



Administrator's Guide



VTScada Admin Guide

Excerpts from the VTScada Help Files

Copyright Trihedral Engineering Limited, 7/26/2016

All rights reserved.

Printed in Canada

Trihedral Engineering Limited

Head Office
1160 Bedford Highway, Suite
400
Bedford, Nova Scotia
Canada
B4A 1C1

Phone: 902-835-1575
Toll free: 800-463-2783
support@trihedral.com
sales@trihedral.com

Trihedral UK Limited

Glover Pavilion, Campus 3
Aberdeen Science Park
Balgownie Drive, Aberdeen
UK, AB22 8GW

Phone: +44 (0) 1224
258910
Fax: +44 (0) 1224 258911

Trihedral Inc.

Suite 160
7380 Sand Lake Road
Orlando, Florida
USA
32819

Phone: 407-888-8203
Fax: 407-888-8213

Trihedral Calgary Office

Suite 505 - 888 4 Ave SW,
Calgary, AB,
T2P 0V2
403.921.5199

Contents

Manage Applications	30
Contact Trihedral Engineering Limited	30
What's New...	31
Moving to the Current Version	88
Explore the Features of VTScada	109
Application Manager (VAM)	149
Change the VAM's Color Theme	151
Application Configuration	153
Application Information	154
predefined Date Codes	155
predefined Date Codes	158
Application Properties	160
Display Tab of the Edit Properties Page	164
Alarms Tab of the Edit Properties Page	169
Historical Data Viewer Tab of Edit Properties	177
Other Tab of the Edit Properties Page	181
Sort and Filter the Application Properties Dialog	184
Add a Property	186
Copy a Property	189
Change a Property's Value	193
Set a Workstation-Specific Property Value	195
Unsaved Configuration Changes	198
Application Properties Files	199
Configuration Hierarchy	200
Editing Application Properties	200
Import Edited Files	202
Application Property Components	205
Rules for Application Property Files	206
Workstation-Specific Properties	207
Section Names for Property Files	208
<ALARM_MANAGER>	210
[Areas]	213

[LABELS]	213
Sections for Realm Area Filtering	214
[REALMAREAS] Section	215
[*-REALMAREAS] Section	215
[<Area>-REALMAREAS] Section	216
Alarm Notification System Properties	217
AlarmCheckMail	219
AlarmCheckMailFastPoll	219
AlarmDialerStatusTemplate	219
AlarmDialerTemplate	220
AlarmEditEmailAck	220
AlarmEmailAckSubjectTemplate	220
AlarmEmailAckTemplate	221
AlarmEmailStatusTemplate	222
AlarmEmailSubjectTemplate	223
AlarmEmailTemplate	224
AlarmNotifyEmailAcknowledge	225
AlarmNotifySMSAcknowledge	226
AlarmPagerStatusTemplate	226
AlarmPagerTemplate	227
AlarmPriorityIndicatorShowNormalUnacked	228
AlarmSMSAckTemplate	228
AlarmSMSStatusTemplate	229
AlarmSMSTemplate	230
AlphaNumericXFormScheme	231
AnswerAlarmCalls	232
CallOutDelay1	232
CallOutDelay2	232
CallOutPriority	233
DialCancelOnAck	233
DialCancelOnNormal	233
DialerConnectDelay	234
DialerLocation	234

DialerPort	234
DialerSpeechInit	235
DialerVoice	235
DialInControl	235
DialOnActive	235
DialOnClear	236
EchoPhoneThroughSpeaker	236
EnableLexiconDialog	236
GiveUpCallTimeout	237
HideMenuOnOutgoing	237
IncomingCallSection	237
MaxCallAlarmPriorityReported	237
MaxPagerBaudRate	238
MenuRepeatMax	238
DialerAckIndividualAlarms	238
PhoneKeyFeedback	238
PINRetries	238
PINTimeOut	239
RepeatMenuTime	239
RosterDelay	239
SkipLogonDialout	239
SMTPPort	240
SpeechEngine	240
UseOldSpeechEngine	240
UseSMTPOverTLS	241
Application Properties for Alarms	241
AckAllRequiresConfirmation	245
ActiveAlarmFlash	246
ActiveCommColor	246
ActiveFlashRate	246
AlarmAutoNavEnable	246
AlarmAutoNavHold	247
AlarmAutoNavTimeout	247

AlarmAutoNavWindowed	248
AlarmCheckMail	248
AlarmCheckMailFastPoll	249
AlarmColor	249
AlarmDatabaseGroups	249
AlarmDatabasePurgeDelay	250
AlarmDatabasePurgeEnable	251
AlarmDatabasePurgeRate	251
AlarmDisplayDateFormat	251
AlarmDisplayTimeFormat	251
AlarmEventDescWidth	252
AlarmEventDesc0 – AlarmEventDesc21	252
AlarmFlashTime	253
AlarmFlashTitleBar	253
AlarmFlashTitleBarOnVIC	254
AlarmIndDisable	254
AlarmIndDisableOnVIC	254
AlarmKeySize	255
AlarmListBGColor	255
AlarmMaxPriority	255
AlarmMinPriority	255
AlarmOperatorVarName	255
AlarmPageHistoryRecordHardLimit	256
AlarmPageHistoryRecordLimit	256
AlarmPopupsEnable	257
AlarmPrintDateFormat	257
AlarmPrintTimeFormat	257
AlarmPrintPort	257
AlarmPriorityDescWidth	257
AlarmRevUnack	258
AlarmRPCEnable	258
AlarmSeparatorString	258
AlarmSnapshotCount	259

AlarmSoundDisable	259
AlarmSpeechEnable	259
AlarmSpeechInit	259
AlarmSpeechQuality	260
AlarmSpeechTemplate	261
AlarmSpeechVoice	262
AlarmStateDesc0	262
AlarmStatRange0 – AlarmStatRange3	262
AlarmStatRange0Label – AlarmStatRange3Label	264
AlarmStatusDesc0 – AlarmStatusDesc5	267
AlarmStatusDescWidth	267
AlarmStatusField	267
AlarmTemplateDateFmt	268
AlarmTemplateTimeFmt	268
AlarmTimeStampField	268
AlarmTxtColClear	268
AlarmTxtColDisable	269
AlmColumn1	269
AlmColumn2	269
AlmColumn3	269
AlmColumn4	270
AlmColumn5	270
AlmColumn6	270
AlmColumn7	271
AlmDBArea	271
AlmDBHPUnits	271
AlmDBHPValue	271
AlmDBMessage	272
AlmDBOperator	272
AlmDBPointName	272
AlmDBPriority	272
AlmDBStatus	273
AlmDBTimeStamp	273

AlmDBType	273
AlmHdg1	273
AlmHdg2	273
AlmHdg3	274
AlmHdg4	274
AlmHdg5	274
AlmHdg6	274
AlmHdg7	275
AlmListTextColor	275
AlmPgLineStyle	275
AlmPgStartList	275
ApplyMuteSilencePerComputer	276
ApplyMuteSilencePerUser	277
AlmTagsOnly	277
BackupAlarmPriority	278
ClientAlarmSoundOn	278
Cycles	278
FlashUnackedAlarmsOnServer	278
FlashUnackedAlarmsOnVIC	279
HighlightUnackedAlarms	279
MaxMuteDuration	279
MaxShelveDuration	280
MinMuteDuration	280
MinShelveDuration	280
MuteAlarms	280
NoteMinLengthForAck	280
NoteMinLengthForShelve	281
NoteMinLengthForUnshelve	281
NoteRequiredForAck	282
NoteRequiredForShelve	282
NoteRequiredForUnshelve	283
SecurityAlarmArea	283
UnackAlarmFlash	283

UnackFlashRate	283
WavAmplitude	284
WAVType	284
Color Properties	284
BadQualityColor	286
ButtonFace	286
ButtonHighlight	286
ButtonShadow	287
ButtonTextColor	287
DefaultBGColor	287
DefaultPageColor	287
DefGraphicBColor	288
DefGraphicPColor	288
DialogBGColor	288
DigitalIndicator0Color	288
DigitalIndicator1Color	288
DigitalIndicator2Color	289
DigitalIndicator3Color	289
DigitalIndicatorAlarmColor	289
DigitalIndicatorInvalidColor	289
FieldHighlight	289
FieldShadow	290
GrayedText	290
GridColor	290
InvalidColor	290
MenuBgnd	291
MenuTextColor	291
NormalColor	292
OffColor	292
OnColor	292
OpaqueBackground	292
PollDisabledColor	293
ReceiveColor	293

SelectedBGnd	293
SelectedText	294
State0DefColor	294
State1DefColor	294
State2DefColor	295
State3DefColor	295
TransmitColor	296
UnselectedBgnd	296
UnselectedText	296
WindowBgnd	297
WindowFrame	297
Communication Driver Properties	297
#DataLines	299
BackupSwitchCount	299
BadQualityColor	299
CIP_O_to_T_RPI	300
CIPTimeoutMultiplier	300
CommFailColor	301
CommStatsQualityFactor	301
CommStatsUpdateRate	302
DataFlowModuleName	302
DataFlowStationName	302
DemoMode	303
DFSimulateOn	303
DisableCommStats	303
DNP3DataInvalidOnFail	304
DNP3DelayedResponseTimeout	304
DNP3FailoverCount	304
DNP3MaxFileSize	304
DNP3SharedRPC	304
DriverRPCOptimization	305
FastPollCommColor	305
FastPollDuration	305

FastPollRate	305
InactiveCommColor	305
ModiconVTSTMaxBlock	306
NoInitialDriverDial	306
NoSoftDriverFailure	306
SNMPAgentEnable	307
SNMPAgentInformRetryInterval	307
SNMPAgentInformRetryLimit	307
SNMPAgentIPListener	308
SNMPAgentMaxTCPSize	308
SNMPAgentMaxUDPSize	308
SNMPAgentReadCommunity	308
SNMPAgentSessionTimeout	309
SNMPAgentTagNotifyMode	309
SNMPAgentTrapCommunity	309
SNMPAgentTrapHost	310
SNMPAgentTrapPort	310
SNMPAgentWriteCommunity	310
SNMPAgentWriteEnable	310
VTSDriverClearDataOnServerLossDelay	311
SQLDataQueryDriverDefaultDBType	311
SQLDataQueryDriverDefaultTableName	311
SQLDataQueryDriverMaxTagsPerQuery	312
Display Manager Properties	312
AutoOpenIdeaStudio	313
BitmapDirExt	314
BMPPath	314
DialogMoveTime	314
DisplayManagerTitle	314
DispMgrAspectRatio	315
DispMgrBitmap	315
DispMgrBMPMarginBottom	315
DispMgrBMPMarginLeft	316

DispMgrBMPMarginRight	316
DispMgrBMPMarginsWin	316
DispMgrBMPMarginTop	316
DispMgrDateFormat	316
DispMgrFullScreen	317
DispMgrHeight	317
DispMgrHidden	318
DispMgrHoriz	319
DispMgrMinHeight	319
DispMgrMinMaxDisabled	319
DispMgrMinWidth	320
DispMgrPageStyle	320
DispMgrResizable	321
DispMgrTimeFormat	322
DispMgrTitleBorder	322
DispMgrVert	322
DispMgrWidth	323
DispMgrWPageStyle	323
DispMgrX	324
DispMgrY	325
NumHistoryItems	325
ScaleDisplayContent	325
ShowUnlinkedIndicators	326
SiteDetailsWindowed	326
TitleLogoTarget	326
ToolBoxOn	327
ToolBoxTranslucent	327
Editing and Debugging Properties	327
Language	328
NoModal	328
NoOpChangeDialog	329
NVShowCheckFilesDlgCount	329
NVShowDialogs	329

OnTop	329
General Properties	329
AutoActivate	330
AutoStart	330
DisableGoToPage	330
DoNotStart	330
HideFromVAM	331
LocalScopeSyntax	331
SyncOEMLayers	332
VAMIcon	332
Internet Server and Client Properties	333
BrowserHeight	333
BrowserWidth	333
BrowserX	334
BrowserY	334
CloseSessionOnLogout	334
RealmAreasExcludeInvalid	334
RootNamespace	335
Logging & Reporting Properties	335
DiskFreeSpaceCheck	336
DiskFreeSpaceDrives	336
DiskPcentLogRestart	336
DiskPcentLogStop	336
FileListMax	337
HistorianBroadcastMaxSize	337
HistorianBroadcastMinInterval	337
HistorianConnectionRetryDelay	337
HistorianDataAgeSweepIntervalDivisor	337
HistorianDefaultArchiveInterval	337
HistorianFailoverInterval	338
HistorianWriteBufferMaxLength	338
HistorianWriteBufferMaxTimeDiff	338
LegacyHistoryPath	338

LogPath	338
SoapServicesRealmName	339
SQLQueryHideLegacyTables	340
SQLQueryHistoryNoOverridesTableName	340
SQLQueryHistoryNoOverridesTableSupportsTPP	340
SQLQueryTableTPPs	341
StorageLocation	341
StorageType	342
TraceUserConfigActions	342
UseLegacyHistoryPriorTo	342
Modem Manager Properties	342
AnswerCalls	344
CallInterval1 Through CallInterval10	344
CallOutDelay1	345
CallOutDelay2	345
CallOutPriority	345
CycleDelay	346
CycleLength	346
DataIdleTime	346
DialResetTime	346
DialWaitTime	347
GuardTone	347
HangUpDelay	347
HelloPacketLength	347
InitialDataDelay	348
InitModemsDisabled	348
MaxHandOffCount	348
MinModemsFree	348
MMCycleTime	349
MMLogDateFormat	349
MMLogLevel	349
MMLogTimeFormat	350
MMMaxQTime	350

MMRPCTimeout	350
MMUnAvailRetry	350
ModemAlarm	351
ModemAutoReset	351
ModemManagerLogSize	351
ModemMmaster	351
<ModemName>Device	352
<ModemName>Disabled	352
ModemRetries	352
ModemSpeechTO	352
ModemTCPIPPort	353
SiteRetries	353
SquelchDetectDelay	353
SquelchIdleTime	354
SquelchPacketLength	354
UseSerialAreaInModemCall	354
UseUnimodem	355
Port Properties	355
SerialShareSemaphore	355
SerPortDisconnectDelay	356
TCPIPPortMaxRcvLen	357
TCPIPPortMaxXmtLen	357
UseSerialAreaInModemCall	357
Mobile Browser Properties	358
ContainerTerm	358
EnableMobileMaps	358
IdleWebSessionTimeout	358
MobileBrowserAutoRefreshPeriod	359
MobileBrowserDisablePageGraphics	359
MobileBrowserSnapshotRefreshPeriod	359
MobilePageMaxRenderTime	359
Object Selection Marquee Properties	360
MarqueeDashColor	360

MarqueeSolidColor	360
MarqueeSpeed	360
Operator Logging Properties	360
OperatorLogArea	361
OperatorLogging	361
OperatorLogName	362
OperatorLogTemplate	362
Page Properties	363
AnalogInputWidth	364
DefaultPage	364
DefaultPageColor	364
DialogBGColor	364
DigitalInputWidth	365
DisableUSDialog	365
DOWidth	365
IODrawGap	365
IODrawHeight	366
MaxWinPage	366
OpaqueBackground	366
Page	366
PageButtonToolTipBalloonStyle	367
PageButtonToolTipDelay	367
PageButtonToolTipEnable	367
PageButtonToolTipFont	368
PageSnapshotCacheThresholdCount	368
PageSnapshotCacheThresholdPct	368
PageSnapshotsMaxInMemory	369
PageToolTipLabel	369
PopupCloseOnPageClose	369
PopupLimitAction	370
PopupPageLimit	371
ProgSpawnTitle	371
StretchBackground	371

TPPath	371
UseOldSiteDialog	372
Report Generation Properties	372
AnalogSummaryReportTimeUnits	373
DefaultEmailSubject	373
EmailServer	373
EmailSubject	373
ReportBrowseDir	373
ReportDateFormat	374
ReportOutputDir	374
ReportTempDir	374
ReportTemplateDir	374
ReportTimeZoneAware	374
ReportXPos	375
ReportXSize	375
ReportYPos	376
ReportYSize	376
ScreenReportsInExcel	376
StartOfWeek	377
Application Settings for RPC	377
ABSharedRPC	378
CIPENIPSharedRPC	378
DataradioSharedRPC	378
DDESharedRPC	378
DNP3SharedRPC	379
DriverSetupDelay	379
MDSSharedRPC	379
ModiconPortSharedRPC	379
ModiconSharedRPC	381
OmronSharedRPC	382
OPCClientSharedRPC	382
RemCfgTransLog	382
SiemensS7PortSharedRPC	382

SiemensS7SharedRPC	383
Security-Related Settings	383
AccountLockoutTime	386
AccountRateWindow	386
ADGroupPrefix	387
ADRefreshPeriod	387
AutoAddADUsers	387
AutoLogOff	387
AutoLogOffMax	388
AutoLogOffMin	388
ForcePasswordAltIdSync	388
GroupLogin	388
MaxFailedLoginAttempts	389
MaxRateFailedLoginAttempts	389
NameSpaceDelimiter	390
NoteAddRequiresAuthentication	391
OEMEncryptKey	391
PasswordDisplay	391
PasswordMinLen	392
PasswordTimeLimit	392
PasswordWarningTime	392
pcProxBaudRate	392
pcProxConnectCheckTO	392
pcProxDatabits	393
pcProxEnable	393
pcProxExcludePortx	393
pcProxParity	394
pcProxPortNum	394
PcProxPortScanHigh	395
pcProxPortScanLow	395
pcProxStopBits	395
PrivBitsTotal	395
PrivDescX	396

PromptForBadAltID	397
ReadOnlyStation	397
RootNamespace	397
SharedContexts	397
SharedSecurity	398
SysPrivDefault	398
SysPrivSuppress	398
UserName	399
Snap Grid Properties	399
GridColor	399
GridDense	400
GridShiftX	400
GridShiftY	400
GridVis	400
SnapOn	401
XGrid	401
YGrid	401
Tag Properties	402
AnalogControlName	403
AnalogScaledMaxDefault	403
AnalogScaledMinDefault	404
AnalogStatusName	404
AnalogUnscaledMaxDefault	404
AnalogUnscaledMinDefault	404
AreaExclude	404
AreaFilter	405
CanRedefineOEMType	405
DefaultAnalogDeadbandFractionOfFullScale	405
DefaultCalculationDeadbandFractionOfFullScale	406
DigitalControlName	406
DigitalStatusName	406
HelpFile	407
InvalidText	407

ParmChangedColor	408
ParmInfoCreatedByLabel	408
ParmInfoCreatedOnLabel	408
ParmInfoDateFormat	408
ParmInfoHistoryEnabled	408
ParmInfoLastModByLabel	409
ParmInfoLastModOnLabel	409
ParmInfoTimeFormat	409
PulseInName	409
ParmOverrideColor	410
RateOfChangeTagRPCInterval	410
RateOfChangeTagRPCThreshold	410
RememberNewTagParameters	410
SiteToolsConfirmOutput	411
SQLLoggerDefaultLogInterval	411
SQLLoggerDefaultMaxDataAge	411
SQLLoggerDefaultTagDataTableName	411
SQLLoggerDefaultTagIdTableName	411
SQLLoggerDeleteInterval	412
SQLLoggerDeleteOffset	412
SQLLoggerGroupSharedRPC	412
SQLLoggerLogInvalids	412
TagField1Name	412
TagField2Name	413
TagField3Name	413
Time Synchronization Manager Properties	413
TimeSyncEnable	414
TimeSyncMicroAdjust	414
TimeSyncRPCQMax	414
TimeSyncUpdtItrvl	414
Tooltip Properties	415
NoBalloonTips	415
ShowTip	415

TipBack	415
TipFore	416
TipOff	417
TipOn	417
Trending and Historical Data Viewer Properties	417
AITrendEnable	420
DITrendEnable	420
DontLogTrendPens	420
HDVAnalogAlarmsVisibility	421
HDVAnalogLegendAverage	421
HDVAnalogLegendDescription	421
HDVAnalogLegendHighScaleValue	422
HDVAnalogLegendLowScaleValue	422
HDVAnalogLegendMax	422
HDVAnalogLegendMin	422
HDVAnalogLegendValue	423
HDVAnalogPenAverageVisibility	423
HDVAnalogPenMinMaxVisibility	423
HDVAnalogPenScale	424
HDVAnalogPenStyle	424
HDVAnalogPenVisibility	424
HDVAnalogPenWidth	425
HDVAnalogScalesVisibility	425
HDVDataRetrievalMsg	425
HDVDataRetrievalMsgColor	425
HDVDataRetrievalWaitTime	425
HDVDateFormat1	426
HDVDateFormat2	426
HDVDigitalGridColor	426
HDVDigitalLegendAverage	426
HDVDigitalLegendDescription	427
HDVDigitalLegendHighScaleValue	427
HDVDigitalLegendLowScaleValue	427

HDVDigitalLegendMax	427
HDVDigitalLegendMin	428
HDVDigitalLegendNumberOfStarts	428
HDVDigitalLegendOnTime	428
HDVDigitalLegendValue	429
HDVDigitalPenStyle	429
HDVDigitalPenVisibility	429
HDVDigitalPenWidth	430
HDVDigitalScalesVisibility	430
HDVDisplayTimeSelectionScrollBar	430
HDVDisplayToolBar	430
HDVGridCellColor	431
HDVGridLineColor	431
HDVGridViewColor	431
HDVGridViewSortOrder	431
HDVHorizontalGridColor	431
HDVMaxNoteWindows	432
HDVPlotTextColor	432
HDVLayoutBGColor	432
HDVLayoutTextColor	432
HDVLegendVisible	432
HDVNotesLegendDescription	433
HDVNotesLineVisibility	433
HDVNotesPenStyle	433
HDVNotesPenVisibility	434
HDVNotesPenWidth	434
HDVPlotBGColor	434
HDVPlotViewColor	434
HDVShowAllScales	434
HDVShowTimeScales	435
HDVSimpleLegend	435
HDVTimeCursorColor	435
HDVTimeFormat1	435

HDVTimeFormat2	435
HDVVerticalGridColor	436
TrendOnTop	436
Wizard Engine Properties	436
WizardFinishText1	436
WizardFinishText2	437
WizardFinishText3	437
WizardFinishTitle	437
WizardWelcomeLabel	437
System Properties – Setup.ini	438
Setup.ini [APPS] Section Variables	440
Setup.ini [LABELS] Section Variables	441
Setup.ini [LAYER] Section Variables	441
AutoExportToUCDelay	442
AutoExportToUserCopy	443
AutomaticDeploy	443
AutoRecover	443
ConfigListBroadcastWait	443
NolconFile	443
RepositoryCommentDisable	443
RepositoryCommentMinLen	444
RepositoryShowCloneHistory	444
ScriptIconFile	444
SyncServAuditDeferTime	444
SyncServConnectTimeout	444
SyncServSyncTimeout	445
Setup.ini [LINKTOLERANCE-...] Section Variables	445
Setup.ini [OEM] Section Variables	446
HideVAM	447
HideWAM	447
NoSplash	448
OEMHelp	448
OEMPath	448

OEMRestrict	449
OEMVersionNum	449
Setup.ini [REMOTE] Section Variables	449
ClientCabPath	450
HTTPServerMaxHeaderLength	450
HTTPServerMaxHeaders	450
HTTPServerThreads	451
ManualVICServerLists	451
RefreshRate	451
VICMonitorLogFileName	451
Setup.ini [RPCManager-AllowIP] Section Variables	451
Setup.ini [RPCManager-ExcludeIP] Section Variables	452
Setup.ini [RPCMANAGER-NETPRIORITY] Section Variables	453
Setup.ini [SYSTEM] Section Variables	455
AccountsChangeDlgWait	456
ActivateProgressDelay	456
AutoLogon	456
CompileProgressDelay	457
ConvertProgressDelay	457
DbTraceDaysToPreserve	457
DbTraceFileSize	457
DialogServiceFailoutTime	458
EnableShowHide	458
ErrorLogFileName	458
HelpServerPath	458
HTTPAllow	459
HTTPDeny	459
LogOffUponHide	460
LowBatteryPercent	460
LowBatteryTime	460
MinAltIDLength	461
MobileSlippyMapTilesSource1	461
OrderlyShutdown	461

PrintWidth	462
QuickAddTypeGUID	462
ReloadWCProgressDelay	462
RememberLoginDuration	462
RepoClashWait	462
RPC Manager Properties	463
ShutdownOnLowBattery	464
SlippyMapRemoteTileSource1	464
TagNameDelimiter	464
UseXPCompatibleFont	465
VICAutoAddDebugTools	465
Setup.ini [Themes] Section Variables	465
Setup.ini [TRACE] Section Variables	465
TraceBrowser	466
TraceCM	466
TraceDispMgr	466
TraceDlg	467
TraceELM	467
TraceMenuEd	467
TraceModem	467
TraceNav	467
TracePageMgr	467
TracePLimit	468
TraceRamRecs	468
TraceRPC	468
TraceSQL	468
TraceSS	468
TraceTagCfg	468
TraceToFile	468
TraceTool	469
TraceVAM	469
Backups	470
ChangeSets – An Application in One File	472

Create a ChangeSet File	477
Apply a ChangeSet File	478
Create a Template ChangeSet	480
File Management Tools	481
Maintain the File Manifest	482
Import/Export Files	486
Import File Changes	489
Monitor...	492
Monitor Internet Client Connections	492
Data Logged by the Internet Client Monitor	496
Driver Statistics	497
ODBC Statistics	498
Secure Your Application	500
Best Practices for Security	503
Windows Security Integration	505
Enable Windows® Authentication	507
Windows Authentication Notes	509
Locating the Security Dialogs	513
Activate Security	515
Deactivate Security	517
Accounts and Roles	518
Create Accounts	521
Add Privileges to Accounts	528
Configure Alternate Identification	531
Built-In Roles	532
User Groups	534
Configure User Groups	536
Protect Pages and Output Tags	538
Add New Application Privileges	539
Restrict Access to a Page	541
Restrict Access to Output Controls	543
Rules for Privilege Scope	544
Example: Managing Complex Security	547

Options for Security Settings	549
Automatic Log-off Time Period	552
Password Options	552
Confirm Change to Password Options	553
Suppress or Reveal Privileges	554
Shared Security Between Applications	554
Read-Only Workstations	557
SSL Certificates for Internet Security	559
Generate a Request for an SSL Certificate	561
Process an SSL Certificate	564
Redundant SSL-Protected Servers	567
Technical Reference for Security	568
Proximity Card Readers	568
System Privilege Reference for Developers	569
Enabled Features of a Secured Application	582
Storage of Security Data and Configuration	583
Security-Related Settings	584
AccountLockoutTime	587
AccountRateWindow	587
ADGroupPrefix	588
ADRefreshPeriod	588
AutoAddADUsers	588
AutoLogOff	589
AutoLogOffMax	589
AutoLogOffMin	589
ForcePasswordAltIdSync	589
GroupLogin	590
MaxFailedLoginAttempts	590
MaxRateFailedLoginAttempts	591
NamespaceDelimiter	591
OEMEncryptKey	592
PasswordDisplay	592
PasswordMinLen	592

PasswordTimeLimit	592
PasswordWarningTime	593
pcProxBaudRate	593
pcProxConnectCheckTO	593
pcProxDatabits	593
pcProxEnable	593
pcProxExcludePortx	594
pcProxParity	594
pcProxPortNum	595
PcProxPortScanHigh	595
pcProxPortScanLow	595
pcProxStopBits	596
PrivBitsTotal	596
PrivDescX	597
PromptForBadAltID	597
ReadOnlyStation	597
RootNamespace	598
SecurityAlarmArea	598
SharedContexts	598
SharedSecurity	599
SysPrivDefault	599
SysPrivSuppress	599
UserName	600
Troubleshooting	601
Tooltips Do Not Appear	602
Generate a Crash Dump from the Source Debugger	602
Generate a Crash Dump from Windows Vista	603
Generate a Crash Dump with Windows 7 or Later	606
Use the Windows® Event Viewer	610
Adjusting the Virtual Address Space	611
Add Scroll Bars to a Page	613
Hardware Device Limited License – Cannot Connect to Device	614
Cloning a VTScada Workstation	615

VTScada as a Windows® Service	617
Service Installation	619
Accounts and Permissions	622
Service Command Line Reference	623
Service Error Dialogs	623
Index	626

Manage Applications

Intended audience: Developers & Managers who maintain existing VTScada applications. (Many management tools are also used when building an application.)

Topics include: Configuring how your application looks and works through the use of property values stored in configuration files. Maintaining a backup of the application and stored history. Securing the application. Monitoring the health of the application and the hardware that it is running. Troubleshooting techniques.

Also included in this section is information for distributing both the entire application and incremental updates. Running VTScada as a Windows® service. Using the VTScada Application Manager.

Contact Trihedral Engineering Limited

Our head office is located in Canada, on the shores of the Bedford Basin in Halifax, Nova Scotia.

Please contact your closest office or visit our website: <http://www.trihedral.com>, to learn more about how Trihedral can help you.

Trihedral Engineering Limited

1160 Bedford Highway, Suite 400

Bedford, Nova Scotia, Canada

B4A 1C1

Toll Free: (800) 463-2783

Telephone: (902) 835-1575

Facsimile: (902) 835-0369

Email: info@trihedral.com

Technical support: support@trihedral.com

Scotland office:

Glover Pavilion, Campus 3, Aberdeen Science Park

Balgownie Drive, Aberdeen, UK

AB22 8GW

Phone: +44 (0) 1224 258910

Facsimile: +44 (0) 1224 258911

Orlando, Florida office:

7380 Sand Lake Road, Suite 160,

Orlando, FL

32819

Phone: 1.407.888.8203

Facsimile: 1.407.888.8213

Calgary AB, Canada office:

Suite 505 - 888

4 Ave SW,

Calgary, AB,

T2P 0V2

Phone: 1.403.921.5199

What's New...

With each new release, Trihedral makes VTScada more powerful and at the same time, easier to use. Explore each category to learn what new features are available for you with VTScada version 11.2.

Note: If you have legacy applications that you want to run in the new version of VTScada, please take time to read the upgrade notes for

every version between what you had been running and the current version. Depending on how your application was created, you may need to take certain steps to ensure that it will continue to run.

New Features in VTScada 11.2:

Features for Operators and Developers:

New features in the alarm system include new tags, widgets, and more. All are covered in the following group:

Alarm System

New Alarm Page

Feature	The Alarm Page has a new look and many new features.
Benefit	<p>Increased usability including:</p> <ul style="list-style-type: none"> • Being able to sort and filter by nearly any property including messages. • View statistics for any alarm. • Customizable display for records using XML. • Advanced customization with display modules to represent alarm data any way you wish. • Limit the display to 10, 30 or 90 days to save time when loading. • Adjust the default display limit of 1000 items using the AlarmPageHistoryRecordLimit property.

