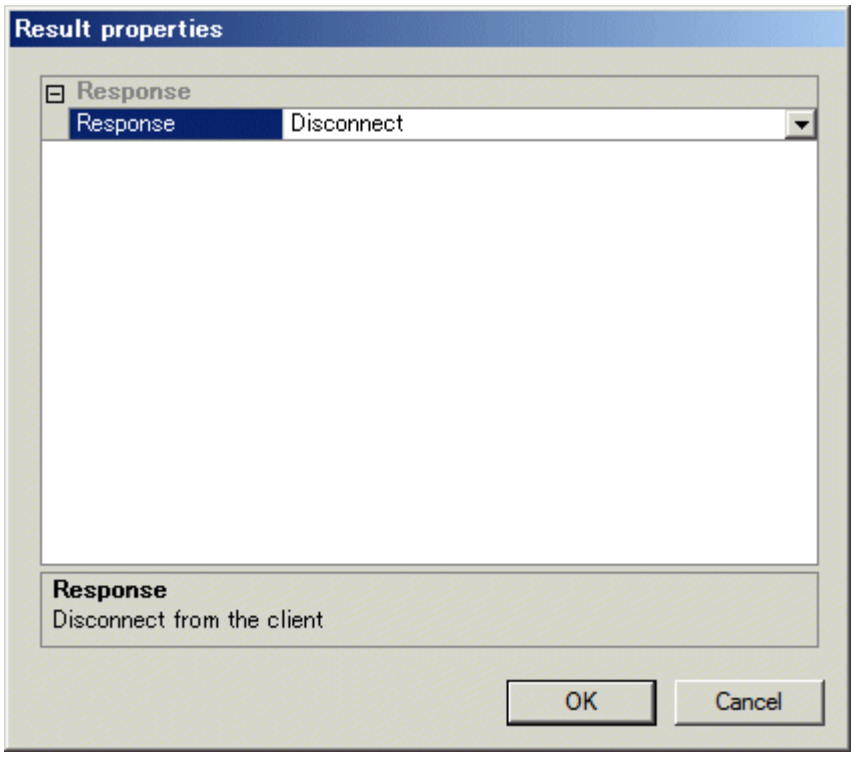



Result properties ダイアログが表示されますので、プライベート IP アドレスだった場合に接続を許可するために Response ドロップダウン・メニューで Allow（許可）を選択して OK ボタンをクリックします。

追加された Result Allow に対して Expression evaluator からマウスカーソルをドラッグして以下の状態とします。




7. Result 欄から Result を右側の欄へドラッグします。

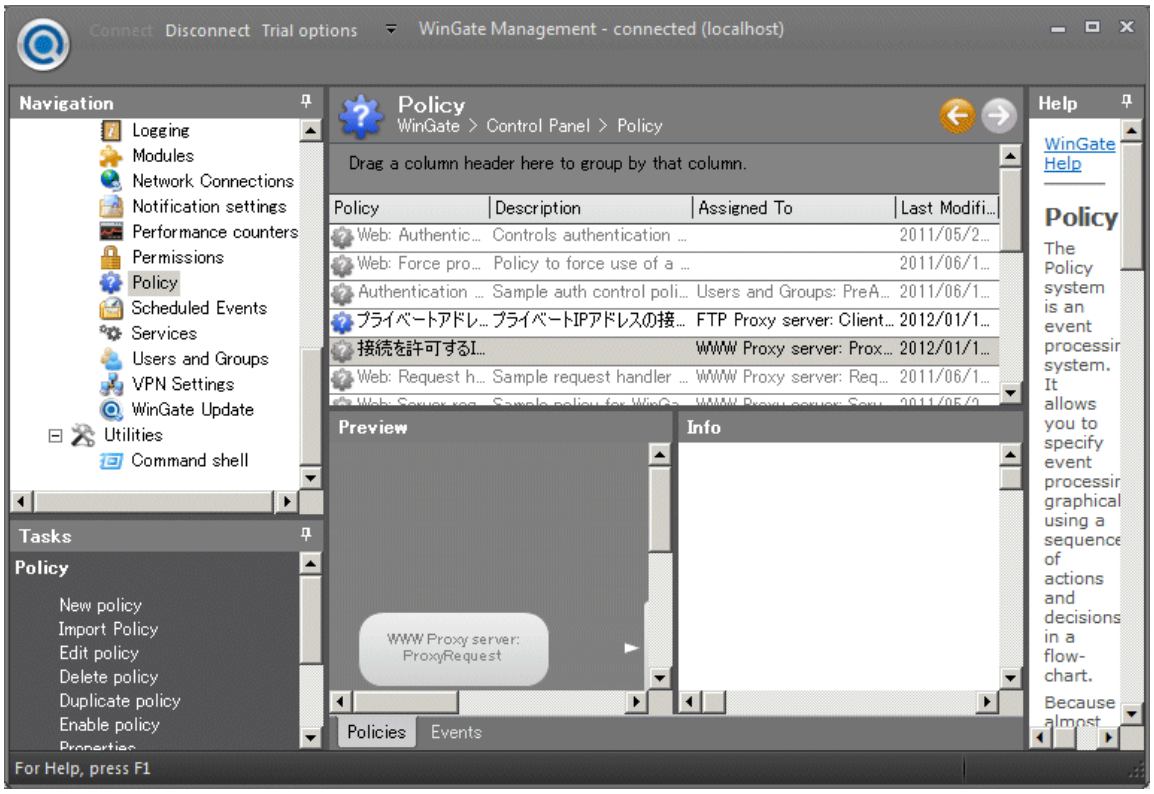



Result properties ダイアログが表示されますので、非プライベート IP アドレスだった場合に接続を拒否するために Response ドロップダウン・メニューで Disconnect（切断）を選択して OK ボタンをクリックします。

追加された Result　Disconnect に対して Expression　evaluator からマウスカーソルをドラッグして以下の状態とします。

8. Save ボタンで設定内容を保存して右上の閉じるボタン（×）でダイアログを終了します。

9. 作成されたポリシーが追加されます。




以上でプライベート IP アドレスのみの接続を許可するポリシー設定は完了となります。
WinGate の NAT 機能を使用している場合には、手順 1 で Source Type で Any NAT Controller を選択して後の手順を行ってください。
設定完了後は、クライアント PC などから接続して動作を確認してください。

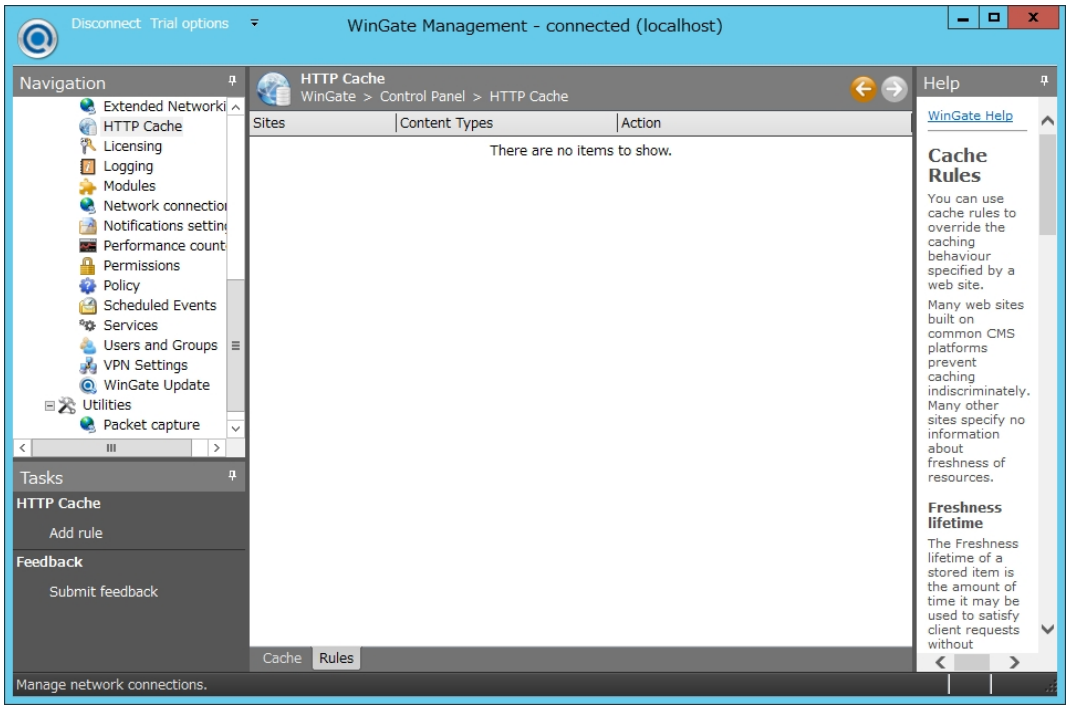
**特定のページをキャッシュしない**

WinGate の HTTP Cache で特定の URL をキャッシュしない設定を行います。
幾つかのサイトはキャッシュを行うことにより、ページの表示やダウンロードする内容に正しく表示できない場合があるかもしれません。
特定のサイトのキャッシュを許可しない場合は、以下の手順によりサイトの URL に基づき、キャッシュを行わない設定が可能となります。