Improved Alarm Priority Tag

Feature	Add symbols and text to the display configuration of all alarms having a given priority.
Benefit	The priority of each alarm is instantly identifiable,

using shape, color and a number or text.

Alarm symbol widgets

Feature	Alarm priorities are displayed using shape, color and text instead of simply color. These are included in alarm lists by default, and may be drawn on any page to indicate specific active alarms.
Benefit	Easier to recognize and respond to alarms.

New tag type: Alarm Database

Feature	Alarm Database Tags link alarms to Historians.
Benefits	<p>VTScada events, and user-created alarms use separate Alarm Databases. You can filter alarm lists to show the contents of all databases or just one selected database.</p> <p>Specify the Historian to be used by each alarm.</p> <p>Organize alarms into groups for display or security reasons.</p> <p>Boundaries between months are irrelevant when viewing alarm history.</p>

Alarm history is now stored using the VTScada Historian

Feature	Alarm databases write to an Historian rather than a separate alarm storage.
Benefit	<p>No more limits imposed by alarm files.</p> <p>Values are stored using UTC time stamps.</p> <p>Legacy applications will have their alarm history converted from local server time to UTC time.</p>

"Shelved" is no longer an alarm configuration property

Feature Shelving an alarm is an operational change, not a configuration property.

Benefit Encourages better adherence to standards for SCADA alarm systems.

Set a time limit for shelving or muting an alarm.

Feature Shelving or muting of alarms can be set to expire after a few minutes or hours.

Benefit Never worry about forgetting to re-enable the alarm notifications.

Require a note when operators acknowledge, shelve or unshelve an alarm.

Feature The Alarms page of the Application Configuration dialog includes options to force a note when acknowledging, shelving or unshelving an alarm. Minimum note lengths can also be specified.

Benefit Ensure that a record is kept of the reasons for operational actions in the Alarm Page.

Off-delay added to alarm definitions.

Feature An alarm with an off-delay will trip immediately, but will not return to the normal state until after the delay time, regardless of the triggering tag's value.

Benefit Similar to a deadband, but using time rather than value.

"Disable by design" available for all alarms

Feature Alarm configuration in Digital Status, Selector

Switch, Pump Status and Network Status tags updated to have the same options as other alarm configuration panels

Benefit All alarms can be configured to be disabled and enabled in response to operational conditions.

Add notes to alarm records

Feature A note can be added to any item in an alarm list.

Benefit Record why alarms happened or actions taken in response to the alarm.

New alarm reports

Feature Four new reports are available from the Alarms Page.

Benefit Look for "bad actors", identify alarm storms, review a history of alarm activation & trip events, or review numbers of alarms grouped by priority as you work towards ISA 18.2 compliance.

Confirmation required to acknowledge all

Feature The Acknowledge All and Acknowledge Shown tools now require that the operator confirm this action before proceeding.

Benefit Reduce the likelihood of accidentally acknowledging all alarms instead of the currently selected alarm. This feature is controlled by the property, Ack-AllRequiresConfirmation.

Create display groups for alarm databases

Feature	Use the new property AlarmDatabaseGroups to defined named groups of databases.
Benefit	Select the group name in the alarm page to view only alarms from the defined set of databases.

Fundamentals

VTScada Anywhere Client

Feature	A zero-footprint, JavaScript-based client for your VTScada applications.
Benefit	View and operate your applications in any of the major web browsers on any operating system.

Updated Select Type dialog in the Tag Browser

Feature	The Select Type dialog is now organized with tag groups and a list of recently-created tags.
Benefit	Makes it easier to find the type of tag you want to create, and provides more information about the differences between similar types.

Site lists retain your scroll position when returning to the page

Feature	Scroll though a long site list and then click to open the site page. Upon returning to the Sites List page, the list will still be scrolled to where you left it.
Benefit	Faster navigation in applications that have many sites.

Address the Memory() function in the Workstation Status driver

Feature	In an analog tag attached to the Workstation Status
----------------	---

driver, the address can now use an expression to call the Memory() function.

Benefit Measure (and log) the exact amount of memory being used by VTScada, not just the approximate number reported by the operating system.

Hide running applications.

Feature Applications can be hidden from view while running. Only authorized users may reveal the user interface.

Benefit For sites that support hosted systems, this can reduce visual clutter on the VTScada servers.

Faster retrieval of Historian data

Feature History retrieval is now significantly faster when processing data that was not logged in chronological order.

Add your own topics to the built-in help system

Feature Using an HTML template, and a bit of VTScada code, you can create your own topics with the VTScada help system and link those to pages or tags.

Benefit No need to buy a help authoring tool to generate CHM files. Your topics will become a part of the built-in help system.

Limited distribution for applications created or modified using an evaluation license.

Feature An application created or modified while using an evaluation license cannot be installed at a site that

	has a run-time license.
Solution	Create the ChangeSet for distribution at your properly-licensed development workstation.

The Idea Studio

Widgets that are set invisible no longer run at all

Feature	If a widget is given an opacity of zero, it both vanishes and stops working
Benefit	Previously, invisible widgets would still respond to a click. This is no longer the case.

Expanded list of photo-realistic meters

Feature	Nearly twice as many photo-realistic meters are now available.
Benefit	Greater flexibility when designing your user-interface.

Widgets to toggle polling

Feature	Two new widgets for Polling Drivers and Data Flow stations
Benefit	Operators can enable or disable polling using either a check box or a button.

Building your own meters

Feature	New scale and legend widgets have been provided and existing meter-part widgets have been updated.
Benefit	Easier to build your own photo-realistic meters. Use the scale and legend components for any custom widget you might want to create.

Rounded rectangles

- | | |
|----------------|---|
| Feature | The list of shapes has been expanded by the addition of rounded rectangles. |
| Benefit | An expanded list of tools for display building. |

Tag Configuration

Enable client data storage for Historian tags

- | | |
|----------------|---|
| Feature | For use with Historians that are storing alarm database information, this feature enables all client computers to store a local copy of the database. |
| Benefit | Enables isolated clients to modify the alarm system database and obtain alarm data from local storage. |
-

Persisted values across restarts for String I/O tags

- | | |
|----------------|---|
| Feature | A String I/O tag, configured for output and with the driver parameter cleared, will retain its value across application restarts. |
| Benefit | Useful for storing values within an application and for option selections from a list. |
-

Transaction Tag

- | | |
|----------------|--|
| Feature | Used to record a collection of historical values as a single transaction. |
| Benefit | These are useful for material-handling applications that must record transfers of custody. |
-

CIP Driver improvements

- | | |
|----------------|--|
| Feature | The CIP driver now reads the PLC tag configuration |
|----------------|--|
-

into memory before initiating reads.

Also, standard Allen Bradley addressing is now fully supported.

Benefit Enables polling of data by an index instead by PLC tag name resulting in faster performance.

More driver tags are standard with VTScada

Feature The following device drivers, previously available only by request, are now a standard part of every VTScada installation.

Benefit Nothing extra to install in order to communicate with devices compatible with:

Improved Roster Tag

Feature Roster callout types are disabled if the required device is not configured.
All roster configuration is disabled if no callout type is available.

Benefit Prevents the selection of a non-functional method for sending alarm notifications.

Context Tags Site Display – Display children only

Feature The Site Display list for Context tags now includes the option, "Only Display Child Tags".

Benefit Useful for context tags that exist only to organize sites, and should not themselves be shown in site lists.

Set a default zoom level in site tags

Manage Applications

Feature	Tags that can be displayed on a map (Context types, Polling Driver, Data Flow RTU drivers, and Station tags) can be assigned a default zoom level, to be used when mapped.
Benefit	Open a map to show as much or as little of the surroundings as you want.

Support for BCD8 addressing

Feature	Read BCD8 data using any driver. Write using the Modbus Compatible driver.
Benefit	Support for a wider range of devices.

Features for Programmers:

Coding Enhancements

RPC Timing Utility

Feature	The RPC timing utility can help you identify slow connections between servers, unintended IP addresses and servers that are being overloaded with RPC calls.
----------------	--

Easier to see tag names in the Source Debugger

Feature	If the value currently displayed in the Source Debugger is a tag, the name of that instance will be shown in parentheses after the value, and also in a tooltip.
----------------	--

Color Parameters in Widgets and Pages

Feature	Text parameters in widgets and pages can be given the modifier Color.
----------------	---

The properties dialog will then display a color selector rather than a text entry field for the parameter.

Trace Viewer Enhancements

Feature	The Trace Viewer will now indicate that a filter is active. New controls make it easier to add and clear filters.
----------------	--

Custom filtering of site lists

Feature	For those creating site tags from scratch, two callback modules may be added for custom filtering of the list and map: CustomSiteListGetSubTags and CustomSiteMapGetSubTags
----------------	---

Updated example for the Wizard Engine

Feature	A new example brings the Wizard Engine chapter up to date.
----------------	--

Functions

New or changed functions

 "." operator	Use instead of the "\" scope operator when the search should include only the local scope.
Droplist	The width will adjust automatically to show the longest string in the list.
GetUserSession	New parameter to control whether Invalid or the Display Manager's root session should be returned when a valid session is not found.
HistorianGetData	Historian data can be read in reverse chronological order

GetTagHistory	by specifying a negative value for the number of entries to be retrieved.
IsVicSession	New optional parameter, IsVICSession.
LocalScope	May be used as a shortcut for Scope(Obj, Name, TRUE).
Pack	An optional parameter can be added to allow structures to be packed more efficiently. At Pack-time, instead of storing a dictionary containing the structure definition a short name or number is stored as a key to the structure definition. The key is then used to look up the structure definition in a dictionary provided to Unpack.
SetInstanceRefBox	Programmatically, set the module reference box of a single module instance.
SetShelved	(Alarm Manager) Parameter list has changed completely.
UnPack	See notes for Pack.
WinComboCtrl	The width will adjust automatically to show the longest string in the list.
WindowOptions	Option 16 now also redirects vertical panning on Anywhere Client touch screens. New option 32 will redirect horizontal panning.

Deprecated functions

AlarmManager\Acknowledge
AlarmManager\Active
AlarmManager\Disable
AlarmManager\Enable
AlarmManager\Event
AlarmManager>ListAdd
AlarmManager>ListRemove

AlarmManager\Normal
AlarmManager\NormalTrip
AlarmManager\Popup
AlarmManager\OffNormal
AlarmManager\Register
AlarmManager\SetEnable
AlarmManager\Transaction
AlarmManager\Trip
AlarmManager\Unregister

Obsolete functions

AlarmManager\ActiveMonitor
AlarmManager\DoAcknowledge
AlarmManager\SetShelved
AlarmManager\ShelvedEvent
AlarmManager\StartSound

Properties

New or changed properties and settings

AlarmDatabaseGroups	Define groups of alarm databases to be viewed together in alarm lists.
AlarmDatabasePurgeDelay	It is possible to create orphaned alarms, especially if the tag database is modified outside VTScada. These are purged automatically upon startup, following a delay in seconds specified by this property.
AlarmDialerTemplate	New default:

	%T. %A %W %F %W %M.
AlarmDialerStatusTemplate	Alarm status is %S.
AlarmDisplayDateFormat	New default: 30
AlarmDisplayTimeFormat	New default: 5
AlarmEmailAckTemplate	Acknowledged %N
AlarmEmailAckSubjectTemplate	Acknowledged %A
AlarmEmailStatusTemplate	%NStatus: %S
AlarmEmailSubjectTemplate	The VTScada System: %A %P Priority Alarm
AlarmEmailTemplate	New default: %D %T%NArea: %A%NName: %F%NDesc: %M
AlarmPageHistoryRecordLimit	Maximum number of records to display in an alarm list.
AlarmPagerTemplate	New default: %D %T. %A. %F. %M.
AlarmPagerStatusTemplate	%S.
AlarmSMSTemplate	New default: %D %T%N%A%N%F%N%M
AlarmSMSStatusTemplate	%N%S
AlarmSMSAckTemplate	Acknowledged:%N%A%N%F%N%M
AlarmTemplateDateFmt	New default: 30
AlarmTemplateTimeFmt	New default: 5
AlarmEventDesc9 – 21	New alarm event descriptions added.
AlarmSnapshotCount	Maximum number of alarm events until the alarm database saves snapshots of their state
AlarmSnapshotInterval	Maximum time in seconds to wait until alarm database saves snapshots of their state
AlarmSpeechQuality	Now defaults to 6 instead of -1.

ApplyMuteSilencePerComputer	Controls whether the Mute and Silence controls of the Alarm Page affect only the current computer or whether the settings will affect all computers that the current user logs onto
ApplyMuteSilencePerUser	Controls whether the Mute and Silence controls of the Alarm Page affect only the current user (resetting when a new user logs on) or whether the settings will affect all users who subsequently log on at the current workstation.
NoteRequiredForAck, NoteMinLengthForAck	Require a note when alarms are acknowledged and set the minimum length of that note.
NoteRequiredForShelve, NoteMinLengthForShelve	Require a note when alarms are shelved and set the minimum length of that note.
NoteRequiredForUnshelve, NoteMinLengthForUnshelve	Require a note when alarms are unshelved and set the minimum length of that note.
MaxPagerMessage	New default: 256
MinShelveDuration	Minimum length of time in seconds, for which an operator may shelve an alarm.
MaxShelveDuration	Maximum length of time in seconds, for which an operator may shelve an alarm.
MinMuteDuration	Minimum length of time in seconds, for which an operator may mute an alarm.
MaxMuteDuration	Maximum length of time in seconds, for which an operator may mute an alarm.
OperatorLogTemplate	New default: ^C ^F ^O ^I ^N
RosterDelay	New default: 10

Obsolete properties and settings

AlarmAcknowledgePrint

AlarmActivePrint

AlarmDisablePrint

AlarmEnablePrint

AlarmEventPrint

AlarmListAddPrint

AlarmListRemovePrint

AlarmModifyPrint

AlarmNormalPrint

AlarmNormalTripPrint

AlarmOffNormalPrint

AlarmTripPrint

AlarmFileName

AlarmLogFreq

AlarmLogPath

AlarmMaxRec

AlarmPrintOn

AlarmRefreshRate

AlarmSendAllInfo

AlarmSpeechSetting

AlmMuteAllow

AlmSilenceAllow

AlmSilenceOnAck

AlmSrvLossArea

AlmSrvLossMessage

AlmSrvLossMsgAct

AlmSrvLossMsgNorm

AlmSrvLossMsgReg

AlmSrvLossOperator

AlmSrvLossPriority

DefaultDialerUser

PagerShowActiveCount
PhoneKeyFeedback
SecurityAlarmPriority
SkipLogonDialIn

New Features in VTScada 11.1:

Features for Operators and Developers:

Fundamentals

OPC Core Components

Feature	The latest version of OPC Core Components will be installed. Older versions will be removed during the VTScada installation.
Benefit	Avoids failures that can result when multiple OPC versions are installed.

Revision files to limit ChangeSet size

Feature	Create a Revision File on the remote computer, then use it when generating a ChangeSet intended to update that station.
Benefit	The ChangeSet being generated will not include older features, already present on the remote workstation. This can mean significantly smaller ChangeSet files.

Site by Site Control over Site Lists

Feature	Configure each site tag in your application to control how and whether it will be used in the site list
----------------	---

	of a Site page.
Benefit	Hide sites that should not be included. Control whether a click will drill into the site or open the Site Details page.

Analog Statistics and Digital Statistics in Site Lists

Feature	Analog Statistics tags and Digital Statistics tags can now be included as folders in the site list of the Sites page.
Benefit	View all collected statistics in a convenient format.

Run VTScada as a Service

Feature	VTScada can be run as either a service or as an interactive program
Benefit	May be used in environments where the security policy forbids leaving a logged-on Windows user on a server or workstation.

Operator Notes

Feature	Operator Notes have been completely redesigned, including a new user interface, advanced search features, a print-page option, and more. Historical Data Viewer notes also use this new feature, blending the Operator Notes page into the HDV display.
Benefit	Use notes for your log books. Find notes based on content, date or author. Add comments to older notes, but not change existing notes. View both Operator Notes and System Notes (created in the HDV) in one place.

Tag configuration on run-time licenses

Feature	Tag properties can be adjusted by anyone with the Tag Modify security privilege, even on run-time only workstations.
Benefit	Change I/O addresses, scaling values and other tag properties without delay.

ChangeSet improvements

Feature	ChangeSet file extensions now match their type (.ChangeSet, .Snapshot and .Template). The ChangeSet user interface has been updated.
Benefit	Greater clarity for the uses of ChangeSet files.

Control over pop-up pages

Feature	Using application properties, limit the number of pop-up pages that may be open at any time. Optionally, force all open pop-up pages to close when a new one opens.
Benefit	Avoid losing track of important dialog windows in a sea of open pages.

Improved Sites page navigation

Feature	The Sites page has been improved, with new tool buttons for modifying the appearance and with better use of theme colors.
Benefit	Easier to adjust and navigate.

Site-Details page: Confirmation prompts controlled by a new property

Feature	All output controls on a Site Details page will ask for confirmation or not, based on the property SiteToolsConfirmOutput.
Benefit	Change only a single variable to control all output controls in the Site Details page.

Automatic navigation to a page showing a new alarm

Feature	You can configure VTScada to automatically show a page where the tag related to a recently-activated alarm is displayed.
Benefit	Enables operators to see alarms in the context of the related equipment. If controls are provided to allow operators to deal with the cause of the alarm, then this feature can help the operator find those controls quickly.

Windows error reporting configured on installation

Feature	Proper configuration for obtaining crash-dumps is done automatically for you.
Benefit	Ensures that if something does go wrong, you'll have the files you need to get help from Trihedral's technical support team. We look after crash-dump configuration for you

Calendar control includes buttons to scroll year by year

Feature	Buttons have been added to the calendar control to allow you to step between years. Also, fields that accept a time value, such as report start and end times, now allow you to type directly into the fields rather than using scroll buttons.
----------------	--

Benefit Faster to find alarm history and notes, and to set the date range for reports.

Windows error reporting configured on installation

Feature Proper configuration for obtaining crash-dumps is done automatically for you.

Benefit Ensures that if something does go wrong, you'll have the files you need to get help from Trihedral's technical support team. We look after crash-dump configuration for you

CIP Driver Improvements

Feature Automatically attempts to reopen a channel after a period of no communication.
Enables the timeout to be set according to the CIP protocol's standard for calculating that value.
Improved handling of string values

Benefit Reduces the likelihood of a timeout after periods of no communication.

The Idea Studio

New selection options in the Tag Links panel

Feature Choose whether to show all widgets in the list, or only selected ones.

Benefit Easier to find the widgets you want to work with.

Site Alarm List Widget

Feature Draw an alarm list, filtered for children of the linked site.

Benefit Display a list of alarms occurring only in child tags of a site, or in tags with a matching area property.

String Entry Widget

Feature Provides a data-entry field for String I/O tags.

Benefit A data entry field that is optimized for text values. May also be used with Analog Input or Analog Control tags that are configured for text output

String Droplist Widget

Feature Provides a list of pre-configured output options for use with a String I/O tag.

Benefit A data entry selection droplist that is optimized for text values. May also be used with Analog Input or Analog Control tags that are configured for text output

Easier to use Frames

Feature The tools to apply color to a frame have been changed

Benefit Much easier to make your frames and folders look the way you want.

Alignment snaps

Feature Toggle alignment snaps off or on with a single button.
Fine-tune alignment snap settings.

Benefit Easier to use and easier to disable when not needed.

Right-click in a palette to open menu configuration options

Feature	A context menu has been added to the Idea Studio palettes.
Benefit	Edit the MenuItem tags that make up the palette, directly from the palette.

Live feedback from the color selection dialog

Feature	As you select colors in the dialog, the selected object updates in the Idea Studio.
Benefit	See how your colors will look on the page before making your selection.

Import entire folders of images in one step

Feature	Rather than import images one-at-a-time, you can now select several images to import, or import an entire folder of images.
Benefit	Expand the palette of images quickly and easily.

Count of tags linked to the current page

Feature	The Tag Links Panel of the Idea Studio now includes a count of tags linked to widgets on the current page.
Benefit	More information about your pages.

Tag Links Panel automatically includes all widgets

Feature	The Tag Links Panel shows all widgets on a page, not just selected ones. The same is true of the Search and Replace dialog.
Benefit	Faster editing.

Rotate and mirror images in widgets

Feature	Image formatting commands now apply to the images that make up a widget.
Benefit	Rotate, mirror, and otherwise reformat equipment, indicator light, and other widgets.

Multi-Image Widgets Panel

Feature	A new panel enables you to choose which images within a multi-image widget to change.
Benefit	Control over what to edit and what not to within a widget.

Several widgets updated to provide more options for configuration and control

Feature	<ul style="list-style-type: none">• The slider widget now enables the number of steps to be defined.• The appearance of the Note List Widget has been updated to reflect the new Operator Notes design.• A new widget, Add Note Field is available so that operators can create new notes without changing pages.• The droplist control and numeric entry widget now allow a confirmation dialog.• New default settings in the Image Change widget make it appear to work like a Style Tag-aware widget, without actually being linked to a Style Tag.• Text widgets (Numeric Value, etc.) have access to the Format ribbon, allowing complete control over their appearance.• Custom map icons no longer need to have a pulse beacon or site icon added. The functions provided by those items are now included automatically.
----------------	---

- Folders allow a parametrized Unique ID, allowing folders within a parametrized page to save the last tab viewed.
- The Numeric Entry widget now has a confirmation option and provides new control over its appearance.
- Option to link text to a parameter or widget within the text editor.

Benefit Greater control over the user-interface elements.

Tag Configuration

Configure Context tags to display as connectors between sites

Feature Draw a pipe or line between two sites by linking those sites to Context tags configured as connectors.

Benefit Lines or pipes that link to sites. The appearance can be configured, and since these are a feature of Context tags, you can add as many properties or child I/O tags as required to define and track characteristics of the connection. (Added with version 11.1.22)

Snapshot expressions replaced by parameter expressions

Feature Tag configuration expressions that can use Steady State, and update after tags have started.

Benefit Configure tag parameters using information obtained from hardware after I/O has begun.

Modbus Compatible Driver now supports Koyo addressing

Feature Use Koyo addresses for your I/O tags when connected to a Modbus Compatible Driver.

Manage Applications

Benefit Automatic, internal translation to standard Modbus addresses.

New tag: String I/O

Feature The String I/O tag can both read and write text values.

Benefit Provides direct support for text input or output. Padding can be added to enforce a minimum length, using extra spaces.

DNP3 driver enhanced

Feature Binary output now includes the option Select Before Operate(SBO).

Benefit Operate-type controls meet NERC standard CIP-002-1 R3.2

Calculation tags gain a built-in Historian connection

Feature New calculation tags will be logged by default, just as Analog Status tags are.

Benefit Eliminates the error of forgetting to add logging to your Calculation tags. A configurable deadband of 0.25% reduces the logging of system noise.

Defaults changed in Analog Statistics and Digital Statistics

Feature Default timespan choices for all statistics now include only "Last Hour" and "Today".

Benefit Less chance of creating excessive numbers of statistics tags.

Container tags can specify which of their children are listed in the Sites page

Feature	Filter the Sites page for any context or site to remove unneeded child tags.
Benefit	Site pages that include only the information that operators need to see.

Display-scaling parameters for Analog Status and Calculation tags

Feature	High and Low Scale values can be defined in these tags for display purposes.
Benefit	These scaling values set the default scale range for the HDV and various widgets, without affecting the tag's value. Note that the Engineering Units property moves to the Scaling tab from the I/O tab with this change.

Define analog scaling defaults in properties

Feature	Create your own default values for analog scaling.
Benefit	Preconfigure the default scaling values to match your system.

Enable Logging option for tags with built-in logging

Feature	Configure logging of Analog Status, Digital Status and Pump Status tags to be enabled or disabled according to conditions.
Benefit	Stop collecting data during equipment downtime or other events.

Define default deadband ranges for Analog Status and Calculation tags

Feature	Use application properties to define default dead-band values, as a percentage of the display scale.
Benefit	Avoid logging system noise in these automatically-logged tags. Explicit deadband values can still be set on a tag-by-tag basis.

OPC Client Driver no longer defaults to requesting an update each polling interval.

Feature	Data is updated only on a change of value or quality. Optionally, you may select the older method of polling the OPC server at the rate controlled by the attached I/O tag.
Benefit	Greatly reduced load on the OPC Server host.

Warning when attempting to attach a logger to a logged tag

Feature	When attempting to attach a logger to a tag that is already configured for logging, you will now see a warning message.
Benefit	Less chance of misconfiguring a system.

Show Communications and Show Statistics dialogs updated

Feature	For all drivers, the Show Comms and Show Stats dialogs have been updated to use a consistent look.
Benefit	Relevant information presented in a standardized format.

Alarm System

Alarm shelving

Feature	Disable alarm notifications without disabling an
----------------	--

	alarm. Events continue to be recorded in the alarm history.
Benefit	Perform system maintenance without distraction from alarms, but also without needing to disable those alarms.

Change to alarm roster behavior:

Feature	Prior to version 11.1.13, an alarm would continue to use the roster that was active when the alarm triggered, regardless of whether a roster change occurred before the alarm was acknowledged. Since 11.1.13, unacknowledged alarms will move to the active roster whenever a roster change occurs.
Benefit	Greater clarity for roster rules.

Alarm page – Acknowledge List replaces Acknowledge All

Feature	Acknowledge only the alarms shown in the filtered list.
Benefit	Do not acknowledge alarms other than those you intend to acknowledge.

Enable alarm notifications in the VIC title bar

Feature	Configure your VTScada Internet Clients to indicate alarms by a flashing indicator or title bar or both.
Benefit	Clear notification of alarms when other indicators may not be available.

Trending and Reports

ODBC interface supports parametrized queries

Feature	Parametrized queries can be sent to the optional VTScada ODBC interface. No extra configuration or programming is required.
Benefit	Greater compatibility with third-party ODBC query tools.

Plot from the Alarm page or the Tag Browser

Feature	From both the Tag Browser, and any alarm list, you can right-click on a tag in the list and open the Historical Data Viewer for the associated tag. (Subject to your security privileges, and the associated tag being part of the Trenders group.)
Benefit	Convenient for viewing a trend plot of a tag that triggered an alarm, or that is being examined in the Tag Browser. You may also select multiple tags in the Tag Browser before clicking the Plot button. All will be included in the trend graph.

Redesigned Historical Data Viewer

Feature	A completely new look for the Historical Data Viewer.
Benefit	The pen legend has been moved to the bottom of the viewer, leaving more room for wide graphs and allowing more information to be shown in the legend.

Expanded features for the HDV grid view

Feature	View raw, logged data in the HDV grid, or view any of average, minimum or maximum values for selec-
----------------	---

ted time periods within the grid.

Benefit Provides a powerful tool to gather and view information about your processes. Also, what is shown can be exported, providing a new way to send raw or processed data to a file for use in a report.

Hide tags in the trend window

Feature You can temporarily hide pens (tags) in the Historical Data Viewer by clicking an icon in the pen legend.
The pen properties dialog can now be opened either by a double-click on the pen legend, or via a new icon within each entry.

Benefit Easier to use the Historical Data Viewer.

Export to a single sheet

Feature When exporting multiple tags from the HDV, you can now choose to send that data to one worksheet / table / file, or to separate ones.

Benefit Easier to create reports using exported data.

New Draw HDV widget

Feature Draw a trend graph or grid on any page, showing selected child tags of a context or a previously-created pen group. You have complete control over the widget's appearance.

Benefit Monitor the history of selected tags on any page.

Value label within the plot

Feature The value of the selected pen, at the marker line, will be

shown in a new label.

Benefit View the value of a selected pen at the marker line location without needing to refer to the legend.

HDV tag selection dialog is resizable

Feature Change the width of the tag selection dialog as needed.

Benefit Easier to view long tag names.

Adjust HDV display properties in the Application Configuration dialog

Feature A new tab has been added to the Edit Properties page of the Application Configuration dialog.

Benefit Provides a convenient way to control colors and other display characteristics of the HDV and Operator Notes display pages.

Mobile client's trend view uses HDV pen properties

Feature The mobile browser's implementation of the HDV matches the thick client HDV.

Benefit Consistent scaling in both thick and thin client views.

Security

Windows Security Integration

Feature Log on to VTScada using your Windows account.

Benefit IT departments can manage a single account for their employees, instead of both a Windows account and a VTScada account.

Users can log in using a proximity card reader

Feature User accounts can be configured with an alternate ID, which is their swipe-card.

Benefit Log into your VTScada account the same way that you enter your secured building.

Lockout after consecutive failed logon attempts now time-sensitive

Feature A lower threshold is used for rapid logon attempts than for slower attempts, differentiating between an automated attack and a forgetful operator.

Benefit Operators get more logon attempts before their account is locked, without making it easier for an automated attack to succeed.

ODBC driver now honors Realm Area Filtering restrictions

Feature The ODBC manager will take Realm Area Filtering into account when SQL queries are made against the VTScada data store, rejecting requests for tag data outside the user's designated list of areas.

Benefit Increased security.

Internet Client and Mobile Browser

VTScada Internet Client for those who cannot run Internet Explorer®

Feature If connecting to the VTScada Internet Server with a browser other than Internet Explorer, you will now be given an option of downloading the stand-alone client, or using a mobile connection.

Benefit Never again see the message, "This feature is available only for Internet Explorer".

Features for Programmers:

Functions

New or changed functions

CIs	Returns from the list of obsolete functions. May be used on both workstations and internet clients.
SortArray	Sorts an array of arrays based upon the key information provided by the second parameter. The array is sorted in-place.
GetTagHistory	New parameter to enable all records to be returned in the case where two or more records have a matching time stamp.
ModifyBitmap	Set bit 1 of the Alias parameter to TRUE when feathering should not be applied to stretched images. New parameter: Rotation.
TextBox	New parameters allow highlighting of selected text within the TextBox.
SendMail	Added an optional parameter, Port, to be used to set the SMTP port number. The property SMTPPort will still be checked if this is not set, but is otherwise marked as deprecated.

Properties

New or changed properties and settings

AnalogScaledMaxDefault	Holds the default value for the maximum scaled value, corresponding to the maximum unscaled value as read from hardware.
AnalogScaledMinDefault	Holds the default value for the minimum scaled value, corresponding to the minimum unscaled value as read from hardware.
AnalogUnscaledMaxDefault	Holds the default value for the maximum unscaled value (raw equipment value) as read

	from hardware.
AnalogUnscaledMinDefault	Holds the default value for the minimum unscaled value (raw equipment value) as read from hardware.
DefaultAnalogDeadband-FractionOfFullScale	Set the default deadband for Analog Status tags as a percentage of the scale.
DefaultCalculationDeadband-FractionOfFullScale	Set the default deadband for Calculation tags as a percentage of the scale.
AccountRateWindow	The window of time, measured in seconds, used to distinguish between logon attempts made by a person and those made by an automated attack.
MaxFailedLoginAttempts	Changed to 25
MaxRateFailedLoginAttempts	Sets the number of times in a row that a user may attempt to log on with an incorrect password, and within the time span defined by AccountRateWindow, before being locked out of the system for AccountLockoutTime minutes.

General Programming Features

New properties for custom tag types:

ValueIsErrorStatus	Informs Indicator Light widgets that the associated System
ValueIsErrorAbove	Style tag's error-indicator colors should be used rather
ValueIsErrorBelow	than the digital status colors.

A module for custom tag types, which will be called whenever the tag stops

TagShutdown Module—If this subroutine is added to tags that you create from code, it will be called whenever the tag stops.

New Features in VTScada 11.0

Features for Operators and Developers:

Fundamentals

Windows XP no longer supported

Feature	VTScada version 11 will not function on operating systems older than Windows Vista / Server 2008.
Benefit	<p>Able to use and build on the full feature set of modern operating systems.</p> <p>Earlier versions of VTS are still available and supported for customers who must use Windows XP or older operating systems.</p> <p>The VTScada Internet Client for version 11 remains compatible with remote users running Windows XP.</p>

VTS is now VTScada

Feature	The VTScada layer has been fully merged into the core product.
Benefit	<p>All the features of VTScada are now available in all applications, ensuring that your application is not built with a reduced feature set.</p> <p>To avoid confusion with other products that use the letters "VTS" the product is now referred to as "VTScada" only. Where necessary for backward compatibility, some programming tools will continue to use the name, "VTS".</p> <p>A shell of the original VTScada layer still exists as "VTScada Legacy Layer" for use by legacy applications.</p>

Quick application setup

Feature	The first time you run VTScada, the Add New Application dialog will open automatically. The starting page is now the tiled page menu rather than Overview.
Benefit	Helps you start development work immediately.

ChangeSet improvements

Feature	Operators can double-click a ChangeSet file in Windows Explorer™ to start VTScada (if it isn't already running) and apply the file. ChangeSet files have a distinctive icon, to help you distinguish them from the VTS executable shortcut.
Benefit	Fewer steps are required. The ChangeSet will be used to create a new application, or will be applied to an existing application, as appropriate.

Commonly used application properties are easier to find

Feature	The Edit Properties page of the Application Configuration dialog has been redesigned so that commonly used properties are easy to find and change.
Benefit	No need to hunt through a long list to find the properties you use most often.

The ODBC driver now supports the Java® ODBC bridge

Feature	If your license includes the ODBC driver option, you can now query the VTScada log files and alarm history from Java applications.
Benefit	Expanded options for reporting.

The Idea Studio – Tools for drawing your application

The Idea Studio is a completely new development environment. Now, you can work on one (or many) pages, while the application continues to run in the background. The Configuration Toolbox has been replaced by palettes and context-sensitive ribbons.

Palettes for widgets, images and shapes

Feature	User-interface elements are kept in palettes that you can configure through the use of new menuitem tags.
Benefit	Widgets are tag animations. In earlier versions of VTS (VTScada) these were referred to as "drawing methods". The palette does more than provide a storage location for widgets, it also includes configuration options. For example, in the Equipment palette, all the pumps, motors and valves are actually a single widget, the Status Color Indicator, configured to show different images.

Alignment snaps

Feature	Alignment and spacing snaps that help you place new objects relative to existing ones.
Benefit	Easier to draw well-organized pages. Options are provided to let you enable or disable the snaps and to fine-tune the settings.

A customizable quick-access toolbar

Feature	Customize the toolbar at the top of the Idea Studio
Benefit	By placing often-used commands such as "Text" or the link to the Tag Browser at the top of the Idea Stu-

dio, you can access them with a single click instead of searching through menus.

A file menu for creating and organizing pages

Feature	The file menu, and the page tabs at the bottom of the Idea Studio, make it easy to work with pages and user-created widgets, adding new, opening existing, copying, deleting and editing properties.
Benefit	Easier to manage and work with your pages and user-created widgets.

Draw first, link to tags later

Feature	Sketch your application first, then link the graphic widgets to tags.
Benefit	Provides a way of building applications that many people find to be more intuitive. Those who are used to creating tags and then drawing them from the Tag Browser can continue to do so. Unlinked widgets are marked as such, ensuring that you never mistake simulated values for real values.

Tag Links panel

Feature	Search and replace links between tags and widgets
Benefit	Convenient for checking and changing links without needing to open the properties dialog of each widget. Use the Search and Replace dialog to change several links in one place.

Import images by dragging them to the palette

Feature	Drag an image from a Windows™ folder to your image palette.
Benefit	Easily expand the collection of images available for use.

New equipment and indicator widgets

Feature	Version 11 adds a wide range of equipment images that change color to match the state of the linked tag, LED readouts, LED meters, indicator lights, push-buttons, toggle switches and a new Draw HDV with multiple pens on any page.
Benefit	Create a modern-looking user interface.

Style Settings tags

Feature	Certain display conventions (red for "off" and green for "on", or vice-versa) can be configured in the new Style Settings tag. Widgets that use this tag need not be configured individually.
Benefit	Faster development and a consistent user-interface. If there are variations from one part of the application to another, multiple style settings tags can be created, one for each style. Style Settings tags do not count towards your license limit.

An improved tool for drawing pipes and lines

Feature	Lines and pipes are now represented by a path object.
Benefit	Better appearance, especially for pipes, which can

now have diagonal segments. Easier to edit.
If an older application is upgraded, existing pipes will remain as they were until they are edited. When edited, they will be replaced with the new paths.

Tiled images

Feature	Photo-realistic images can be tiled to create realistic backgrounds, etc.
Benefit	Improved screens, including water, bricks, metal and more.

Everything can have an opacity value

Feature	All shapes, images and widgets can be partially or completely transparent.
Benefit	More options for creating a better-looking the user interface.

Better images / gray-scale images

Feature	Many images in the palette have been replaced with updated versions. Also, now that there are improved tools for colorizing an image, images that had been duplicated in multiple colors are now provided in gray, allowing you to add whatever color you want.
Benefit	Create a modern-looking user interface.

Tags: New and Improved

Configuration tags do not count against your license limit

Feature	Your application can include an unlimited number of menu item tags, font tags, alarm tags (yes, alarm tags) and other types used for configuration. Only tags that perform I/O
----------------	--

are counted.

Benefit Easier to estimate your license needs and no penalty for configuration that is stored in a tag.

Redefine Type replaces Update Type in the Tag Browser

Feature The tool for changing a type definition in the Tag Browser has been improved.

Benefit Built-in VTScada types are protected from being accidentally redefined.

Context tags gain a Location tab

Feature A new tab in the Context tag's properties dialog helps you to add the settings required to make the tag work in a site map, including the ability to select a custom pin or open an alternative to the standard Site Draw page.

Benefit No need to search for the keywords required for a standard configuration task.

Warning when deleting tags linked to widgets

Feature If the tag you are deleting is linked to a widget (that is, drawn on any page) then you will be warned before delete operation finishes. You can click in the warning dialog to cancel the delete and open the Go To Page dialog, to review how the tag is being used and take appropriate action.

Benefit No chance of forgetting that a tag was in use you delete it.

Menus and Navigation

Menu Item tags

Feature	<p>The page menu is now managed using tags. The menu editor is no more.</p> <p>The palettes within the Idea Studio are also managed using menu tags.</p>
Benefit	<p>Having a common user interface for managing page menus and palette items will simplify development work.</p> <p>Menu Item tags do not count towards your license limit.</p>

Tiled menu

Feature	<p>In addition to the traditional text menu, there is now a tabbed menu – a grid of pages showing a live view of each. Recently visited pages are shown across the top of the screen.</p> <p>The tile menu shows live views of pages. Create a folder, add pages, then view the folder to see all the pages at once.</p>
Benefit	<p>Operators can quickly find the page they need using a preview rather than searching through text.</p> <p>Use folders to organize pages within the menu.</p>

View several pages on one screen

Feature	<p>The new tiled menu shows live previews of pages. Create a folder, put 2, 3, 4 or more pages within it, then simply view that folder in the tiled menu to see all the pages at once.</p>
Benefit	<p>View several screens at once without needing to buy multiple monitors.</p>

Note: in the tiled menu, pages are view-only. You must navigate to a single page before using operator controls.

Go To Page button

Feature	From both the Tag Browser, and any alarm list, you can right-click on a tag in the list and go immediately to any page that contains a widget linked to that tag. (Subject to your security privileges.) Note: You are advised to set security privileges on every page rather than rely on obscured navigation links to prevent unauthorized access to pages.
Benefit	View the tag's value in the context of operation.

The title logo is now a navigational tool

Feature	A click on the title logo opens a page of your choice. Defaults to the top-level tiled menu. Previous and Next buttons below the logo function like those in a web browser.
Benefit	Rapid navigation.

Pin often visited pages to the navigation bar

Feature	The open page is always shown as a button on the navigation bar. Click the pin icon in this button to create a permanent shortcut to this page. Reorder the pins as desired.
Benefit	Rapid navigation.

Limit the number of pop-up pages that can be open

Feature	Set a limit on how many pop-up pages may be
----------------	---

opened at once.

Define what will happen when an operator attempts to exceed this number.

Close all pop-up pages when the operator changes the main display page.

Benefit Avoid "lost" pages and improve system performance by preventing your operators leaving many pages open.

Trending and Reports

Control the order of tags in a report

Feature Sorting buttons have been added to the Reports page.

Benefit Organize the information in your reports the way you want.

Internet Client and Mobile Browser

View full application pages in the mobile browser

Feature When using the mobile internet client (MIC) you may choose to view pages the same way that they are shown in the VTScada Internet Client (VIC). The bandwidth-efficient option remains available.

Benefit The MIC is more powerful than ever before.

VTScada Internet Client for those who cannot run Internet Explorer®

Feature If connecting to the VTScada Internet Server with a browser other than Internet Explorer, you will now be given an option of downloading the stand-alone client, or using a mobile connection.

Benefit Never again see the message, "This feature is avail-

able only for Internet Explorer".

Features for Programmers:

Functions

Translucency in graphics functions

Feature	The GUI series of most graphics functions will now examine the Visibility parameter for a value between 0 and 1, using that parameter as an alpha setting.
Benefit	GUI-x graphics can now be translucent. Does not apply to Windows controls including WinButton, WinComboCtrl and WinEditCtrl.

New style bits in the Window() function

Feature	The Window function has three new style bits: Bit 21 is reserved. Bit 22 enables the window to be used as a target for items dragged from the palette. Bit 23 enables the window to serve as a palette. Bits 22 and 23 cannot both be set for a given window.
Benefit	Required by the drag & drop palette feature.

OLEDrag and OLEDrop

Feature	Call-back functions that you can add to enable drag & drop functionality in any window.
----------------	---

GUITransform: Options parameter now defined

Feature	If bit 1 of the Options parameter is set, this is considered a GUIStretch object.
----------------	---

If bit 2 is set, the transform may be dragged from palette to window.

Benefit Required by palettes and ribbons.

GetINIProperty has two new parameters

Feature Two optional parameters have been added to GetINIProperty.

Benefit Parameter 3 returns the comment that accompanies the property
 Parameter 4 returns "FALSE" if the property was not found.

Other new or updated functions

CaptureImage Creates an image handle from a GUIStretch operation.

NewGraphics Returns a code pointer to the selected graphic object or objects.

SaveImage Takes an image handle and saves it to an image file on disk.

PathDraw Draws a multi-segment line or pipe.

GUIText New option to exclude the top-most transform from being used with the scale factor. Enables proper scaling of text within a page.

DBListGet New filter (16) to check whether a specified bit has been set.
DBListSize

Properties

New or changed properties and settings

UseXPCompatibleFonts Obsolete.

AlarmNotifyEmailAcknowledge Controls whether a confirmation email is sent after acknowledging an alarm via email.

DispMgrFullScreen	Now defaults to 0.
DispMgrResizable	Now defaults to 1.
AlarmLogFreq	Defaults to (M). (Carried in from the deprecated VTScada legacy layer.) <i>Obsolete in 11.2</i>
Page	Defaults to the new PageMenuPage instead of Overview. (Tiled page menu.) In ScadaAce applications, the default page is SiteListWithMapPage(Invalid, "1", "15").
DialerLocation	The VTScada System ... except for ScadaAce applications, which use: The Scada Ace System
AnalogScaledMaxDefault	Holds the default value for the maximum scaled value, corresponding to the maximum unscaled value as read from hardware.
AnalogScaledMinDefault	Holds the default value for the minimum scaled value, corresponding to the minimum unscaled value as read from hardware.
AnalogUnscaledMaxDefault	Holds the default value for the maximum unscaled value (raw equipment value) as read from hardware.
AnalogUnscaledMinDefault	Holds the default value for the minimum unscaled value (raw equipment value) as read from hardware.

General

RGB colors now include an alpha (opacity) value

Feature	All colors that use RGB notation now accept an additional value, alpha. " <code><aaRRGGBB></code> ".
Benefit	Any object can be defined as partially transparent. Legacy applications with only RGB values, " <code><RRGGBB></code> ", will assume

an alpha value of FF (fully opaque).

SNMP Agent available to serve tag values over SNMP

Feature	The SNMP Agent can be configured serve tag values, configured for SNMP access, to a remote SNMP NMS client.
Benefit	Provides a new way to allow access to tag data.

Source files registered with WordPad™

Feature	If source files (*.SRC) are not already associated with an editor on your computer, then the VTScada installation will associate them to WordPad files. (WordPad is a trademark of Microsoft Ltd.)
Benefit	Easier for new users to access source code files.

New Features in VTS 10.2

Features for Developers & Operators:

Reports support Excel's Open XML format (10.2.09)

Feature	Reports written to the .XLS format have a limit of 256 columns. You may now specify the .XLSX format (if supported by your version of Excel) to create reports with up to 65535 columns.
Benefit	Reports can be generated for more than 256 tags at a time.

Comm Link Sequencer Tags (10.2.09)

Feature	Forces the serialization of requests from multiple devices that attempt to use the same port at the same time.
----------------	--

Manage Applications

Benefit	Ensures that communication will continue to flow when large numbers of devices that otherwise would not share a communication port without conflict are included your application.
----------------	--

Internet Server configuration – checks for conflicts (10.2.08)

Feature	When you are configuring a VTS Internet Server, a realm or a WAP server, VTS will check for other services that may already be using the port you assign.
Benefit	A warning dialog helps you avoid conflicts that will interfere with your server.

Site Details page updated (10.2.07)

Feature	Optimized for speed over VIC connections.
Benefit	Cleaner look and faster loading. Better organization of displayed I/O tag data.

New Frames (10.2.07)

Feature	New formats available when drawing a frame.
Benefit	Cleaner look and faster loading. This feature relates to the optimized Site Details page.

New security privilege – tag type update (10.2.07)

Feature	A new security privilege has been created – Tag Type Modify.
Benefit	Denied to all accounts by default. The ability to redefine types is both powerful and dangerous. By limiting access to this feature, managers can reduce the risk of accidental updates to tag type definitions.

Create your own map icons (10.2.06)

Feature	Use any shape you like, rather than marking site locations with a pin.
Benefit	Flexibility in how you locate your sites on a map.

Display text in the alarm list using the matching priority colors (10.2.06)

Feature	Set AlmListTextColor to invalid to cause messages to display using the alarm's priority.
Benefit	Restores an older feature to the alarm display list.

Option to open an exported tag file automatically (10.2.06)

Benefit	Save time when working with an exported tag file by having it open automatically.
----------------	---

ScadaAce layer added (10.2.05)

Feature	A new OEM layer has been added for the Motorola ScadaAce product.
Benefit	Build ScadaAce – based applications with only a few clicks. See: ScadaAce Applications.

Support added for SNMP v3 (10.2.05)

Feature	The SNMP driver now supports version three of the protocol.
Benefit	Improved security.

Site maps

Feature	Dynamic maps that show the location of sites having latitude and longitude properties.
Benefit	Operators can see station locations, and use the marking pins to open the associated Site Draw pages for those sta-

tions. Since maps are dynamic, the operators can easily change the display from one area of the city (state, country...) to another.

Site pages replace Station pages.

Feature	The automatically-generated station page, used with Polling Drivers and DataFlow RTU drivers has been replaced by the updated Site page.
Benefit	All the information operators are used to seeing still exists, but in an improved format. Additionally, a Site Map is built into each Site page.

Tag renaming

Feature	Tags now have both a display name (what you are used to seeing) and a unique ID.
Benefit	This enables you to move a tag from one context to another, and also to change the displayed name.

Updated process for working with tags and types in an external database

Feature	In both Import/Export Tags (now Sync/Export tags) and in the Manage Types pages of the Application Configuration menu, any import is followed by your choice of a fresh write to the external file (synchronizing it with the application's tag database), or by a deletion of the external file. Also: the exported tag database will now include all child tags defined as part of a type, allowing you to easily add or edit parameter overrides.
Benefit	Less chance of the exported tag database becoming out of sync with the internal tag database.

New types of tag: Motorola IP Gateway and Motorola ACE Driver

Feature VTS now provides native support for Motorola ACE RTU networks.

Benefit Expanded range possible applications for VTScada.

Select multiple tags in the Tag Browser

Feature You can now select more than one tag at a time in the tag browser for certain operations.

Benefit Faster to copy, enable/disable or delete when working with several tags.

TRUE color

Feature The color selector has been expanded to allow true color selection for all graphic objects.

Benefit Better looking applications.

Expanded scales in the Historical Data Viewer

Feature The HDV graph now shows intermediate scale values (configurable).

Benefit Easier to read values within the scale range.

DNP3 addressing – assist dialog

Feature An address assist dialog has been added to the DNP3 driver to help you configure addresses quickly and correctly.

Benefit Easier configuration with less chance for error.

Phoenix GSM/GPRS modem now supported by the SMS Appliance tag

Benefit Greater range of hardware support.

Station tags updated to include a Polling Sequence number (when used with a Polling driver).

Benefit	Improved organization of data in reports.
----------------	---

Improved installation

Benefit	Streamlined installation process with fewer prompts and more information.
----------------	---

Changes to display manager properties no longer require a restart.

Benefit	Most display manager properties can now be changed without requiring the application to be restarted.
----------------	---

Features for Programmers:

PIPListenerGroup Function (10.2.09)

Feature	A member of the P-Tools group (Dialog Library), this function draws a droplist of all available IP Listener Groups.
----------------	---

Benefit	To be used for custom drivers that can receive in-bound TCP or UDP messages.
----------------	--

Support added to read and write unsigned 32-bit integers

Feature	Functions that read or write buffers, files and streams now include a format option for 32-bit unsigned integers.
----------------	---

The Options parameter of GUITransform is now reserved, rather than required.

Feature	Existing code will not be affected by this change. New code can safely ignore the parameter.
----------------	--

BCC field added to the SendMail function

Feature	Code that calls SendMail directly may now include an optional list of BCC: email addresses. This feature is only available to code; it is not available in the user interface for configuring an email server.
----------------	--

Hierarchical accumulator

Feature	An module that you may use to create an accumulation (count) of any value associated with tags. You can then retrieve a count of that value for tags at and below a given parent in a tag hierarchy.
Benefit	The alarm manager now uses this to allow you to obtain (through code) a count of active or unacknowledged alarms within a site (or below any given tag in a hierarchy).

Programmatic support for 24bit/32bit true color

Feature	<p>Support has been added, and graphics-related functions modified, to allow true color graphics. RGB values may be entered in the form "<AARRGGBB>" using hexadecimal notation.</p> <p>Updated functions include:</p> <ul style="list-style-type: none">• VStatus. Option 10 now returns the background color as an RGB string rather than a palette index.• GetSystemColor. Now returns an RGB color string instead of a palette index.• PrtScr now prints in full, true-color mode rather than 256 colors.• All Z- and GUI- graphics functions that take color parameters have been updated where possible. ZPipe and GUIPipe are the two exceptions.• Other updated functions include Pen, PalStatus, Brush, MakeBitmap, WinEditControl, WinCom-
----------------	---

boControl and Window.

- The following functions have been removed. They will compile and compute parameters, but otherwise do nothing.
 - AnimateState
 - CollapseTree
 - DragState
 - HighlightedModule
 - HighlightState
 - HighlightTree
 - LastSelectedModule
 - LastSelectedState
 - ModuleCollapsed
 - Moduletree
 - ModuleTreeSize
 - MoveSelState
 - MoveSibling
 - MoveState
 - Palette
 - PickModule
 - PickState
 - ReadNum
 - ReadText
 - SelectStates
 - SetStateColor
 - ShadowTree
 - StateDiagram
 - StateHighlighted
- Palette colors 243, 247, 248, and 252 are now fixed, rather than allowed to follow the Windows theme.
- The Palette.pal file is obsolete.

Benefit An additional benefit is that printed outputs will now look much better than was possible with 256-color support.

Encrypt parameter values in your custom tag files

Feature When creating custom tags, you may define fields to be encrypted. This affects only how the values are stored on disk, not how they are displayed in VTScada.

Benefit Protect data from unauthorized access by persons who have access to your server, but not VTScada.

New Functions:

Feature The following functions have been added:

- DBInsert
- GetSessionContainer
- GetSessionContainerTags
- MapDraw
- ModifyTags (Use instead of StartTag for all new code)
- WatchForTagChanges

Related Information:

...Moving to the Current Version

Moving to the Current Version

Your VTScada license entitles you to upgrades for a period of time after purchase. (Maintaining a Support Plus contract provides unlimited upgrades.) You can find the end date of your paid upgrade period in the About dialog, accessible from the VTScada Application Manager. Each new version of VTScada introduces new tools and sometimes changes how older features work.

Notes:

Please review the lists of changes for each version of VTScada between the one you are upgrading from and the current one, to find additional tasks that you may need to perform.

In all cases, create a backup of your application before starting.

In general, it is better to install a new version on top of an older version.

General Upgrade Procedure:

In a networked system, upgrade one workstation at a time, starting with the primary server.

1. Shut down VTS/VTScada.
2. Run the installation program, installing to the existing folder.
3. Restart VTScada and run your application.
Confirm that the application runs as expected.
4. Proceed to the next workstation.

VTScada 11.2

- The updated SHA-256 signing certificate used for Trihedral drivers will be recognized by older Windows® operating systems, but they will not be able to save your response to the "Always trust content from Trihedral?" prompt. The question will be repeated during each installation.

This is a known problem with Windows 7 and Windows Server 2008 workstations. A hotfix is available from Microsoft at: <https://support.microsoft.com/en-us/kb/2921916>

- The IVONA voice engine is no longer supplied with VTScada. Customers who have this engine from earlier releases may continue to use it with version 11.2 and beyond. Your license will not expire.
- Wide Area Protocol (WAP) support has been removed from VTScada.
- CIP driver addressing has changed. All I/O tags with the older style, which used formatted bit addresses, must be manually reconfigured to use the new format. This is a one time only process.

Old system:

- a. Array Tags Of INT or DINT -> TagName[n][b]
- b. Array tags of BOOL -> TagName.n
- c. Simple tags of INT & DINT -> TagName[b]/BIT

New system

- a. Array Tags Of INT or DINT -> TagName[n].b
 - b. Array tags of BOOL -> TagName[n]
 - c. Simple tags of INT & DINT -> TagName.b
- Widgets that are invisible (Opacity == 0) no longer start. Some applications may have used invisible widgets to control the trend view that would open in response to a click in a certain area. That technique will no longer work. You can work around this by changing the opacity to an extremely small, but non-zero value for widgets that you do not want to see, but do want to continue to respond in the user-interface.
 - The following punctuation characters are now defined in the speech lexicon to be pronounced as if they were a space character. (That is, treated as a break between words.) Users may define alternate pronunciations, if desired.
_ @ # \$ % + = < > & / \ * ; |
 - Fonts with a weight less than four (4) will be extremely faint on an Anywhere client. Fonts with a weight greater than seven will be extremely dark. If using font weights less than four or greater than seven, you may need to adjust these for use with the Anywhere client.
 - The Alarm Manager module, SetShelved, has a new parameter list. All legacy code that used this function must be updated before being used in 11.2
 - Special handling for orange 241 and transparent black is no longer supported for .PNG format files. These colors will work as they always have for .BMP files.
 - The "." character now serves as the equivalent of Scope(, , TRUE). Thus, Obj.Value is equivalent to Scope(Obj, "Value", TRUE).

Note the following:

- When writing expressions, the "." character should now be used instead of the backslash operator when the intent is to reference a value that should be in the referenced scope.

- In earlier versions of VTScada, the "." character was legal within variable names. (No longer true.)
- To avoid problems that would occur if a legacy application with the "." character in variable names was loaded into version 11.2, the property declaration "LocalScopeSyntax = 0" will be added to Settings.Startup when those legacy applications are added to an 11.2 installation. This will prevent the "." character acting as a local scope operator in those applications.
- If you are certain that your legacy application does not contain variable names that include the "." character, you may set LocalScopeSyntax to 1 in order to make use of the "." character as a scope operator in new code.
- The AlarmManager server list is no longer used in 11.2. You should now use the SystemAlarmHistorian server list in its place.
- When you first start your legacy application in 11.2, VTScada will copy the "Default for Workstation" section of the AlarmManager server list into the server list of SystemAlarmHistorian. It does not copy the workstation-specific settings since they will probably not apply within the new paradigm. It is not necessary to have workstation-specific lists of servers now that Historian client-storage is enabled in the System Alarm Historian tag.
- For custom tags, the use of GetAlarmObjVal is now obsolete, as is the requirement to place multiple built-in alarms into their own submodules of the tag structure.
- Any overrides of Alarm Manager modules may continue to work, but should be tested thoroughly. As of version 11.2, the technique of overriding an Alarm Manager module to add extra functionality has been deprecated in favor of custom hooks.
- Several Alarm Manager functions are deprecated in favor of new functions and work-methods. Refer to the following in the VTScada Programmer's Guide and Function Reference:
 - Alarm Manager
 - Adding Alarms to Custom Tags
 - Alarm Functions

- Any custom code that is using “AlarmManager” as an RPC service name will no longer work. The AlarmManager no longer has its own service. This code should be updated to use “SystemAlarmHistorian” as the service name.
- For the sake of backward compatibility, \AlarmManager\ThisService remains but is now set equal to “SystemAlarmHistorian”. Similarly, \AlarmManager\RPCStatus is now a pointer to the SystemAlarmHistorian’s RPCStatus.

Alarm History Conversion:

The alarm and event history of your existing application must be converted to use the new alarms database, introduced with version 11.2.

Before starting the process, consider the following:

- The conversion must be run on an Alarm Manager Server.
 - If your application has not been configured with a server list for primary and backup servers, then you can and should run the process on the current workstation.
 - If your application does have primary and backup servers (and, possibly workstations that are not on the server list) then ensure that you are working on an Alarm Manager server.
 - You do not need to run the process on the current primary server, except that the primary server might have a more up-to-date list of alarms.
 - It is *not* a good idea to change the server list just before running the conversion as VTScada may take a few moments to transfer all records from the old primary to the new one.
 - To be sure of the server configuration, you may leave the conversion dialog open while you open the Application Properties dialog and review the information in the page, Edit Server Lists.
- Does your application require more AlarmDatabase tags?

Alarm and event history is now stored using the VTScada Historian. In part, AlarmDatabase tags link alarms to Historian tags. There are two main reasons why you might consider adding more:

- Security in applications that use Realm Area Filtering. If your alarms are linked to separate databases Realm Area Filtering can be applied to the database tags. Operators will be able to see only alarms in databases that they are permitted to see. This is not a requirement for Realm Area Filtering, merely a possible convenience. Realm Area Filtering rules still apply based on each tag's area.
- Efficiency in very large applications. The fewer alarms there are in a database, the faster the Alarm Page will load those alarms. This also results in smaller history sets, which means synchronizing and filtering will be faster.

If either of the above is true, then it is possible (but not necessary) that you may want extra Alarm Database tags. If neither is true, then do not add extra Alarm Database tags.

If adding new Alarm Database tags, note that the only method for linking alarms to databases is to make the alarm tag (or status tag containing an alarm) a child of the Alarm Database tag.

The Alarm DrawList widget is obsolete. Any custom code that used this widget must be replaced with the replacement Alarm List. The Alarm List can be extensively customized through code.

Obsolete Alarm Manager Variables

The following publicly-accessible variables within the Alarm Manager became obsolete as of VTScada version 11.2

General

DBSysVal	The current alarm database. This can be used to obtain information from the database using DBListGet and DBListSize.
CurrentServer	A text name indicating the workstation acting as the Alarm Manager server.

RPCStatus	The current RPC connection status; a value returned by the RPC Manager's Register subroutine.
Remote	Set to true when the alarm source is from a remote workstation. This workstation is not the Server.
BitmapDatabase	The object pointer to the Bitmap Database. This is where preloaded images are stored. (For more details, see the "Bitmap" keyword description above.)
ListChange	Value changes or can be changed to indicate a change in the database. It should be set to any valid value that is different from the current value.
AckAll	When set to a non-zero value, all unacknowledged alarms are acknowledged. AckAll is reset to zero after this takes place.
AckFilter	If set to a valid field filter, all alarms meeting the filter condition will be acknowledged. AckFilter is reset to invalid after this takes place.

Alarm Sounds

Silence	When true, alarm sound is turned off for the alarm generating a sound.
SoundPriority	The priority of the alarm generating a sound.
SoundAlarm	The object value of the alarm generating a sound.

Cycles The number of cycles for which to play tones (< 0 means continuous).

Record Configuration

FieldCount The number of fields in the alarm.

FieldNames The names of the fields.

FieldSizes The field sizes as defined for the Alarm Manager's database.

Filter Dialog Configuration

FilterCount The number of filters in the filter dialog

FilterName The text names for the filters

FilterIndex The field indices for the filters

VTScada 11.1

- For custom drivers, note that CoalesceRPC is obsolete and has been removed. DriverRPCOptimization should be used instead.
- If you are using LogNTEvent in custom code, and have been using "VTS" as the third parameter, you should revise this to use "VTScada" instead.
- If your application has an OEM layer that is marked, "Do not start", the upgrade process will hang. To avoid this problem, do the following:
 - Temporarily allow the OEM layer to be started, then start your application. This enables both the application and the OEM layer to be upgraded.
After the upgrade you may restore the Do not start property of the OEM layer.

Alternatively, you could skip the upgrade of the OEM layer by manually marking the OEM layer as having been upgraded. Do this by adding the property,

"MenuItemsAutoGenerated = 1" to the Application section of Settings.Dynamic. Note that one consequence of not upgrading the OEM layer is that custom images and widgets in that layer will not appear in the palette unless added manually at a later time.