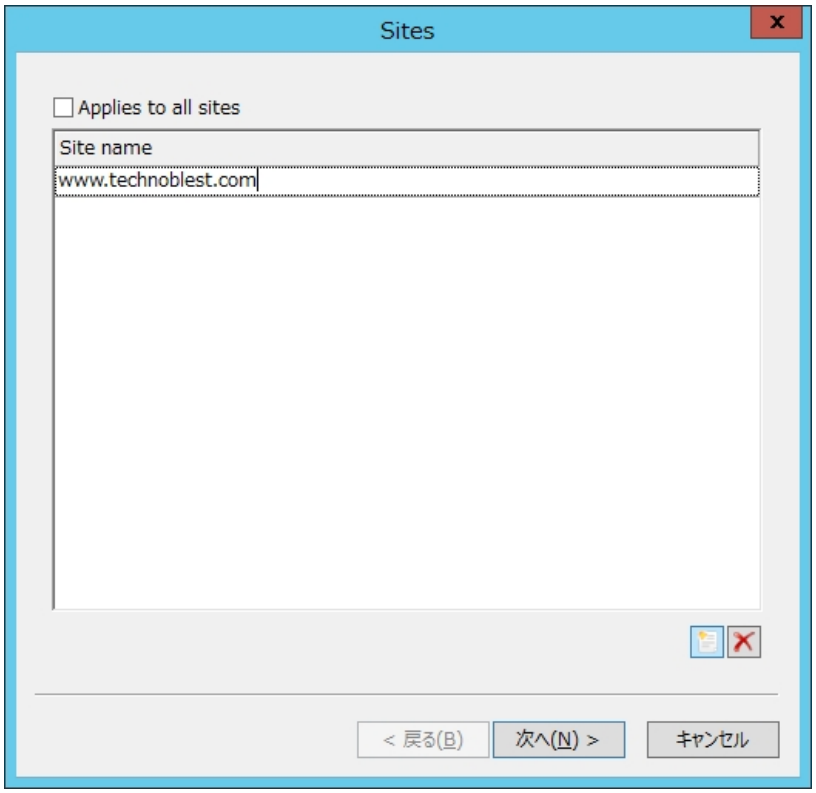
HTTP キャッシュルールを使用する方法とポリシーを利用する方法があります。

**HTTP キャッシュ ルールを使用する方法（複数のルールを設定する場合は、Enterprise 版が必要です。）**

1. WinGate Management より HTTP Cache、Rules タブを開きます。




2. Tasks、HTTP Cache より Add rule をクリックします。

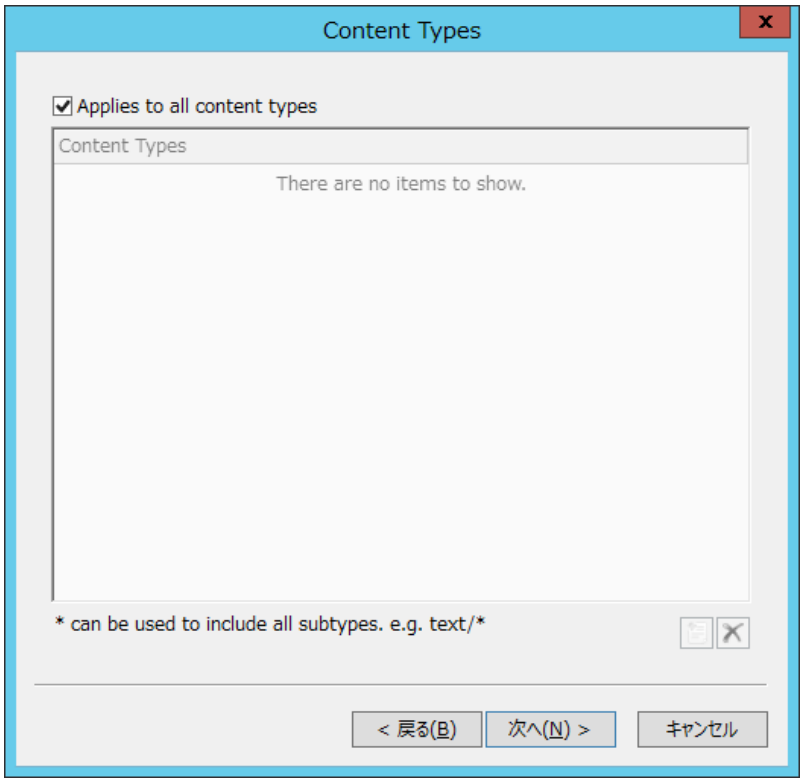



Applies to all sites のチェックを外し、表示されている New Site の文字を、キャッシュしないことを望むサイトに変更します。

※www.technoblest.com のように URL を設定してください。（ワイルドカードをご利用いただくことはできません。）

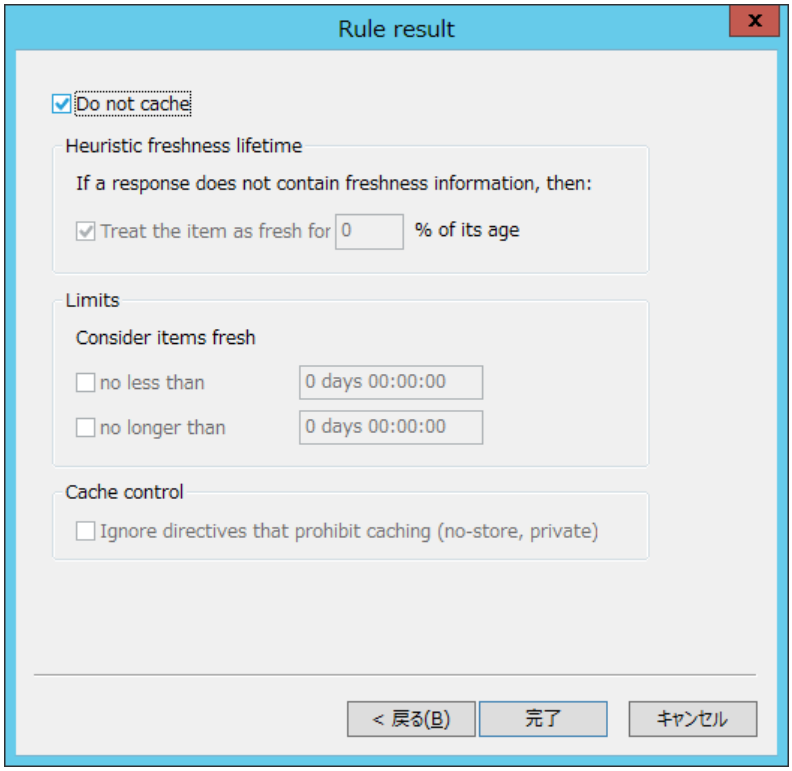
次へをクリックします。

3. Content Type ダイアログが表示されます。



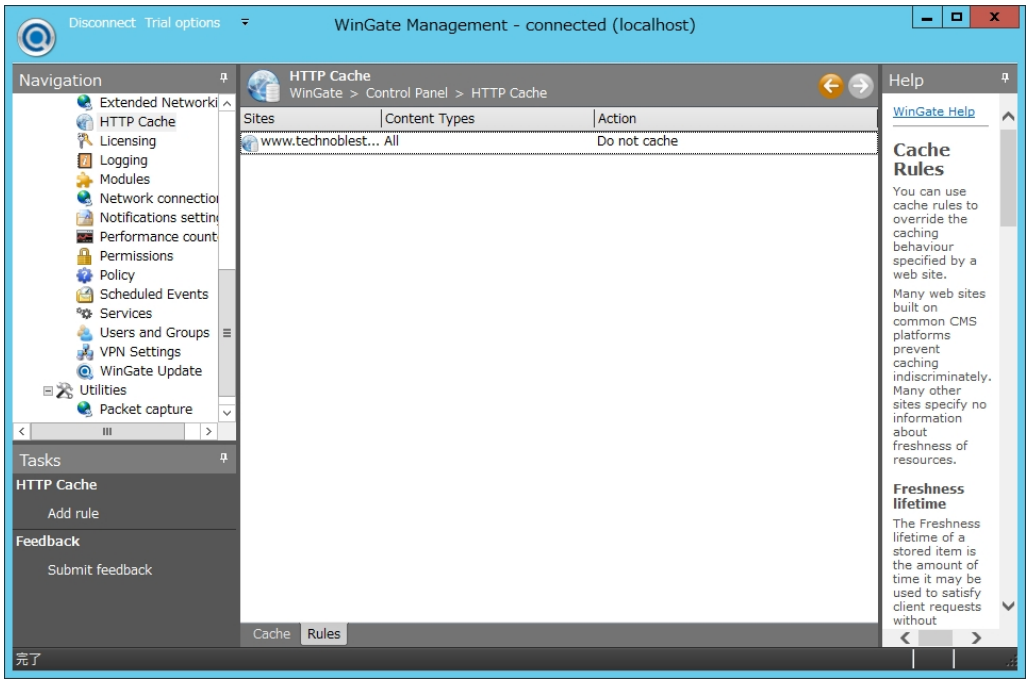

そのまま、次へをクリックします。

4. Rule result ダイアログが表示されます。




Do not cache をチェックし、完了ボタンをクリックします。

5. 作成したルールが追加されます。



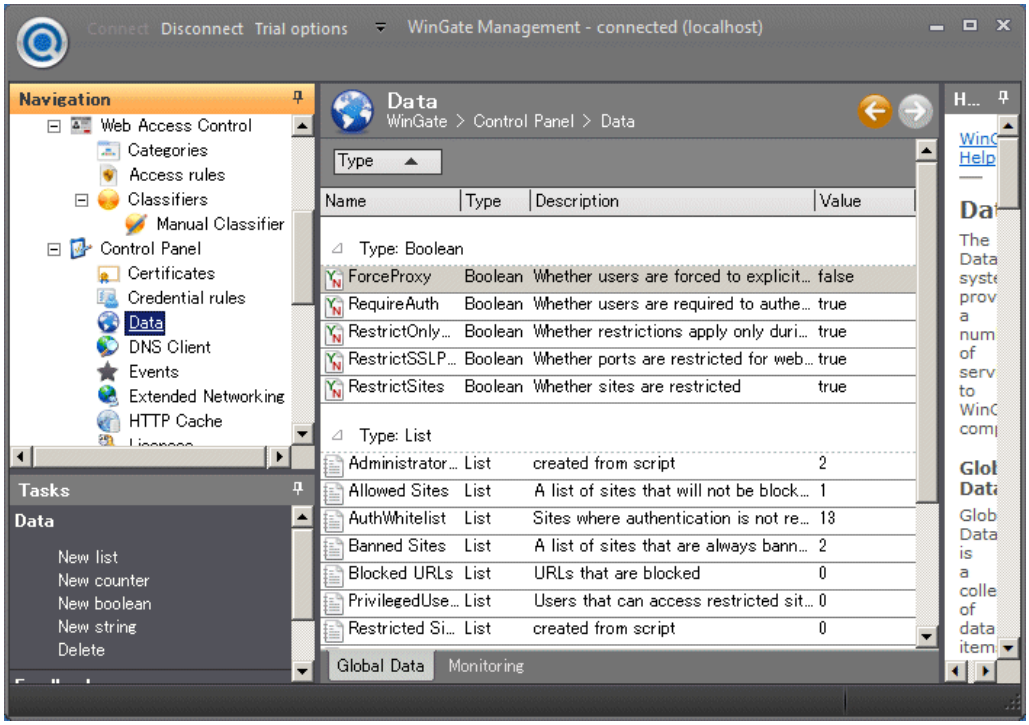

以上で HTTP キャッシュ ルールを使用したキャッシュしないサイト設定は完了となります。

※既にキャッシュされている場合、キャッシュされた情報は利用され削除されません。

**ポリシーを使用する場合（Enterprise 版のみ）**

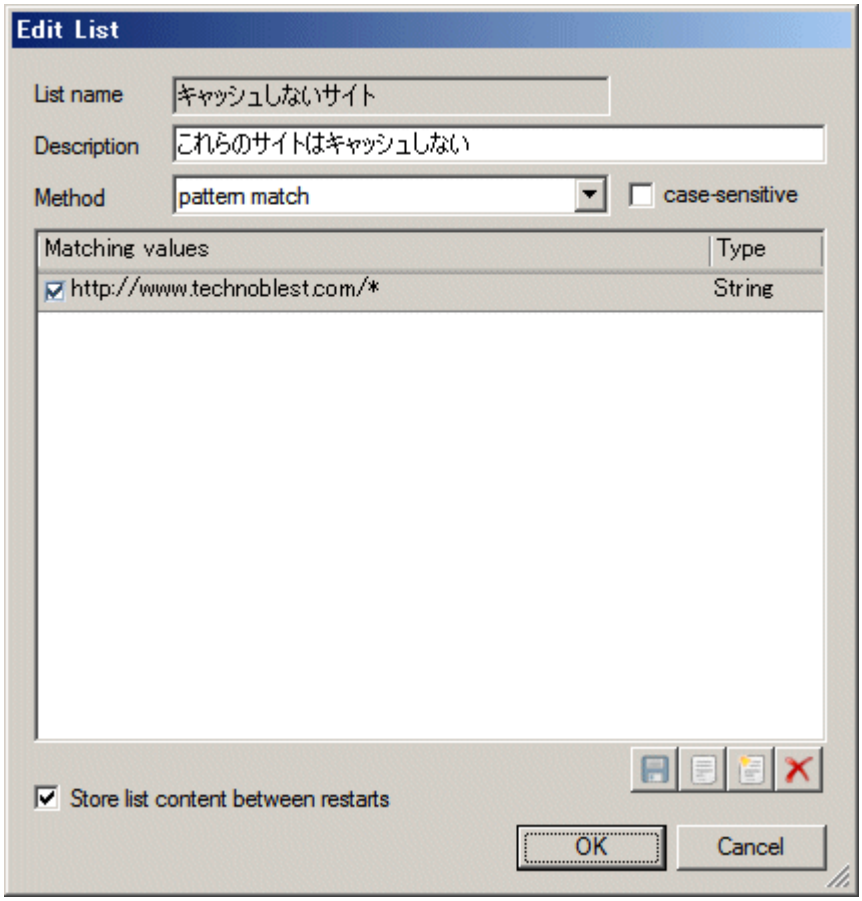
1. 最初にキャッシュしないサイトのリストを作成します。

   WinGate Management の Navigation より Data を選択し、Global Data タブを開きます。



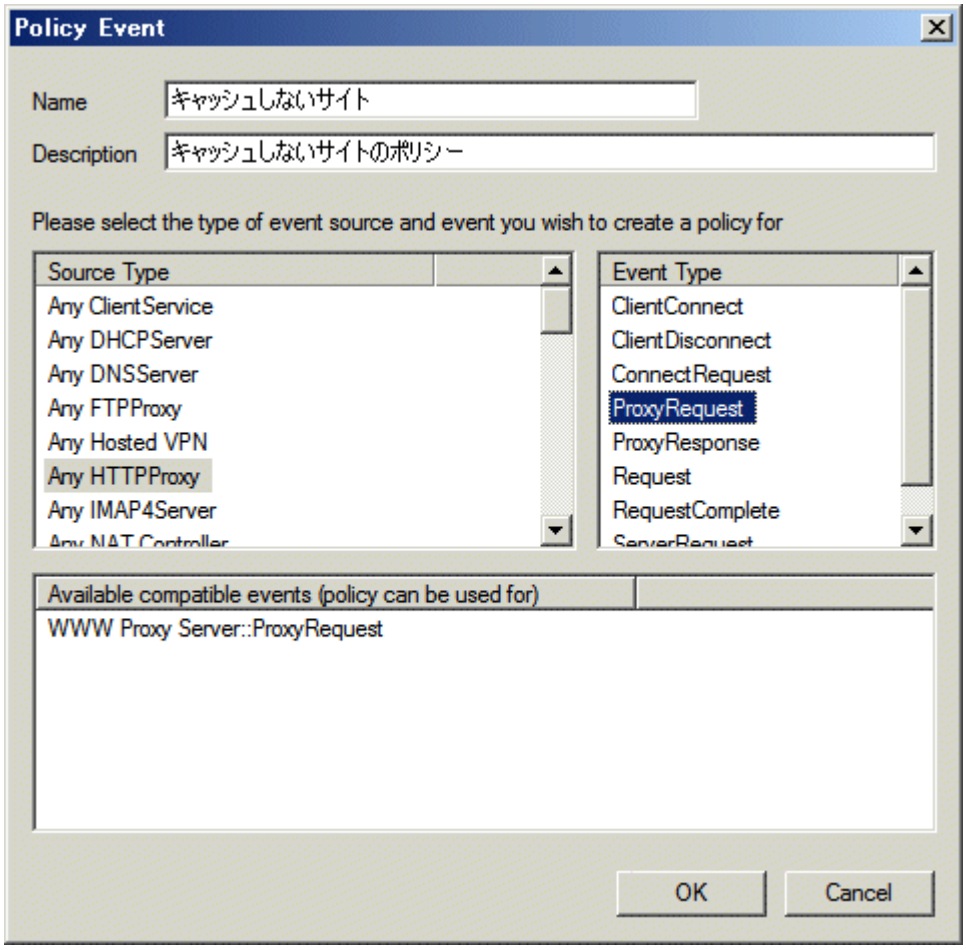

   Tasks の Data から New list をクリックします。

2. Edit List ダイアログが開きます。



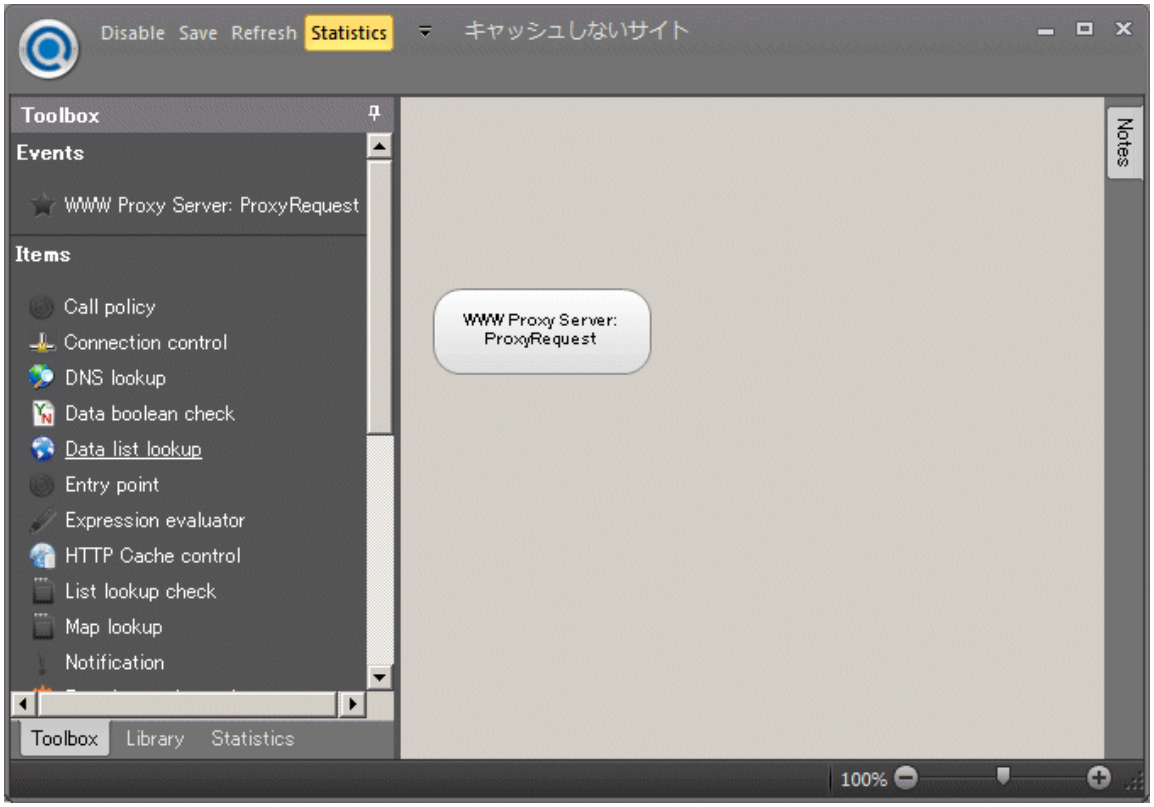

List name（リスト名）に任意のリスト名を入力、Description（説明に）（任意）にこのリストの説明を入力します。
Method（方法）のドロップダウン・メニューより Pattern match（パターンマッチ）を選択します。
右下のボタンより、右から2番目の新規ボタンをクリックし、リストにキャッシュしないサイトの URL を入力します。（http:// を含む URL となります。また、その URL に関連するサイトをキャッシュしない場合は、”＊“（ワイルドカード）を最後に付与してください。）
OK ボタンでダイアログを終了します。

3. WinGate Management の Navigation より Policy（ポリシー）を選択します。
   Tasks より New Policy を選択します。




Name（名前）に、ポリシーの名前、Description（説明）に、そのポリシーの説明（任意）を入力します。
Source Type（ソースタイプ）で Any HTTPProxy を選択、Event Type で ProxyRequest を選択します。
OK ボタンでダイアログを終了します。

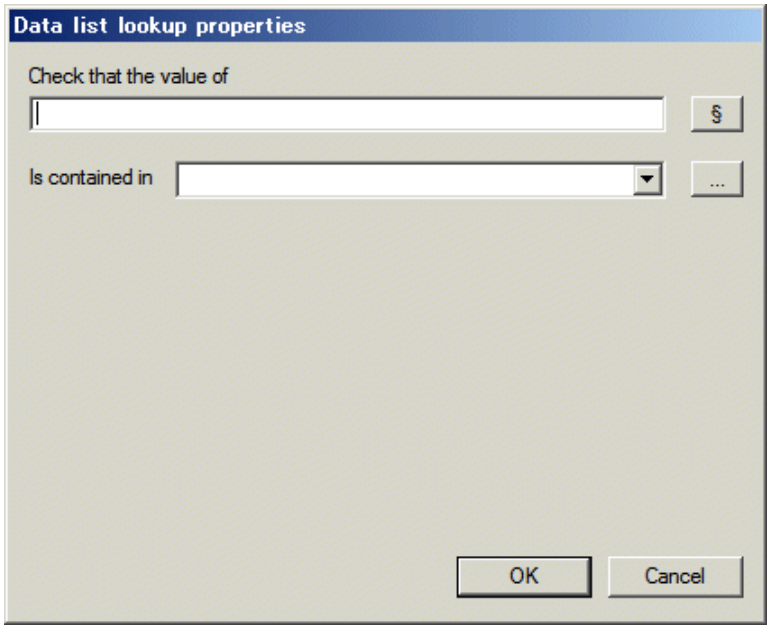
4. Policy ウインドウが表示されます。



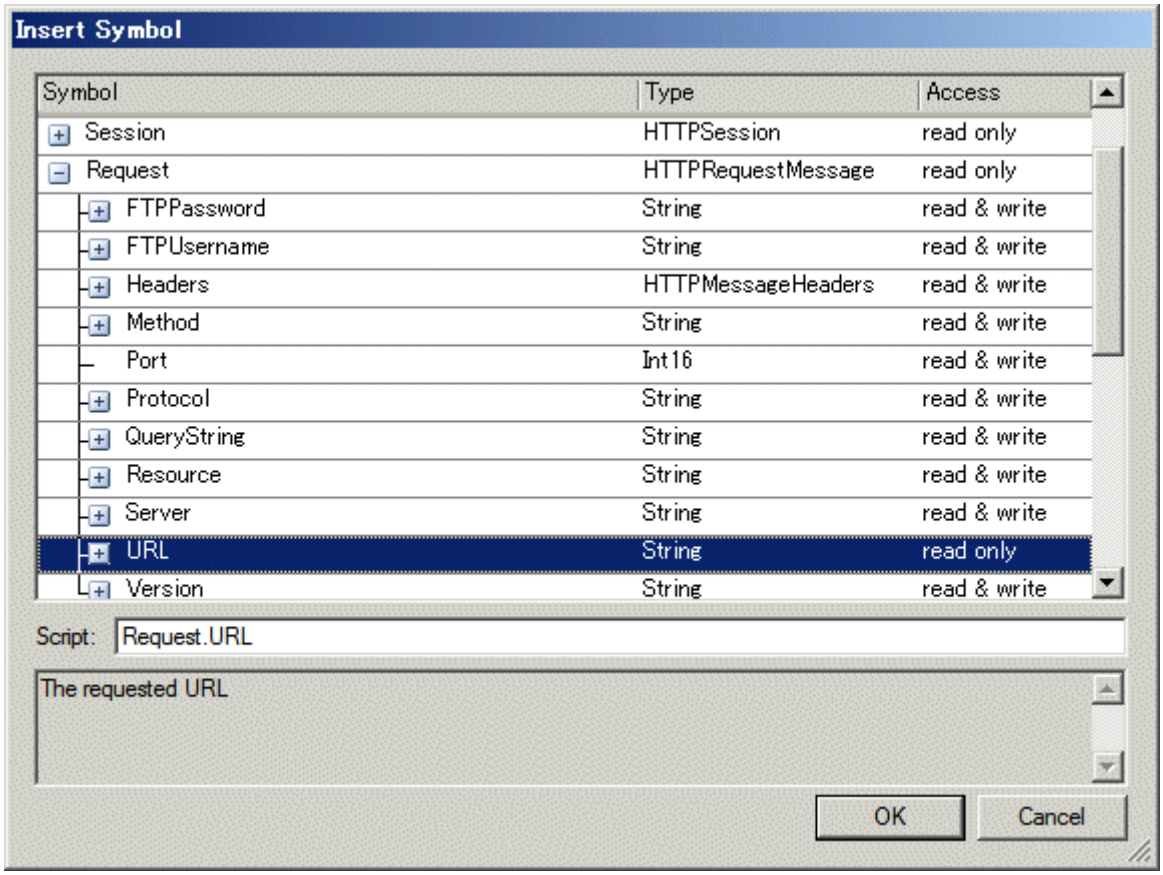

Event の WWW Proxy Server: ProxyRequest を右側の欄へドラッグします。

5. Items から Data list lookup を選択して、右側にドラッグします。

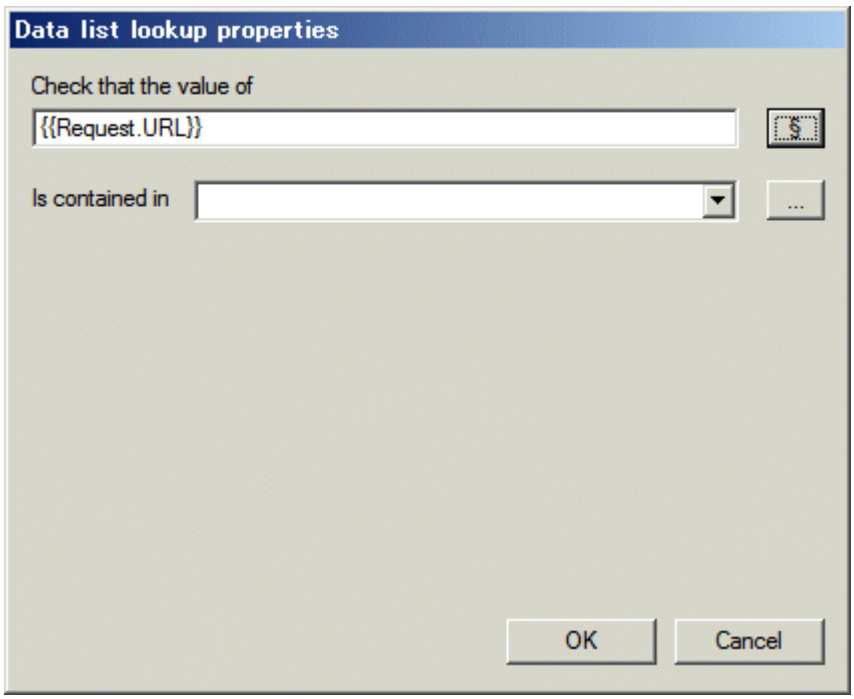
   Data list lookup properties ダイアログが表示されます。