- The ModifyBitmap function now uses a second bit in the Antialias parameter. Bit 1 controls whether feathering should be applied to stretched images that are also anti-aliased (bit 0 set to TRUE). You may need to set this parameter value to "3" when using ModifyBitmap to keep certain images from bleeding outside their bounding boxes.
- Improvements to the code underlying the Alarm Notification System have the following repercussions:
 - If your VTScada network includes workstations running versions prior to 11.1 and workstations running version 11.1 or later, then changes to the active roster will not be synchronized across that version divide.
 - If there is no Default area roster, alarms that do not have matching rosters will no longer call out using a randomly selected roster.
 - Support for the area, "GeneralAlarm", has been removed.
- Operator notes are transferred automatically to the new Operator Notes tag.
- If using the ODBC interface to perform SQL queries on VTScada data, note that new table structures with UTC timestamps are now available. Legacy tables still exist but are hidden by default using the property, SQLQueryHideLegacyTables.
- Custom modules for exporting tag data now require the parameter, DataMode, to be added after the TimePerPoint parameter.
- Calculation tags now have a built-in link to Historian tags. If your legacy system used Logger tags to record the value of Calculation tags, those loggers will still be present, even though the Calculation's configuration panel no longer shows them. Do not attach a Historian to a Calculation tag that is already being logged by a Logger tag.
- New calculation tags will have logging enabled by default. Existing calculation tags that were not previously logged will continue to not be logged until you decide to attach a Historian.

VTScada 11

- If you are running Microsoft Vista, and no text appears in the VAM, ensure that you have installed the platform update. See: [https://msdn.microsoft.com/en-us/library/windows/desktop/ee663867\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ee663867(v=vs.85).aspx)
- Windows XP™ is no longer supported. Version 11 requires features that are available only in more modern operating systems.
- The VTScada layer has been fully merged into the standard layer. The legacy VTScada layer still exists as a hidden layer, and will be used by legacy VTScada-based applications that are being updated to release 11. One widget (Duplexes) and one font (Notes) have not been merged into the standard layer, but can be found in the legacy layer if required.
- If you have an OEM layer, and if that layer has custom widgets (formerly called "drawing methods"), then you must run the OEM layer once in version 11 before running applications that use it. This will happen automatically, even if the OEM layer is flagged as "never run."
This is required to allow VTScada 11 to create menu item tags for the widgets, thus making them available within the palette.
The OEM layer should not be left running. When started automatically, it will also be stopped automatically.
- The Call-Out List Page is no longer included. Any page, of your own creation, may be used in its place. Legacy applications that have the Call-Out List page will continue to have that page when imported into VTScada 11.
- Many legacy images have been dropped from the palette in favor of modern images. The original image files are still included for the sake of backward compatibility.
- The Mobile Browser interface has several improvements, including the ability to show page graphics. With this new functionality, the mobile client is now licensed as being equivalent to a Internet Client (VIC) connection. Customers who need to limit page graphics in order to conserve bandwidth or server CPU may set the application property, MobileBrowser-DisablePageGraphics.
Existing customers who wish to continue using the older, limited mobile interface and its matching license calculation should contact Trihedral's Technical Support for relevant information.

- The Internet Client Monitor log is now stored in the file VICMonitorLog.txt, located in the installation folder instead of Log.txt located in the BrowserMon folder.
- Hand-coded, custom widgets may not look or work correctly until they have been opened in the Idea Studio.
Click the widget's Set Parameters button, within its Menu Item tag's configuration folder, then click OK.
The recommended method for defaulting the parameters of a custom-coded widget is to add default values to the parameters in the widget's .SRC code.
For example:

```
(
  MyParm = 100;
  AnotherParm = "Default Text";
)
```

Alternatively, a GetParmDefaults subroutine could be added to the widget, which will return an array of parameter defaults. An example follows:

```
<
===== CommandButton\GetParmDefaults
=====
{ Called to determine the default initial parameters for this widget.
}
{ Note - this module gets launched with Code as its parent object. }
=====
=====}
GetParmDefaults
[
  PROTECTED ParmDefaults { Array of parameter defaults to return };
]
Main [
  If 1;
  [
    { Get the parameter defaults that are used for existing (under-
    specified) widgets that lack some parameters. }
    ParmDefaults = ListVars(ParentModule(Self()), "*", 0, 0xFFFF,
    0b100 {parms}, 0, FALSE, 2 {defaults}, FALSE);
    { Fill in parameter values to be used with new widgets if they
    differ from the defaults for existing widgets. }
    ParmDefaults[#UseLegacyButtonStyle] = FALSE;
    Return(ParmDefaults);
  ]
]
{ End of CommandButton\GetParmDefaults }
>
```

- Pipes are no longer drawn as a separate function (GUIPipe). A variant of the Line (GUIPolygon) command is used instead. Pipes in legacy applications will

be converted automatically when either their color or their width is changed. Legacy pipes are not converted upon import, or when moved or re-aligned.

- The lexicon file, `Lexicon.vlx`, will not be copied from your older installation during the upgrade process. If you are installing to a new folder, and you have made changes to your lexicon that you want to keep, you must copy the file `Lexicon.vlx` from the old installation to the new.
- Four font files will be installed with VTScada, for use by widgets and built-in text styles. Review labels and titles in your application pages for scaling and alignment issues after upgrading to version 11.

The new fonts are:

- Open-Sans
 - Sansation
 - Crystal
 - Register
- The Gradient Color Change is deprecated. This was used to make pipes change color according to pump or valve state, but GUIPipes are no longer created.

To replace this feature, link the color property of the pipe (or any other object) to an expression that monitors the value of the tag that was monitored by the gradient color change. For example, given a digital status tag, "Motor1_Status" and a color that should be green when on, red when off, the expression would be: `[<Motor1_Status>] ? "<FF00FF00>" : "<FFFF0000>"`

- The `\Editing` flag is no longer used.
The flag has been replaced by `ParentWindow(Self)\Editing`. All scripts that used the former version must be updated.
- Since the toolbox has been replaced by ribbons, custom toolbox buttons are no longer available.
- The F11 / F12 key now opens the FindPage dialog in all applications.
- Custom driver code that used the group name, "VTScadaDriver" must now use the group name "LiftstationDrivers".
- Changes to default property values:
 - AnswerCalls – Now defaults to TRUE.
 - AlarmLogFreq – Now defaults to monthly.
 - OperatorNotesSecurity – Defaults to none.

- SiteRetries – Defaults to 3.
- ModemManagerLogSize – Defaults to 1000.
- AlarmEventDesc labels – Default labels are those used by VTScada rather than VTScada prior to version 11.
- The following properties are obsolete:
 - AlarmEventDescX
 - AlarmRevUnack
 - AlarmStateDesc0 through Alarm StateDesc5
 - AlmColumn1 through AlmColumn7
 - AlmDBArea
 - AlmDBHPUnits
 - AlmDBHPValue
 - AlmDBMessage
 - AlmDBPointName
 - AlmDBPriority
 - AlmDBTimeStamp
 - AlmDBStatus
 - AlmDBType
 - AlmHdg1 through AlmHdg7
 - AlmPgLineStyle
 - AlmTagsOnly
 - ClientAlarmSoundOn
 - Cycles
 - DataFlowModuleName
 - HTTPWAPport
 - ReportXPos
 - ReportYPos
 - ReportXSize
 - ReportYSize
 - TrendDuration

VTS 10.2

- The ability to rename tags has the following side-effect: The character "]" is no longer legal in a tag name. Existing tags that used this character will display using their immutable name rather than the short name. You can mitigate this by changing TagNameDelimiter in Setup.INI to use an alternative character. ">" is recommended. Short names will then have the form [ShortName> rather than [ShortName]
- GetSystemColor() and option 10 of VStatus() now return an RGB color string instead of a palette number. Custom code that uses this value as a number will need to be updated to use text instead. Code that simply passes the value to other VTS functions will continue to work.
- The following functions have been removed. Code using them will still compile, but the functions will do nothing.
 - AnimateState
 - CollapseTree
 - DragState
 - HighlightedModule
 - HighlightState
 - HighlightTree
 - LastSelectedModule
 - LastSelectedState
 - ModuleCollapsed
 - Moduletree
 - ModuleTreeSize
 - MoveSelState
 - MoveSibling
 - MoveState
 - Palette
 - PickModule
 - PickState
 - ReadNum
 - ReadText
 - SelectStates
 - SetStateColor

- ShadowTree
- StateDiagram
- StateHighlighted

VTS 10.1

- All users will be required to change their password upon first logging in. This is done to ensure that their credentials are stored using the newer encryption algorithm. Note that passwords are now case-sensitive.
- Tag names may not conflict with VTS function names. When starting an older application in version 10.1, any tags with conflicting names will fail to start and will be listed in an error message. If this occurs, your recourse depends on which version of VTS you are upgrading from. Please contact Tri-hedral technical support.
- Now that VTS includes Constructor and Destructor modules, any pre-existing modules that use those names should be re-named. Also, any code that uses the DBTrace Constructor API should be updated.
- Alternate identification has been decoupled from user-passwords and is now a distinct property that may be assigned to designated users.
- Tags in an OEM layer will now start in the dependent layer. You may draw and otherwise use the tags in the dependent layer, and may override tag parameters. If you would prefer that new applications based on your OEM layer have independent copies of tags from that layer, continue to use a Template.ChangeSet.
- Tags that you or a developer have created using VTS script code must contain a refresh module and that module must be called.
- In custom-coded tags, the statement, `Root = Self()` must occur before the call to `Refresh()`.
- Also in custom-coded tags; The expression `"Scope(\VTSDb, TagName)"` will still work if the custom tags are used in the same way that they had been. But, if you wish to use those tags in parent-child tag structures, include parameters that refer to tags that are not root-level tags, and wish to copy your tag to a new scope, then you must change the expression to read `"Scope (Root, TagName)"`.

- Page links, listed in the bottom navigation bar, will not be preserved when your application is upgraded to release 10.1
- With the release of version 10.1.06, the IVONA™ Salli voice (American English) replaces the IVONA Amy voice (British English). Customers who prefer the Amy voice may contact technical support for the required files.
- Since tag names now reflect the tag's position in a parent-child structure, full alarm names may become long. This is reflected in the change of AlarmKeySize to 256. The template alarm message length has been increased from 80 to 128 characters. Changes to the Alarm Manager are as follows. Note that, should you choose to set your own values for any of these applications properties, you should do so only after the application has been updated to version 10.1.

You will need to edit your Settings.Startup file for existing applications. For the change to take effect, the alarm manager (or, more simply, the entire application) must be re-started after you have made the edits.

- AlarmKeySize setting has been increased from 32 (and 64) to 256 in the VTS/VTScada templates.
- The template alarm message length has been increased from 80 to 128 characters.
- DBSystem can now re-size existing DB and LOG files when the Max Key or Text field sizes are changed.
- The AlarmManager can synchronize between servers with different values for AlarmKeySize or message size or both. In earlier versions of VTScada, these applications would fail to synchronize properly.
- Existing applications can modify the AlarmKeySize or alarm message size or both with only a restart required. This should always work when increasing the size(s), but might fail if attempting to decrease them should existing fields fail to fit in the decreased space.
- Code that called HideWAM must be changed to call the newer HideVAM instead. HideWAM is maintained for backward compatibility but is now used only at startup, to set the initial value of HideVAM.
- The use of the variable UserSession in a module to affect GetUserSession's behavior is no longer supported

VTS 10

- No more Config.INI, SecurityManager.INI, workstation.INI, etc.
Configuration variables are now stored in Settings.Startup (loaded only on application start) and Settings.Dynamic (able to be reloaded while an application is running). Also note that the term "configuration variables" has been dropped in favor of "application properties".
- User files are separate from working files.
The files located in an application's root directory and in the Pages directory are "user files". Developers may edit these files, but need to be aware that they must explicitly tell VTS to import the changed files before their edits become part of the working set.
Working files are under version control and are stored in a hidden system folder within the application directory. Any attempt to directly edit a working file will damage your application.
- Points.MDB is obsolete
Developers can export their tags to a Microsoft Access™ (or other) database, or to Excel™ for offline editing, and may import a tag database into an application. Within a working application, tag instances are now stored in a proprietary database format.
- In a networked application, all workstations must be running VTS 10. Remote configuration will not function across different versions.
- The LogManager service is obsolete
Log storage is now handled by Historian tags. These powerful tags allow you to optimize data logging for load balancing and automatic fail-over, even between multiple database storage systems such as Oracle™ and MsSQL Server™.
By default, Trihedral's own proprietary database format will be used for logging. Older applications upgraded to version 10 will automatically be assigned to a default Historian tag.
- Access to legacy tag history.
Data logging in VTS 10 is far more flexible and powerful than ever before. Because of fundamental changes to the way that logged data is stored, you must configure the application property, LegacyHistoryPath, to point to data logged while the application was running on an earlier version of VTScada.
- Application template directories are obsolete.

Template information is now stored within specialized ChangeSet files.

- Changes to the RateOfChange tag.
If you are using these tags, note that they must now reference a Source Tag that is configured for logging.
- The application property OEMRestrict is no longer supported on the VAM.
For networked applications, note that the RPCManager-Inhibits configuration section is now obsolete.
- If using the configuration file, RPCService.INI, this file will automatically be converted to the version 10 format, but you may need to re-enter your server lists.
- There is a Font compatibility issue when the VTS Internet Client (VIC) uses an older version of the Windows™ operating system than the one on the server. When running VTS 10 as a VTS Internet Server on Windows Vista/7/Server-2008, any VICs that are run on Windows XP/Server2003 or older will have many texts clipped. To avoid this, the server must be told to use old fonts by setting UseXPCompatibleFont to 1 in the System section of Setup.INI. If the server is XP/Server2003, the setting is not necessary.
- Configuration variables from Setup.INI are now read as the lowest priority settings for all applications. They will always be overridden by a matching property in the application's Settings.Startup or Settings.Dynamic.
- The following script applications are obsolete and are no longer included with VTS:
ResetRemoteClients DBConvert ODBCBrowse

VTS Programmers should note the following changes, which may affect their custom code.

- Config.INI sections have moved to Settings.Startup & Settings.Dynamic.
All application-level configuration files (those with names ending in .INI) have been replaced with the two files, Settings.Startup and Settings.Dynamic. Workstation-specific configuration files have been replaced by Workstation.Startup and Workstation.Dynamic in the WorkstationSettings folder of the application directory. See: Application Properties.
- StartTag has a new flag which, if set, will update the tag database. By default, this flag is not set. See: StartTag.
- If you have a custom tag type, ensure that the tag parameter metadata is in place. (This was not required in older versions and may not be present in

legacy applications.) See: Tag Configuration Parameters.

- The SecurityManager is now in the VAM layer and overrides to it will not take effect for VAM access to security.
- There is no longer a SecurityManager RPC service. All security accounts and settings are synchronized by the Configuration service.
- AppRoot.SRC replaces AppMod.SRC & AppMod.Web. The AppMod file in an application that is upgraded to release 10 will not be used, but will be retained for use if the application is converted back to an older version.
- In 9.1 and earlier, if you included any code for another module in the same source file as the Appmod.SRC, it would be used. Group modules were typically done this way. As of 10.0, the code for other modules must exist in a separate file other than AppRoot.SRC or they will be ignored without warning.
- Plugins that use default string values (as shown in the following example) will no longer work.

```
[ (POINTS)
  MyTag = "VarForGraphicsInMyTag";
]
```
- EditLockoutManager functions such as "MarkTagForEdit" are now obsolete. The distributed version control system replaces the Edit Lockout Manager. Any custom code that calls the EditLockoutManager will result in an error dialog.
- Libraries no longer combine code across layers and now only use the library at the highest defined layer. Widgets that link into libraries are not affected.
- Web services have a different interface on the script code side. Please see XMLProcessor, and other XML functions for details.
- ExternalValue is no longer supported in input tags.
- OEM code references to Logger, LogManager or LogObjVar need to be changed to use the Historian interface. Of special note is any code that waits for LogManager\Started. See: Historian Manager.
- Modules that are defined outside the scope of the application directory will need to be moved to within the application directory.
- Security Manager plug-ins only work when the application is running.
- Plugins that have references to variables in Code must be preceded by \Code.

- Template directories must be converted manually to template ChangeSets. See OEM Template ChangeSet for instructions.
- DSNName no longer exists as a variable in Code
- The Security Manager no longer supports OEMEncryptKey and Ser-EncryptOEM. These have been replaced by integrated higher level encryption.
- The Notebook tag's AddNote module interface has changed to support the new Historian.
- SelectObject and PSelectObject have new parameters, adding new options for your code.
- SQL module calls no longer allow writing to the default tag database.
- EditIni and EditIniCheckBox library widgets always update the RAM copy and ignore the "Update RAM Copy" parameter.
- RPCManager\Register no longer supports specifying a file name to read the server list from.
- RPCService.INI file contents have been transferred to Servers.RPC.
- ToolExt.INI has been changed to ToolExt.CSV
- WriteIni will first acquire the working copy lock and update the file asynchronously. Use Layer\RecordProperty instead.
- ReadIni does not acquire the working copy lock. It is better to use ReadPropertiesFile instead.
- LogFileName PLUGIN no longer supported.
- LogAlarm PLUGIN no longer supported.
- Files with the extensions of .DAT and .LOG that are accessed from custom code need to be moved to the DataPath directory and code modified to match.
- The default window title will now be the application name rather than "Display".
- Points.MDB is no longer the primary tag database.
- The RPC manager now uses the VTS IANA registered port, 5780 instead of 1160.
- The application property LegacyHistoryPath is required in order to access older data from upgraded legacy applications.

- The RPCManager-Inhibits configuration file section is no more.
- VTS Internet Servers on Vista with clients running XP will need to set the Tahoma font in their Setup.INI files.
- OEMRestrict is no longer supported on the VAM.
- Tag names that consist of only the period and space characters will no longer be considered valid.
- RPCService.INI files will not be converted to the version 10 format automatically. Server lists may need to be re-entered.
- Setup.INI variables are now read as the lowest priority settings for all applications.
- The script applications, ResetRemoteClients, DBConvert and ODBCBrowse no longer exist.
- After updating a legacy application to release 10 and compiling, a full re-compile under the previous version will be required in order to roll back to that version.
- Unless AutomaticDeploy is added to the Layer section of Config.INI prior to conversion, all local changes will be deployed automatically when the application is converted to version 10.
- Existing applications that use VTS as a DDE server and rely on the application window being called "Display" will need one of the following:
 - a) Declare DisplayManagerTitle = Display in Settings.Dynamic
 - b) Update the links to refer to the application name.
- VTScada's ODBC interface was modified to use ODBC3.0 drivers, which may cause changes in returned data types and SQLState return codes.
- Changes to the ODBCStatus function to take the ODBC handle to query for status. This is important to note as otherwise, you will just get the status of the last operation to complete which, given the concurrent nature, might not be the operation you have just executed.
- The following files are obsolete since the release of VTS version 10.
 - AlarmManager.INI -> now part of Settings.Dynamic
 - Config.DB
 - Config.INI -> replaced by Settings.Startup and Settings.Dynamic
 - GDI.WIF -> now part of Settings.Dynamic

- Menu.TXT & Menu2.TXT -> replaced by PageMenu.TXT
- Points.MDB -> replaced by a proprietary data storage system
- SCT.MDB - obsolete
- SecurityManager.INI -> now part of Settings.Dynamic
- Sync.WIF -> obsolete
- Workstation.INI -> replaced by Workstation.Dynamic
- ReportTags.GRP -> replaced by a proprietary data storage system.

Explore the Features of VTScada

You can use VTScada to create monitoring and control applications for water & wastewater, oil & gas, power generation, marine, broadcasting, food & beverage, manufacturing, airport solutions and many other industries. This cost-effective and easily-integrated SCADA solution includes everything you need for a fully-functional monitoring and control system.

VTScada's hardware independence and open connectivity features support all major programmable logic controllers (PLCs) and remote telemetry units (RTUs). Fifteen of the most commonly-used device drivers are included in every installation and many more are available from Trihedral on request.

Configuration is done online. As you build it, your application goes to work immediately. You also have the option of working independently on a second licensed server and deploying your changes only when you are ready. VTScada's distributed version control system enables you to undo configuration mistakes, selectively choosing individual configuration changes from a continuous history.

System Requirements

These VTScada 11 specifications are provided as a guide. Actual system requirements will depend upon your specific application architecture. Trihedral is happy to assist you with this choice. Contact us for recommendations for systems including Panel PCs.

More detail for hardware recommendations can be found on the Trihedral website: <https://www.trihedral.com/scada-system-requirements>

PC Requirements

- 32 or 64-bit version of Windows. (See following table.)
- 2GHz dual-core processor.
- 8GB of RAM.
- 20GB free hard drive space.

Trihedral recommends the use of NTFS formatting rather than FAT32.

FAT32 directories have limited file count capacity for long file names, which may interfere with VTScada's ability to create required files.

- DVD-ROM or BD-ROM drive, if installing from disk.
- A mouse, pointing device or touch screen.

Recommendations

- 64-bit versions of the Windows OS for all systems.
You can run 32-bit VTScada on 64-bit OS, and doing so is recommended for applications with fewer than 10,000 tags.
- 3GHz dual or quad core processors.
More cores won't help to increase performance, but higher clock speeds will.
- 16Gb or more of RAM for systems over 100K tags.
- Solid State Drives (SSD) for the highest performance.
- Avoid using RAID for file-based Historian.
- Keep historian on a separate hard drive from VTScada and the OS.
- Windows-compatible printer to print VTScada pages or reports.
- 100Mb/1Gb Ethernet required for networking.
- A voice modem is required for the VTScada Alarm Notification System to send voice phone notifications.
- An SMS Appliance is required for the VTScada Alarm Notification System to send text notifications.
- A connection to an email server is required for the VTScada Alarm Notification System to send email notifications.
- Sound card and speakers are required for alarm annunciation.

- RS-232 port if needed for communications with serial I/O devices.
- VTScada supports virtual servers. However, more than one VS on one computer, where one of them (i.e. VTScada) is mission critical, is not recommended

Compatible Operating Systems

VTScada Version	Win 10 32 & 64-Bit	Win 8.1 32 & 64-Bit	Win 8 32 & 64-Bit	Win 7 64-Bit	Win 7 32-Bit	Vista 64-Bit	Vista 32-Bit	Server 2012	Server 2008	Server 2008 R2	Server 2003	XP
8.X					✓		✓		✓	✓	✓	✓
9.X				✓	✓	✓	✓		✓	✓	✓	✓
10.X		✓	✓	✓	✓	✓	✓	✓	✓ ^{1.}	✓ ^{1.}	✓ ^{2.}	✓ ^{3.}
11.X	✓	✓	✓	✓	✓	✓	✓	✓	✓ ^{1.}	✓ ^{1.}		

Thin Client Requirements for PCs, Laptops, Smartphones, and Tablets

Requires at least one installed VTScada License to act as the server

Requires one or more concurrent VTScada Thin Client licenses

Windows Desktop/Laptop Systems running the VTScada Internet Client:

- Any networked computer running Windows Server 2003 or newer (no VTScada installation required)
- Launch using Internet Explorer (ensure ActiveX is enabled) using a web address (URL), or...
- Launch from your desktop using a small program downloaded once from your VTScada server via any browser

Other Operating Systems running the VTScada Mobile Internet Client:

- Network connection to a VTScada server
- HTML5-compliant web browser
- Recommended Browsers:
 - Safari® (OS X, iOS)
 - Chrome® (Windows®, iOS®, Android®)
 - Other examples of HTML5-compliant Browsers
 - Opera® (Windows®, iOS®, Android®)
 - Firefox® (Windows®, iOS®, Android®)
 - BlackBerry Browser® (BlackBerry OS®)
 - Internet Explorer Mobile® (Windows Mobile®)

Please Note

- NetDDE is not available on Windows Vista and higher. (It was removed in XP Service Pack II)
- VTScada 10 and higher uses IANA registered TCP/IP port 5780 (not 1160). Configure firewalls to route RPC traffic with that port.
- When reusing internal modems or sound cards ensure that new computers have the correct motherboard slots.
- Ensure 3rd-party software used with VTScada (e.g. accounting, reporting) is compatible with new OS.
- There are no drivers that allow A-Open modems to work with an OS newer than Vista.
- NetDDE is not available on Windows Vista and higher. (It was removed in XP Service Pack II)
- VTScada 10 and higher uses IANA registered TCP/IP port 5780 (not 1160). Configure firewalls to route RPC traffic with that port.
- When reusing internal modems or sound cards ensure that new computers have the correct motherboard slots.
- Ensure 3rd-party software used with VTScada (e.g. accounting, reporting) is compatible with new OS.
- There are no drivers that allow A-Open modems to work with an OS newer than Vista.
 - (1) Many computers running Server 2008 require speakers or audio cards to enable some VTScada Alarm Notification functionality. Manual modem and audio configuration may also be required.
 - (2) Server 2003 requires the following hot-fix to be installed: <http://support.microsoft.com/kb/938397>
 - (3) XP requires Service Pack 3 or higher.

VTScada can run multiple applications simultaneously, but you may need separate hardware for each application. For example, if each application includes the Alarm Notification System option, you will need a dedicated modem for each.

About...

General information about your VTScada license can be reviewed by opening the About box, which can be done from the VTScada Application

Manager:



From the resulting dialog, you can learn the version number of your installation, whether it is a 32-bit or 64-bit license, your serial number and the upgrade period covered by your license.

You can also see the number of tags allowed under your license(*) the number in use, and exactly which of the optional license features are enabled on your workstation.

(*) Only I/O tags count against your license usage.

Basic SCADA Features, Fully Integrated into VTScada

Integrated features reduce integration time and improve long-term reliability

VTScada eliminates the expense of buying, integrating and maintaining third-party add-ons. All mission-critical SCADA components built into the core product.

- Connections to components do not degrade over time
- Upgrading software version does not require re-integration
- Unlock optional components with just a license key number
- Native VTScada Polling Driver replaces expensive master PLC hardware

Out-of-the-box features

- **Advanced Polling Management** – Replaces expensive master PLC devices to poll remote sites. Group and schedule polling cycles for increased efficiency.
- **Full Redundancy** – Easily configure automatic failover to back-up servers, Internet servers and I/O links.
- **Historical Data Viewer** – Generate graphs or tables of historical data that you can annotate and export.
- **Alarms** – Sort or filter current, unacknowledged and historical alarms.

- **Rich Graphic Capabilities** – Photo-realistic meters, switches, animations, grouping, color and transparency adjustment and over 3,500 images.
- **Display Creation Tools** – Drag & drop tool set and object-oriented scripting language allow simple display creation and limitless customization.
- **Auto-generated SCADA Displays** – VTScada creates a display (with I/O and alarms) for each RTU.
- **Security** – Privilege-based user accounts control access to pages, work-stations, Internet clients and alarm notification system.
- **Report Generator** – Create custom or scheduled reports for the screen, printer, file, database or email, Excel or Excel templates.
- **Water/Wastewater Reports** – Daily total and derived flow, pump run-time discrepancy, communication error summaries.
- **Open Architecture** – Library of device drivers enables communication with most brands of PLC and RTU (e.g. S7 Ethernet & DNP3)
- **High-Efficiency Tag Development** – Special analog and digital tag types feature built-in alarms, logging and reports.

More:

- Rate-of-change tag – detects rapid changes in values that indicate expensive leaks and spills
- Trigger tag – initiates actions based on time or value changes
- Configure shutdown when Universal Power Supply runs low
- Configure alarms to re-arm after a defined period once they have been acknowledged

Alarm and Event Management

VTScada applications include an alarm page and alarm lists that can be added to any display.

When an alarm occurs, click the blinking icon at the top-right of the title bar to open the Alarm Page, where you can silence or acknowledge alarms.

Manage Applications

Time	Ack	Status	Area	Name	Description	Current Value	Setpoint	Units
2016-02-26 10:47:21	2	Alarm	Zone 1	Local TCP Port\\Tank 1\\Tank Level	Monitor tank level HIGH	99.9	90	%

The alarm page lists current, active, unacknowledged, disabled, and configured alarms. Sort by nearly any column and filter by any property. Alarm pages also provide a list of time-stamped events including log-on activity, Alarm Notification System activity, set-point changes and more. Remotely acknowledge alarms by touch-tone phone via the VTScada Alarm Notification System, by mobile phone via the SMS Appliance tag, or by smart phone or tablet via the mobile internet connection (MIC).

- Save an unlimited number of alarms and events
- Pop-up dialogs for high priority alarms
- Print any range of the alarm or event history
- Alarm tags built into Analog Status and Digital Status Tags
- Acknowledge alarms while configuring application
- Save an unlimited number of alarms and events
- Pop-up dialogs for high priority alarms
- Print any range of the alarm or event history

- Alarm tags built into Analog Status and Digital Status Tags
- Acknowledge alarms while configuring application

Alarm Notification System

This optional component requires a VTScada software license.

The VTScada Alarm Notification System™ ensures that your mission-critical alarm and process information is always as close as your cell phone, land line, email account, or SMS text messaging device.

Built-in is Better

Since it is a fully integrated component of VTScada, you can trust that it will remain tightly compatible as your monitoring and control system ages, unlike third-party 'bolt-on' dialer products.

Dial-in

To obtain status and alarm information for your telemetry devices over the phone, dial into your VTScada application and enter the same user name and password you use at a standard VTScada workstation.

Outgoing Alarms

Configure your system to automatically send you alarm notifications via text-to-voice phone calls, emails, pagers, and SMS text messages. As of version 10.1, authorized users can remotely acknowledge alarms via email and SMS text message.

Control Your System by Phone

Whether they dial in or receive an automated call, authorized users can use their phones to acknowledge alarms once VTScada has described them. Additionally, they can change system set points, start or stop pumps, or send digital commands to equipment.

Rosters Ensure Every Alarm is Acknowledged

Create rosters of up to 30 authorized personnel. In the event of an alarm, VTScada will call, text, or email each person in sequence until an

alarm is acknowledged or it is passed to another roster. You can configure rosters for entire applications or specific functional areas. There is no limit to number of rosters you can create.

Security

All changes made to security privileges in VTScada are immediately applied to the VTScada Alarm Notification System.

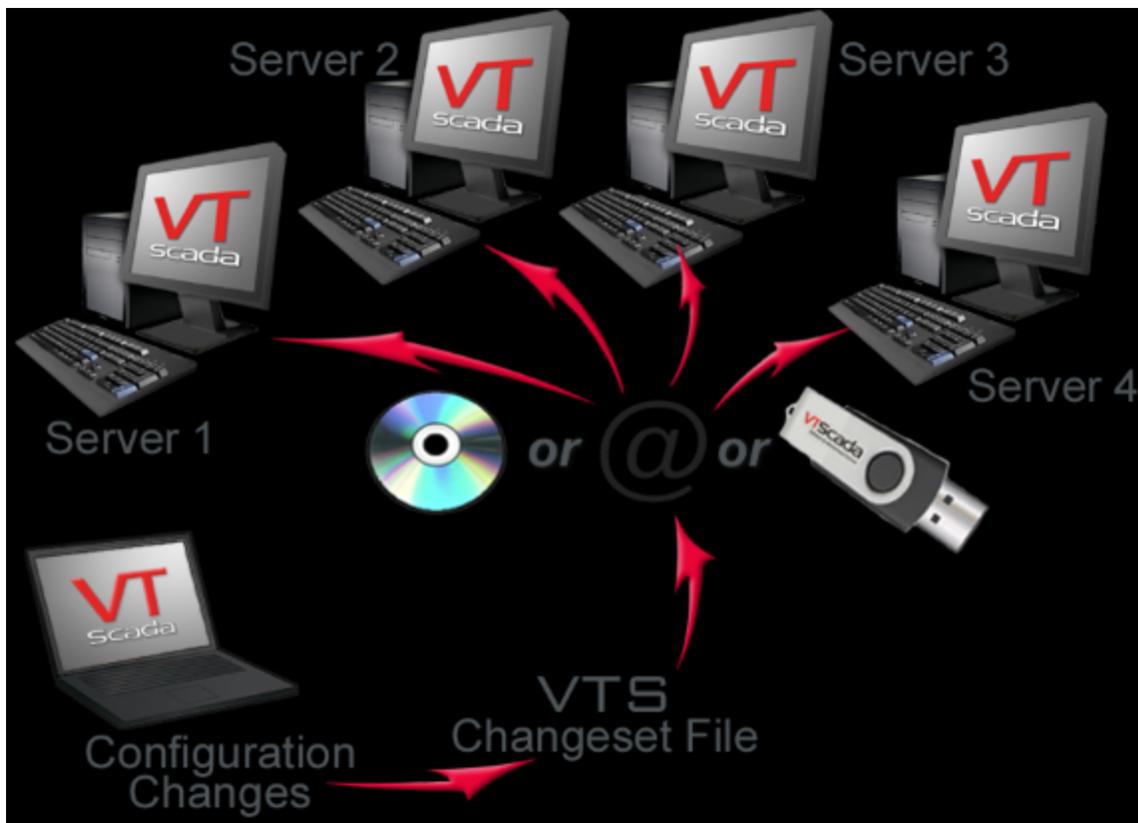
Advanced text-to-Speech Technology

VTScada takes advantage of the latest developments in text-to-speech technology.

Additional Information

- Acknowledge alarms via email and SMS text message
- Alarm messages can adjust for recipient's time zone
- Supports GZIP Encoding

Application Backup and Deployment



Distribute, update, clone or backup applications in a single file.

Introduced in version 10, VTScada ChangeSets help drastically reduce integration costs by allowing you to distribute new or updated applications to multiple computers with a single file. These files are easily created, distributed and imported into VTScada applications by staff with limited technical knowledge.

Roll out applications with a click.

Rolling out new or updated applications has never been easier. Simply double-click a VTScada ChangeSet file to start VTScada and import the entire application.

- Reuse work by cloning existing applications.
- Deliver ChangeSets by email, memory stick or CD.
- Backup/restore applications with complete version history.
- Update OEM layers without affecting end-user applications.
- Import ChangeSets without restart.

Instant Recovery From Problems**Recover quickly from unexpected effects of configuration**

VTScada's integrated distributed version control system records all configuration changes that anyone has ever made to your application. This log includes what changes were made, the time and date of the change, the name of the workstation, the name of the developer who was logged in, and when those changes were distributed to any other computers running the application. You can instantly undo any selected changes and distribute that update to all VTScada workstations without stopping the application.

- Instantly return to any past good version of the application
- Quickly trace problems back to their source

Manage Applications

View the version status of workstations

The current application version on each workstation is shown below.

Local modifications are shown in blue. Deployed versions older than the latest are shown in red/black. Selecting a workstation from the Workstations list will display the Version Log for that workstation.

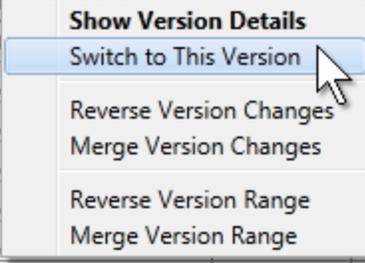
Right-clicking on a Version Log entry will allow you to display more detailed information about that version, reverse the changes from that version in your application or merge the changes from that version into the current version.

Workstations

Workstation	Last Update	Current Version
BARRY	Thu Oct 11, 2012, 14:46:18.462	CHRIS-D248
BLAIR	Tue Sep 24, 2013, 13:28:42.358	BLAIR-D982
BSINK	Mon Oct 01, 2012, 10:12:25.153	BSINK-D203
CARL	Fri Sep 27, 2013, 15:41:59.035	CARLW-D237
CHRIS	Mon Sep 30, 2013, 10:39:50.239	CHRIS-D551

Version Log for CHRISTOPHERL (Total of 1274 records in log)

Version	Time Applied	User	Comment
CHRIS-D551	Mon Sep 30, 2013 10:39:50.239	Logged Off	Setting MenuItemAuto
CHRIS-D550	Mon Sep 30, 2013 10:39:49.797	Logged Off	Application images, wic
CHRIS-D549	Mon Sep 30, 2013 10:39:49.797	Logged Off	Platform information cl
CARL-D237	Mon Sep 30, 2013 10:39:49.797	Logged Off	Import file changes: IO
CHRIS-D548	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.
CHRIS-D547	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.
CHRIS-D546	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.
CHRIS-D545	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.
CHRIS-D544	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.
CHRIS-D543	Sun Jun 09, 2013 14:20:38.089	Demo	Automated commit.



Seamless Full-System Fail-over

Avoid downtime with seamless failover of servers, Internet clients, historians, and I/O networks.

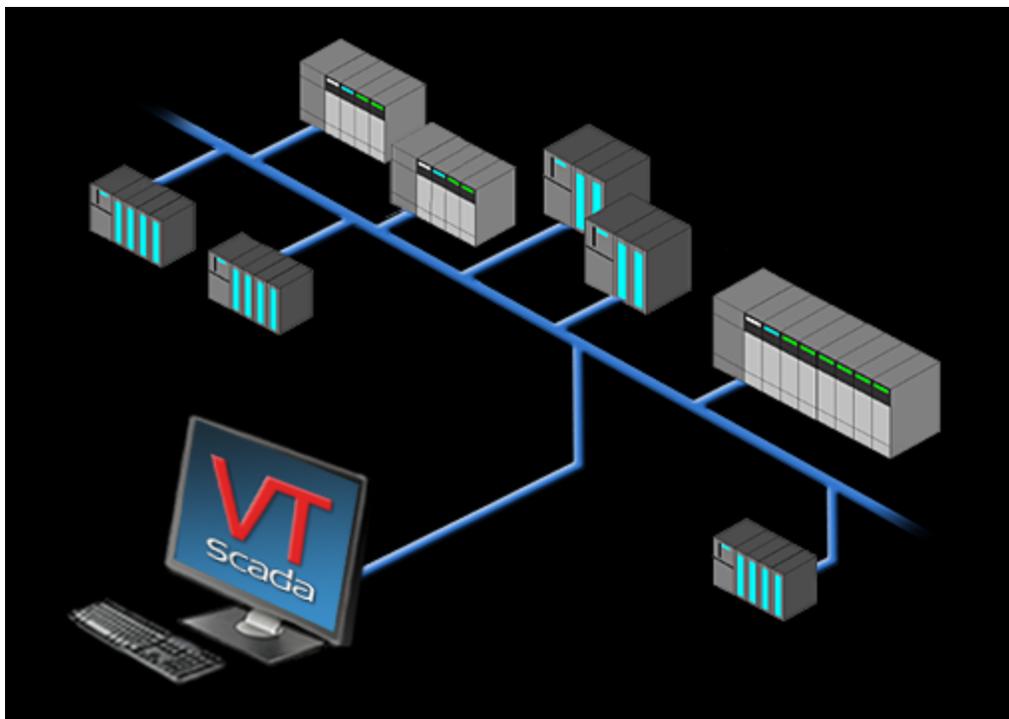
Only VTScada provides this level of system-wide redundancy.

- All workstations can also be backup servers (fewer servers)
- Automatically synchronize restored historians and alarms
- Distribute redundant historians in a variety of standard formats



Hardware Independence

VTScada provides maximum flexibility when choosing monitoring & control devices by supporting most industry standard and even many proprietary I/O protocols. New drivers can be created to meet your needs.



This spares you the expense of replacing existing PLCs, RTUs and pump controllers when the time comes to replace your HMI or SCADA central. Going forward, you are free to purchase hardware brands that best meet your needs and budget.

Direct drivers = less problems = lower integration costs

Other HMI/SCADA products require OPC and DDE Clients from 3rd party suppliers. VTScada provides built-in support for OPC and DDE.

Database Drivers

VTScada includes utilities and drivers that allow you to transfer historical data between VTScada and other software applications. Industry standard database drivers provide the means for 3rd-party applications to make direct data requests into VTScada historical databases. This is especially valuable when using statistical data analysis packages or 3rd party reporting packages.

- Over 100 industry standard protocols (i.e. Modbus, AB, Siemens, etc.).
- Supports Modbus Master/Slave.

- SNMP driver uses UDP-based protocol to speak to oil & gas or broadcasting devices.
- DataRadio diagnostics driver provides real-time signal strength and other diagnostic data.
- Over 100 industry standard protocols (i.e. Modbus, AB, Siemens, etc.).
- Supports Modbus Master/Slave.
- SNMP driver uses UDP-based protocol to speak to oil & gas or broadcasting devices.
- DataRadio diagnostics driver provides real-time signal strength and other diagnostic data.

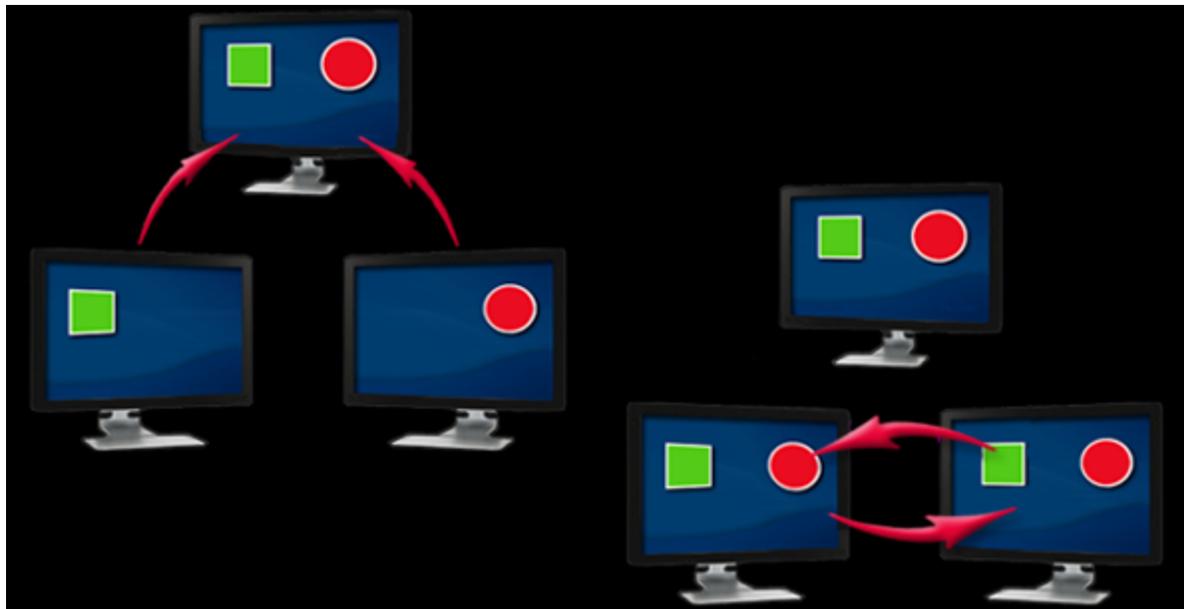
Real-Time, Online Configuration

Configure in real-time with real I/O.

Real-time configuration reduces downtime by allowing you to edit tags and displays (plus many source code and property changes) without restarting your application. VTScada enables multiple users to configure an application simultaneously without a configuration server.

Push changes system-wide without restarting.

Push changes to all networked computers manually or automatically. No application restart is required for most changes. You can even edit tags over VTScada Internet Clients.



Hierarchical Tag Browser

Tags are the building blocks of VTScada applications

Tags represent all application variables, from I/O data and alarms to modems and device drivers. This simplifies configuration and enables all application variables to be maintained in a single database that is tracked by the VTScada Version Control system.

Name	Description	Type	Address	Value
Energy	Pump 1 Energy	Context		
Fault Stats	Pump 1 Fault Stats	Context		
Faults	Pump 1 Faults	Context		
Flow Stats	Pump 1 Flow Stats	Context		
Run Time Stats	Pump 1 Run Times	Context		
Starts Stats	Pump 1 Starts	Context		

The hierarchical Tag Browser

Tags are created and managed using the VTScada Tag Browser. The unique design enables you to model how your real-world elements relate to one another by nesting child tags within parent tags. If you see a pump as an assembly of I/O and communications drivers, you can define it that way. If the pump is one of many in a lift station or other assembly, you can make it a child of the lift-station tag. Build tag structures once, then reuse them many times.

Clone whole subsystems by simply copying the root of a tree of tags. Tags copied to new parent automatically reference their new scope. The VTScada Context Tag makes it easy to group tags.

Get the most from your tag count

VTScada licenses are sold based on the number of I/O tags required by all applications running on a specific computer. If your VTScada SupportPlus Service contract is current, you can expand your tag count by simply paying the difference between the two licenses and entering an updated software key. If not, you will first need to renew it. In version 11, only I/O tags are included in this tag count. Now, include an unlimited number of menu items, fonts, alarms and any other configuration tag type.

Since version 10.2, you can re-name and reorganize tags without losing tag history, page references, or alarms. Multiple tag selection saves significant time when copying, enabling, disabling, or deleting more than one tag.

Edit Tags Outside of VTScada

To create and edit tags outside of VTScada, you can first export them to Access®, Excel®, and SQL Server® or any ODBC-compatible database. Then, once you perform the edits, you can re-import them. These changes are merged with the existing tag database and recorded by the version control system.

Other Rapid-development Features

- Special analog and digital tag types integrate alarming and logging ability to reduce development time.
- VTScada Pump Status Tags automatically associate with pre-configured pump status reports, displaying pump Run Times and starts/stops.
- Pump Status Tags include parameters for high and low alarms. Configure delays to reduce alarms due to minor disturbances.
- 'Log on change' is activated whenever a new tag is added. This helps reduce database size without losing important data.
- New I/O tags automatically flagged as 'Questionable' to assist commissioning.
- Supports unlimited number of tags. (According to your license.)
- Enter manual values for inputs to allow testing without live I/O.
- Quality indicators on input tags.
- Analog tags support deadband and delay when displaying change or triggering alarms.

IDEA Studio

Create Your SCADA Masterpiece

These features require a VTScada Full Development License.

The completely rebuilt VTScada Idea Studio™ helps you quickly develop professional-looking displays by putting the tools you need right where you would expect to find them. Clearly represent your process by dragging & dropping a wide variety of graphics, tag animations, polygons, switches, buttons and meters. Easily select, align and space any combination of elements. Draw or edit striking 3D pipes with just a few clicks. Divide system information logically across multiple pages that can be easily navigated by customizable menus, buttons and hotboxes.

Draw first; add tags later, or vice versa

Develop applications the way you want. If you like to lay out graphics first, you can do that. If you prefer to start by creating all your tags, you can do that too.

Draw with Data

To make it even easier to create high-impact displays, version 11 introduces over 200 ‘widgets’. Widgets are animations, used to display information about your system. Meters, numeric displays, clocks, buttons and custom alarm displays are all examples of widgets.

To add a widget, open a folder corresponding to the tag type you want to draw, drag the appropriate widget from the palette to the page, and then link the widget to the particular instance of the tag that it is to represent. You can even create your own widgets to represent equipment that is unique to your application. You can define widgets to be linked to one tag, or to complex tag groups having many child tags. These allow you to add complete new assemblies such as lift stations, in one step.

More Images and Symbols

The expanded VTScada Graphics Library now contains over 3,500 symbols and graphics. Easily search, sort, or browse to the image you need. You can even drag your own images right onto your displays from your desktop or documents.

TRUE Color SCADA

To help create vibrant looking displays and reports, VTScada now supports 24-bit/32-bit ‘true color’. Use the color selector to pick from more than 16 million colors. Script functions also support true color graphics.

Real-Time Configuration

Since this is VTScada, you can create and edit displays online and then push applied changes to all networked servers and thin-clients without restarting the application. While developing, you can easily switch between Run Time and Development modes.

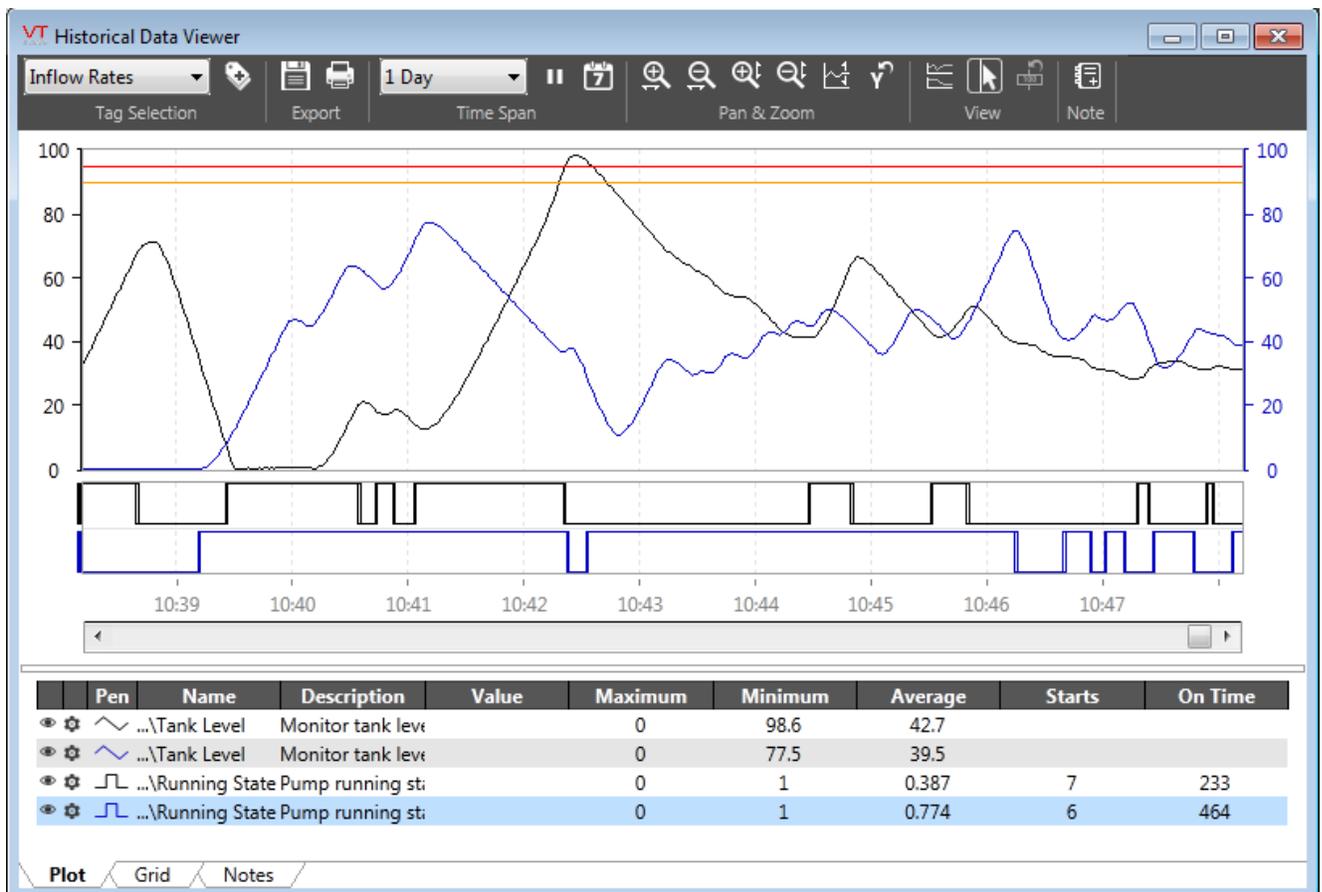
- Import BMP, JPG, WMF and EMF
- Photo-real meters, clocks, compasses, and HOA switches
- Draw grids of tags and their values
- Add nested frames, check-boxes, and tabbed folders.

Manage Applications

- Create reusable drawing objects by grouping multiple graphics and tags
- Import backgrounds, maps, watermarks
- Add 3D graphics created with 3rd party software (Must be flat jpg, png, bmp)

A Better Way to Display Trends

Historical Data Viewer (HDV)



Unlike other software products, VTScada provides a continuous view of both historical and real-time data in a single time-line that covers the entire lifespan of your application. See any number of analog or digital I/O values displayed together as a graph or table. You can also configure the HDV to display each value in its own graph. Add configured buttons to your pages so that operators can open the window with pre-loaded sets of tag values for specific periods.

Historical Data Wherever You Need it

The VTScada Historical Data Viewer (HDV) page can be found in the main menu of every application. You can also embed customized Historical Data Viewers in any user-created display page.

Operator Configurable Groups

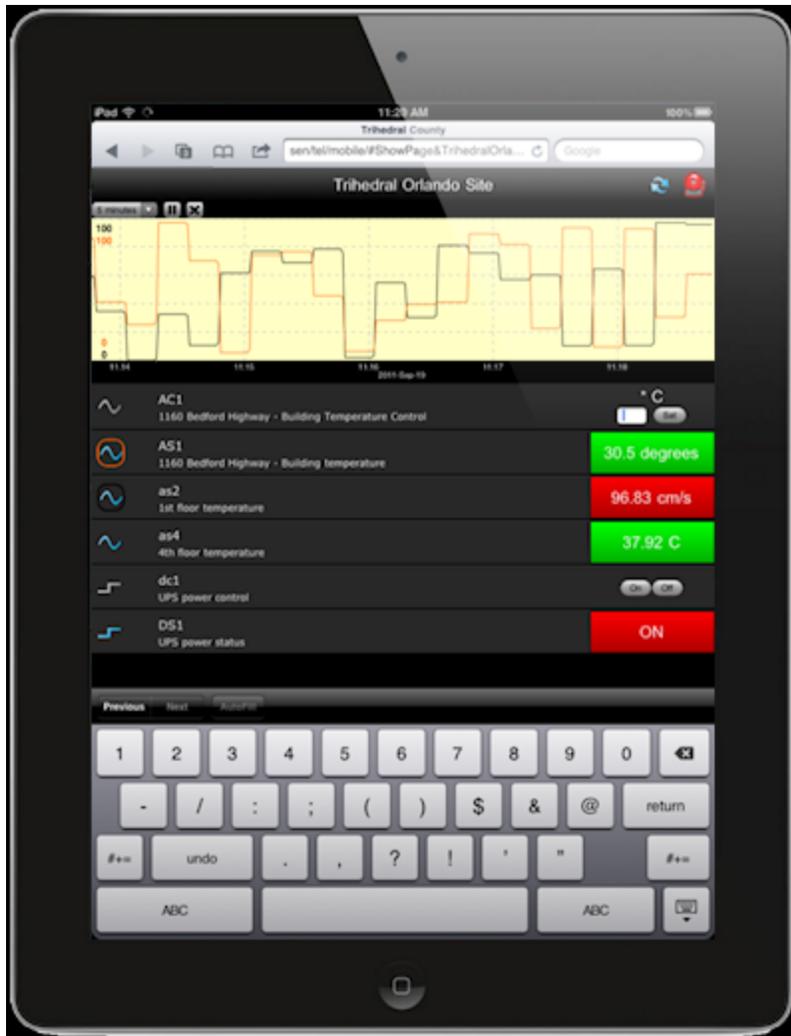
Click on any meter, readout or switch to open an HDV in a separate window. Add more values by clicking other tag-driven graphics or by using the simple tag picker. Once you have adjusted the color and thickness of each value, you can easily save them as a group for easy recall anytime.

Add Permanent Notes

Add encrypted operator notes to points on the time line to provide context for anomalous readings (i.e. faulty sensors, or maintenance).

The Mobile Historical Data Viewer

The optional VTScada Mobile Internet Client includes an integrated HDV that you can easily navigate with a swipe or pinch on your smart phone or tablet.



More Information

- Save groups of tags for later recall
- Easily export any range of data to a file or database
- Add encrypted operator notes to points on the time line
- Combine graphs or separate pens into individual windows
- Display full or minimal scales
- Displays min, max and average values
- Supports logarithmic scaling

Auto-Generated Operator Displays

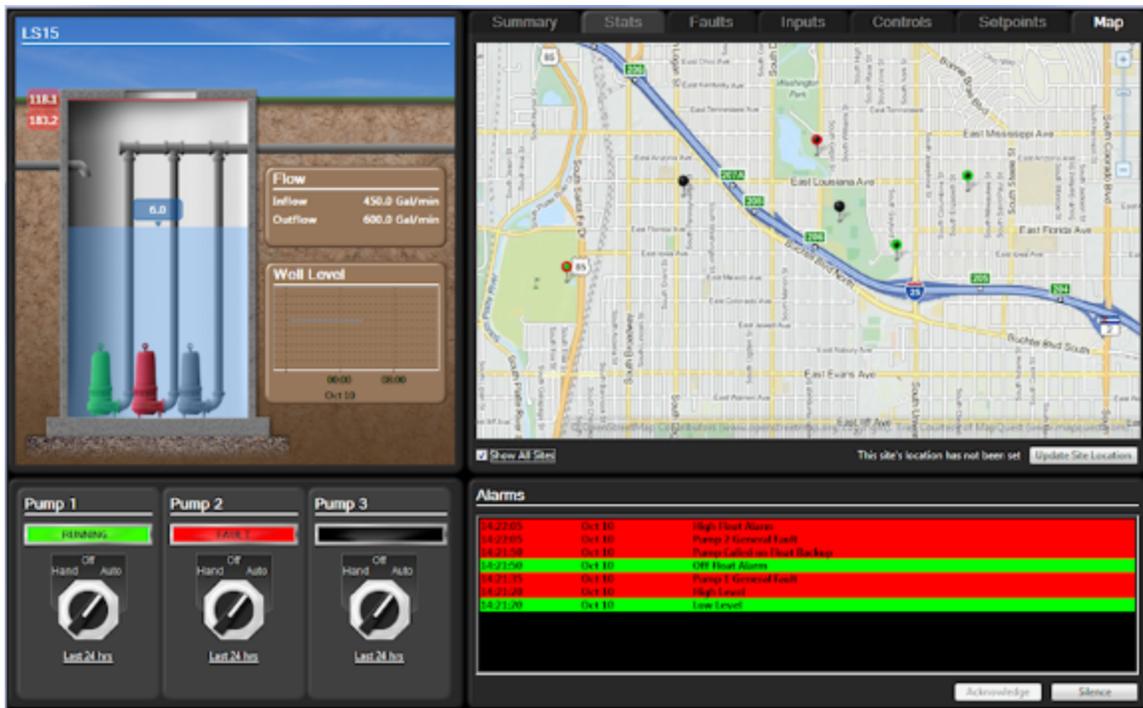
Add a new auto-generated lift station in seconds

Use the VTScada Context Tag to model how your lift station elements relate to each other in a hierarchical structure, then, draw all the elements at once using an attractive template.

- Templates for MultiTrode® MultiSmart® and MPE Pump Controller®
- New tools let you create and reuse your own templates

Application-specific displays pages provide an intuitive operator interface. These include graphical overviews of the process in a full-screen or windowed (user-selectable) view.

A Full Development license enables you to quickly develop displays using objects from the graphics library, tag animations, polygons, etc.





Displays

- Real-time display development.
- Supports unlimited number of display pages.
- Auto-generated display menu, which you can edit as you need.
- Dual and quad monitor support.
- Integrated display navigation.

Graphics

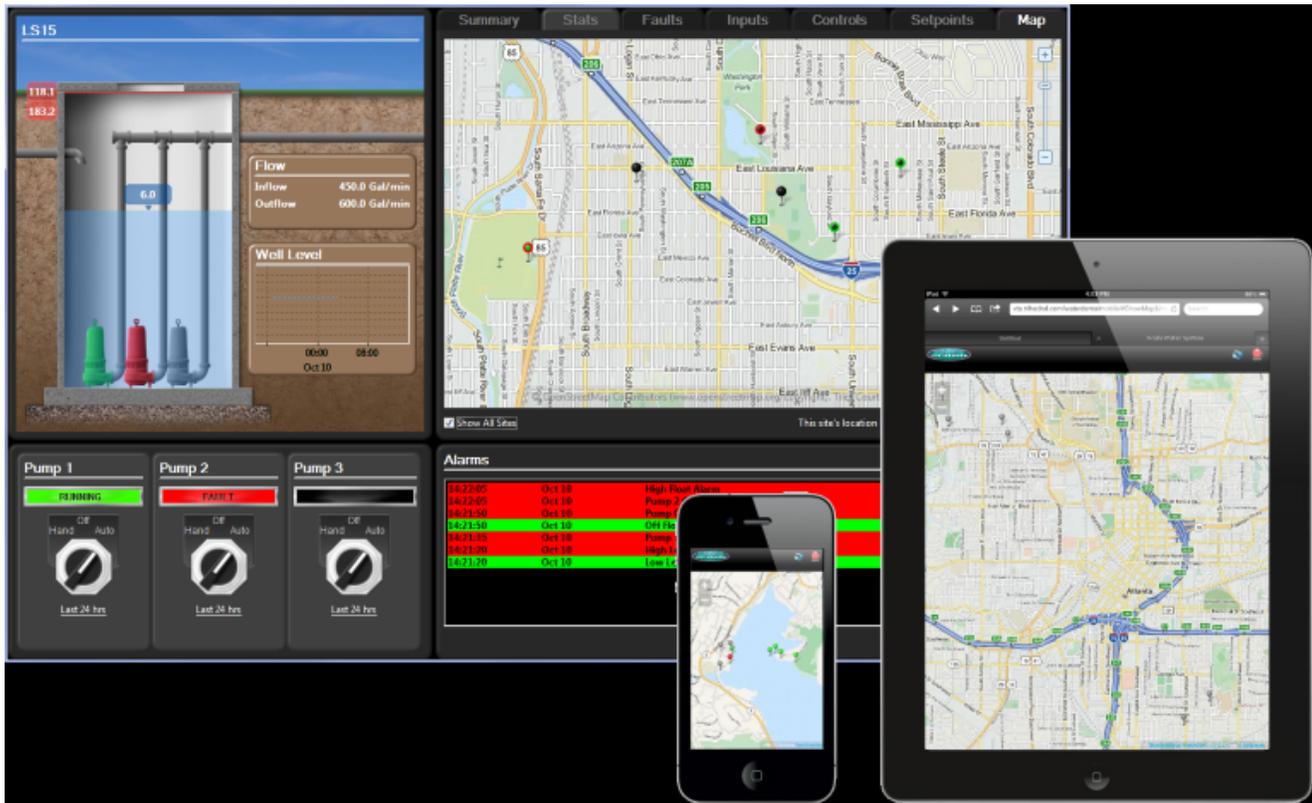
- Photorealistic meter library.
- 3500+ graphic objects library, that can be expanded without limit.
- Adjust color, hue, saturation and transparency of graphic objects.
- Group simple graphics and tags into complex reusable objects such as pump-ing stations.
- Import 3D graphics created with 3rd-party graphics products.
- Supports BMP, JPG, WMF, EMF, TIF and PNG.