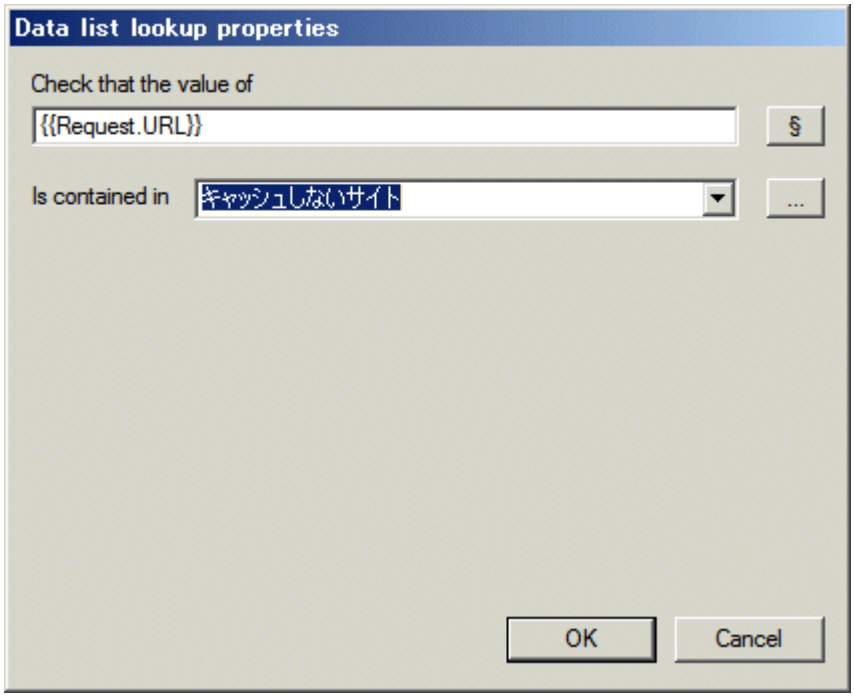

Check that the value of 欄の右側のボタンをクリックし、Insert Symbol（シンボルの挿入）ダイアログを表示します。



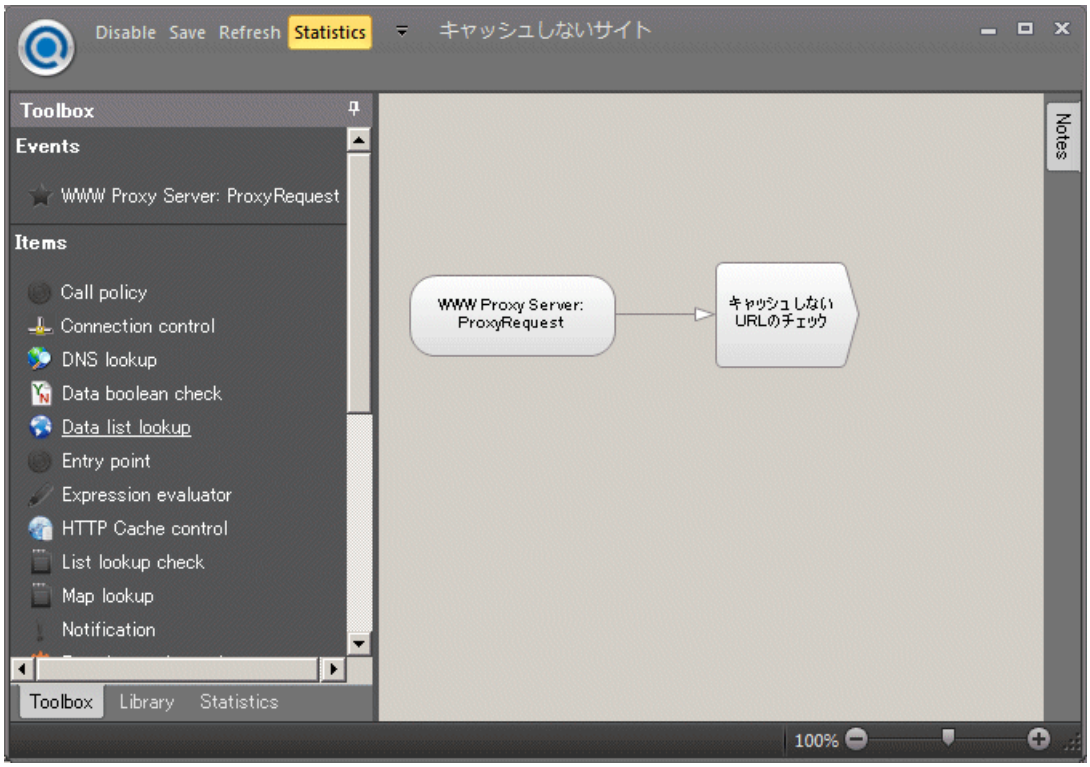

Request より URL を選択し、OK ボタンで終了します。




続いて、Is contained in 欄のドロップダウン・メニューから、先程作成したリストを選択します。

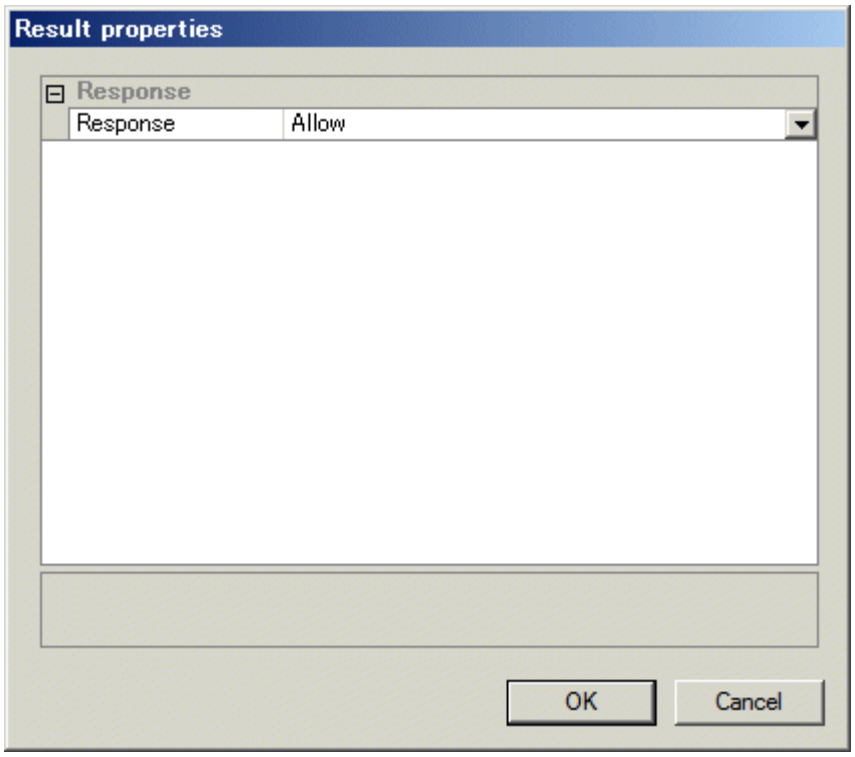



OK ボタンでダイアログを終了します。

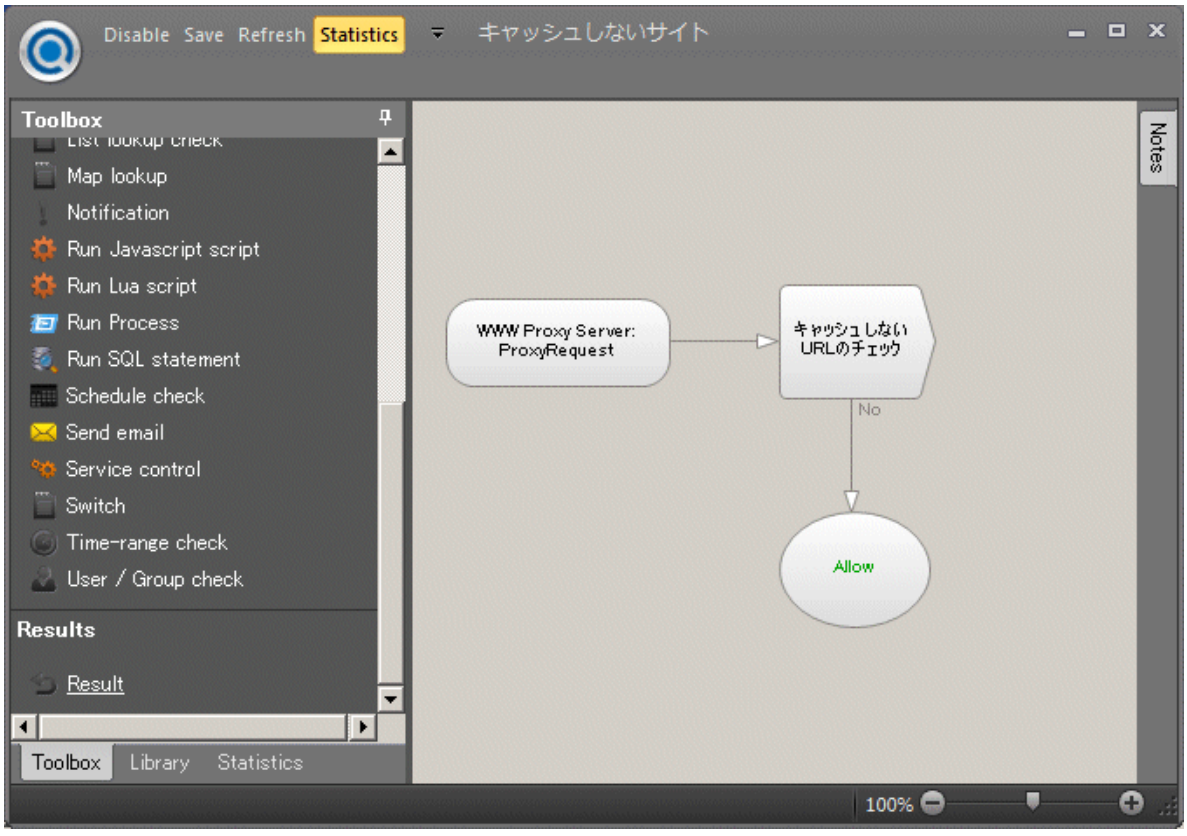



追加された Data list lookup に任意の名前を入力し、WWW Proxy Server: ProxyRequest から Data list lookup へマウスを操作して矢印を向けるようにします。

6. Results から Result を右側の Data list lookup 下にドラッグし、Result properties ダイアログを表示します。これはキャッシュしないリストの URL を一致しなかった場合の動作になるため Response ドロップダウン・メニューから Allow（許可）を選択します。



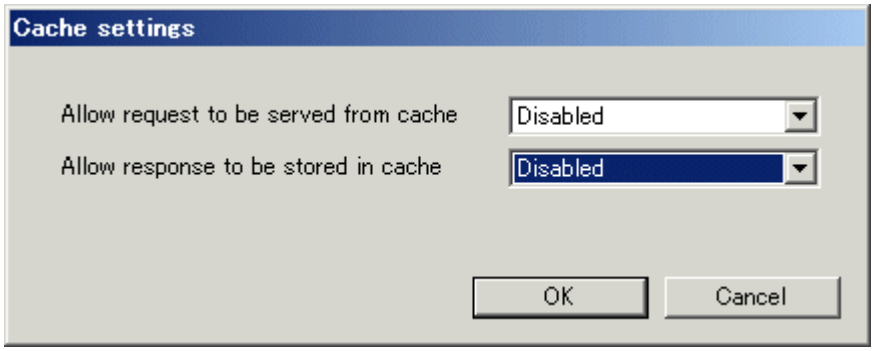

OK でダイアログを終了します。



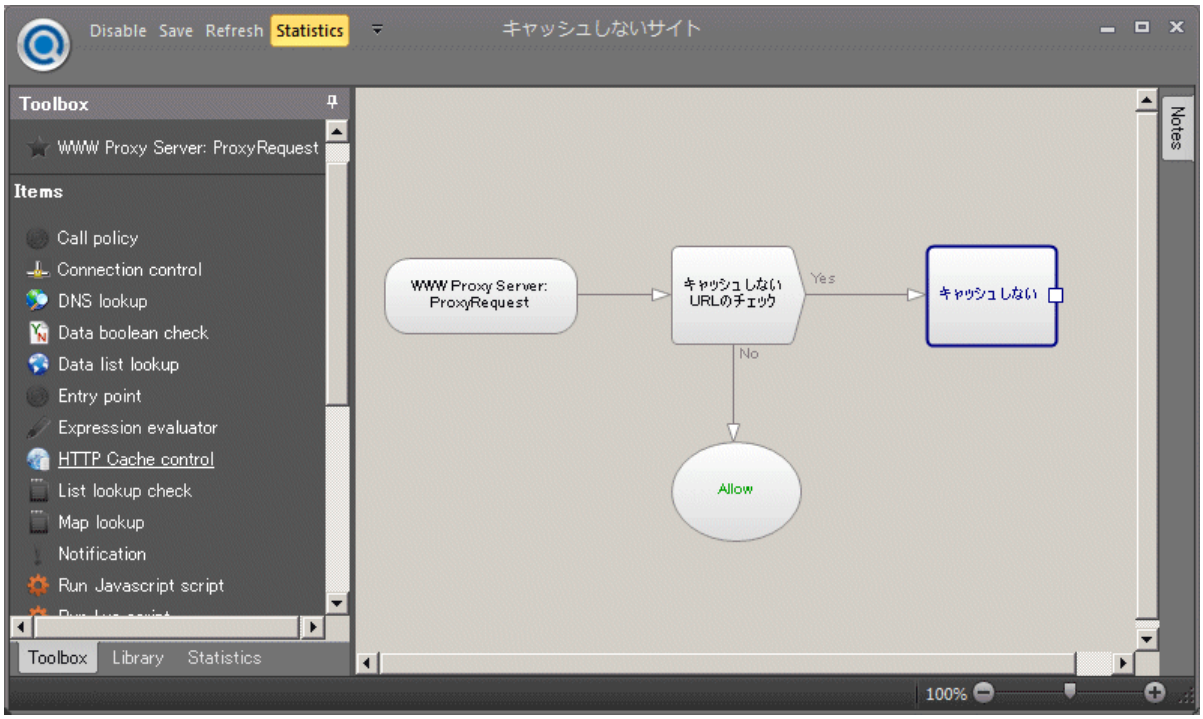

Data list lookup から、追加した Result へマウスをドラッグして矢印を向けます。

7. キャッシュしない動作を追加します。

   Items から HTTP Cache control を Data list lookup の右側にドラッグします。

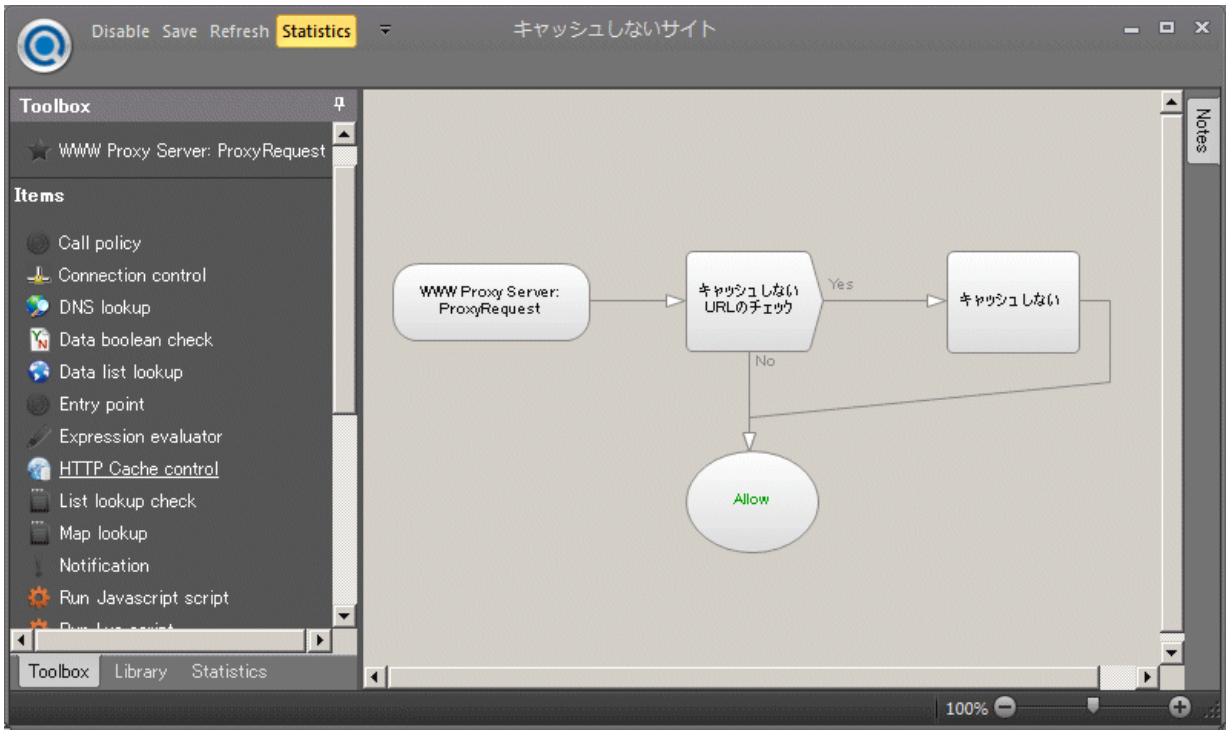



Cache settings（キャッシュ設定）ダイアログが表示されます。
Allow request to be served from cache（保存されたキャッシュからのリクエストを許可）で Disabled（無効）を選択
Allow response to be stored in cache（レスポンスはキャッシュへの保存を許可）で Disabled（無効）を選択
OK ボタンでダイアログを終了します。



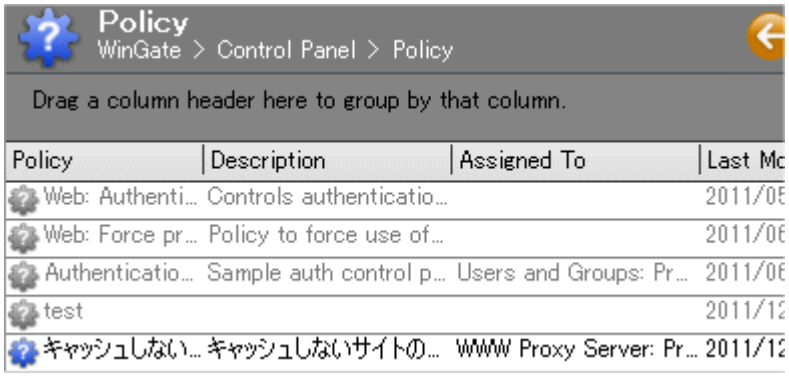

作成した HTTP Cache control に任意の名前を入力し、Data list lookup から HTTP Cache control へマウスをドラッグして矢印を向けます。

8. キャッシュしない動作の後でも通常通りサイトを表示させる為、HTTP Cache control から Result へマウスをドラッグして、以下の状態とします。




Save ボタンクリックして、で Policy ウインドウを閉じます。

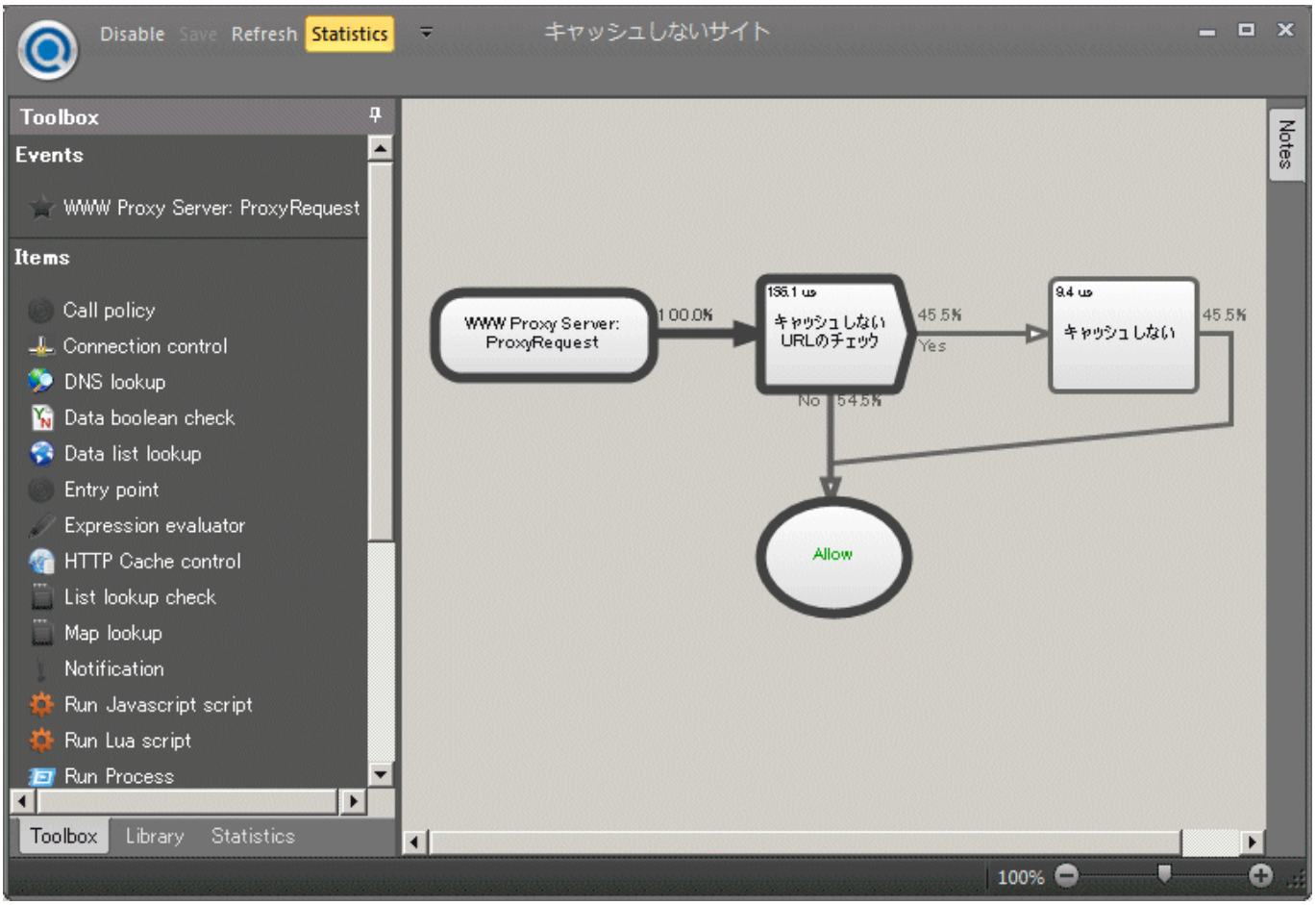
9. Policy 内に新しく作成された Policy が追加されます。




以上で、キャッシュしないサイトのポリシー作成は完了となります。

キャッシュしないサイトの管理は、Data で作成したリストより行ってください。

また、ポリシー作成後は、実際に対象に指定したサイトへアクセスし、キャッシュがされていないかをお試しください。

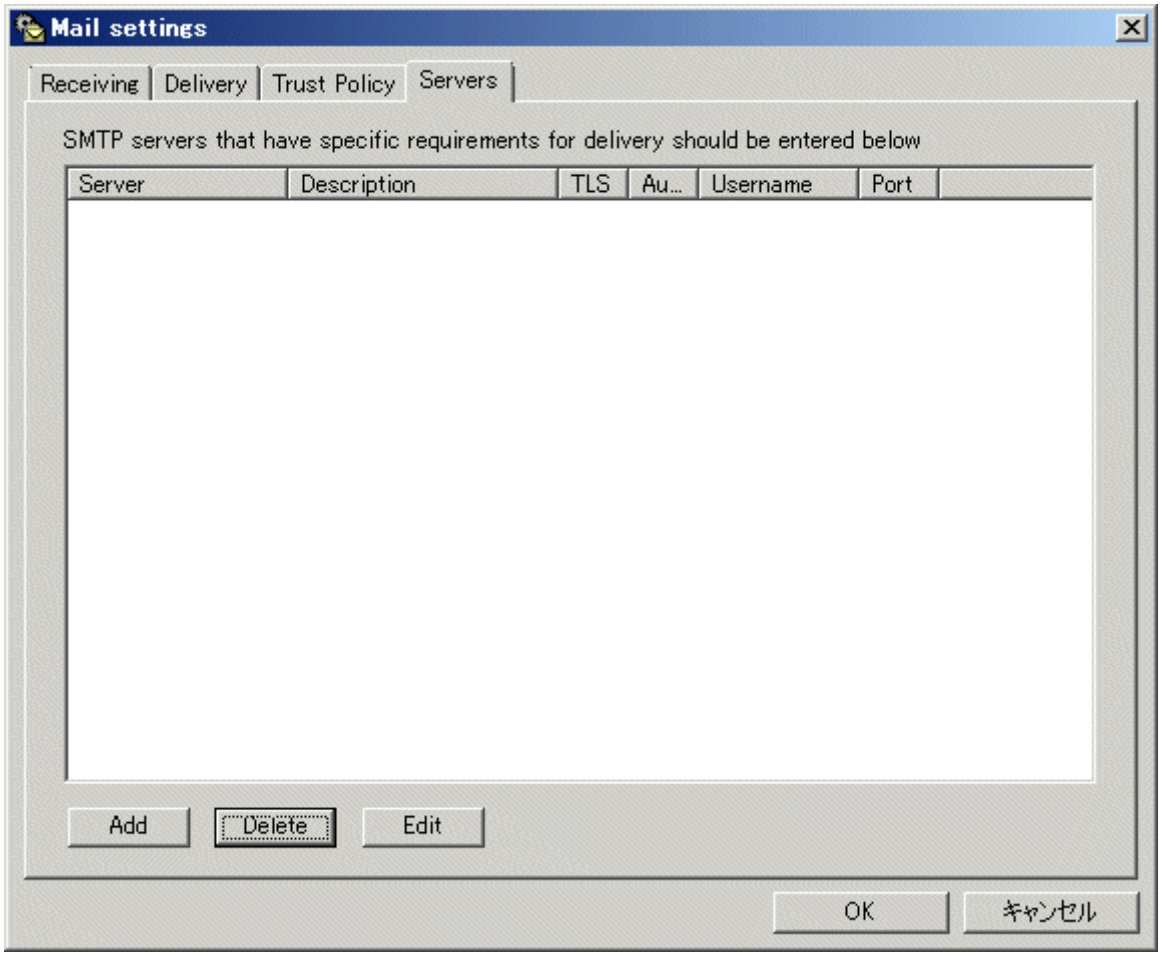



実際に利用されると、上記のように動作状況が記録されます。

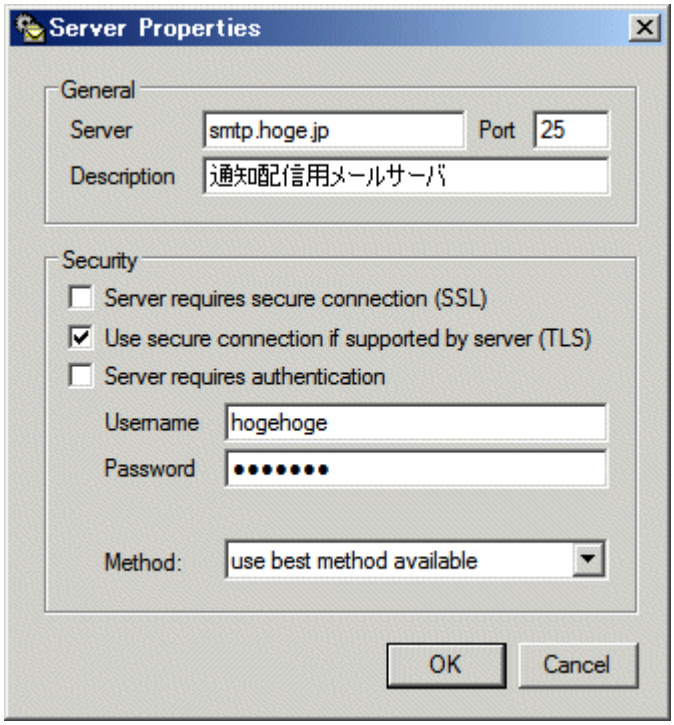
**WinGate で発生したイベントを管理者に通知する**

WinGate のメールサーバー機能を使用せずに、外部のメールアカウントに対して、通知メッセージを配信します。
これにより管理者は、WinGate からの通知メッセージを電子メールで受信することができます。

1. WinGate Management の Navigation より Email をクリックし、Tasks より Mail settings をクリックします。
   表示される Mail settings ダイアログで Servers タブを選択します。
   ※Postmaster アドレスの設定を求められた場合、Delivery タブの System postmaster address 欄に、有効な管理者の電子メールアドレスを入力してください。




2. Add（追加）ボタンをクリックします。




配信に使用する外部メールサーバーの情報を設定します。

Server(サーバー) ＝ 配信に使用する SMTP サーバーの情報を入力します。

Port(ポート) ＝ 配信に使用する SMTP サーバーのポート番号を入力します。

Description(説明) ＝ そのサーバーの説明を入力します。(任意)

Security(セキュリティ)では、配信に使用するサーバーのセキュリティ情報を入力します。

Server requires secure connection(SSL) ＝ サーバーはセキュア接続(SSL)が必要

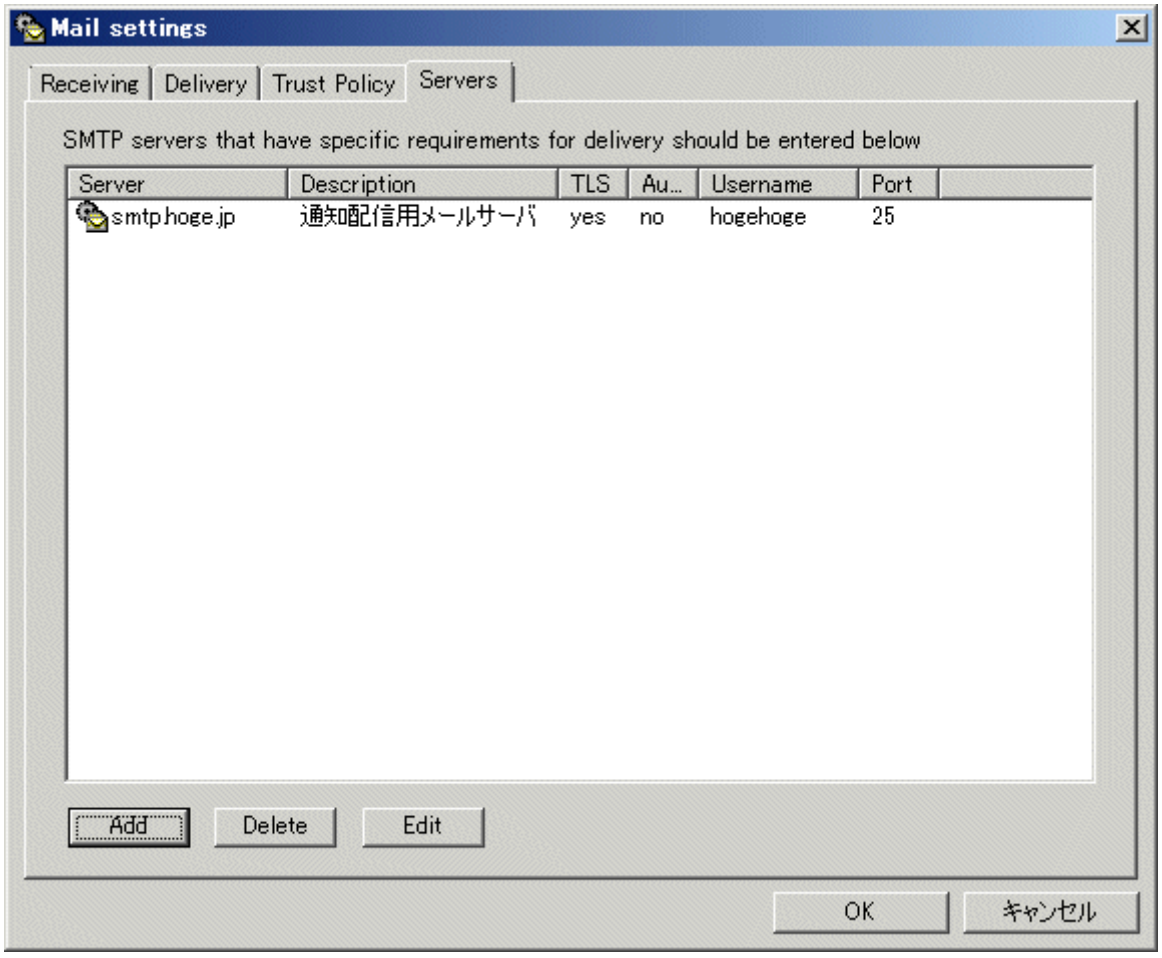
Use secure connection if supported by server(TLS) ＝ サーバーがサポートする場合セキュア接続を使用(TLS)

Server requires authentication ＝ サーバーは認証が必要

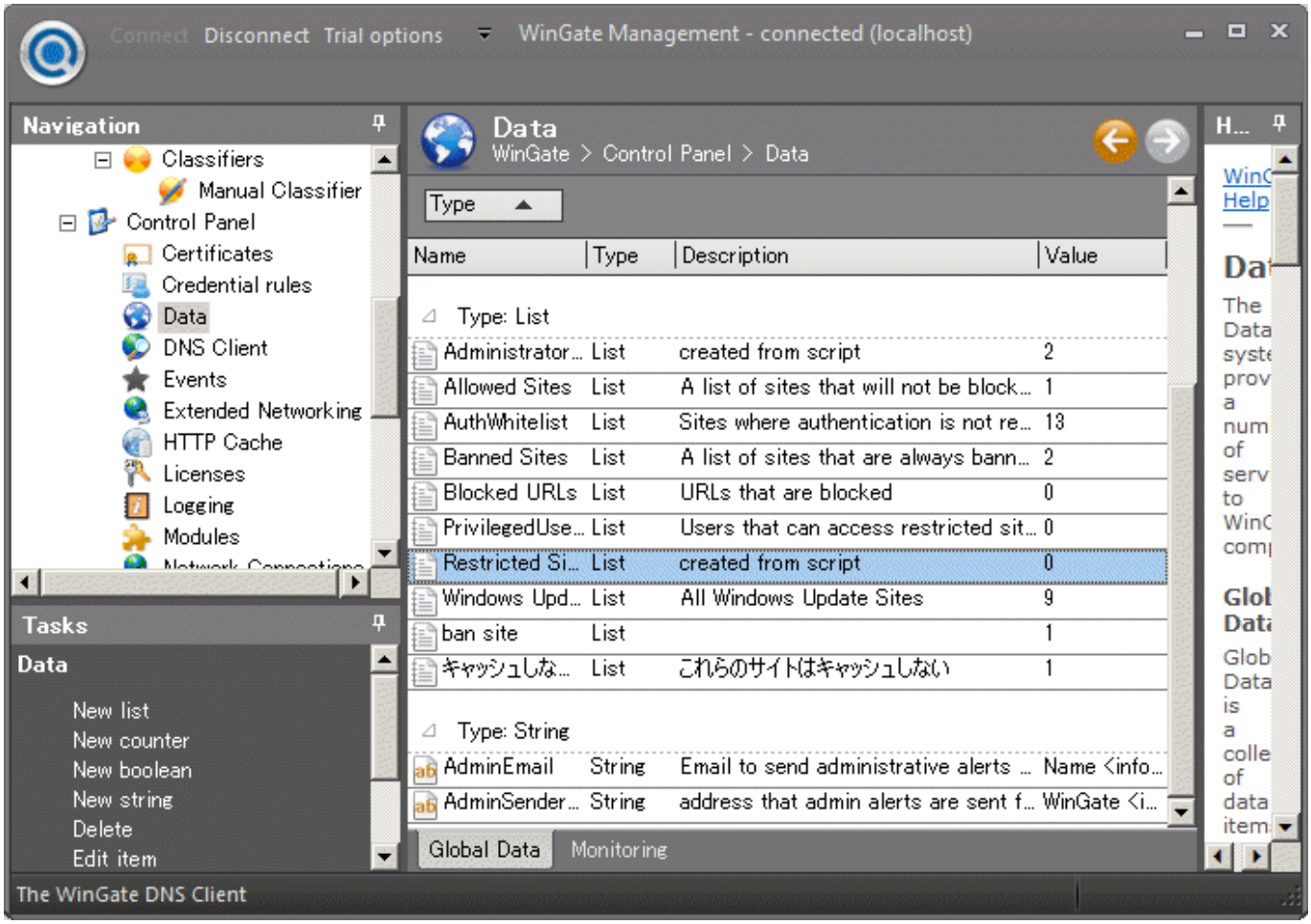
Server requires authentication を選択した場合は、使用する Username(ユーザー名)、Password(パスワード)、Method(認証方法)を設定してください。

OK ボタンでダイアログを終了します。

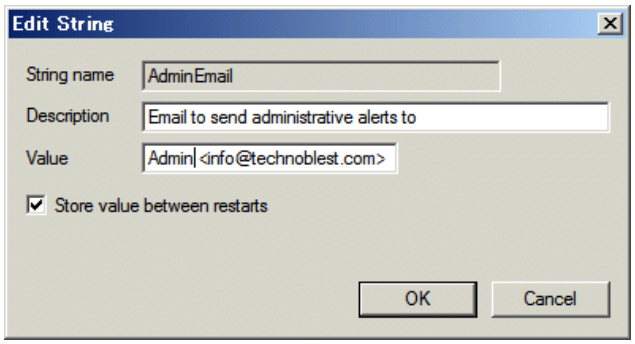
3. Server タブに追加した配信用サーバーが追加されます。

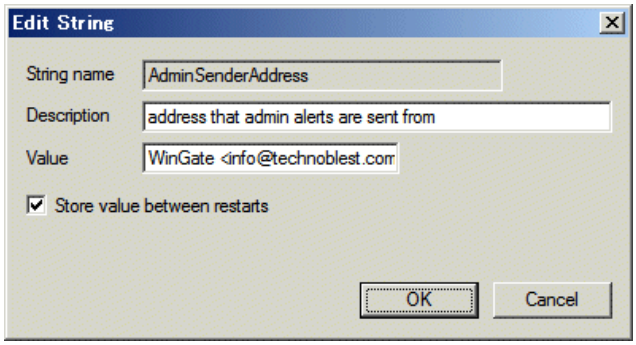



4. 配信先、配信元電子メールアドレスを設定します。
   WinGate Management の Navigation より Data を選択し、Global Data タブを選択します。



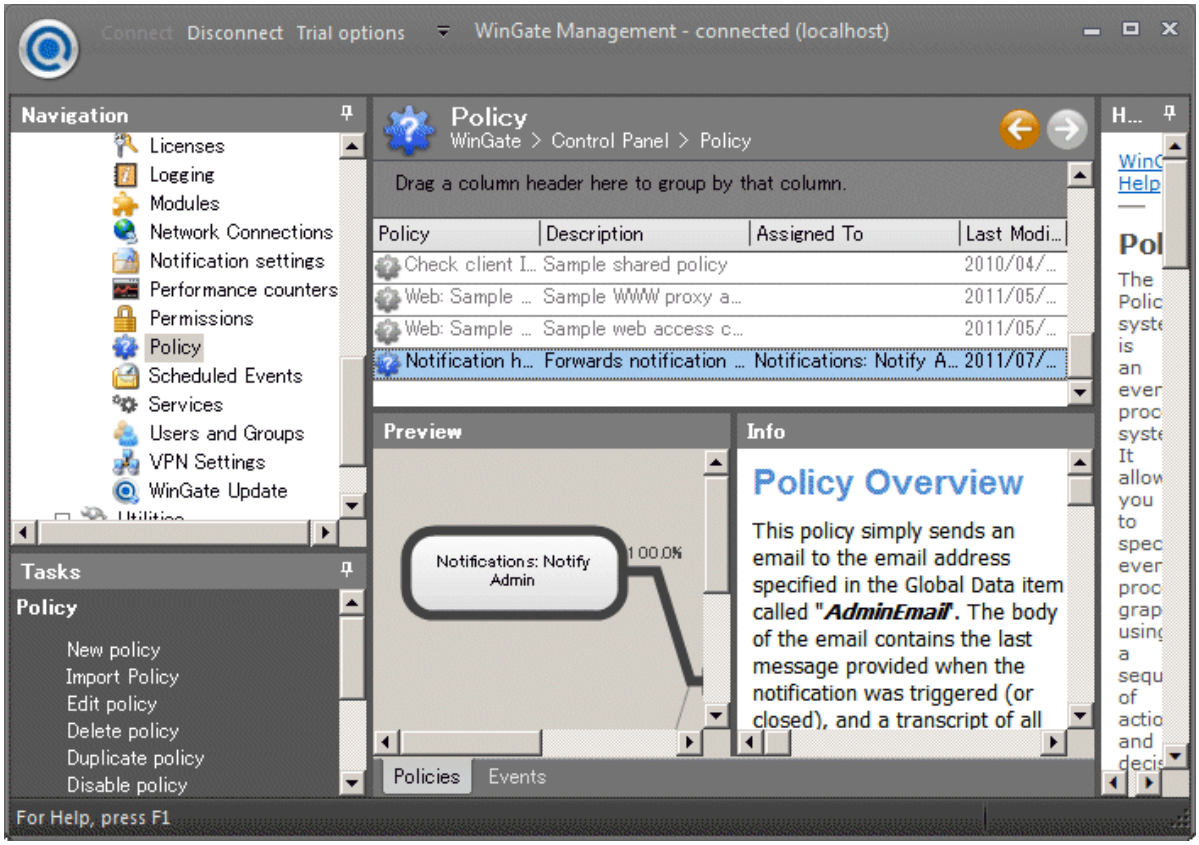

Type String 欄の AdminEmail（管理者電子メールアドレス）、AdminSender（送信元管理者）をダブルクリックして、それぞれの電子メールアドレスを設定します。




ご注意：ここで設定される電子メールアドレスは、先程 Email で設定したサーバーで配信可能な電子メールアドレス、および送信に使用できる電子メールアドレスとしてください。

5. WinGate Management の Navigation より Policy を選択します。



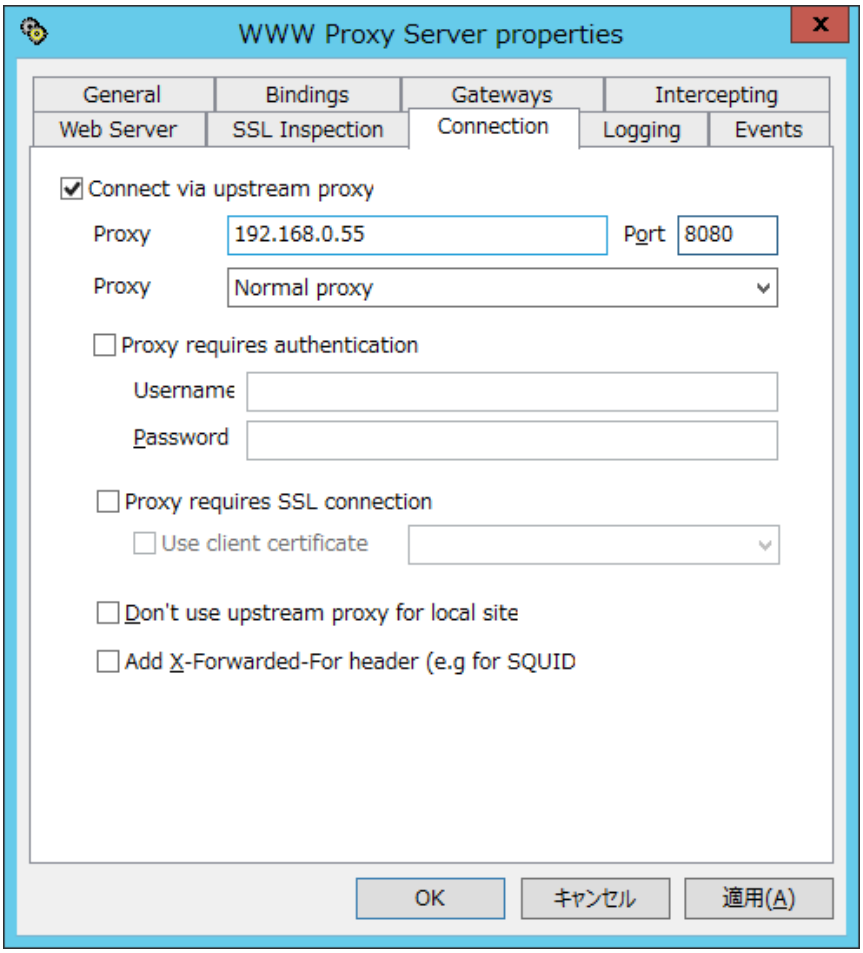

デフォルトで設定されている Notification handler（通知ハンドラ）ポリシーが有効になっているかを確認します。無効の場合は、Notification handler を選択し、右クリックで Enable Policy を選択し、有効にします。

以上で、WinGate で管理者への通知イベントが発生した場合、設定した内容にて、通知メッセージが電子メールで配信されます。

### 多段プロキシの設定

WinGate の上位に他のプロキシサーバーがあり、WinGate の WWW Proxy server の接続を上位のプロキシサーバーへ接続することができます。

設定は、WWW Proxy server properties の Connection タブより行うことができます。




Connect via upstream Proxy をチェックし、Server と Port に使用する上位のプロキシサーバーを指定し、上位のプロキシサーバーの種類に合わせて、Proxy type、および認証（Proxy requires authentication）の設定を行ってください。

上位プロキシサーバーに対して X-Forwarded-For ヘッダを送る必要がある場合は、「Add X-Forwarded-For header」をチェックしてください。

**設定のヒント**： ローカルサイトにアクセスする場合には、上位のプロキシサーバーを使用しない場合、「Don't use upstream proxy for local sites」をチェックすることにより可能となります。

このオプションを使用した場合、WinGate は、デフォルトルート以外のルーティングテーブルに一致した場合に、それをローカルサイトと判断し、上位のプロキシサーバーを使用しないよう動作いたします。

**URL により使用する上位プロキシサーバーを振り分ける**

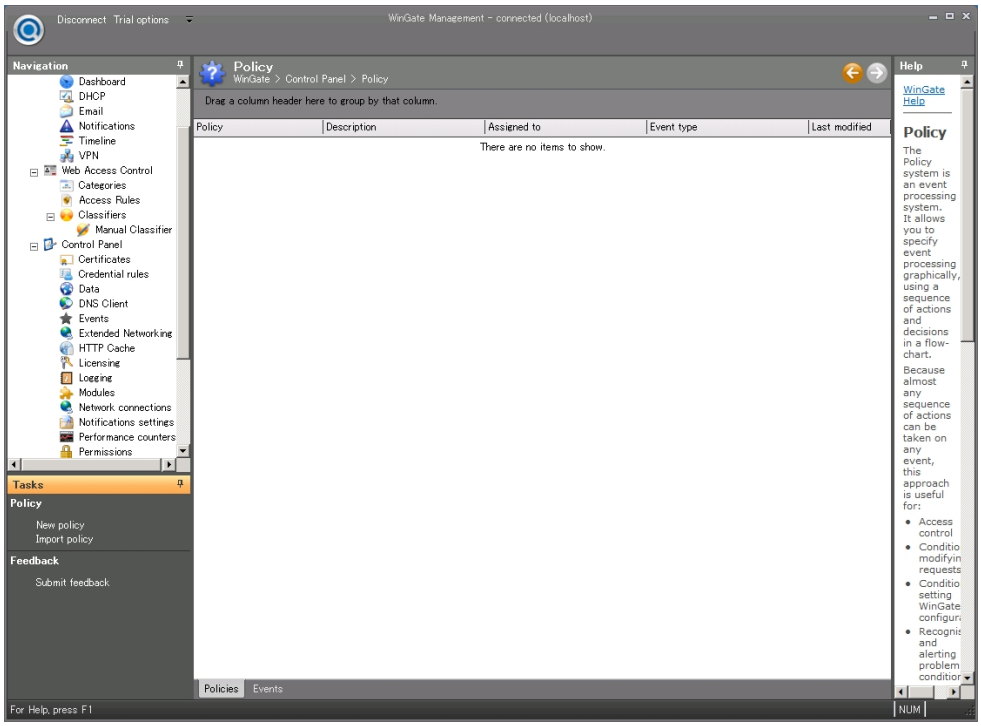
**ご注意:この機能は WinGate Enterprise 版のみで使用可能となります。Standard 版、Professional 版では、この設定は利用できません。**

※この設定は、WWW Proxy Server の ProxyRequest に対して有効となりますので、HTTPS 接続は対象外となります。
※Extended Networking の NAT 機能と WWW Proxy Server でインターセプトを使用している場合、ポリシーで対象とした WWW Proxy Server の ProxyRequest でも適用されます。

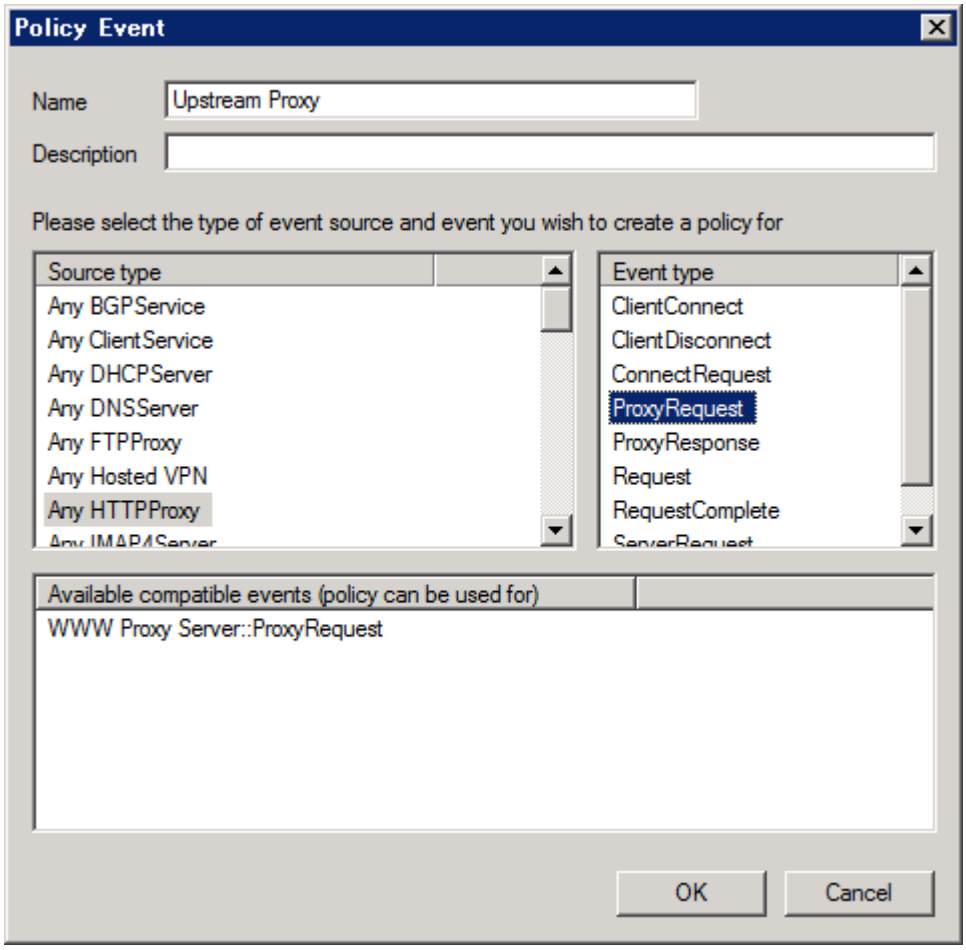
WinGate の上位に他の HTTP プロキシサーバーがあり、特定の URL の場合にのみ上位 HTTP プロキシサーバーを使用する設定となります。