- Integrated animation library.
- Supports background graphics such as maps or watermarks.

Slippy Maps

Put Your SCADA System on the Map

Interact with your remote monitoring sites in the same way you use on-line mapping tools like MapQuest®. Pan and zoom across all your sites with a simple click, toss, or scroll. Add dynamic maps to any graphic display or use the standard map pages.



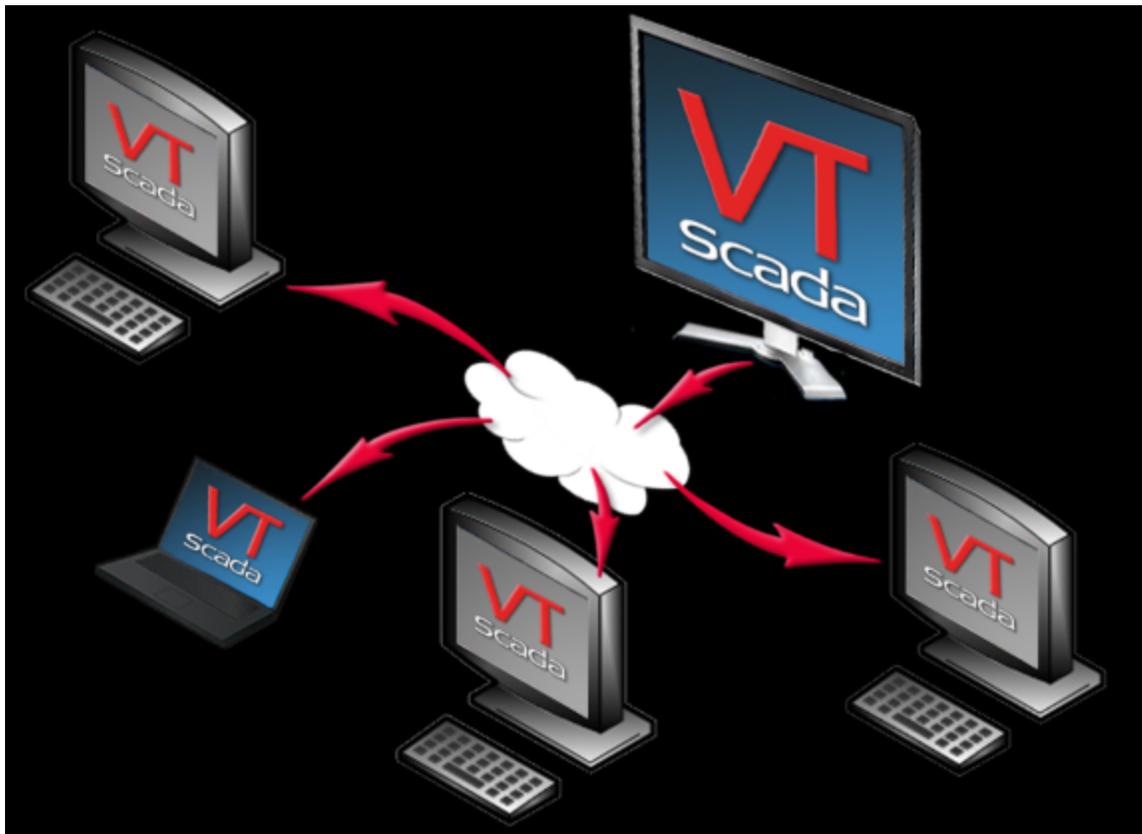
Each site is represented by a pin that changes color based on its polling status. Click a pin to open the associated site. Easily drag pins into place or position them with latitude and longitude coordinates. On-line applications can download map tiles directly from on-line map providers such as MapQuest® *. You can also pre-load these tiles for off-line applications or load your own custom tiles created using third-party graphics programs. Once displayed, map tiles remain cached indefinitely.

Mobile Mapping at your fingertips – The VTScada Mobile Internet Client supports 'slippy maps' on HTML5-compliant mobile devices.

* Map tiles from commercial and open source websites may be subject to terms of license, or use agreements, compliance with which is the user's responsibility.

Secure Remote Access

Integrated within VTScada are three optional software products that provide a variety of methods for remotely accessing your application and process data from remote locations.



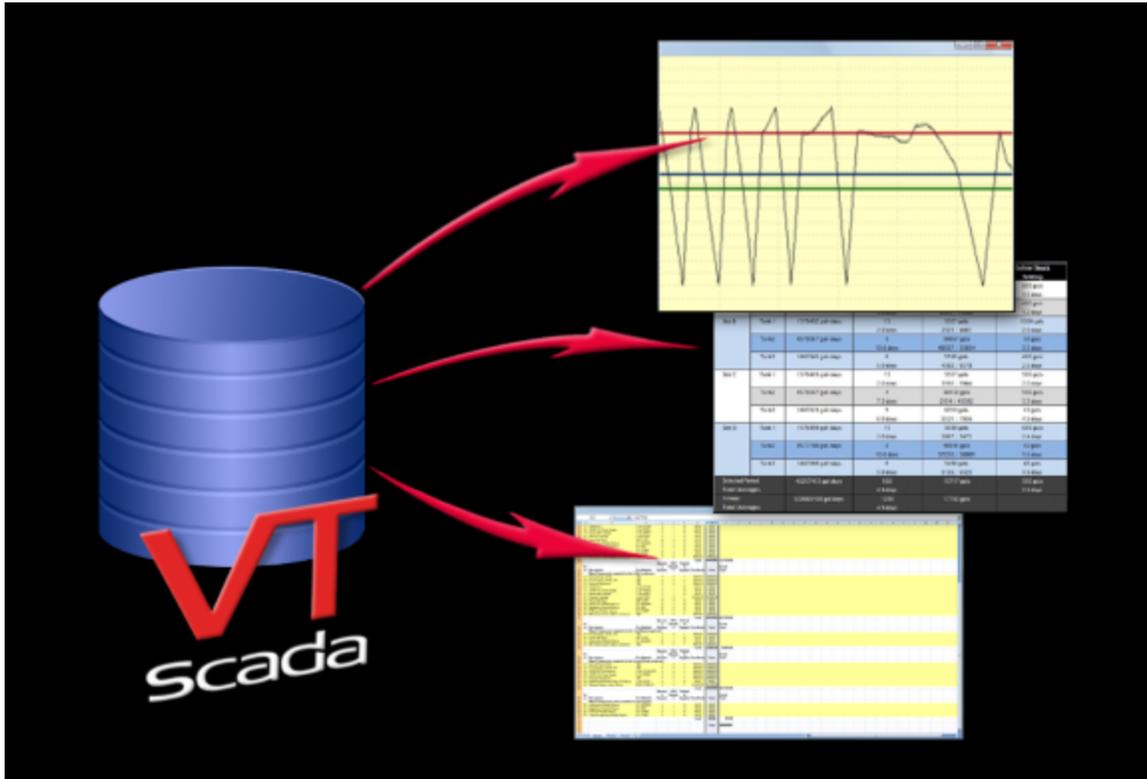
VTScada Internet Client (VIC) enables you to log into your application from any windows computer with Internet access.

VTScada Mobile Internet Client (MIC) is the simplest way to access your process from HTML5-compliant devices such as Android®, iPhone®, and iPad®.

VTScada Alarm Notification System enables you to log in over the phone to access process data and acknowledge alarms. Alarms can also be sent and acknowledged via email or SMS–text message.

VTScada ODBC Server

This optional component requires a VTScada software license.



The VTScada ODBC Server enables you to use industry–standard reporting software like Crystal Reports®, XL Reporter®, Microsoft Access® or Microsoft Excel® to extract system information directly from a VTScada application. Through this interface, you can treat a VTScada application as if it were a SQL database, with each logged tag within it representing a table of timestamps and values. Once the connection is configured, your reporting software can send SQL queries to VTScada to retrieve the logged tag values.

Best of all, you do not need to have VTScada installed on your computer to access the real–time system data you need.

Note: Integration of this product requires a VTScada license key that includes the VTScada ODBC Server and the installation of the VTScada ODBC driver.

OPC Client and Server

This optional component requires a VTScada software license.

VTScada has an extensive library of third-party device drivers that allow it to communicate with monitoring and control hardware from a wide variety of manufacturers. In spite of this, there are some I/O devices for which a direct driver is simply not available. In these cases, OPC can be an effective alternative.

VTScada OPC Server (Optional)

Enables OPC-compliant programs (including other VTScada applications with OPC clients) to send and receive live process data to and from a standard VTScada application.

VTScada OPC Client (Standard)

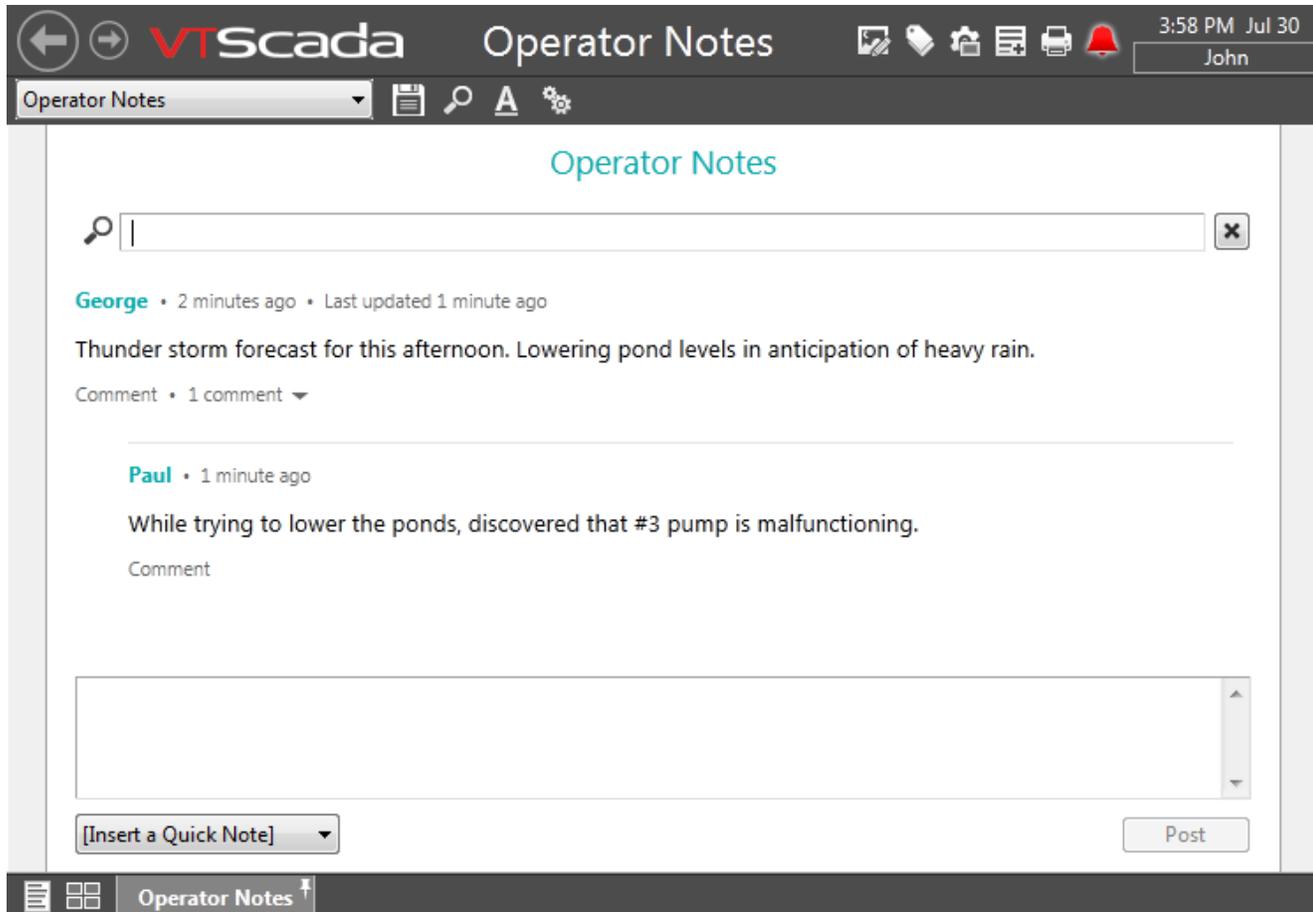
The VTScada OPC Client has long been a standard feature of VTScada. It enables a standard VTScada application to send and receive live process data to and from an OPC-compliant server (including other VTScada applications with configured OPC servers).

Both are fully integrated components of VTScada. The OPC Client is available for no additional cost, while the OPC Server requires an additional license fee.

Both take only seconds to configure.

Operator Notes

Are you required to keep a written operator's logbook to provide traceability for the actions of your users? VTScada simplifies this process by providing an electronic operator's notes display. Notes entered by users are automatically time-stamped and labeled with the operator's name.



Tamper-Proof

Once created, notes cannot be edited and the entire log is saved to an encrypted file, such that the file is unreadable outside VTScada and cannot be edited with a text editor. Comments may be added to correct errors or provide follow-up details.

Accessible from any Workstation or Web Client

Notes are networked so that they can be accessed by any VTScada user with appropriate application security privileges.

Communicate Across Different Shifts and Departments

Operator notes act as a VTScada bulletin board, providing a way for users across the organization and across work shifts to communicate and

record activities (e.g. "Please check engine 1 on backshift. Overspeed during dayshift. Let me know. Bob").

- Notes include timestamp and user name
- Export a range of notes to an HTML format file, for printing anywhere.
- A powerful search tools lets you find notes based on date, author, and content.

Page Notes

Operators can also add the digital equivalent of a yellow-sticky note to any page (or have the note show in all pages. These can be used as reminders or as an in-SCADA messaging system.

Process Displays

Application-specific display pages provide an intuitive operator interface. These include graphical overviews of the process in a full-screen or windowed (user-selectable) view.

Built-in Navigation Tools

All VTScada applications include default page navigation tools including a main menu of all application displays, forward and back buttons, and user-customizable pins to quickly access often used pages.



Display Development

Create your own customized displays using the completely redesigned VTSkada Idea Studio which is available with a VTSkada Full Development License.

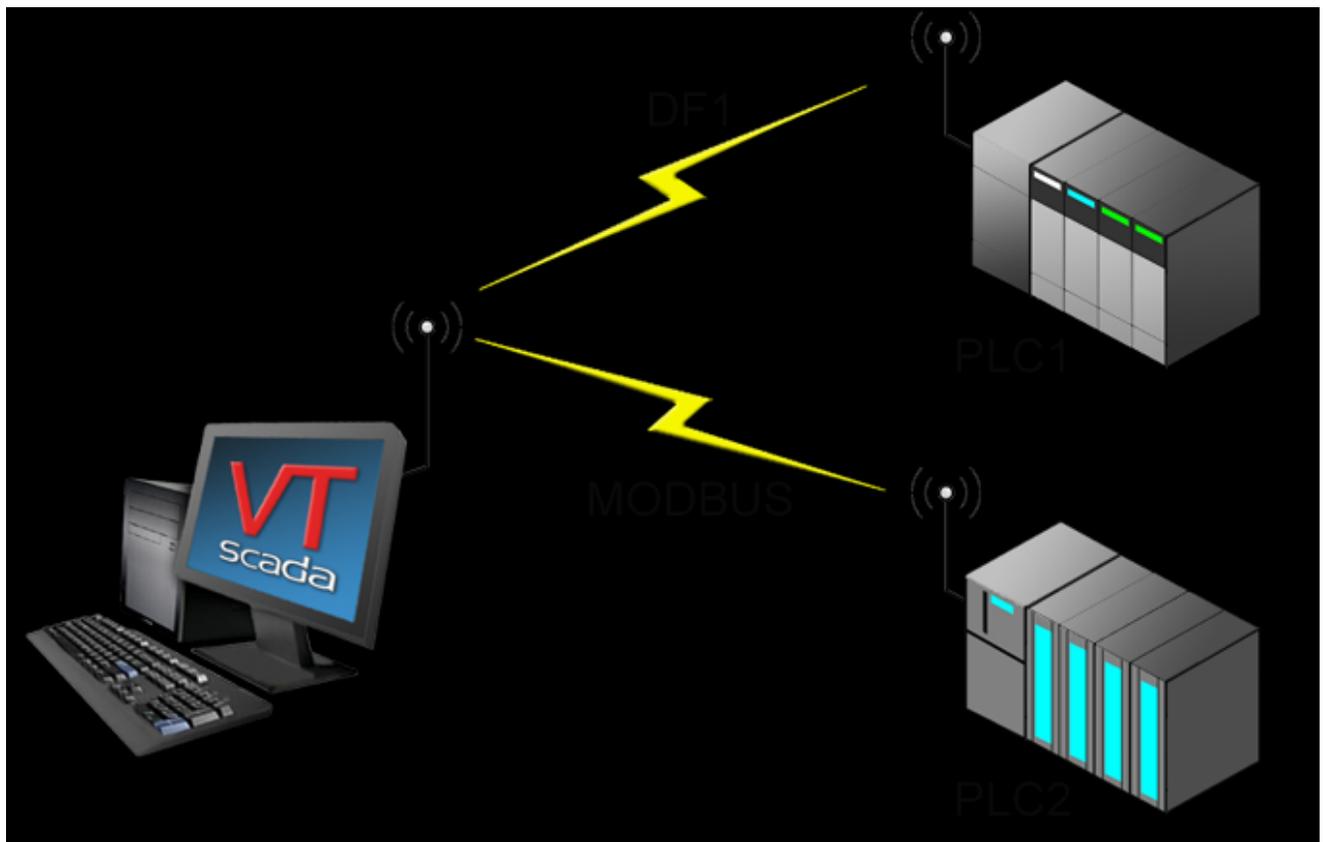
- Dual and quad monitor support.
- View multiple pages on one monitor.
- Design tag widgets without writing code.
- Draw a grid of tags and their values on any page.
- Nested page frames, check-boxes and tabbed folder drawing objects.
- VTSkada Historian and modem statistics panels
- Dual and quad monitor support.
- View multiple pages on one monitor.
- Design tag widgets without writing code.
- Draw a grid of tags and their values on any page.

- Nested page frames, check-boxes and tabbed folder drawing objects.
- VTScada Historian and modem statistics panels

Polling Management

Telemetry devices typically share a common (and costly) communications link. The more efficiently you can use that network the less often you will need to expand it as you add new PLCs and RTUs to your system.

VTScada automatically organizes scheduled polling cycles and communications channels to simplify device communications and reduce integration time.



Eliminate Expensive Master PLCs

VTScada software polls each remote site directly, eliminating the need for a master PLC device. This reduces hardware costs, configuration time and points of failure.

Polling Groups

Devices may be grouped into sets with similar communications channels (i.e. radio, wireless Ethernet gateway), allowing each group's polling cycle to act independently. Each cycle can be independently enabled or disabled. Configure an unlimited number of independent polling groups.

Multiple Polling Modes

Selecting 'Fast poll' mode for a specific RTU in a polling cycle sets a higher polling frequency to help with maintenance or to troubleshoot during emergency situations. You can also configure external triggers to poll on infrequent schedules or on commands from operators.

- Use external triggers to poll on infrequent schedules or on command
- Enable or disable polling in any polling driver

Modem Management

Modems serve a variety of features in control systems, including communicating with I/O devices, providing a connection method for remote VTScada application clients and disseminating messages from the VTScada Alarm Notification System.

Modem Pooling

Since VTScada handles different types of modems in a different ways, modem management must receive close attention. VTScada needs to be able to determine which of the modems is capable of handling each type of communication and direct modem traffic appropriately.

This process is called modem pooling and it enables VTScada to manage a group (pool) of modems efficiently. When a modem is required for an outgoing voice call from the VTScada Alarm Notification System, the VTScada Modem Manager automatically searches its pool of modems for the next available modem capable of handling a voice call.

The same process is followed for outgoing data calls. Similarly, any pooled modem can be configured to allow or deny incoming voice or data calls.

- Supports modem pooling across servers for improved resource efficiency
- Includes custom Unimodem driver

- Data and VTScada Alarm Notification System requests automatically routed to appropriate voice and data modem(s). No configuration necessary
- Supports dedicated modems for functional application areas
- Supports logging of modem activities
- Graphics show modem events, usage stats and modem status

Report Generator

Create Scheduled or Ad-hoc Reports in Seconds

Every VTScada application includes two reporting components; a page for generating ad-hoc reports and a report tag that can be scheduled to trigger predefined reports. Report tags are time zone aware and can run daily, weekly, monthly, manually, or on event.

VTScada includes predefined reports to meet the needs of the water and wastewater industry. Add custom reports as required.

Reports can output to your screen, a file, an Excel® spreadsheet, a template, a database, or as an email attachment.

- Includes pre-configured reports for water and wastewater
- Report scheduler can automatically save important information to file, send it to a printer or email it to appropriate personnel
- Add custom script reports and Excel report templates as needed

Security

Integrated VTScada Security – More Control, Less Complexity

Each application includes its own set of security accounts and settings, which control access to all parts of the application including local workstations, Internet clients, mobile Internet clients, and the VTScada Alarm Notification System. Once deployed, security changes are immediate and application-wide.

A Smarter Approach to Security Management

VTScada 10.1 replaced an ever-growing list of privileges with "Rules." Rules use a combination of a tag, a privilege, and a location to allow you to finely tune what users can do and where. Quickly configure user

accounts by assigning them to a Role which is a predefined set of Rules corresponding to a specific job (e.g. plant operator).

The screenshot displays the user management interface. On the left, there are two lists: 'Users' and 'Roles'. The 'Users' list contains 'Admin', 'demo', and 'Blair*'. The 'Roles' list contains 'Configurer', 'Logged Off', 'Operator', and 'SuperUser'. Below these lists are control buttons for adding (+), removing (-), and other actions. The main area on the right is for configuring a user account. The 'Account Name' field is set to 'Blair'. The 'Password' and 'Confirm Password' fields are masked with dots. Under 'Password Options', the 'Force reset of password at next logon' checkbox is unchecked. The 'Privilege/Role' list shows 'Operator' and 'Application Stop'. At the bottom of this list is an 'Add New Rule' button with a close (X) icon and a user icon.

Windows Security Integration

VTScada 11.1 introduced the ability to integrate with Windows Security, giving you the ability to let authorized users log on with their Windows accounts. Privileges are assigned by membership in Active Directory Security Groups, named for roles within the application.

Enhanced Password Protection

Ensure passwords exceed a minimum length, contain special characters, or expire after a defined period. Accounts can be disabled following repeated failed log in attempts.

Email Server Protection

When emailing alarm notifications, VTScada now supports SMTP email servers requiring Transport Layer Security (e.g. Gmail™).

Group Management

Define what information users can see in large applications. For example, if an application monitors two plants, operators from each plant can be grouped so that they see only the alarms and tags from their respective plants. A third group for managers can be set up to see information from both plants.

Advanced Encryption

The security database uses military-grade encryption as does the security information exchanged between VTScada Internet Clients and Servers. Accounts can also be disabled following repeated failed log in attempts.

Share Security Accounts Across Applications

To reduce duplication and ensure consistency, accounts can now be shared across multiple applications if they are based on a common OEM layer.

More Information

- Supports SSL (secure socket layer)
- No default security account
- Supports USB dongles

VTScada Scripting Language

Advanced Customization With VTScada Scripting Language

In addition to the drag & drop tool set, VTScada provides a variety of tools to help you perform advanced customization. Background scripts, priority functions, external database tools, extensible graphics libraries and a variety of other features allow developers to meet any customer need.

Object-Oriented Scripting

The VTScada scripting language (similar to C++) enables unlimited customization of almost every feature including simple display cus-

tomizations, advanced tag types (with graphics), automated tag creation and complex data-handling functions.

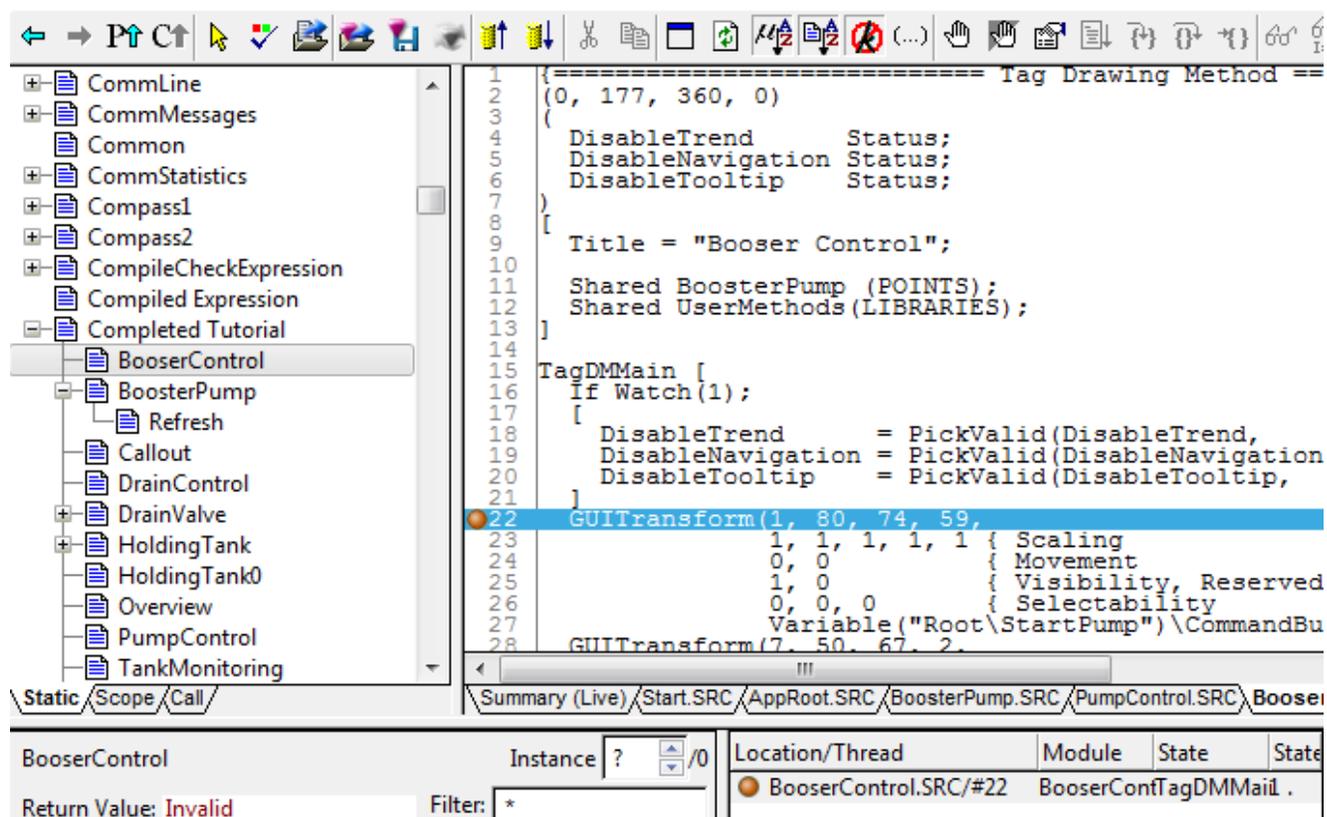
Save Integration Time with Reusable OEM Layers

A unique feature of VTScada is the ability to create OEM code layers. This enables you to develop an extensive set of customized objects (including graphics, functions, displays and reports) and reuse them in any application. This saves considerable development time by allowing you to create multiple applications all based on a template of error-free objects. If you make changes to an OEM layer, you can easily update applications built upon that layer by using a single VTScada ChangeSet file.

- Copy a graphic object and paste it directly into a text editor. Make changes to properties and then paste them back onto your display.
- Create and modify custom tag types.
- Background scripts can run as services to start scheduled tasks or watch for specific events (e.g. run tasks when a user logs in.)

Debugging Tools

Providing the correct information to keep a process running smoothly is the primary goal of any HMI. VTScada takes this one step further by including self diagnostic tools that monitor the health (memory, storage and CPU usage) of all VTScada networked computers, the network connectivity between all VTScada nodes and the radio signal strength for certain types of radios on telemetry networks.



A suite of integrated debugging tools allow users to quickly identify problems in custom code and to test solutions. Tools include line-by-line step-through, variable watching and client/server connectivity monitoring. Additionally, device driver monitoring tools allow users to view communications data and com loss statistics to help debug field device connectivity.

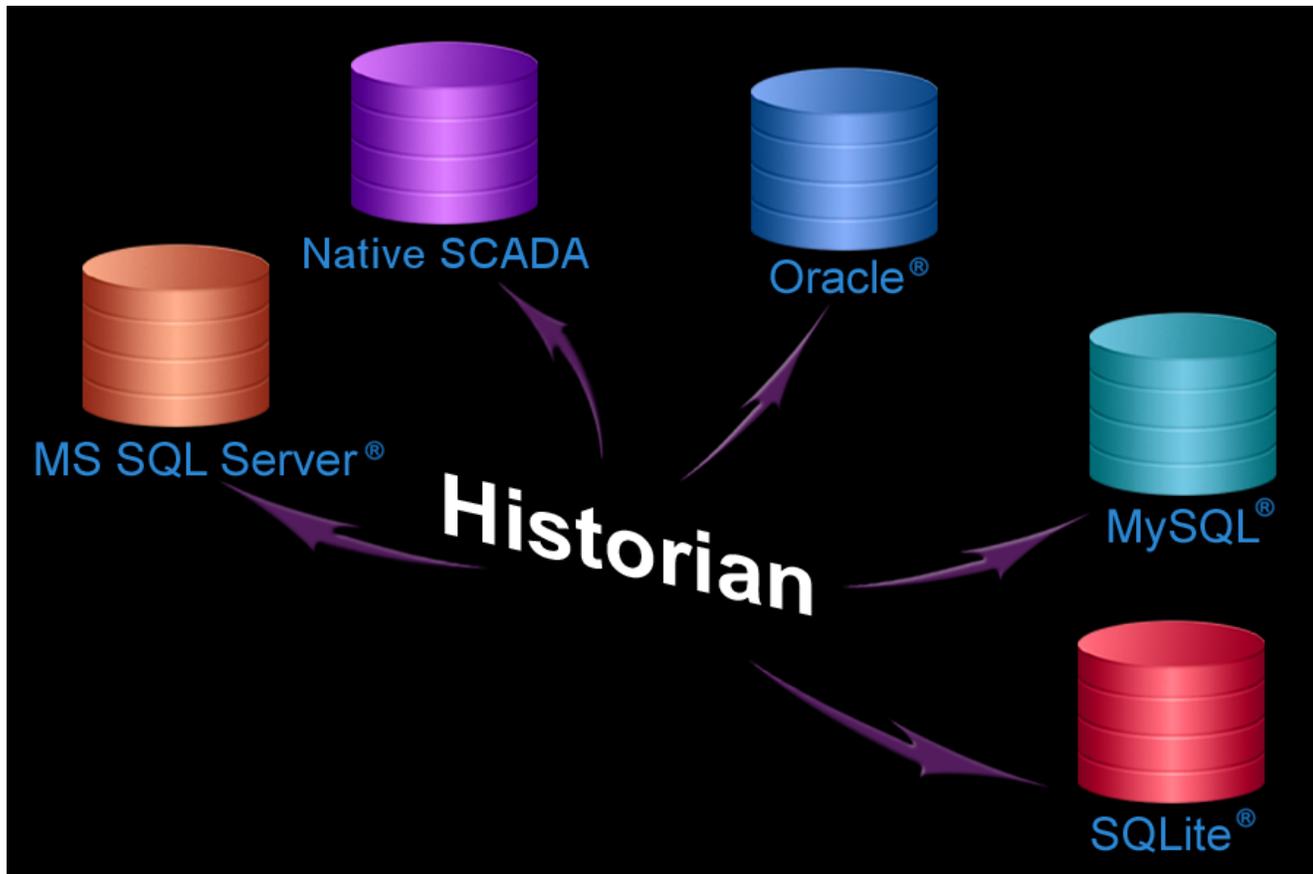
- Logging profiler
- Million thread history with dead threads
- Debugging tools available locally or remotely through VTScada Internet Server
- Automated application tests available
- Tracing of all VTScada activities
- VTScada Source Debugger
- View error statistics and sent/received communications for device drivers
- Automated application tests available
- Code Coverage view, highlighting what code has been run or tested to date.