この設定は、ポリシー機能の Connection control アイテムを利用します。

1. WinGate Management の Navigation、Control Panel より Policy を表示し、画面内で右クリックして「New Policy」を選択します。



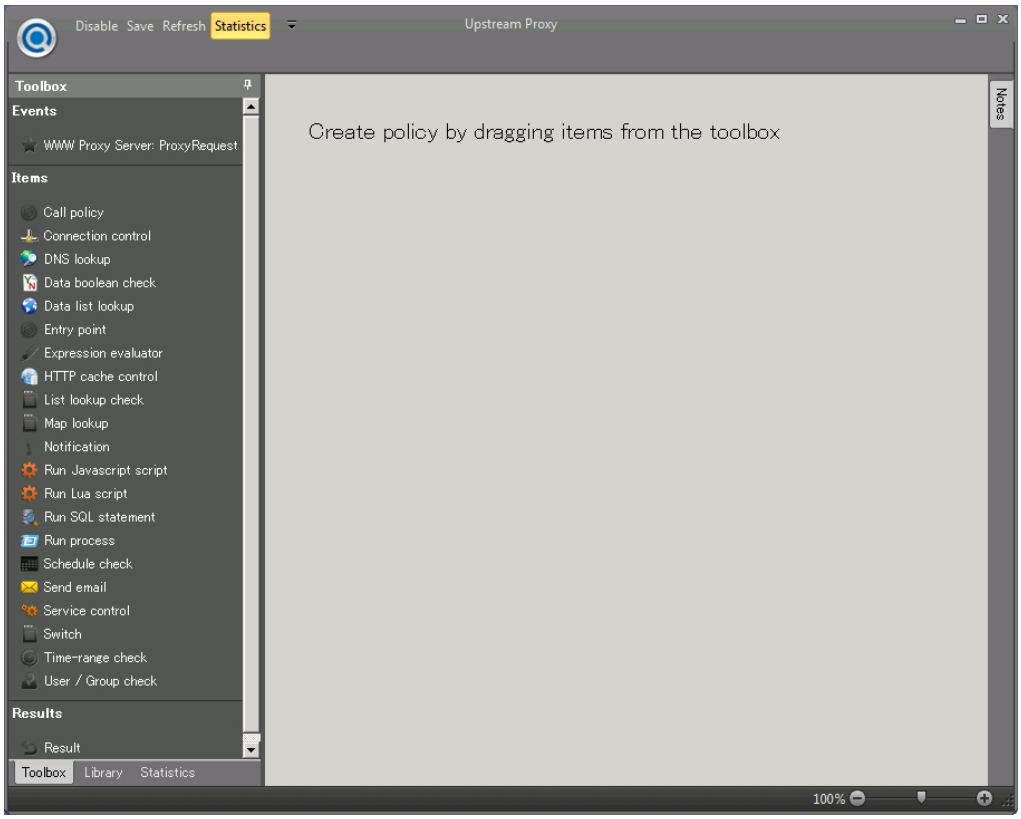

2. Policy Event ダイアログが表示されます。



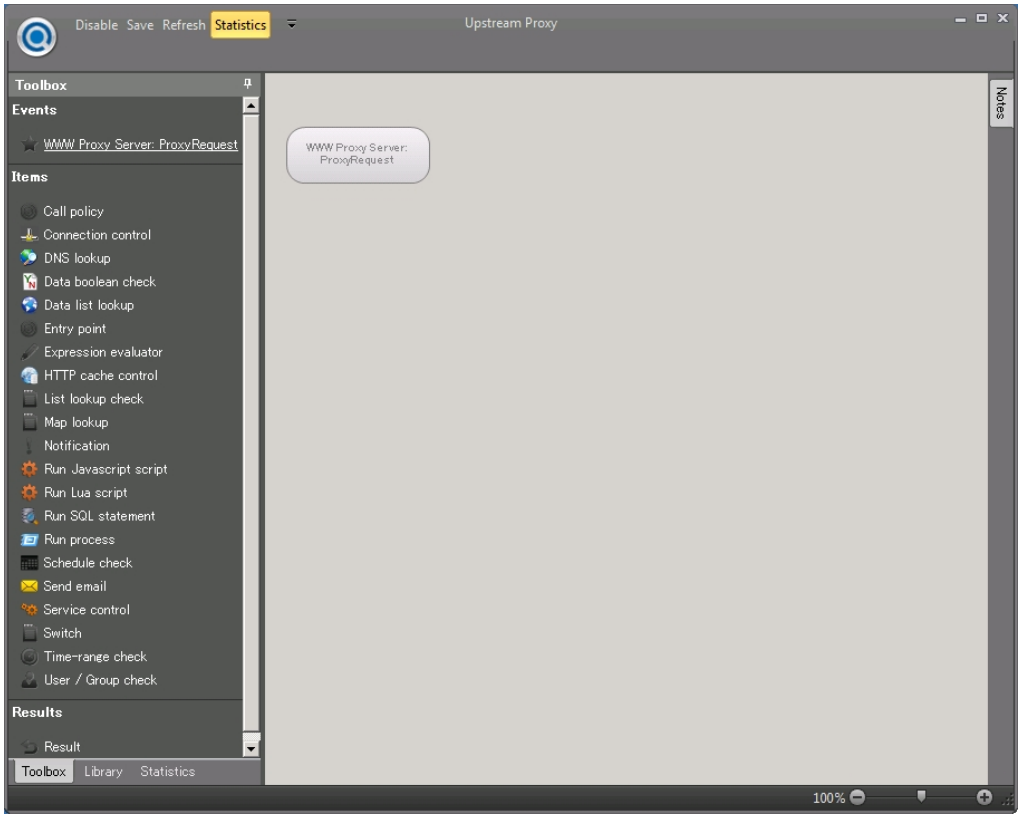

Name に、このポリシーの任意の名前を入力します。

Source type で、「Any HTTPProxy」を選択、Event type で「ProxyRequest」を選択し、OK ボタンで終了します。

3. ポリシーダイアログが表示されます。

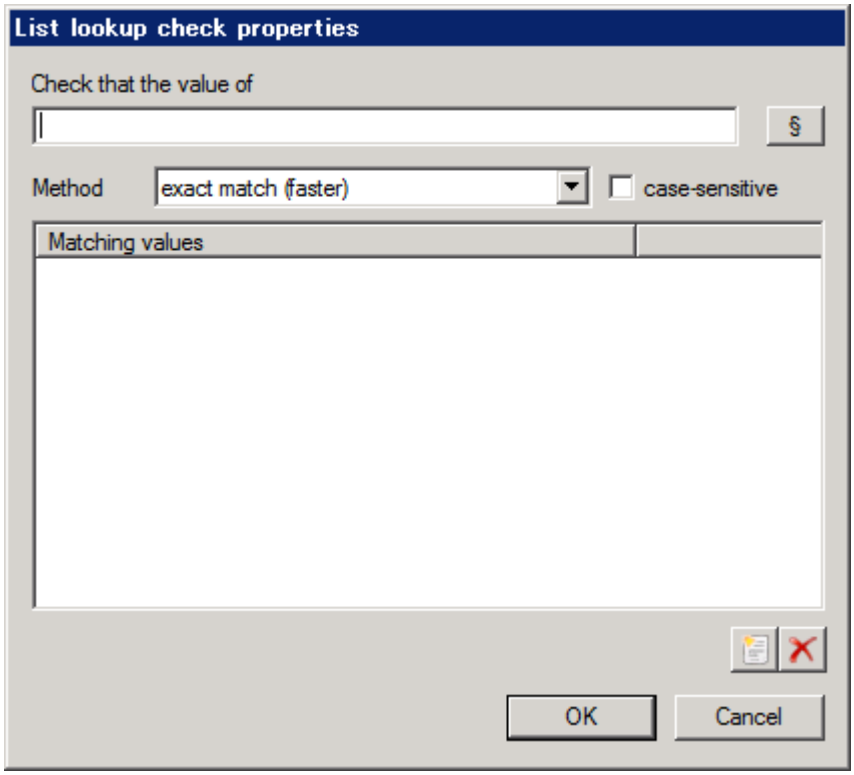


Event より WWW Proxy Server: ProxyRequest を右側にドラッグします。

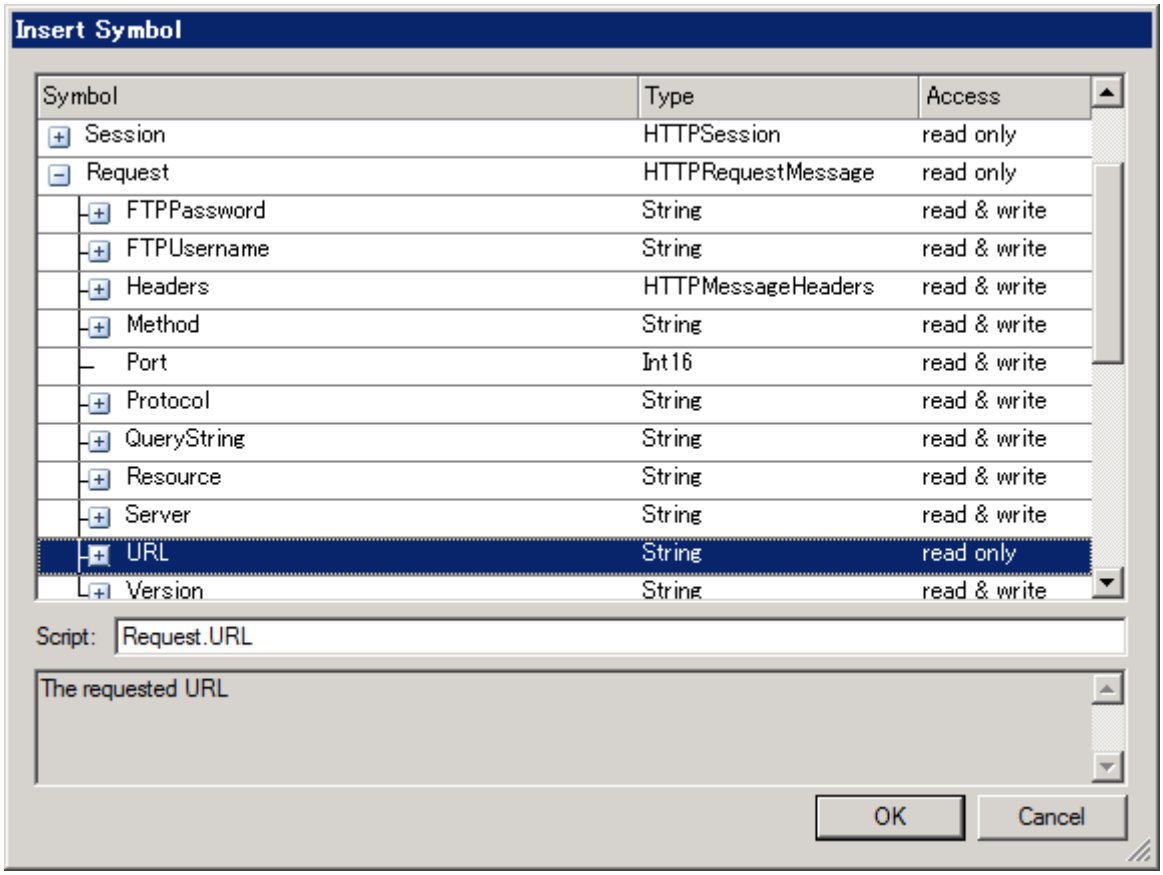



続いて Items より List lookup check を右側へドラッグします。

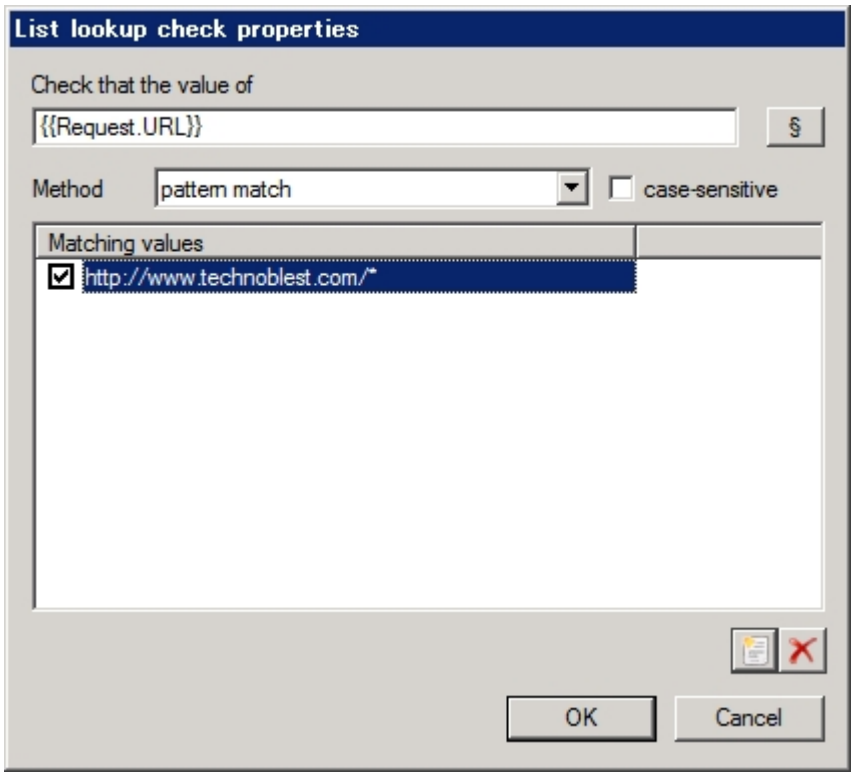
List lookup check properties ダイアログが表示されます。



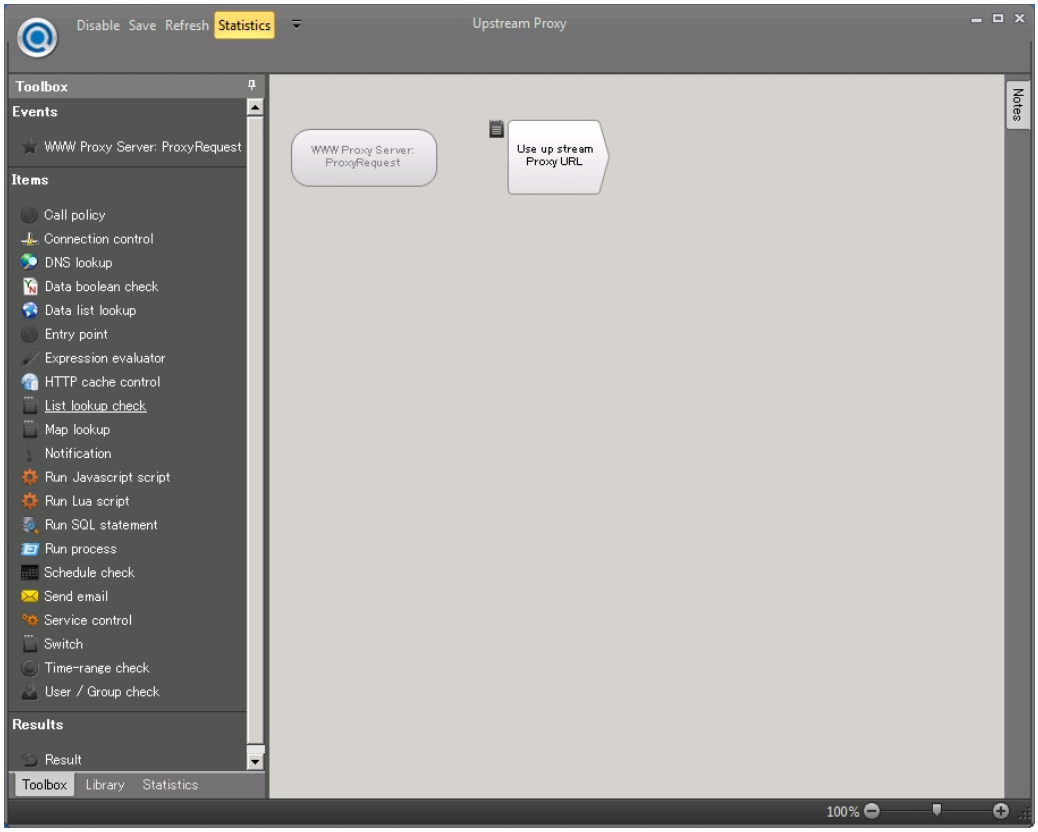

Check that the value of 右側にある Insert symbol ボタンをクリックします。




Insert symbol ダイアログが表示されますので、ここから Request、URL を選択して OK ボタンをクリックします。
List lookup check properties ダイアログの Check that the value of に値が反映されます。

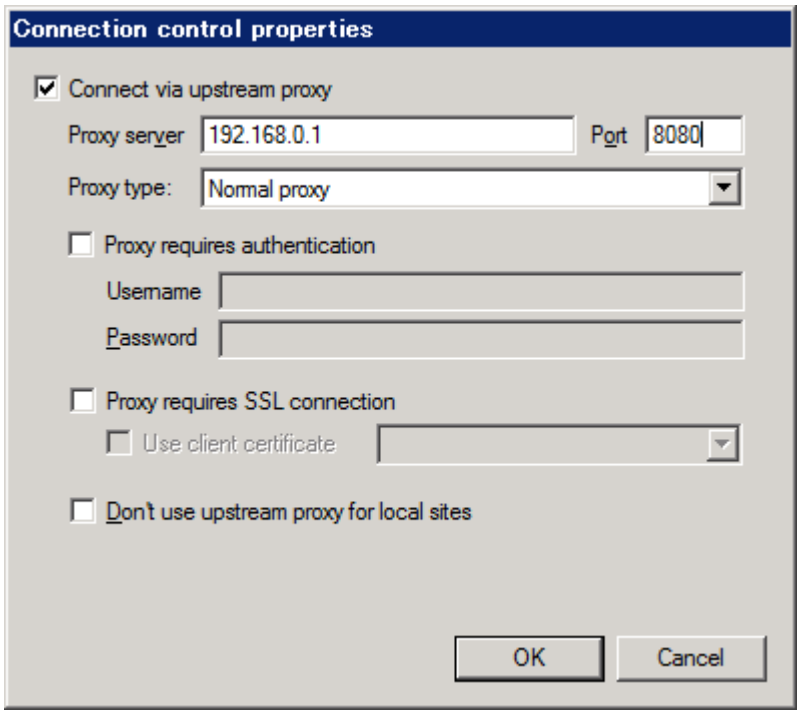



続いて Method ドロップ ダウンメニューから「pattern match」を選択し、右下の「adds a new policy decision」ボタンをクリックして、指定される上位プロキシサーバーを使用する URL（ワイルドカード可）を入力します。
複数指定をする場合は、「adds a new policy decision」ボタンより追加してください。
OK ボタンでダイアログを終了します。

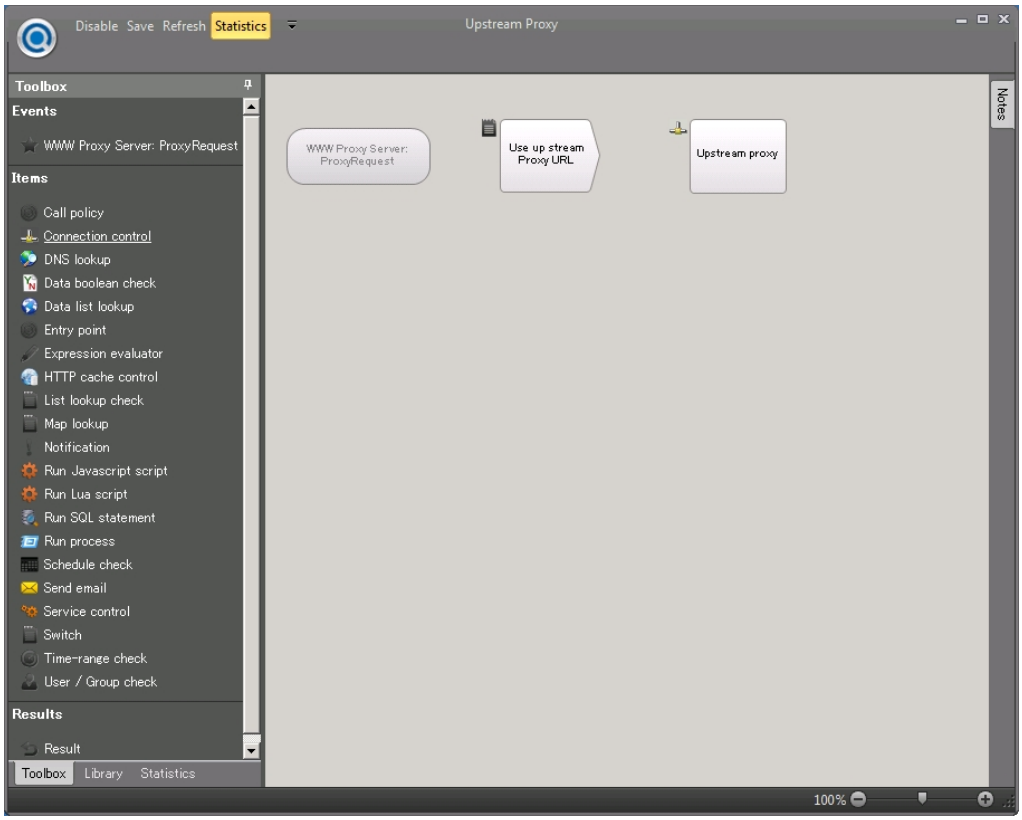



List lookup check アイテムに任意の名前を入力します。

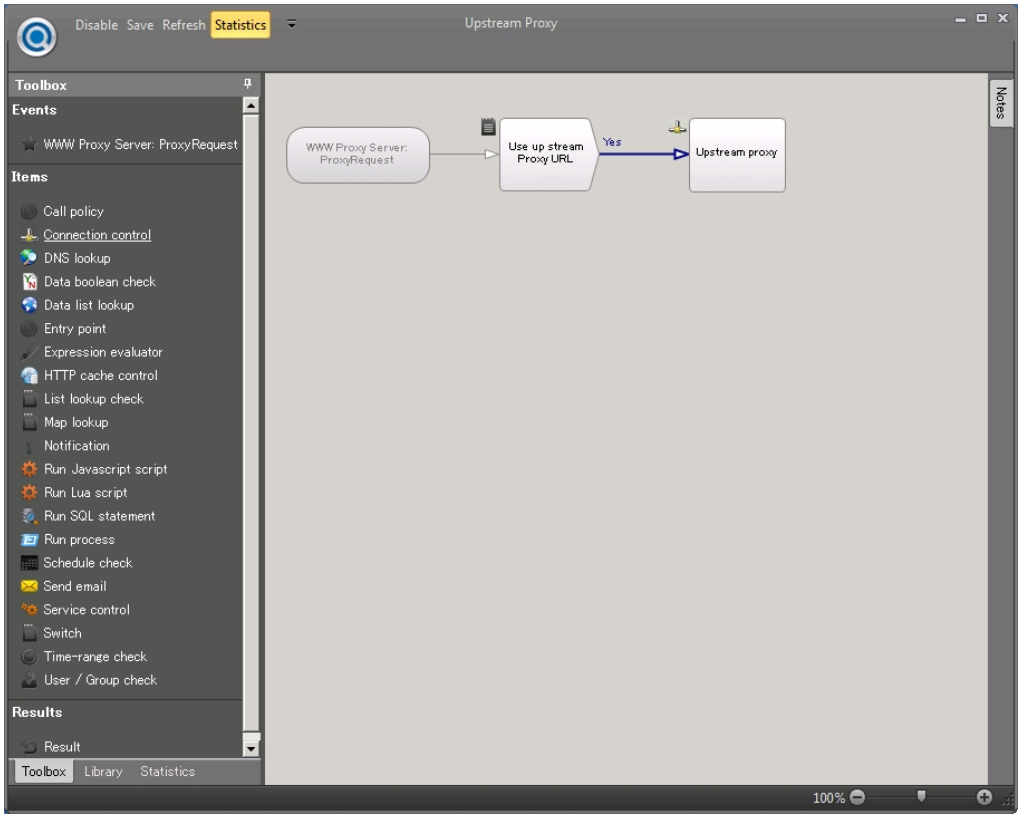
続いて Items から Connection control を右側にドラッグします。
Connection control properties ダイアログが表示されるので、Connect via upstream proxy をチェックして、リストの URL に一致した場合に使用される上位プロキシサーバーを指定します。



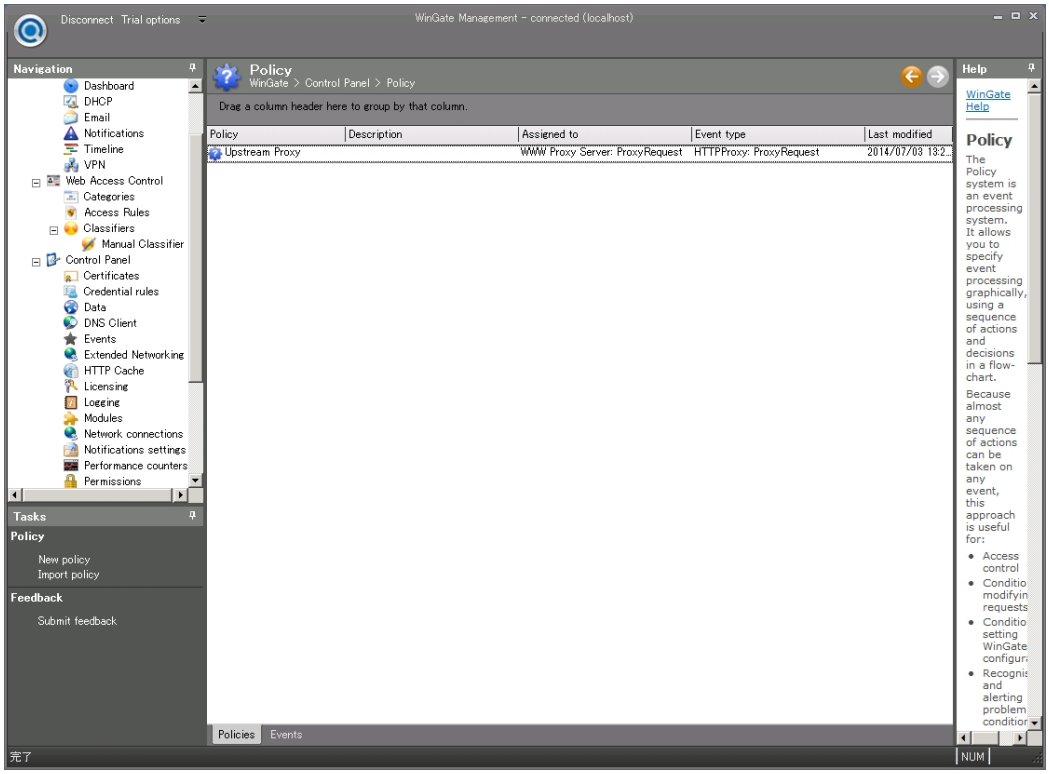

OK ボタンでダイアログを終了します。




各アイテムを以下のように結びます。(アイテムの端からドラッグすることで矢印が現れます。)




ダイアログ左上の Save より設定保存した後、閉じる(×)からダイアログを終了します。




Policy に設定したポリシーが追加されます。

以上で指定した URL へのプロキシリクエストは、指定した上位プロキシサーバーを使用いたします。
ブラウザから接続を行い、実際の動作をご確認ください。
ポリシーのプロパティでは、利用された割合等を確認いただくことができます。

**通常のメンテナンス**

WinGate は、一旦設定が完了いたしますとバックグラウンドで動作するため、設定変更やログ情報の閲覧を行う際に WinGate Management を利用することが考えられます。
しかしながら、定期的に以下の内容をご確認いただく事により、より快適な動作を実行いただけることが考えられます。
WinGate のご運用をいただきます場合、以下の内容を定期的にメンテナンスいただくことをお勧めいたします。

- 定期的に WinGate Management へログインしてください。
  WinGate Management に定期的にログインいただく事で WinGate の状態や通知メッセージを確認いただくことができます。
  通知メッセージには、最新バージョンのご案内やアップグレード保証の期限に関する情報が通知されることがあります。
  定期的に WinGate Management へログインいただく事で、これらの情報をご確認いただくことができます。

- WinGate 最新バージョンの確認
  WinGate Management の WinGate Update は、デフォルト設定で定期的に最新バージョンのチェックを行います。最新バージョンでは、バグ修正や機能追加が行われますので、可能な限り最新バージョンをご利用いただくことをお勧めいたします。

- ディスク容量の確認
  WinGate は、キャッシュファイルやログ情報の保存にディスクを使用いたします。
  デフォルトでは、ログ情報は一定の期間で削除されますが、ご利用いただいております環境やログ保存期間の設定によっては、ログ情報によりディスク容量の不足を招く場合がございます。
  定期的に WinGate サーバマシンにアクセスいただき、ハードディスクの空き容量をご確認ください。

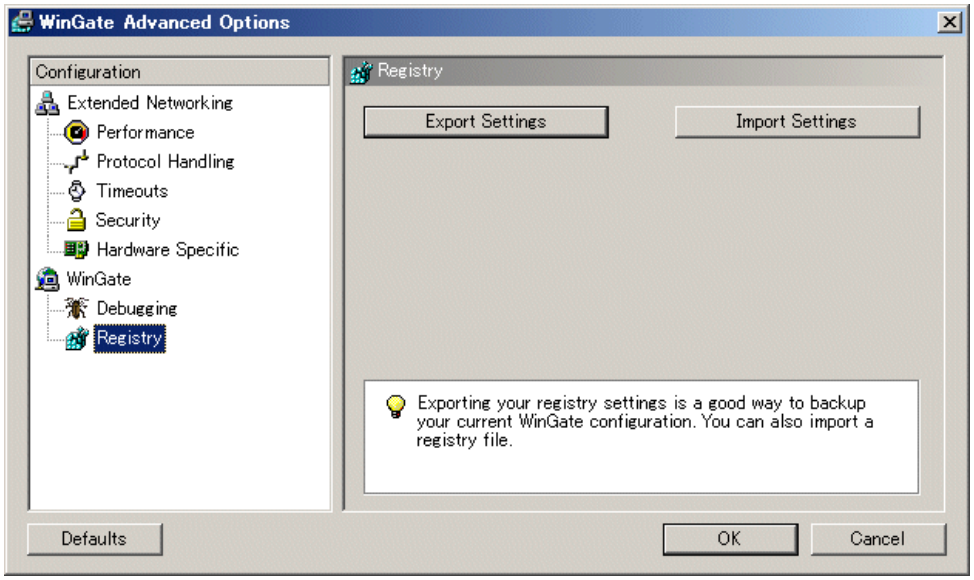
**WinGate 設定情報の保存と復元**

WinGate8.0.4 以降のバージョンをご利用の場合は、261 ページの「WinGate8.0.4 以降のバージョンをご利用の場合」をご参照ください。

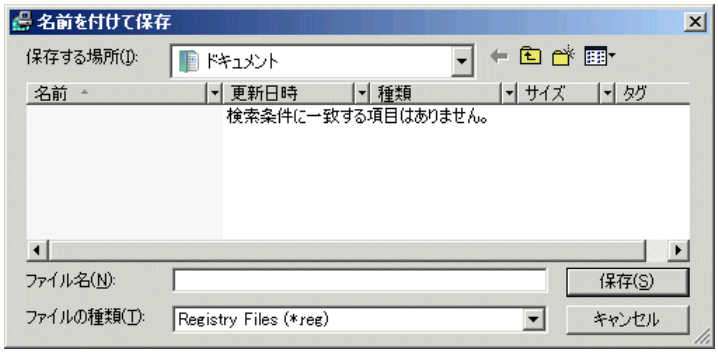
WinGate の設定情報は全てレジストリに書き込まれており、設定情報をバックアップするには、このレジストリ情報を保存する必要があります。（保存されるのは WinGate の設定情報のみとなります。ログ情報などは必要に応じて手動でバックアップしてください。）
※レジストリファイルの取り扱いはシステムへ影響を与える場合がございます。ファイルの取り扱いには十分ご注意ください。

**設定情報の保存（32bit　OS 環境）**
設定情報の保存は、以下の方法にて行うことができます。

- Windows のスタートメニュー、WinGate、WinGate Advanced Options（WinGate 詳細オプション）をクリックし WinGate Advanced Options（WinGate 詳細オプション）ダイアログを表示します。




Registry（レジストリ）を選択し、Export Settings（設定のエクスポート）ボタンをクリックします。




「名前を付けて保存」ダイアログが表示されますので、任意の場所にファイルを保存します。

保存されるファイルは、レジストリファイルとなるため、「 .reg 」の拡張子を持つファイルとなります。

以上で設定情報のバックアップは完了となります。

**設定情報の保存（64bit　OS 環境）**

設定情報の保存は、以下の方法にて行うことができます。

Windows の「ファイル名を指定して実行」で regedit と入力し、レジストリ エディターを起動します。
レジストリ エディターで以下の箇所を展開します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Qbik Software¥WinGate

WinGate 上で右クリックを行い「エクスポート」を選択します。
レジストリ ファイルのエクスポート ダイアログで任意のファイル名を指定して保存します。

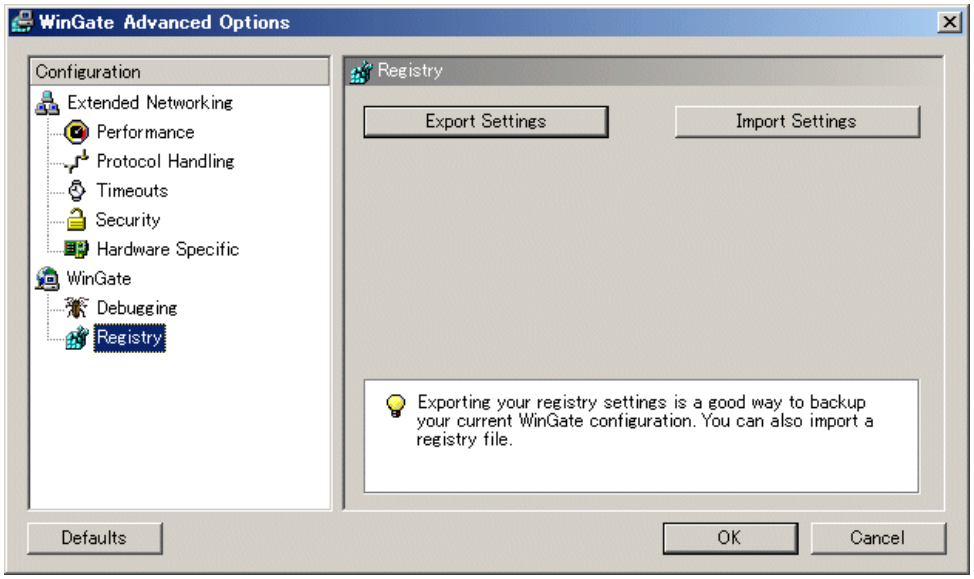
以上で 64bit OS 環境での設定のバックアップは完了です。

**設定情報の復元（32bit　OS 環境）**

◆同一 OS 間での場合

設定情報の復元（インポート）は、Windows スタートメニューの詳細オプション・ダイアログより行うことができます。
インポートを行う前には、WinGate エンジンを停止してください。
または、インポート完了後に WinGate エンジンの再起動を行ってください。（再起動を行わないとインポートされた情報は反映されません。）

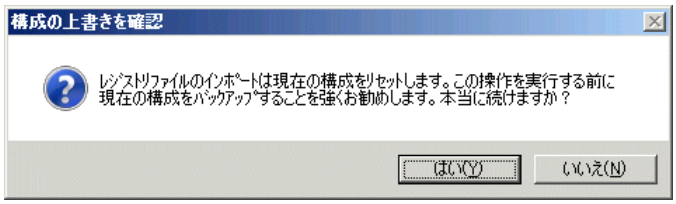
1. Windows のスタートメニュー、WinGate、WinGate Advanced Options（WinGate 詳細オプション）をクリックし WinGate Advanced Options（WinGate 詳細オプション）ダイアログを表示します。



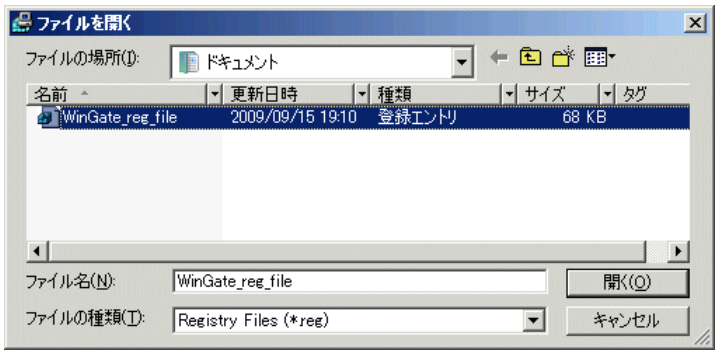

Registry（レジストリ）を選択し、Import Settings（設定のインポート）をクリックします。

2. 構成の上書き確認ダイアログが表示されますので、内容をご確認いただき「はい」をクリックしてください。（「いい

え」をクリックいたしますと中止され元の画面に戻ります。）




3. ファイルを開くが表示されます。




インポートするレジストリファイルを選択して、開くボタンをクリックします。

**※開くボタンのクリックでレジストリファイルの取り込みが開始されます。**

インポートが完了すると元の WinGate Advanced Options ダイアログへ戻ります。

WinGate エンジンが停止されていない状態でインポートが行われた場合、WinGate の再起動を促すダイアログが表示されますので「OK」ボタンで終了してください。（このダイアログは WinGate エンジンの再起動を行いません。手動で WinGate エンジン再起動を行ってください。

以上で設定情報の復元は完了となります。

WinGate Management より設定情報が正しく復元されているかをご確認ください。

**設定情報の復元（64bit　OS 環境）**

※必要に応じてレジストリのバックアップを事前に行ってください。

Windows の「ファイル名を指定して実行」で regedit と入力し、レジストリ エディターを起動します。

レジストリ エディターで以下の箇所を展開します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Qbik Software¥WinGate

WinGate フォルダーを右クリックより削除します。

バックアップされているレジストリファイルをダブルクリックしてレジストリ情報をインポートします。

レジストリ エディターの表示メニューより「最新の情報に更新」を選択し、

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Qbik Software¥WinGate

の配下に正しくインポートされているかを確認します。

**インポートされた内容を反映するために WinGate Engine を再起動します。（Extend Networking を使用している場合は、Windows の再起動が必要となります。）**

以上で設定情報の復元は完了となります。

WinGate Management より設定情報が正しく復元されているかをご確認ください。

**異なる OS 間での場合**

1. WinGate エンジンを停止します。(WinGate エンジンの停止は、タスクトレイに表示されております WinGate エンジンアイコンで右クリックを行い「エンジンの停止」を選択することで行えます。)
2. Windows のレジストリエディタを起動します。(レジストリエディタは、Windows の「ファイル名を指定して実行」で regedit と入力し実行することで開始できます。)
3. レジストリエディタにて HKEY_LOCAL_MACHINE¥SOFTWARE¥Qbik Software を開きます。
4. ″WinGate″キーを削除、または別名に変更します。
5. レジストリエディタを終了します。
6. 保存されたレジストリファイルをダブルクリックし、レジストリ情報の書き込みを行います。
7. WinGate エンジンを開始します。
8. 保存されたレジストリ情報の設定情報が反得されているかを GateKeeper よりご確認ください。

※レジストリの操作は Windows の動作に影響を与える場合がございます。操作には十分ご注意ください。
※ インポートされるレジストリ情報は、対応するレジストリに上書きされます。

**32bit 版 OS と 64bit 版 OS で WinGate のレジストリ情報を移行する場合のご注意**

32bit 版 SO でエクスポートした WinGateConfig.reg ファイルを 64bit 版 OS でインポートした場合、WinGate はインポートされたレジストリ情報を利用しません。(逆の場合も同様です。)
WinGate の設定情報が、それぞれの OS で異なるレジストリに保存されているために、この現象が発生いたします。
32bit Windows では WinGate の構成情報は"HKEY_LOCAL_MACHINE¥SOFTWARE¥Qbik Software¥WinGate"に保存されます。
64bit Windows では、WinGate の構成情報は"HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Qbik Software¥WinGate"に保存されます。
メモ帳などのテキストエディタで、それぞれの OS 用にエクスポートされたファイルを編集することにより正しくインポートする事が可能となります。
32bit WinGateConfig.reg を 64bit Windows でインポートするために変換するには:
1. メモ帳でエクスポートされた WinGateConfig.reg ファイルを開きます。
2. メモ帳の編集メニューから置き換えをクリックします。
3. 検索する文字列に 'SOFTWARE¥Qbik Software' を入力します。
4. 置換後の文字列に 'SOFTWARE¥Wow6432Node¥Qbik Software' を入力します。
5. 全て置き換えをクリックします。
6. 置き換えが完了したら、キャンセルをクリックします。
7. ファイルメニューから保存をクリックします。
(64bit Windows の設定情報を 32bit Windows へ取り込む場合は、3 と 4 の内容を逆にします。)
編集が完了したレジストリファイルを、通常通りインポートしてください。インポート完了後に設定が正しく反映されているかをご確認ください。

WinGate の詳細オプション(Advanced Option)にて、エクスポートされた WinGate の設定情報(レジストリファイル)をインポートする場合、詳細オプションのインポートを使用すると、設定情報を正しくインポートすることができません。

64bit OS 環境でインポートを行う場合は、詳細オプションのインポート機能を使用せず、32bit アプリケーション用のレジストリエディタを使用してレジストリファイルのインポートを行ってください。
32bit アプリケーション用のレジストリエディタは、Windows のファイル名を指定して実行より %systemroot%¥syswow64¥regedit と入力いただくことで実行いただけます。（※レジストリエディタの操作は Windows の動作に影響を与える場合がございますので、操作には十分ご注意ください。）

**Kaspersky AntiVirus for WinGate の移行・復元についてのご注意**

Kaspersky AntiVirus for WinGate の設定情報についても WinGate のレジストリファイル内に記載されております。
Kaspersky AntiVirus for WinGate のレジストリ情報は、Kaspersky AntiVirus for WinGate のバージョンにより互換性を持っておりません。
保存された WinGate の設定情報と同一バージョンの Kaspersky AntiVirus for WinGate の設定情報の復元は、上記でご紹介しております手順にて可能となりますが、保存されたレジストリ情報がインストールされている Kaspersky AntiVirus for WinGate と異なる場合、設定情報の復元を行うことにより Kaspersky AntiVirus for WinGate が動作しない場合、またはバージョン警告が表示され動作しない場合がございます。
この場合、一旦保存された WinGate 設定情報と同一バージョンの Kaspersky AntiVirus for WinGate をインストールいただきました後に、最新バージョンの Kaspersky AntiVirus for WinGate へアップグレードいただくか、先に移行元の Kaspersky AntiVirus for WinGate をアップグレードした後、設定情報の保存を行ってください。
ご不明な点は、弊社までお問い合わせください。