Historical Data Logging

Built-in Data Logging

The VTScada Historian is part of every VTScada application. Built for speed, it can log data at up to 4,000 values a second and sync across a WAN at up to 160,000 values a second. It can also share process data with third-party reporting tools via the VTScada ODBC Server. Any tag configured with a connection to the Historian begins logging process data to the historical database automatically. If equipment downtime must be represented as "no data" rather than zero values, then you can configure logging to stop while the equipment is offline.

- Fast robust data logging and historical synchronization across networks
- Historical data are separated into monthly folders for easy archiving
- Log process data based on time of day or changes in value
- Avoid logging system noise by using deadbands
- Configure logging by tag



Supported Database Formats

In addition to the native VTScada Historian, VTScada supports Oracle®, SQL Server®, MySQL®, and SQLite® database formats.

Protect Your Historical Data by Using Distributed Historians

VTScada is the only monitoring & control software that supports an unlimited number of redundant, synchronized historians spread across multiple servers. Should the primary database server fail, all the application's workstations and Internet clients automatically fail over to the next available backup database. When the primary is restored, missing historical data is automatically restored from the backup databases. Synchronize databases across a WAN at up to 160,000 values a second.

Easily backup or share data by logging to multiple database formats.

When it comes to data logging, the VTScada Historian provides the best of both worlds. Take advantage of the superior performance of the native database format. Simultaneously, log across a network to an Oracle, SQL Server, MySQL or SQLite database in a different building.

Web Services (SOAP)

This optional component requires a VTScada software license.

The SOAP (XML) interface enables third-party business applications to do more than simply retrieve data from the VTScada Historical Database. Enterprise-level business solutions, such as enterprise resource planning (ERP) systems, are able to use VTScada services that you choose to make available from your application.

This may be as simple as developing remote reporting and monitoring applications or as complex as a delivery scheduling system that relies on calculations done in VTScada to predict when material deliveries will be required.

Business applications make requests to VTScada over a network via a Simple Object Access Protocol (SOAP) interface. VTScada interprets these requests, performs the requested actions and responds in the requested format.

Note: Adding VTScada Web Services to your application requires an understanding of XML, SOAP, and VTScada programming techniques.

- Supports SQL calls from 3rd party apps to VTScada native database
- Supports SELECT commands and WHERE clauses

Related Information:

...What's New... – List of features, by the version they were introduced in.

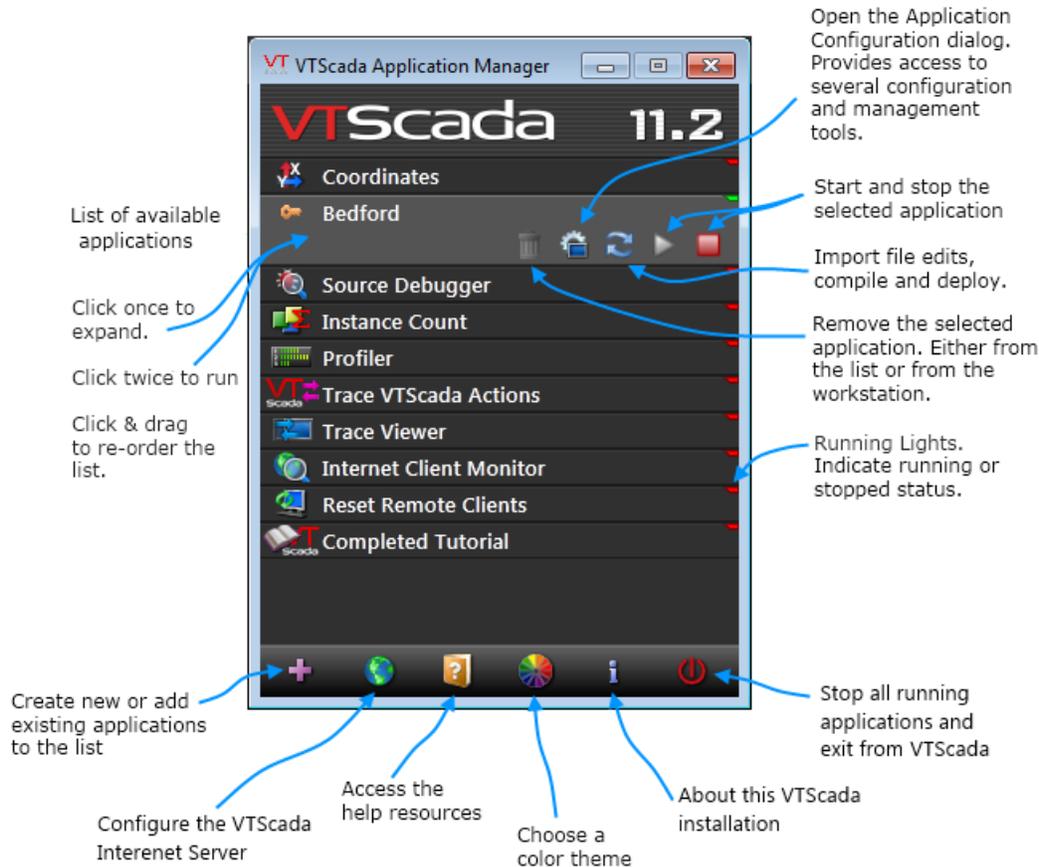
...Moving to the Current Version – Important information and warnings for anyone moving a legacy application to the current version of VTScada

Related Tasks:

...See also: Install the Completed Tutorial in the VTScada Developer's Guide

Application Manager (VAM)

The primary tool for both creating and managing applications is the VTScada Application Manager (VAM).



If the Toggle Visibility feature has been enabled for an application, it's entry in the VAM will have an additional button:



This will not be used at most sites. For more information see: Hide a Running Application in the VTScada Developer's Guide.

The VAM provides many functions. The following table will help guide you through its features. Note that the VAM is organized such that the command buttons along the right edge apply to selected applications.

Buttons along the bottom edge apply to VTScada itself, rather than to any specific application.

Create Applications	<p>The Add button provides access to several options for creating an application. You can build applications from scratch, copy a remote application to this workstation, add an existing application to the VAM, or use a ChangeSet to create a copy of an application.</p> <p>See: Add Applications in the VTScada Developer's Guide</p>
Start and Stop Applications	<p>The Start and Stop buttons in the VAM are used for this purpose. You can also configure an application to start automatically.</p> <p>Start a VTScada Application – See the VTScada Operator's Guide</p>
Configure Application Properties	<p>Application properties (formerly known as configuration variables) control how your application looks and works. These values are set using the Application Properties page, accessed through the Properties button of the VAM.</p> <p>See: Application Properties</p>
Copy or Clone Applications	<p>You can use ChangeSets to create a copy of your application for backup or distribution purposes. A clone is a special case of a copy, often used if you want a duplicate to experiment with.</p> <p>See: ChangeSets – An Application in One File</p>
Version Management	<p>VTScada uses a version control system to maintain a history of every change made to an application. You can restore the application to an earlier stage of development at any time.</p> <p>Because of how the versioning system works, changes made outside of the VTScada user interface, such as file edits or modifications to the tag database, must be imported before they are put into effect and under version control. Also, new files such as images that are added to an application must be explicitly imported.</p> <p>See: See: Version Control in the VTScada Developer's Guide Import/Export Files See: Import and Export Tags in the VTScada Developer's Guide Maintain the File Manifest</p>
Review Application	<p>Detailed information about your application, the version of</p>

Details	VTScada that you are running and the workstation that you are running it on, are all available through the VAM. This includes useful information about what features your VTScada license provides and can be helpful when debugging problems. See: Learn About Your Copy of VTS in the VTScada Developer's Guide
Secure Your Application	VTScada security uses a privilege system whereby users are assigned specific rights controlling what they can do within the program. ...See: Secure Your Application in the VTScada Admin Reference
Manage Server Lists	Many VTScada applications are designed to run simultaneously on several servers and workstations. This enables VTScada to run more efficiently by sharing the resources of several machines, and provides security in the form of automatic fail-over should a server fail. See: Client/Server Configuration in the VTScada Developer's Guide
Backup Logged Data	VTScada provides powerful data logging abilities. You can configure your application to VTScada's own storage format, or you can configure for logging to be done using one or more commercial database programs (even multiple different programs simultaneously). See: Backups.

Related Information:

...Hide the VAM – See the VTScada Admin Guide

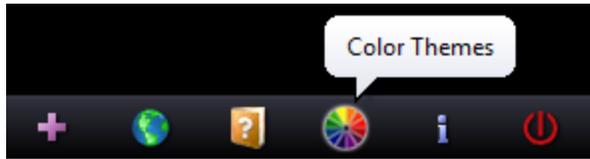
Change the VAM's Color Theme

The VTScada Application Manager can be personalized using any of over two-dozen color themes.

The VAM's color theme will also be used inside applications, unless the applications are otherwise configured with their own color theme.

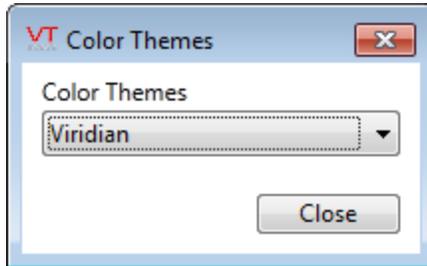
To select a color theme for the VAM

1. Click the Color Theme button.



The selection dialog opens.

2. Choose a theme.



As you select each theme, the VAM will change color to match.

Related Information:

...Color Theme Definition – See the VTScada Programmer's Guide – How themes are defined. How to create your own themes.

Application Configuration

The Application Configuration Dialog contains a large collection of tools for managing your application.

Note: If security is enabled, then you must have at least the Configure privilege in order to open this dialog.

Open the Application Configuration Dialog from the VAM:

1. In the VTScada Application Manager (VAM), select the application.
2. Click on Application Configuration.

Open the Application Configuration Dialog from within an application:

1. While an application is running, click on the Configure button.

Open the Application Configuration Dialog from within the Idea Studio:

1. Open the Idea Studio.
2. Expand the File menu.
3. Click on Application Configuration.

Related Information:

...Application Properties – Complete reference.

...Display Tab of the Edit Properties Page – Commonly used properties for the display.

...Alarms Tab of the Edit Properties Page – Commonly used properties for alarms, including email configuration.

...Other Tab of the Edit Properties Page – Assorted commonly used properties.

...ChangeSets – An Application in One File – Create & Apply ChangeSets.

...Maintain the File Manifest – Control which files are part of your application.

...Application Information

The following related topics can be found in the VTScada Developer's Guide:

...Client / Server Configuration

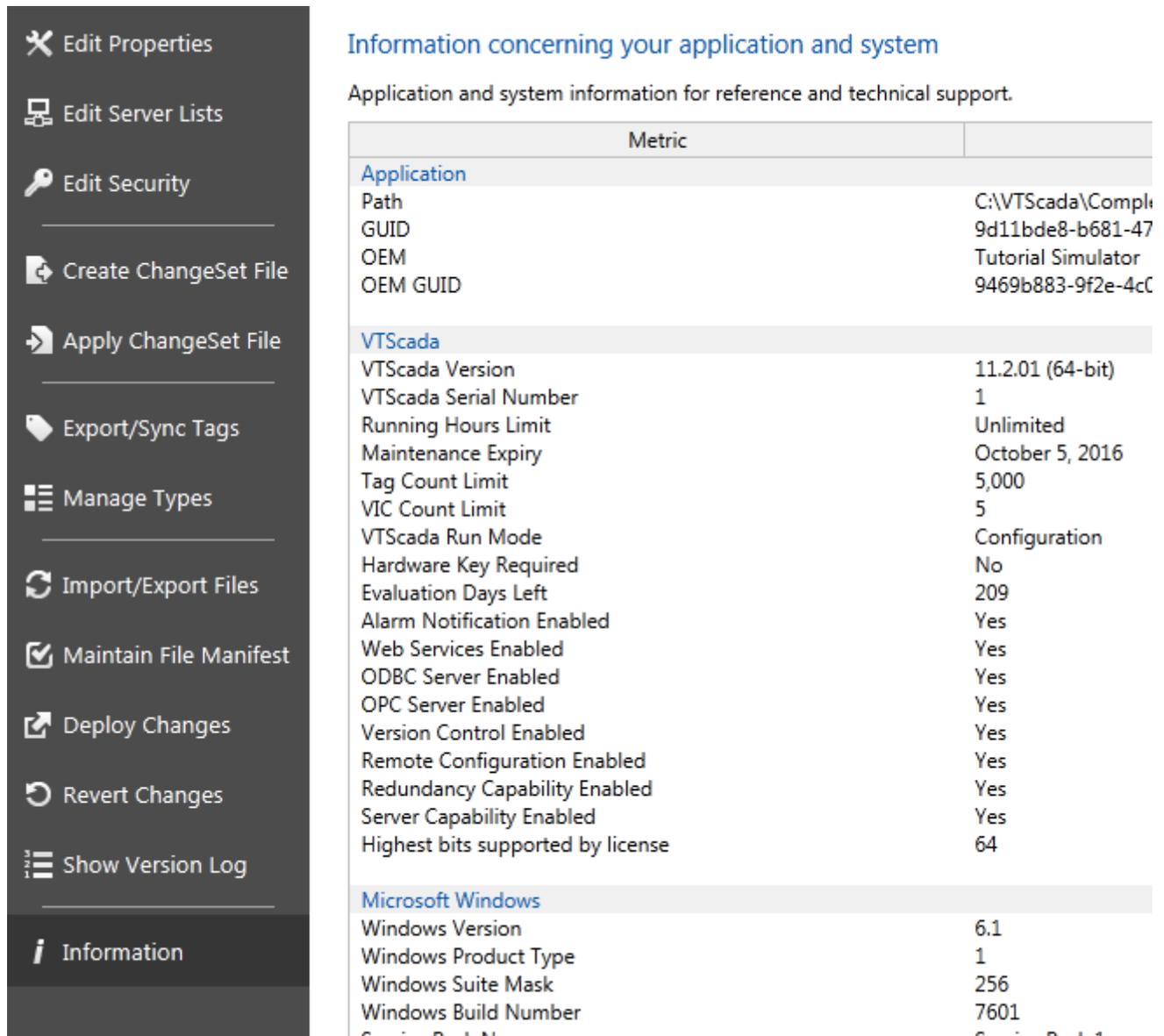
...Import and Export Tags – Import / Export Tags.

...Local Changes versus Deployed Changes – Deploy / Revert Changes

...The Version Log – Review and roll-back configuration changes.

Application Information

This page of the Application Configuration dialog provides detailed information about your application, your copy of VTScada, and the workstation on which the application runs. You can use this to discover the OEM layer that the application is built upon, which VTScada features are enabled with your license key, and key details about your computer's operating system version and hardware features.



Information concerning your application and system

Application and system information for reference and technical support.

Metric	
Application	
Path	C:\VTScada\Compl
GUID	9d11bde8-b681-47
OEM	Tutorial Simulator
OEM GUID	9469b883-9f2e-4cC
VTScada	
VTScada Version	11.2.01 (64-bit)
VTScada Serial Number	1
Running Hours Limit	Unlimited
Maintenance Expiry	October 5, 2016
Tag Count Limit	5,000
VIC Count Limit	5
VTScada Run Mode	Configuration
Hardware Key Required	No
Evaluation Days Left	209
Alarm Notification Enabled	Yes
Web Services Enabled	Yes
ODBC Server Enabled	Yes
OPC Server Enabled	Yes
Version Control Enabled	Yes
Remote Configuration Enabled	Yes
Redundancy Capability Enabled	Yes
Server Capability Enabled	Yes
Highest bits supported by license	64
Microsoft Windows	
Windows Version	6.1
Windows Product Type	1
Windows Suite Mask	256
Windows Build Number	7601
Service Pack Name	Service Pack 1

Related Information:

...See also "About..." in the VTScada Developer's Guide

predefined Date Codes

Use any of the following numeric date codes to format a data as shown. If you require a custom format, you can build one using the text codes shown in Date Formatting Strings.

Dates using these codes will always be displayed in English, regardless of system configuration.

All examples showing Monday, August 13, 2012.

Note: Use only the number in the first column – the second two describe the result of the code in the first column. They are not codes that you can use in the function.

Date Code	Example	Description
0		no date
1	120813	yyMMdd
2	08/13/12	MM/dd/yy
3	08-13-12	MM-dd-yy
4	Aug 13, 2012	MMM d, yyyy
5	August 13, 2012	MMMM d, yyyy
6	13 Aug 12	dd MMM yy
7	13 Aug 2012	dd MMM yyyy
8	13/08/12	dd/MM/yy
9	13-08-12	dd-MM-yy
10	13Aug12	ddMMMyy
11	13Aug2012	ddMMMyyyy
12	Aug 13/12	MMM d/yy
13	20120813	yyyyMMdd
14	08/13	MM/dd
15	08-13	MM-dd
16	08/12	MM/yy
17	08-12	MM-yy
18	08/2012	MM/yyyy
19	08-2012	MM-yyyy
20	Aug 13	MMM d

Application Configuration

21	August 13	MMMM d
22	Aug 2012	MMM yyyy
23	August 2012	MMMM yyyy
24	13/08	dd/MM
25	13-08	dd-MM
26	Aug	MMM
27	August	MMMM
28	12-08-13	yy-MM-dd
29	12/08/13	yy/MM/dd
30	2012-08-13	yyyy-MM-dd
31	2012/08/13	yyyy/MM/dd
32	12-W35-01 ⁽¹⁾	yy-WeekOfYear-DayOfWeek ⁽²⁾
33	12/W35/01	yy/WeekOfYear/DayOfWeek
34	2012-W35-01	yyyy-WeekOfYear-DayOfWeek
35	2012/W35/01	yyyy/WeekOfYear/DayOfWeek
36	12226	yyDayOfYear
37	2012226	yyyyDayOfYear
38	12-226	yy-DayOfYear
39	12/226	yy/DayOfYear
40	2012-226	yyyy-DayOfYear
41	2012/226	yyyy/DayOfYear
42	Mon, 13 Aug 2012	ddd, d MMM yyyy

⁽¹⁾ Week Of Year is preceded by the character W.

⁽²⁾ "DayOfWeek" and "WeekOfYear" are descriptions rather than format codes that you could use.

Related Information:

predefined Time Formats – Use for displaying time.

Date – The function that uses the codes listed above.

predefined Date Codes

Use any of the following numeric date codes to format a data as shown. If you require a custom format, you can build one using the text codes shown in Date Formatting Strings.

Dates using these codes will always be displayed in English, regardless of system configuration.

All examples showing Monday, August 13, 2012.

Note: Use only the number in the first column – the second two describe the result of the code in the first column. They are not codes that you can use in the function.

Date Code	Example	Description
0		no date
1	120813	yyMMdd
2	08/13/12	MM/dd/yy
3	08-13-12	MM-dd-yy
4	Aug 13, 2012	MMM d, yyyy
5	August 13, 2012	MMMM d, yyyy
6	13 Aug 12	dd MMM yy
7	13 Aug 2012	dd MMM yyyy
8	13/08/12	dd/MM/yy
9	13-08-12	dd-MM-yy
10	13Aug12	ddMMMyy
11	13Aug2012	ddMMMyyyy
12	Aug 13/12	MMM d/yy
13	20120813	yyyyMMdd
14	08/13	MM/dd
15	08-13	MM-dd

Application Configuration

16	08/12	MM/yy
17	08-12	MM-yy
18	08/2012	MM/yyyy
19	08-2012	MM-yyyy
20	Aug 13	MMM d
21	August 13	MMMM d
22	Aug 2012	MMM yyyy
23	August 2012	MMMM yyyy
24	13/08	dd/MM
25	13-08	dd-MM
26	Aug	MMM
27	August	MMMM
28	12-08-13	yy-MM-dd
29	12/08/13	yy/MM/dd
30	2012-08-13	yyyy-MM-dd
31	2012/08/13	yyyy/MM/dd
32	12-W35-01 ⁽¹⁾	yy-WeekOfYear-DayOfWeek ⁽²⁾
33	12/W35/01	yy/WeekOfYear/DayOfWeek
34	2012-W35-01	yyyy-WeekOfYear-DayOfWeek
35	2012/W35/01	yyyy/WeekOfYear/DayOfWeek
36	12226	yyDayOfYear
37	2012226	yyyyDayOfYear
38	12-226	yy-DayOfYear
39	12/226	yy/DayOfYear
40	2012-226	yyyy-DayOfYear
41	2012/226	yyyy/DayOfYear
42	Mon, 13 Aug 2012	ddd, d MMM yyyy

⁽¹⁾ Week Of Year is preceded by the character W.

(²) "DayOfWeek" and "WeekOfYear" are descriptions rather than format codes that you could use.

Related Information:

predefined Time Formats – Use for displaying time.

Date – The function that uses the codes listed above.

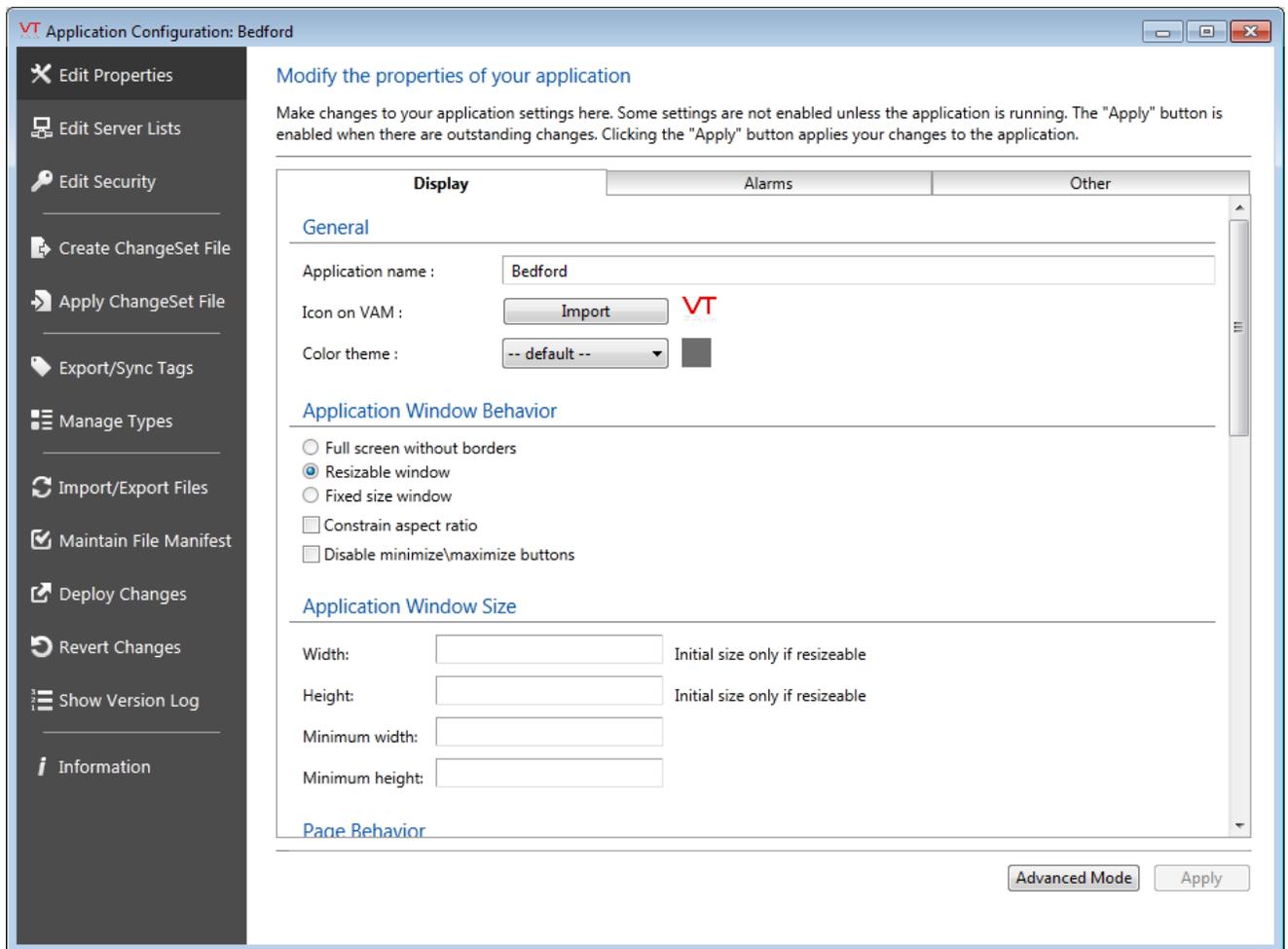
Application Properties

Note: This chapter includes properties that affect an application and can be set in Settings.Dynamic or Settings.Startup. Refer also to the chapter, System Properties, for properties that affect VTS as a whole and are stored in Settings.INI.

Note that properties in the [LAYER] section of Settings.INI may be used in your application's Settings.Dynamic file, creating an application-specific override of the global property.

Well over 1000 properties are available in VTScada, giving you enormous control over the appearance and behavior of your application. Property values are inherited from one layer to another, which means that your application will automatically have all the settings of the application it is based on. Any of these can be changed as required, and most can be changed using dialog boxes built into the VTScada user interface. You can view, edit and add all properties directly using the Applications Properties page of the Application Configuration page.

Note: The terms "Settings" and "Properties" are interchangeable.



The Application Properties page opens to a simplified view, where three tabs contain the most commonly used properties. You can access the full selection of properties at any time by clicking the Advanced Mode button at the lower right corner of the page.

By changing properties for your application, you can:

- Choose to run the application in a window instead of in full screen.
- Change labels on the screen – perhaps to create an application for a language other than English.
- Control what is said by spoken alarms.
- Decide whether alarm pop-up messages are to be enabled.
- And much more.

The general steps to set a value for a property using the Application Configuration dialog are as follows:

1. Open the Application Configuration dialog.
2. Open the Edit Properties page.
3. Find the property...
 - a. The most commonly accessed properties can be found in one of the three tabs of the basic mode: Display, Alarms, or Other.
 - b. For other properties, click the Advanced Mode button to view a list of all. The list can be sorted by name, type, and value.
 - c. Advanced Mode: If the property has not yet been set in the current application, copy it from the underlying OEM layer. OEM properties are shown in gray and have a check mark in the OEM column.
 - d. If the property is not listed, click the Insert button to add it.
4. Change the property's value.
5. Apply the changes.
6. Deploy the changes if *Automatically deploy local changes* is not checked in the "Other" tab of the basic mode.

Properties are stored in text files, in one of three locations:

- Properties that affect VTScada in general are stored in Setup.INI, located in the VTScada installation folder. This file can be changed only by direct editing. Changes take effect only upon VTScada being restarted.
- Properties that affect a specific application are stored in Setting.Startup and Settings.Dynamic, within the application folder. Properties from the [LAYER] section of Setup.INI can be overridden by adding a copy to one of these files.
- Properties that affect a specific workstation are stored in a sub-folder of the application named WorkstationSettings. These files are named after the workstation they affect, but also use the extensions .Startup and .Dynamic.

Related Information:

...System Properties – Setup.ini – Properties that affect VTScada as a whole.

...Application Properties Files – Structure and location of the files affecting an application.

...Unsaved Configuration Changes – Error dialog description.

Related Tasks:

...Application Configuration – Find and open this dialog.

...Sort and Filter the Application Properties Dialog – Save time when looking for a property.

...Add a Property – Used in the rare instance that a property is not already in one of the files.

...Copy a Property – Make a local copy of an OEM property, with its own value.

...Change a Property's Value – Control the appearance or behavior of your application.

...Set a Workstation-Specific Property Value – Have a different appearance or behavior from one workstation to another.