**WinGate8.0.4 以降のバージョンをご利用の場合**

WinGate8.0.4 では、設定情報エクスポート、エクスポートの新機能として、WinGate Configuration Utility が追加されました。

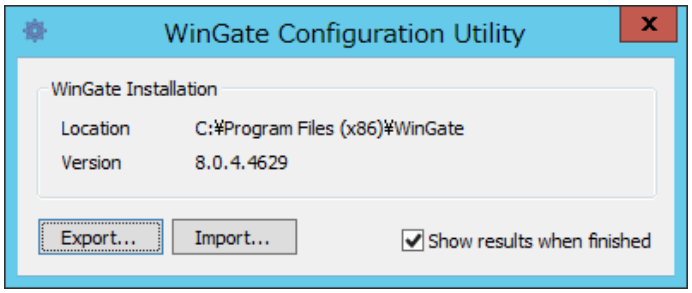
WinGate Configuration Utility をご利用いただことにより WinGate の設定情報を容易に保存、復元いただくことが可能となります。

WinGate Configuration Utility は、64bit、32bit 環境に依存せずご利用いただくことができます。

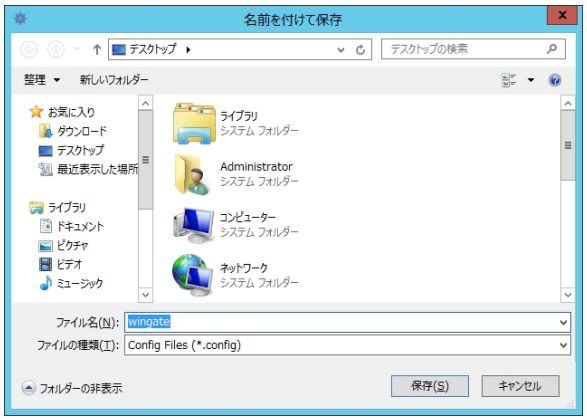
**ご注意:WinGate Configuration Utility で設定をエクスポート/インポートする際は、WinGate を停止いただく必要がございます。WinGate を停止せずに、これらの操作を行った場合、予期しない結果を生じる場合がございます。**

**WinGate Configuration Utility を使用した設定情報のエクスポート手順**

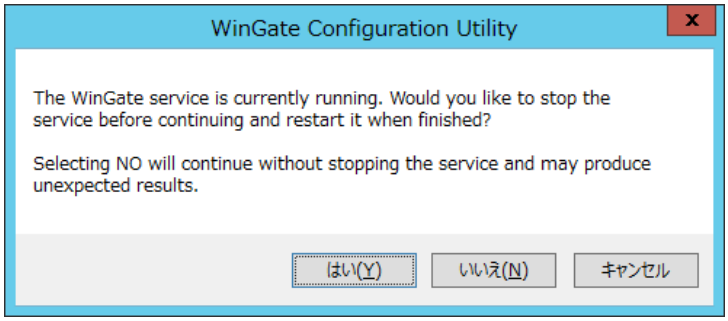
1. WinGate エンジンを停止します。
2. Windows スタートメニュー、全てのプログラム、WinGate より WinGate Configuration Utility を選択します。
3. WinGate Configuration Utility ダイアログが表示されます。




4. Export ボタンをクリックします。
5. 名前を付けて保存ダイアログが表示されますので、ファイル名、保存場所を指定して「保存」ボタンをクリックします。



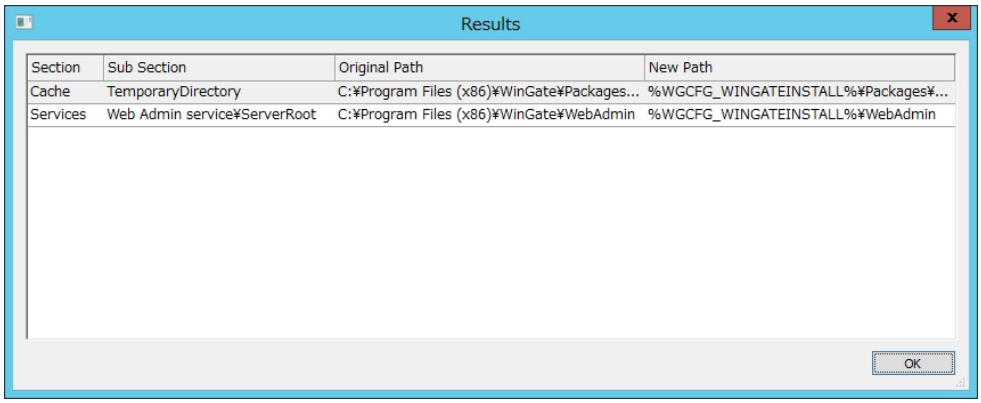

WinGate エンジンが停止されていない場合、以下のダイアログが表示されます。




「はい」を選択した場合、WinGate Configuration Utility は、WinGate エンジンを停止し、エクスポート完了後に

自動的に WinGate エンジンを開始します。
「いいえ」を選択した場合、WinGate Configuration Utility は、WinGate エンジンを停止せずにエクスポートを行いますが、この場合予期しない結果を生じる場合がありますので、「はい」を選択して WinGate エンジンを停止してエクスポートを行っていただくことをお勧めいたします。

6. エクスポートが開始され、指定した場所にファイルが保存されます。(WinGate エンジンが停止されていない場合は、WinGate エンジンの停止、エクスポート、WinGate エンジンの開始の順番に実行されます。)
7. Show results when finished が選択されている場合、完了後に Result ダイアログが表示されます。




OK ボタンで Result ダイアログを終了してください。

8. ダイアログ右上の閉じるより WinGate Configuration Utility ダイアログを終了してください。

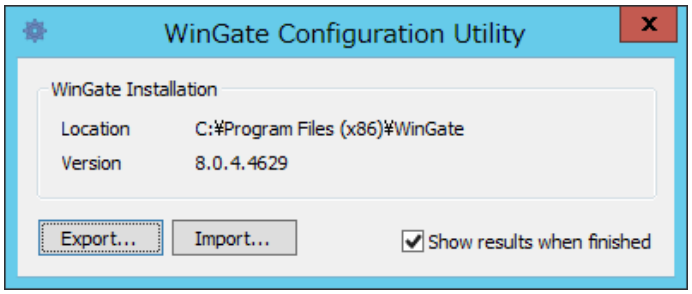
以上で WinGate Configuration Utility を使用した WinGate 設定のエクスポートは完了となります。WinGate Configuration Utility を実行いただく前に、手動で WinGate エンジンを停止いただいております場合は、WinGate エンジンを開始してください。

**WinGate Configuration Utility を使用した設定情報のインポート手順**

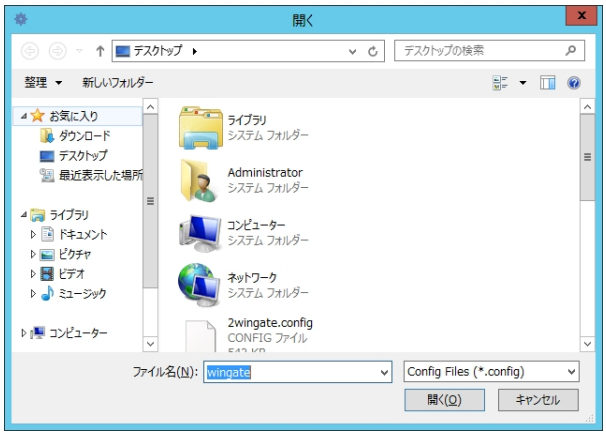
**ご注意:**

- WinGate の設定情報は、保存されている設定内容に全て上書きされます。必要に応じて、現在の設定情報を事前にバックアップ(エクスポート)してください。
- WinGate のインストールが、保存されている設定ファイルのインストール環境と同一であることを確認してください。
- WinGate ユーザー・データーベースを使用してル場合、Administrator パスワードやユーザー情報も保存されているファイルの状態へと復元されます。
- WinGate Configuration Utility は、Windows のネットワーク接続、NIC のプロパティにある、WinGate Network Driver の状態を復元いたしません。必要に応じてインポート後に WinGate Network Driver の有効/無効を Windows のネットワーク接続、NIC のプロパティより確認、および設定してください。

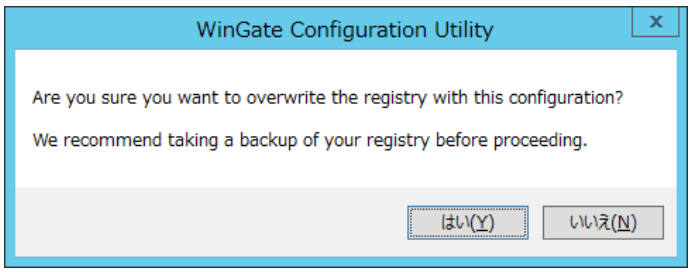
1. WinGate エンジンを停止します。
2. Windows スタートメニュー、全てのプログラム、WinGate より WinGate Configuration Utility を選択します。
3. WinGate Configuration Utility ダイアログが表示されます。




4. 開くダイアログが表示されますので、インポートする WinGate の構成ファイル（xxxxx.config）を指定して「開く」ボタンをクリックします。

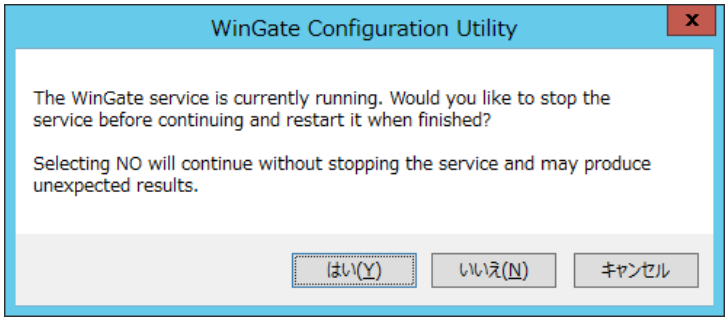



5. 確認ダイアログが表示されます。




インポートするファイルが正しい場合、「はい」をクリックします。

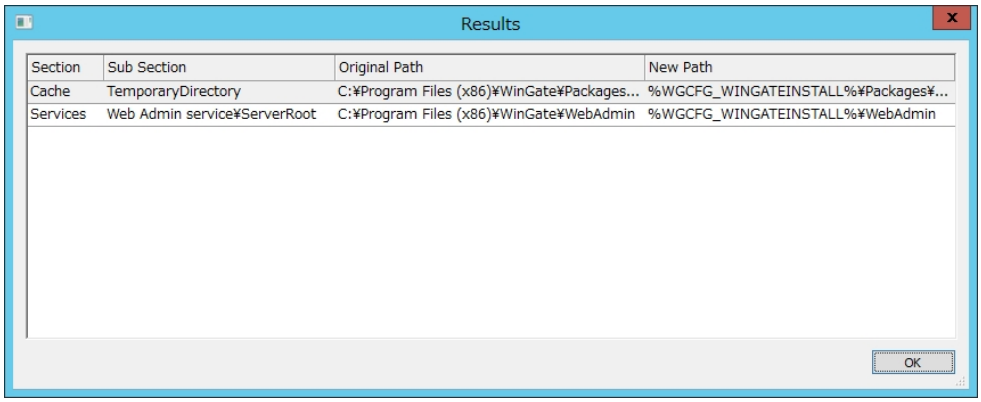
WinGate エンジンが停止されていない場合、以下のダイアログが表示されます。




「はい」を選択した場合、WinGate Configuration Utility は、WinGate エンジンを停止し、インポート完了後に自動的に WinGate エンジンを開始します。

「いいえ」を選択した場合、WinGate Configuration Utility は、WinGate エンジンを停止せずにインポートを行いますが、この場合予期しない結果を生じる場合がありますので、「はい」を選択して WinGate エンジンを停止してインポートを行っていただくことをお勧めいたします。

6. インポートが開始されます。（WinGate エンジンが停止されていない場合は、WinGate エンジンの停止、インポート、WinGate エンジンの開始の順番に実行されます。）
7. Show results when finished が選択されている場合、完了後に Result ダイアログが表示されます。




OK ボタンで Result ダイアログを終了してください。

8. ダイアログ右上の閉じるより WinGate Configuration Utility ダイアログを終了してください。

以上で WinGate Configuration Utility を使用した WinGate 設定のインポートートは完了となります。WinGate Configuration Utility を実行いただく前に、手動で WinGate エンジンを停止いただいております場合は、WinGate エンジンを開始してください。

WinGate エンジン開始後は、WinGate Management を開始して、設定情報が正しくインポートされているかをご確認ください。

**WinGate のアクティベーションについて**

WinGate をご使用いただくには、何らかの方法で必ずアクティベートを行っていただく必要があります。

WinGate はアクティベートを行わない限り WinGate をご使用いただく事はできません。（試用版につきましても試用版のライセンス情報を有効にするために、アクティベートを行っていただく必要があります。）

アクティベートはインターネット、又は電子メールを使用して行っていただく事ができます。
多段プロキシ環境などでも、インターネットを通じたアクティベーションを行っていただくことができます。（WinGate のアクティベーションは、インターネットエクスプローラで指定されているプロキシ設定を使用いたします。）
インターネットを使用したアクティベートでは、問題がない場合は、すぐにアクティベートが行われライセンスが有効となります。
電子メールによるアクティベートでは、ライセンスを発行するまでに、1～5 営業日ほどお時間をいただく場合がございます事をご容赦ください。
アクティベーション情報を発行させていただくお時間などの面から、インターネットを通じたアクティベーションを行っていただくことをお勧めたします。

アクティベーションは 1 ライセンスで、1 つまで許可されるため、1 つのライセンスキー情報で重複したアクティベートを行うことはできません。

WinGate マシンの移行などによりライセンスキー情報を移行する場合は、必ず Qbik ライセンスビューアより、デアクティベート（アクティベーション情報の解除）を行ってください。これを行わない場合、アクティベートした情報が残されたままとなり、そのライセンスキー情報を移行先のマシンでアクティベートすることができません。

**ハードウェア、OS トラブル時などの WinGate アクティベーション情報の解除**

ハードウェアの故障など何らかの理由によりデアクティベートが不可能となりました場合は弊社サポートまで、以下の情報をお書き添えいただき電子メールをお送りください。アクティベート情報の解除を手動にて対応させていただきます。**※対応は弊社営業日、営業時間内となります。**

- お名前、ご連絡先（法人様の場合は、会社名）
- 電話番号
- 電子メールアドレス
- ご購入日、ご購入店名
- ライセンス登録名、ライセンスキー情報

## トラブルシューティング

WinGate をご利用いただきました際に問題が発生いたしました際のトラブルシューティングの事例をご紹介しております。

### WWW Proxy を使用して Web サイトが表示できない

このような問題が発生した場合、WinGate 自体に問題が発生しているか、インターネット接続に問題が発生しているかをご確認いただき、原因の切り分けを行うことができます。

幾つかの確認方法がございますが、最も容易な方法として以下の内容をご確認ください。

### 原因の切り分け方法

WinGate サーバー マシンからのインターネット接続に問題が発生していないかをご確認ください。

最も簡単な方法は、WinGate サーバー マシンがインターネット接続を持つ場合、WinGate サーバー マシンのブラウザから Web サイトへの接続を確認する方法となります。

通常 WinGate がインストールされているマシンのブラウザは、WinGate に依存することなく、Web サイトへのアクセスを行えることが考えられます。(ブラウザのプロキシサーバーで自身をプロキシサーバーとして指定している場合は、これを解除してください。また、多段プロキシ構成が必要となる環境では、上位のプロキシサーバーをブラウザのプロキシ設定で指定してください。)

もし、ブラウザで Web サイトが表示いただけない場合、WinGate サーバー マシンが持つ、インターネット接続に何らかの問題が発生していることが考えられます。

ブラウザで Web サイトが表示いただけました場合、WinGate で何らかの問題が生じていることが考えられます。

その他の確認といたしましては、コマンドプロンプトからの Ping の疎通や nslookup による名前解決の確認などの方法が考えられます。

Windows ファイアウォールやファイアウォール製品で WinGate WWW Proxy Server の接続ポートがブロックされている。この場合、ファイアウォール製品で WinGate が接続受け付けているインターフェース、またはポートを許可する設定を行ってください。

### インターネット接続に問題がなく、WinGate の問題である可能性が高い場合

以下の内容をご確認ください。

- WinGate Management の Activity 画面の確認

WinGate Management の Activity には、クライアントマシンからの接続状況がリアルタイムで表示されます。

Activity にクライアント接続が表示されていない場合、WinGate はクライアントからの接続を受け付けていない(受け付けられていない)状態であることが考えられます。

このような場合、WinGate の WWW Proxy Server のプロパティより、Bindings をご確認いただき、WinGate で指定したネットワークインターフェースの IP アドレス、ポートで接続が受け付けられる状態であるかをご確

認ください。
WinGate の設定に問題がなく、クライアントからの接続が行えない場合、WinGate とクライアント間の接続に問題が発生していないかをご確認ください。

- Activity にクライアントが表示されても、クライアントマシンで Web ページが表示されない
  このような場合に考えられる内容は、WinGate の WWW Proxy Server で設定されているゲートウェイ（Gateway）が誤っている（または利用できない）場合や WinGate の DNS Client 設定で設定されている DNS Server で名前解決が行えないことが考えられます。
  これらの設定が適切に行われているかをご確認ください。

- WinGate Management へログインできない
  WinGate Management は、WinGate サービスの実行プログラム（WinGate.exe）とは別の独立した実行プログラム（GateKeeper.exe）で動作しております。
  WinGate Management は、WinGate の Remote Control Service（リモート・コントロールサービス）へ接続して、WinGate の情報を表示します。
  WinGate Management へログインできない場合、幾つかの要因が考えられますが、Remote Control Service が使用するポートがブロックされていない場合、WinGate 自体が、何らかの要因により接続を受け付けられない状態となっていることも考えられます。

**その他の現象**

その他 WinGate で発生する現象に関しては、ログファイルに何らかの情報が記録されている場合がございます。
WinGate7 以降では、デフォルトで警告やエラーを Global ログファイルに記録いたします。
Global ログファイルは、WinGate インストールディレクトリ、Logs、Global フォルダー内に保存されておりますので、テキストエディタなどを使用して、現象発生時のログファイルにエラーなどが記録されていないかをご確認ください。
また、WinGate が不正に終了した場合、WinGate インストールディレクトリ内に、現象発生時の日時をファイル名に持つダンプファイル（.DMP）が、自動的に生成されます。WinGate の不正終了などの現象が発生いたしました場合、サポートへこのダンプファイルをお送りください。

**より詳細な原因の調査**

発生した現象の内容によっては、容易に原因を特定することができない場合もございます。
発生した問題を調査するためには、現象のトリガーとなる動作、発生パターン、WinGate の機能として関連する箇所が特定できている場合に、よりスムーズに調査が行える場合がございます。サポートへご連絡をいただきます場合は、これらの情報をお送りください。また、現象の発生が特定のトラフィックにより引き起こされる場合などは、パケットキャプチャーツールによる対象のパケットキャプチャデーターが調査のための、より有用な情報となる場合もございます。

**WinGate のパフォーマンスに関するトラブルシューティング**

WinGtae7 以降では、設定やご利用いただく環境により WinGate のパフォーマンスに影響を与える場合があります。

- **ログ設定**

  WinGate7 のログ設定（Logging）は、Diagnostic（診断）ログでは、デフォルトで Warning（警告）のみが記録されるよう設定されています。これを Debug（デバッグ）などに変更いただいております場合は、取得するログ情報が増え、WinGate のパフォーマンスに影響を与える場合がございます。

- **HTTP Cache（HTTP キャッシュ）**

  **WinGate7**

  WinGate7 の HTTP Cache は、デフォルトでは MDB データーベースに、キャッシュインデックスを保存して利用いたします。

  1GB を超えるキャッシュサイズや 1GB 未満でも多くのキャッシュインデックスを持つ場合や頻繁にキャッシュインデックスが更新、パージされる環境では、インデックスの参照や更新などに時間がかかり、WinGate の WWW Proxy Server のパフォーマンスが低下する場合があります。

  このような場合、キャッシュボリュームサイズを減らし調整を行うか、HTTP Cache 機能自体を無効化する方法が考えられます。

  **WinGate8**

  WinGate8 では、キャッシュシステムが、メモリ/ファイルを使用した方式へ変更されております。

  大きすぎる単一のキャッシュボリュームは、パフォーマンスに影響を与える場合がございます。

  キャッシュの利用状況などを確認しながら適切なキャッシュサイズ、アイテム数などをご検討ください。

- **Timeline（タイムライン）**

  WinGate7 より追加されたタイムライン機能は、WinGate Management の Timeline 画面に WWW Proxy Server のトラフィックをユーザー毎にグラフ表示する機能を提供します。

  これは、データーを MBD データーベースに格納し、表示を行うため、データーが膨大になった場合などに、WinGate のパフォーマンスに影響を与える場合があります。

  Timeline は、デフォルトでは、1 ヶ月以前のデーターを月に一度パージするように設定されていますが、この間隔を短くしていただくことで、Timeline データーベースのサイズを削減いただくことができます。

  また、この機能を使用していない場合、Timeline Settings より Tracking する Activity 項目を全て解除していただく事により事実上、機能を無効化していただくことができます。

  WinGate8.1.0 以降では、デフォルトのデーターベースが、SQLite へ変更されました。中/大規模なユーザーで WinGate を使用し、Timeline 機能をご利用いただいておりますお客様は、WinGate8.1.0 へアップグレード後、SQLite へデーターベースを変更いただくことを強くお勧めいたします。（この変更により以前のデーターベースに保存されているデーターは継承されません。）

- **他社アンチウイルス、ファイアウォール製品をご利用いただく場合のご注意**

  WinGate をご利用いただいております PC を保護するためにアンチウイルス製品をご利用いただきます場合は、WinGate のインストールディレクトリをウイルススキャンの対象外としていただく事を強くお勧めいたします。（ログディレクトリやキャッシュディレクトリを WinGate のインストールディレクトリ以外に設定変更して

いる場合は、それらのディレクトリも対象としていただく事を強くお勧めいたします。）
WinGate は、ログやキャッシュファイルへ正常にアクセスできない場合に、動作に影響を持つ場合があり、アンチウイルス製品のスキャンによりこのような状況が発生する可能性があるためです。
また、アンチウイルス製品に含まれるファイアウォール機能と WinGate の Extended Networking 機能の競合により問題が発生する場合がございます。

- **Windows Server 2012 環境で特定の Web サイトで表示の遅延が発生する**

Windows Server 2012 の ECN（輻輳情報通知機能）が有効となっており、この影響により、特定の Web サイトを表示する際に遅延が発生する場合やファイルのダウンロードで遅延が発生する場合がございます。
本現象が発生いたします場合、Windows Server 2012 で ECN 機能を無効化することで解決いただける場合がございます。
ECN 機能は、以下の手順で無効にしていただくことができます。
※変更の適用について Windows や WinGate の再起動の必要はございません。
※ECN 機能の無効化による影響、および ECN 機能に関する詳細につきましては、サポート対象外となります。
※ECN 機能の詳細に関しましては、マイクロソフト社へご確認ください。
※ECN 機能を必要とする場合は、マイクロソフト社、ネットワーク機器メーカー様へご確認ください。

1. 管理者権限で Windows へログインしていることを確認してください。管理者権限でログインしていない場合は、管理者権限でログインしてください。
2. Windows のスタートメニューを右クリックし「コマンドプロンプト（管理者）」を選択して管理者：コマンドプロンプトを開始します。
3. コマンドプロンプトにて以下のコマンドを実行して TCP グローバル パラメーターの状態を確認します。

   netsh interface tcp show global

   表示される TCP グローバル パラメーターで「ECN 機能」が enabled となっております場合は有効、disabled となっている場合は無効となります。disabled となっている場合は、ECN 機能は無効となっておりますので、この機能の影響ではございません。そのままコマンドプロンプトを終了してください。
   enabled となっております場合、以下のコマンドにより ECN 機能を無効化します。

   netsh interface tcp set global ecncapability=disabled

   正しくコマンドが実行されましたら、再度 netsh interface tcp show global コマンドを実行して 「ECN 機能」が disabled （無効）となっているかを確認してください。
   以上で ECN 機能の無効化は完了となります。

   ECN 機能を再び有効にする場合は、以下のコマンドを実行してください。

   netsh interface tcp set global ecncapability=enabled

**Extended Networking の無効化**

WinGate をインストールする際に Extended Networking をインストールした場合、Extended Networking 機能のみをアンインストールすることはできません。

しかしながら以下の方法で無効化することができます。（無効化した場合、NAT、Router、ファイアウォール、ポートセキュリティ、VPN 機能を利用することはできません。）

1. WinGate Management へログインします。
2. Navigation、Control Panel、Extended Networking をクリックし Extended Network Driver ダイアログを表示します。
3. General 内の Status 右にございますボタンをクリックし ENS Driver Boot Control ダイアログを表示し「Do not load ENS driver when system starts」を選択し
   OK ボタンで ENS Driver Boot Control ダイアログを終了し、続いて Extended Network Driver ダイアログを OK ボタンで終了します。
4. WinGate Management を終了します。
5. Windows コントロール・パネルよりネットワークと共有センターを開き、アダプタの設定の変更より接続に使用している NIC のプロパティを開きます。
6. NIC のプロパティダイアログ内に WinGate Network Driver がございますので、 このチェックを外してください。（全ての NIC で同様に WinGate Network Driver のチェックを外してください。また、OS の種類によっては、WinGate Network Driver がない場合がございます。その場合、この操作は必要ありません。）
7. ダイアログを終了し、PC を再起動します。

再起動完了後にネットワーク接続、および WinGate が正しく使用できるかをご確認ください。

**ログの確認方法について**

WinGate のログは、Diagnostic（診断）ログと Usage（使用）ログに分かれて記録されます。

Diagnostic ログには、デフォルト設定では、エラー情報が記録記録され、Usage ログには、リクエストや処理内容などが表示されます。

Usage ログは、WWW Proxy server、SMTP Delivery Service、WinGate NAT などの限られたサービスのみで利用可能です。（Standard 版では、利用できません。）

各サービスで、より詳細なログを取得する必要がある場合には、Diagnostic ログで取得されるログレベルを変更することにより、エラーや警告以外のログ情報を取得することが可能となります。（取得できるログの内容は、サービスにより異なります。）

ログレベルを変更した場合、取得されるログ情報が増加するため、ログファイルの容量にご注意ください。

WinGate を利用するクライアントが、WWW Proxy server を経由して、どのようなサイトを利用したかについては、WWW Proxy server の Usage ログをご参照ください。

そのリクエストに対して何らかの問題が生じた場合は、Usage ログから対象となるリクエストを参照し、同じ日時を持つエラーを Diagnostic ログから確認してください。

**Diagnostic ログに記録される WWW Proxy server 関連のエラーとその内容について**

以下は、Diagnostic ログで記録されることがある WWW Proxy server に関連した代表的なエラーの一部となります。（全てのエラーログではございません。）

Server closed connection prior to completion of transaction
接続先のサーバーが、トランザクション完了前に接続を閉じたことを意味します。

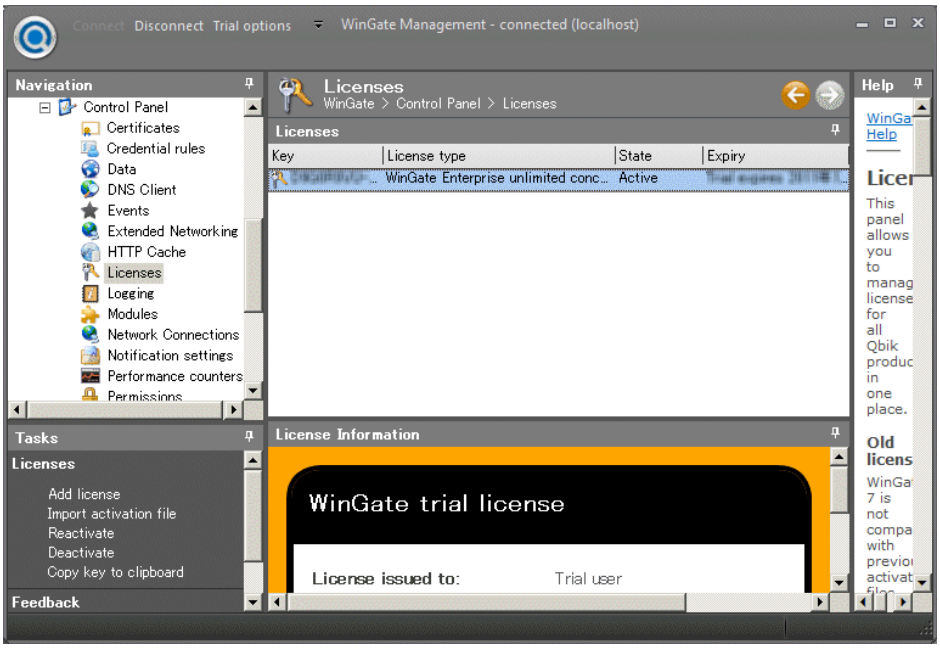
Connection to Remote Host timed out
リモートホストへの接続でタイムアウトが発生したことを意味します。

Connection refused by Remote Host
リモートホストにより接続が拒否されたことを意味します。

Connection Reset by Remote Host
リモートホストにより接続がリセットされたことを意味します。

**アップグレード保証期間の確認**

WinGate のアップグレード保証有効期限は、WinGate Management 内の Licensing より確認いただくことができます。




表示されている WinGate ライセンスの Expiry に表示されている日付、またはライセンスを選択すると下の License Information 内に有効期限の情報が表示されます。

Kaspersky AntiVirus for WinGate の購読期限についても、同様に確認いただくことができます。

**アップグレード保証更新、Kaspersky AntiVirus for WinGate の購読期限更新の適用**

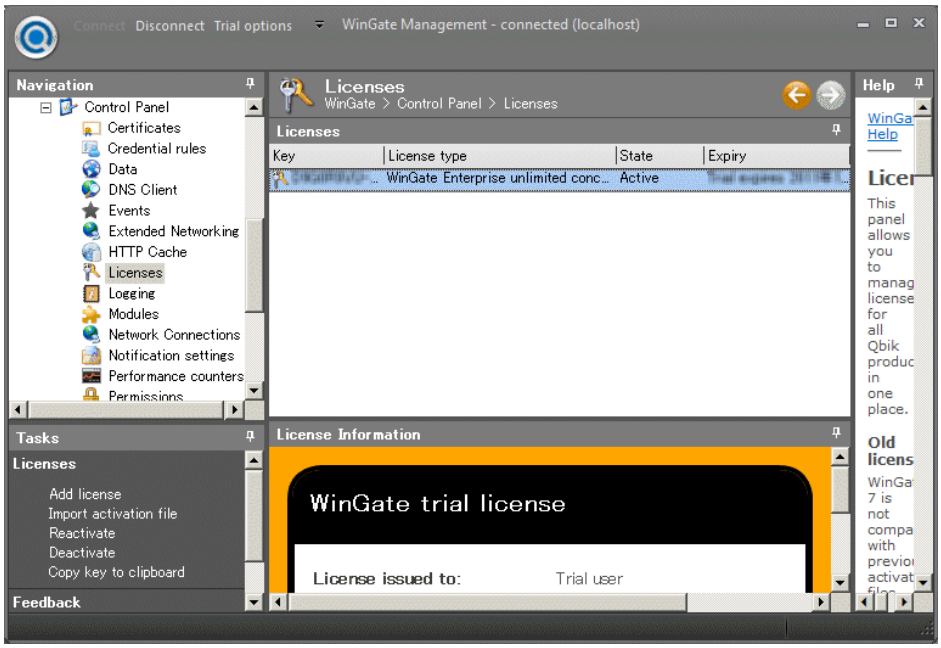
※WinGate の再起動が必要となります。再起動中は WinGate がご利用いただけなくなります。

アップグレード保証、および Kaspersky AntiVirus for WinGate の購読期限を更新いただきました後、更新を適用いただくには、ライセンスキーの再アクティベート（Reactivate）を実施いただく必要があります。（オンライン アクティベーションをご利用いただくことをお勧めいたします。）

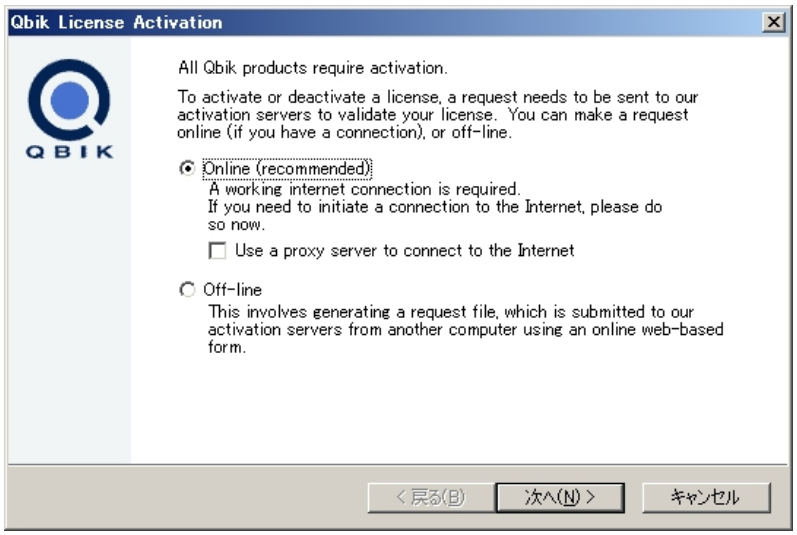
Reactivate は、WinGate Management 内の Licensing より実施いただくことができます。

以下はオンラインでのリアクティベート手順となります。

1. Licensing 画面で Reactivate を実施するライセンスを選択いただき、Reactivate をクリックしてください。

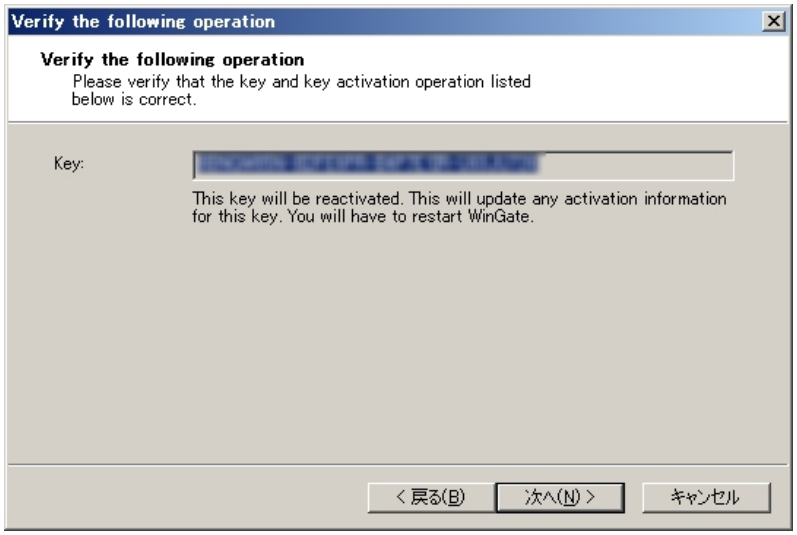



2. Qbik License Activation ダイアログが表示されます。

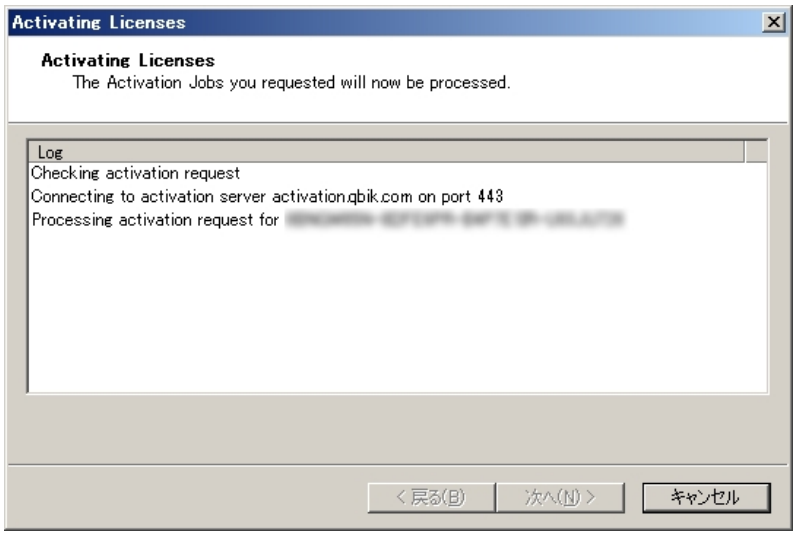



次へをクリックします。

3. ライセンスキー情報が表示され、Reactivate を行うことを確認する内容が表示されますので、キー情報などに問題がない場合「次へ」をクリックします。




4. オンラインでのアクティベーションが開始されます。




Reactivate が成功すると Log 内に Successful が表示されます。

Error が表示された場合には、WinGate マシンのインターネット接続をご確認ください。インターネット接続に問題がなく、エラーが表示される場合、弊社までご連絡ください。

5. 完了ボタンをクリックして Reactivate を終了します。

Reactivate 完了後は、WinGate の再起動が必要となります。

「はい」ボタンをクリックして、WinGate の再起動を行ってください。

以上で、Reactivate は終了となります。

WinGate Management の Licensing より有効期限情報が更新された日付となっているかをご確認ください。

**WinGate の種類、ユーザー数を変更した場合の適用方法**

WinGate の種類、ユーザー数を変更した場合、新しいライセンスキー情報にてアクティベーションを行う必要がございます。(WinGate の再インストールを行う必要はございません。)

1. WinGate Management の Licensing より Add License をクリックし Qbik License Activation ダイアログを表示します。

Online(オンライン)を選択して、「次へ」ボタンをクリックします。(オンラインでアクティベーションを行う場合、WinGate マシンがインターネットへ接続されている必要があります。)

2. Enter License ダイアログが表示されますので、Activate a purchased License を選択し、新しいライセンスキー情報を入力し、「次へ」ボタンをクリックしてアクティベーションを行います。

3. アクティベーションが開始され、完了すると「succeed」(成功しました)と表示されますので完了ボタンをクリックしてください。
以上でオンラインアクティベーションは完了となります。

ライセンスを有効にするために WinGate を再起動する必要があります。ダイアログの指示に従い WinGate の再起動を行ってください。

4. WinGate の再起動完了後、WinGate Management の Licensing から新しいライセンスキーが正しく適用されているかをご確認ください。(※もし古いライセンスキー情報が残っている場合、古いライセンスキーを選択し、Deactivate(アクティベーションの解除)を行ってください。この場合も解除完了後に WinGate の再起動が必要となります。)

**お問い合わせに関して**

弊社での WinGate の技術サポートは、電子メールによる受付のみとなっております。
また、技術サポートは、WinGate に付属しておりますアップグレード保証の期限内で提供されます。
アップグレード保証は、開発元でのライセンス発行日から起算し 1 年間となります。保証期間内のお客様は、弊社サポート条件によりサポートをご提供させていただきます。
その他、WinGate の技術的な内容、最新版情報などに関しても、弊社 WinGate Web サイトをご参照ください。

最新バージョンの WinGate は、機能修正や機能追加を含みます。アップグレード保証期間内の場合、最新バージョンへのアップグレードにより問題を解決できる場合もございます。お問い合わせをいただきます前に、最新バージョンへのアップグレードについてもご検討ください。最新バージョンでの修正内容は、WinGate Web サイト、リリースノートにて公開しております。

お問い合わせをいただきます場合、以下の内容をお送りくださいますようお願い申し上げます。
お客様情報を確認できない場合、サポートを承ることができない場合がございますことをご了承ください。

- 会社名、お名前、ご連絡先（メールアドレス、お電話番号）**（必須）**
- ご購入日、ご購入店名
- ライセンス登録名、または、ライセンスキー情報**（必須）**
- ご利用いただいております WinGate の種類、および詳細なバージョン情報（8.2.5 など）**（必須）**
- WinGate をご利用いただいております OS
- WinGate の構成内容、ログ情報（お問い合わせに関連したログ情報が記録されている場合）
- お問い合わせ内容（できるだけ詳細にご記載ください。）
- WinGate インストールディレクトリ内に DMP ファイルが生成されている場合、現象発生時の DMP ファイル

お問い合わせをいただく内容によっては、弊社よりご連絡をさせていただく場合がございます。必ずご連絡先の電話番号をお書き添えください。

※ライセンス登録名・ライセンスキー情報を確認できない場合、ご回答をさせていただくことができない場合がございますことをご了承ください。
※最新バージョンへアップグレードいただけない場合、サポートをご提供できない場合がございますことをご了承ください。
※ご回答までに2～3営業日ほどお時間をいただきますことをご了承ください。
※ご回答いたしました内容に基づき直接的、間接的に発生した損害については弊社では一切責任を負いませんのでご了承ください。
※お問い合わせをいただきました内容の解決をお約束するものではございません。
※お送りをいただきました電子メールに含まれます情報は、弊社個人情報の取り扱いに関するポリシーに基づき適切に取り扱いいたします。

お問い合わせ先:
〒252-0324 神奈川県相模原市南区相武台 1-24-6-2F
テクノブレスト株式会社
TEL: 046-259-1458（販売に関するお問い合わせ） FAX: 046-259-1459
電子メール:wg_support@technoblest.com（技術サポート）、sales@technoblest.com（販売に関して）
お問い合わせ受付時間:月曜日～金曜日 10:00 ～12:00、13:00 ～17:00（祝祭日など弊社の非営業日を除きます）
詳細なサポート条件、営業日などの情報につきましては、弊社 WinGate Web サイト、および弊社 Web サイトをご参照ください。
WinGate Web サイト: http://www.wingate.jp/
テクノブレスト株式会社 Web サイト: http://www.technoblest.com/

2013 年 7 月作成

2015 年 2 月 18 日　アクティベーション内容の追加、設定例の修正
2015 年 1 月 15 日　設定例の追加
2015 年 1 月 14 日　コピーライト表記の変更、その他追加、修正
2014 年 10 月 24 日　トラブルシューティングの項目を追加
2014 年 7 月 23 日　システム必要条件を一部変更
2014 年 7 月 22 日　お問い合わせ情報を一部変更、必要条件の一部追加・変更、トラブルシューティングを一部追加、内容の一部修正
2014 年 7 月 3 日　設定事例を追加
2014 年 5 月 8 日　サービス固有の設定に追加、その他細かな修正
2014 年 4 月 4 日　弊社住所を変更、トラブルシューティングを一部追加
2014 年 2 月 28 日　WinGate8.1.0 の Timeline データーベースの変更に対応
2013 年 12 月 3 日　インストール完了後に確認する内容の追加、その他に幾つかの追加
2013 年 11 月 7 日　WinGate 設定情報の保存と復元の内容を追加（WinGate8.0.4 に対応）
2013 年 9 月 9 日　WinGate 設定情報の保存と復元の内容を追加
2013 年 8 月 26 日　Services、WWW Proxy の Filter に関する説明を追記
※WinGate7 より変更が適用されていない箇所に関しては WinGate7 の情報をそのまま利用しています。今後内容を随時更新する予定です。

**テクノブレスト株式会社**

※本書の内容は全ての動作を保証するものではありません。また、本書を使用して発生いたしました問題に関しましては、弊社は一切の責任を負いません。内容は予告なしに変更される場合がございます。本書の内容を変更、転載する事はできません。テクノブレスト株式会社の許諾なく、本ガイドに含まれる情報を使用または第三者に開示しないものとします。ガイドをご覧いただきますお客様はこの内容に同意いただいたものとなります。著作権はテクノブレスト株式会社にあります。