Property Listings by Type:

...Alarm Notification System Properties

...Application Properties for Alarms

...Color Properties

...Communication Driver Properties

...Display Manager Properties

...Editing and Debugging Properties

...Logging & Reporting Properties

... Mobile Browser Properties

...Modem Manager Properties

...Port Properties

...Object Selection Marquee Properties

...Operator Logging Properties

...Page Properties

...Report Generation Properties

...Application Settings for RPC

...Security-Related Settings

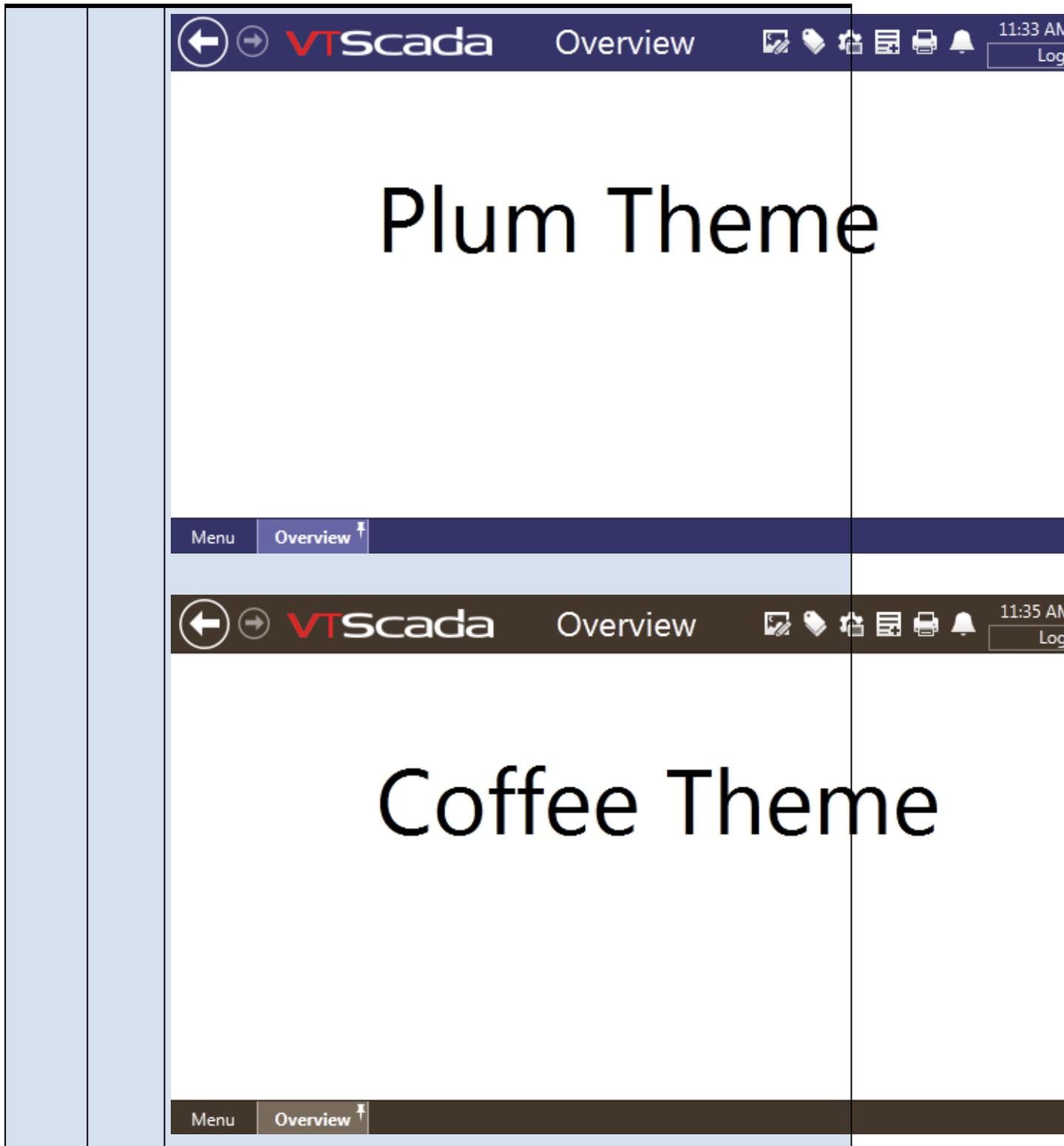
- ...Snap Grid Properties
- ...Tag Properties
- ... Time Synchronization Manager Properties
- ... Tooltip Properties
- ...Trending and Historical Data Viewer Properties
- ... Internet Server and Client Properties
- ... Wizard Engine Properties

Display Tab of the Edit Properties Page

The Display tab includes the following elements:

General

Property	Stored as	Description
Application Name	Name	Holds the displayed name of the application. Changes to this property do not affect the path to the application folder. Stored in the [Application] section of Settings.Dynamic.
Icon on VAM	VAMIcon	Select any image to be used to represent the application in the VAM. Images larger than 38x20 pixels will be scaled to fit. In order for the icon to blend smoothly into the VAM, rather than appearing as a rectangle, any pixels in the image file that are not a part of the actual icon should be transparent. Stored in the [Application] section of Settings.Dynamic.
Color Theme	AppTheme	Select the overall color theme for the application. This controls the title bar, navigation bar, dialogs, and the color used for the application in the VAM. Stored in the [Layer] section of Settings.Dynamic.





Application Window Behavior

Property	Stored as	Description
Full screen without borders	DispMgrFullScreen	When selected, options for the window size and title bar decorations are disabled. The application will fill whatever screen it is displayed within. You should design the application to fit the smallest screen that it will be displayed on.
Resizable border	DispMgrResizable	Operators may drag the window borders to the size they want to view. Scroll bars will be added if the application size exceeds the window. Options to control the window size become available. Title bar decorations may be configured

Application Configuration

Fixed size window	(a combination of the above two properties)	Width and height may be set in the following section. Minimum window size options are not relevant.
Constrain aspect ratio	DispMgrAspectRatio	This option is available only when the resizable border has been selected. Any change to one dimension of the page is matched by a change to the other.
Disable min\max buttons	DispMgrMinMaxDisabled	Only available in combination with resizable border option.

Application Window Size (Values measured in pixels.)

Property	Stored as	Description
Width	DispMgrWidth	Sets the initial width of resizable windows. Sets only the width of constrained windows.
Height	DispMgrHeight	Sets the initial height of resizable windows. Sets only the height of constrained windows.
Minimum width	DispMgrMinWidth	Only for resizable windows, ensures that the width is no less than this value. Does not apply to constrained or full-screen windows.
Minimum height	DispMgrMinHeight	Only for resizable windows, ensures that the height is no less than this value. Does not apply to constrained or full-screen windows.

Page Behavior

Property	Stored as	Description
First page at startup	Page	Choose which page will be shown upon application startup. You may return to the last page viewed, or use the drop-down list to select any page in the application. If you choose a parametrized page, you should set the values that will be used for those parameters using the Set Page Parameters button. Failing to do so will result in the operator being prompted for para-

		meter values when the application starts.
Background color	DefaultPageColor	Sets the default color for all pages that have not been configured with their own background color.
Stretch contents	ScaleDisplayContent	<p>When checked, the page display will be scaled to fill the available area of each window, excepting the editor window.</p> <p>This option is useful in the case that the application is displayed full-screen on many computers, each having a different screen size.</p> <p>Note: Automated display scaling works reasonably well when enlarging the page. It cannot do as good a job when shrinking a display for a smaller screen. In particular, labels embedded within buttons or widgets are more likely to be truncated than scaled down.</p> <p>Always design for the smallest screen that the application will be displayed upon.</p>

Title Bar Contents

Configuration may be set independently for the standard display (Normal page) and for pop-up pages. When selected, the default is to use all decorations for the normal page and no decorations for pop-up pages. The title bar includes ten separate items, each of which may be displayed or suppressed. The title bar itself must be selected for display in order for any of the decorations to have meaning.

Time format & date format: Use the selectors to choose how time and date should be displayed in the title bar. If the available options do not include the format you prefer, open the Advanced Mode and change the values for DispMgrDateFormat and DispMgrTimeFormat.

Task Bar Contents

As with the title bar, configuration may be controlled independently for a normal page and for pop-up pages. The default is to show all task bar tools on the normal page and none on a pop-up page.

Page buttons are added by operators, and are unique to each operator. Choosing "Show Page Buttons" does not cause any to appear if the operator has not added them using the pin button, but deselecting the option will cause an operator's page button shortcuts to vanish.

Related Information:

- ...Alarms Tab of the Edit Properties Page
- ...Historical Data Viewer Tab of Edit Properties
- ...Other Tab of the Edit Properties Page
- ...Sort and Filter the Application Properties Dialog

Alarms Tab of the Edit Properties Page

Elements in the Display tab of the Edit Properties page are as follows:

Visual Indicators

Property	Stored as	Description
Flash alarm icon in title bar when there are unacknowledged alarms.	AlarmIndDisable AlarmIndDisableOnVIC	When checked, the alarm icon in the title bar will flash rather than simply showing red. If your internet connection is limited by bandwidth restrictions, we recommend that you do not enable this option for the VIC display.
Flash title bar red when there are unacknowledged alarms	AlarmFlashTitleBar AlarmFlashTitleBarOnVIC	When checked, the entire title bar will flash red while there are unacknowledged alarms that are visible to the logged-on user. If your internet connection is limited by

		bandwidth restrictions, we recommend that you do not enable this option for the VIC display.
Flash unacknowledged alarms in alarm lists	FlashUnackedAlarmsOnServer FlashUnackedAlarmsOnVIC	When checked, unacknowledged alarms in the alarm list will flash, in order to draw operator attention. Separate options exist for the server and VIC ¹ displays. If your internet connection is limited by bandwidth restrictions, we recommend that you do not enable this option for the VIC display.
Highlight unacknowledged alarms in alarm list	HighlightUnackedAlarms	When checked, unacknowledged alarms will be shown with a highlight color in alarm lists.
Allow pop-up notification when alarm trips	AlarmPopupsEnable	Pop-up alarm notifications must be enabled on an alarm-by-alarm basis, but may not be enable at all unless this option has been selected.

Sounds and Speech

¹VTScada Internet Client. Allows you to connect to an application over the Internet with many of the features of a full VTScada workstation.

Application Configuration

Property	Stored as	Description
Disable all alarm sounds	AlarmSoundDisable	When checked, alarms will be silent.
Speak alarms instead of playing sounds	AlarmSpeechEnable	Enables spoken alarms on the server. Other configuration may be required. See: Spoken Alarms on the Server or WorkstationSpoken Alarms on the Server or Workstation in the VTScada Developer's Guide
Configure speech lexicon	file: Lexicon.VLX	Opens the Configure Lexicon dialog, where you may adjust the pronunciation of words phonetically.

Automatic Page Navigation

Property	Stored as	Description
Enable automatic page navigation when an alarm triggers	AlarmAutoNavEnable	When checked, new alarms will cause the application to open a page where the alarm tag (or triggering tag) is displayed. If drawn on several pages, VTScada will decide the most suitable. If drawn on none, the alarm page will open.
Open the target page in a pop-up window.	AlarmAutoNavWindowed	Relevant only if the preceding option is also selected. Causes the automatically-opened page to be opened in a pop-up window if possible. Ignored if the page is configured to never open in a pop-up window. Subject to limits imposed by

		PopupPageLimit.
Time without user activity preceding an alarm, to enable automatic navigation.	AlarmAutoNavTimeout	Automatic navigation will occur only if there has been no user activity for the set number of seconds preceding the alarm.
Minimum time to display a page after switching to it.	AlarmAutoNavHold	Number of seconds to hold one automatically-opened page before another may open. Has no effect on operator navigation.

Alarm Notes Properties

Property	Stored as	Description
Require note when acknowledging alarm	NoteRequiredForAck	When set, operators must create a note when acknowledging an alarm. Notes will be added to the notebook associated with the alarm's database.
Minimum length of acknowledge note	NoteMinLengthForAck	Minimum length of acknowledge note. If a minimum length is not provided, the note dialog will open, but operators can click OK to close it without saving a note. (Empty notes will not be recorded.) This may be useful if notes are suggested, but not required. Set a minimum length to enforce note creation. This will be true of the following properties as well.
Require note when shelving alarm	NoteRequiredForShelve	When selected, operators must add a note when shelving an alarm.
Minimum length of shelving note	NoteMinLengthForShelve	Minimum length of shelve note.

Application Configuration

Require note when unshelving alarm	NoteRequiredForUnshelve	When selected, operators must add a note when unshelving an alarm.
Minimum length of unshelving note	NoteMinLengthForUnshelve	Minimum length of unshelve note.

Alarm Notification

The options in this section apply only to VTScada licenses that include the Alarm Notification System.

While the term "dial" is used, these options apply equally to alarms sent by email or SMS-text message.

Property	Stored as	Description
Dial-out priority: <ul style="list-style-type: none"> • Do not dial • Dial on priority 1 only • Dial on priority 1 or 2 	CallOutPriority	Use the options in this section to control which priority-level alarms will be sent to remote operators. The choice made here affects the following two options, since a delay before dialing does not apply to alarms that are not dialed out at all.
Delay to notify on priority 1 alarms	CallOutDelay1	Controls the number of seconds that VTScada will wait for a priority 1 alarm to be acknowledged by a local operator before it is sent to a remote operator.
Delay to notify on priority 2 alarms	CallOutDelay2	Controls the number of seconds that VTScada will wait for a priority 2 alarm to be acknowledged by a local operator before it is sent to a

		remote operator.
Delay between calls	RosterDelay	Sets the length of time that VTScada will wait between making calls. The call sequence is controlled by a roster, configured within the application. If the roster fails to send a notification to one contact, no delay is used before attempting the next (if any).
Initial section	IncomingCallSection	Alarms sent by phone are organized according to a menu. You may choose which page of the menu will be spoken first, allowing operators to immediately hear the most relevant information without needing to step through a menu.
Echo phone through speaker	EchoPhoneThroughSpeaker	If the server has a properly configured sound card and speaker, alarms that are dialed out can also be spoken at the server.
Answer Inbound Calls	AnswerAlarmCalls	If set to 0, prevents the Alarm Notification System audio discriminator from being registered with the Modem Manager. This would be useful in an application where the Alarm Notification System is not being used for incoming voice calls, but other drivers are registered for incoming data calls. 30 seconds of time can

Application Configuration

		thereby be saved from each inbound call. Not to be confused with the Modem Manager property, AnswerCalls.
Dial when alarm triggers	DialOnActive	Controls whether active alarms should dialed out.
Dial when alarm clears	DialOnClear	When set true, the alarm system will dial out when the alarm clears.
Cancel call when alarm is acknowledged	DialCancelOnAck	If one operator acknowledges the alarm while the notification system is calling another, this option will cancel the phone call.
Cancel call when alarm clears	DialCancelOnNormal	Controls whether or not unacknowledged alarms whose condition has become normal should be dialed out to operators

Outgoing Alarm Emails

These properties are stored in an encrypted format, and cannot be modified in the Settings.Dynamic file.

Protocol	Only SMTP is allowed.
Email server name or IP	The name or IP address of your email server. This information should be available from your system administrator or your email provider. It will typically take the form: "mail.yourcompany.com" for an internal email server or, using Google's Gmail as an example, "smtp.gmail.com".
Email server port number	The port number used by your email server. Always check with your provider to determine the port to use, but for most local email server programs, this will be 25.

	If using Transport Layer Security, the port will usually be 587. For more information, see: SMTPPort.
Email transport layer security	Controls whether TLS is used for communications. This is required by some email servers, such as Google's Gmail.
Email from address	The text you fill in here will be used in the FROM: field of all emails sent by the system. Note that some email servers will check that this is a valid email address and will reject the message if it is not. If you are configuring for alarm acknowledgment by email, this field must include the email address configured in the Incoming Alarm Email Acknowledgments section. The field may also contain a common name as well as the address. For example: "VTScada System" <VTSSystem@YourCompany.com> Multiple addresses may be used, separated by semi-colons. In the case of alarm acknowledgment by email, the other addresses will be each receive a copy of the acknowledgment.
User name	Use if your SMTP email server requires user authentication.
Password	As with Username, use this field if (as is usually the case) your SMTP email server requires user authentication. Both the user name and the password are encrypted for storage.

Incoming Alarm Email Acknowledgments

These properties are stored in an encrypted format, and cannot be modified in the Settings.Dynamic file.

Protocol	Only POP3 is allowed.
Email server name or IP	The name or IP address of your email server. This information should be available from your system administrator or your email provider. It will typically take the form: "pop.yourcompany.com" for an

	internal email server or, using Google's Gmail as an example, "pop.gmail.com".
Email server port number	The port number used by your email server. Always check with your provider to determine the port to use, but for most local email server programs, this will be 110. If using Transport Layer Security, the port will usually be 995. For more information, see: SMTPPort.
Email transport layer security	Controls whether security is used for communications. This is required by some email servers, such as Google's Gmail.
User name	Use if your POP3 email server requires user authentication.
Password	As with Username, use this field if (as is usually the case) your POP3 email server requires user authentication. Both the user name and the password are encrypted for storage.
Maximum message size in bytes	Reject any message larger than this size. Use this field to block emails with large attachments, which might otherwise delay legitimate alarm acknowledgments.

Related Information:

...Display Tab of the Edit Properties Page

...Historical Data Viewer Tab of Edit Properties

...Other Tab of the Edit Properties Page

...Sort and Filter the Application Properties Dialog

...Email Setup for Alarms and Reports – Reference notes and instructions for email configuration can be found in the VTScada Admin Guide.

Historical Data Viewer Tab of Edit Properties

Elements in the Historical Data Viewer tab of the Edit Properties page are as follows:

General

Property	Stored as	Description
Show plot time selection scrollbar	HDVDisplayTimeSelectionScrollBar	Enables a scrollbar that operators can use to view values that no longer show in the current Plot display. Does not apply to the Grid display.
Show plot time scales	HDVShowTimeScales	Enables the display of time values below the plot so that operators are able to know when events occurred. Does not apply to the Grid display.
Show plot legend	HDVLegendVisible	Enables the display of the list of pens that are included in the plot. The legend includes a link to configure each pen's display properties, a command to hide or reveal the pen, and a set of statistics which update as the cursor is moved across the displayed time.
Use simple legend	HDVSimpleLegend	Applies only if the plot legend has been enabled. All statistics other than value at cursor position are removed from the legend when this option is enabled.
Sort grid in ascending order	HDVGridViewSortOrder	If selected, the grid tab will have the most recent time at the top of the list. When not selected, the most

Application Configuration

		recent time is at the bottom of the list.
Add Note requires extra authentication	NoteAddRequiresAuthentication	When selected, operators who are adding notes to the Operator Notes page or to the Notes tab of the HDV will be prompted to confirm their identity by providing their user name and password. The note will be attributed to the user name used for confirmation, which might not be the same as the logged-on operator. Applies to all instances of the Operator Notes interface.
Time format	HDVTimeFormat1 and HDVTimeFormat2	Use the drop-down selection to choose the format used to display time stamps. The display adjusts automatically, choosing the time format property or date format property that is most appropriate for the time span included in the graph or grid.
Date format	HDVDateFormat1 and HDVDateFormat2	Use the drop-down selection to choose the format used to display dates. The display adjusts automatically, choosing the time format property or date format property that is most appropriate for the time span included in the

		graph or grid.
--	--	----------------

Colors

Property	Stored as	Description
General Back-ground	HDVLayoutBGColor	The general colors relate to the overall configuration of the page outside the plot, grid and legend. This general background color is also used for the Operator Notes page.
General Text	HDVLayoutTextColor	Sets the color used for text outside the plot area.
Plot Background	HDVPlotBGColor	Plot colors relate to all components within the plot area.
Plot Text	HDVPlotTextColor	Sets the color used for text within the plot area.
Plot Grid Lines	GridLineColor	Sets the color used for the grid lines of the plot area.
Plot Cursor Line	HDVTimeCursorColor	
Grid Background	HDVGridCellColor	Grid colors relate to all components within the grid list.
Grid Text	HDVGridTextColor	
Notes Background	HDVNotesBGColor	Notes colors relate to all components in the notes tab. These colors apply to both the Notes page of the HDV and the Operator Notes page.
Notes Text	HDVNotesTextColor	

Related Information:

...Display Tab of the Edit Properties Page

...Alarms Tab of the Edit Properties Page

...Other Tab of the Edit Properties Page

...Sort and Filter the Application Properties Dialog

Other Tab of the Edit Properties Page

Elements in the Display tab of the Edit Properties page are as follows:

Application

Settings that affect only the current workstation.

Property	Stored as	Description
Automatically deploy local changes.	AutomaticDeploy Stored in Setup.INI	If not checked, all changes made to this application will be local until you use the Deploy Changes option of the Application Configuration dialog.
Automatically start the application when VTScada starts.	AutoStart	It is often the case that the sole purpose of a workstation is to use VTScada to monitor and control equipment. Since the VTScada application is often the only program that

		will run on that computer, it makes sense to configure it to start automatically.
Disable comment dialog when applying changes.	RepositoryCommentDisable	The comments you type when applying a change may be the only record of why the change was made. Although not advised, you may check this option to disable the comment dialog.

OEM Layer

Settings that should be used only for applications that serve as OEM layers.

Don't show this layer in the VAM.	HideFromVAM	Applications must be loaded into the VAM in order to be used as an OEM layer, but you may wish to hide them for vari-
-----------------------------------	-------------	---

		ous reasons.
Don't allow this layer to run.	DoNotStart	Applications that serve as OEM layers are seldom run. Check this option to prevent operators from starting yours.
Synchronize the configuration of OEM layers via derived applications.	SyncOEMLayers	It can be difficult to maintain a server list for both the primary application and its OEM layer application, especially if the OEM layer is used at more than one site. You should therefore set this property. When set TRUE, the OEM layer will use the dependent application's server list when synchronizing configuration changes.

VTScada Application Manager

Settings for all applications.

Property	Stored as	Description
Hide the VAM from users without the Application Manager View privilege.	HideVAM	Prevent tampering by hiding the VAM from all but authorized users. Note: If using this setting, the application must also be set to start automatically.
Don't show the splash screen at startup.	NoSplash	Speed VTScada startup by skipping the splash screen.
Enable the "Toggle Visibility" icon on the VTScada application list. Note that this Setup.INI property affects all applications.	EnableShowHide	If enabled, authorized users can hide the application while it continues to run.
When hiding an application, log the current user off. Note that this Setup.INI property affects all applications.	LogOffUponHide	EnableShowHide must be set. Forces a log-off when the application is hidden.

Related Information:

...Display Tab of the Edit Properties Page

...Alarms Tab of the Edit Properties Page

...Historical Data Viewer Tab of Edit Properties

...Sort and Filter the Application Properties Dialog

Sort and Filter the Application Properties Dialog

There are many application properties. Finding the one you need, or even trying to browse through similar properties may take time. Three shortcuts have been provided to help you find properties faster.

Sorting: Click on the title of any column to sort the list by that column.

You can click the title a second time to sort in the opposite order.

Application Configuration

Filtering: Enter a portion of the name you are searching for in the field provided, then either press enter or click on the filter button. You should use the * wildcard for any portion of the name that you are not sure of. For example, to find Display Manager properties that begin with the letters "Disp", enter "Disp*" in the field.

Modify the properties of your application

To add an application property, click the "Insert" button. To delete an application property, select the property to delete and click the "Delete" button. To copy a property (for example, to override a setting for a particular workstation), select the property to copy and click the "Copy" button. To modify an application property, select the property and modify the property fields. You can sort by clicking on the column headings.

The changes you make are not applied until you click the "Apply" button.

Disp* Hide OEM Properties

Property Name	Section	Value	Workstation	Restart	OEM	Comment
DispMgrFullScreen	System	0	-- default --			Flag - TRUE to display in full screen mode
DispMgrResizable	System	1	-- default --			Flag - TRUE to allow application to be resized
DispMgrWidth	System		-- default --			Width of window in pixels if not in full screen mode
DispMgrHeight	System		-- default --			Height of window in pixels if not in full screen mode
DispMgrX	System		-- default --			X coordinate of window if not in full screen mode
DispMgrY	System		-- default --			Y coordinate of window if not in full screen mode
IntegerFormatLabel	Labels	Display Format	-- default --		<input checked="" type="checkbox"/>	
LeadingZerosLabel	Labels	Display Leading Z	-- default --		<input checked="" type="checkbox"/>	
DisplayWithLabelLabel	Labels	Display with Label	-- default --		<input checked="" type="checkbox"/>	
DisplayLastLabel	Labels	Display last	-- default --		<input checked="" type="checkbox"/>	
DisplayOrderLabel	Labels	Display Order	-- default --		<input checked="" type="checkbox"/>	
DispTimeLabelsLabel	Labels	Display time label	-- default --		<input checked="" type="checkbox"/>	
DisplayMaxLabel	Labels	Displayed Value N	-- default --		<input checked="" type="checkbox"/>	
DisplayMinLabel	Labels	Displayed Value N	-- default --		<input checked="" type="checkbox"/>	
DisplayManagerTitle	Labels		-- default --		<input checked="" type="checkbox"/>	
GroupPageDisplayLabel	Labels	Display	-- default --		<input checked="" type="checkbox"/>	
GroupGraphicDisplayLabel	Labels	Display	-- default --		<input checked="" type="checkbox"/>	
DispMgrHoriz	System		-- default --		<input checked="" type="checkbox"/>	For multi-manager mode ONLY - number of windows
DispMgrVert	System		-- default --		<input checked="" type="checkbox"/>	For multi-manager mode ONLY - number of windows
DispMgrMinMaxDisable	System	0	-- default --		<input checked="" type="checkbox"/>	Flag - TRUE to disable the minimize and maximize buttons

Hide OEM Properties: Check the Hide OEM Properties option in order to limit the display to only those properties that are set in the current application.

Troubleshooting:

- The property cannot be found.

You may be trying to find a property that is not included in the default files. Refer to the instructions for adding a property.

- The property is gray and cannot be changed.
This property exists in the OEM layer. It affects the current application, but cannot be changed here. Refer to the instructions for copying a property to the current application.

Related Information:

...Application Properties Files – Structure and location of the files affecting an application.

...Unsaved Configuration Changes – Error dialog description.

Next Steps:

...Add a Property – Used in the rare instance that a property is not already in one of the files.

...Copy a Property – Make a local copy of an OEM property, with its own value.

...Change a Property's Value – Control the appearance or behavior of your application.

...Set a Workstation-Specific Property Value – Have a different appearance or behavior from one workstation to another.

Add a Property

A small number of properties are not included in the default Settings.Startup or Settings.Dynamic files. For example, if you are defining realm-area filtering, you will need to add a series of properties to designate the areas for each realm.

There are two methods for adding a property: To add a property to the Settings.Dynamic file or a Workstation.Dynamic file, it is easiest to use the Insert button in the Application Configuration dialog.

If adding a property to the Settings.Startup file, or if you are adding a property to a hidden section, then you should use a text editor to work directly in the file.

Another reason that you might add a property is if you wish to override a configuration setting from the file Setup.INI. Most commonly, this will be done in order to re-define a VTScada label within an application.

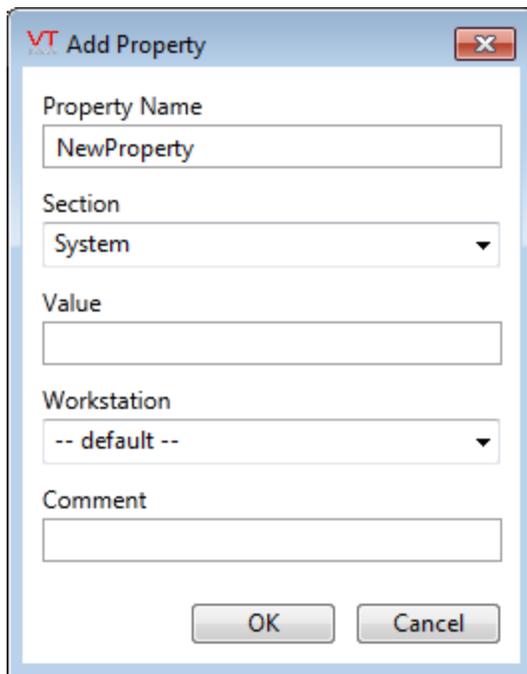
Notes:

- Property names may not include the following characters []<>=;
- Properties must be added within the correct section, otherwise they will be ignored.

Steps to add a new property using the Application Configuration dialog:

1. Open the Application Configuration dialog and select the Edit Properties page.

2. Click on the Insert button
The Add Property dialog will open.



3. Enter the Property Name.
4. Select or Enter a section.
Properties will be ignored if they are added to the wrong section of the Settings file.
5. Enter a value for the property
6. [optional] Select a workstation if this property is to be in effect on only that

- one.
7. Enter a comment, describing the new property.
Comments will be stored on the line below the property in the Settings.Dynamic file.
8. Click OK
The dialog closes. Note that the new property will not be saved until you apply your changes.
9. Click Apply.
The Comment dialog will appear.
10. Type a comment into the Comments dialog and click OK.
This comment is for the VTScada version control system and should explain why the new property is being added, unlike the earlier comment that explains what the property does.

Steps to add a new property using a text editor:

1. Start a text editor that does not add formatting to your document.
2. Open or create the file that the property should be added to.
 - a. Use Settings.Startup for properties that require a re-start.
 - b. Use Settings.Dynamic for hidden security manager properties.
 - c. Use WorkstationName.Startup or WorkstationName.Dynamic in the WorkstationSettings sub-folder for properties that apply only to a specific workstation.
3. Locate the appropriate section name for the property.
Section names are enclosed in square brackets. Each property listed in the reference section of this chapter will identify the section it must belong to.
4. Add the property using the format, `PropertyName = Value`
5. Add a comment to the following line using the format, `; Comment describing property.`
Comments must not be included on the same line as the property definition.
Comments on the same line will be taken as values for the property.
6. Save the file
7. In the VAM, click Import File Changes, or (better) use the Import/Export Files page of the Application Configuration dialog to import the new or edited file.

The Import/Export Files method is preferred because it enables you to review all changes in the file before proceeding with the import.

Troubleshooting:

- The new value has no effect.
Check that the property name is spelled correctly and that a legal value has been assigned.
Check that the property has been declared in the correct section.
Ensure that comments are not included on the same line as the property declaration.
Ensure that the file changes have been imported.
If the property requires a re-start, shut down the application and re-start it.

Related Information:

...Sort and Filter the Application Properties Dialog – Save time when looking for a property.

...Application Properties Files – Structure and location of the files affecting an application.

...Unsaved Configuration Changes – Error dialog description.

Next Steps:

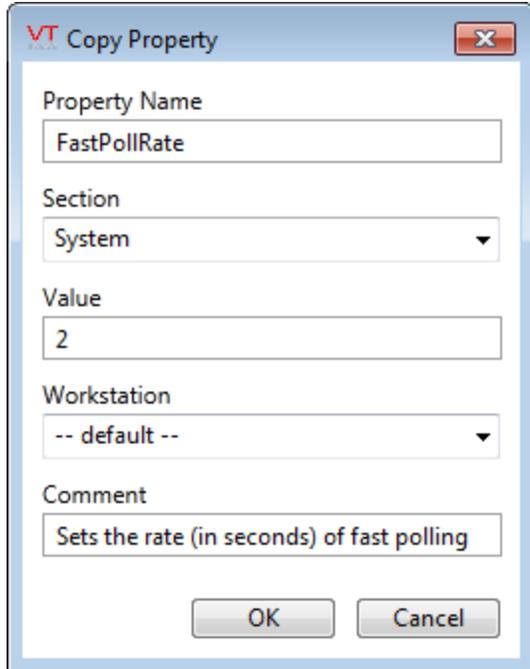
...Change a Property's Value – Control the appearance or behavior of your application.

...Set a Workstation-Specific Property Value – Have a different appearance or behavior from one workstation to another.

Copy a Property

This dialog shares many features with the one used to add a new property. There are two reasons to copy a property:

- To create a local copy of an OEM property, which you may then change for the current application.
- To set a workstation-specific value for a property.



The image shows a dialog box titled "VT Copy Property". It has a standard Windows-style title bar with a close button. The dialog contains the following fields:

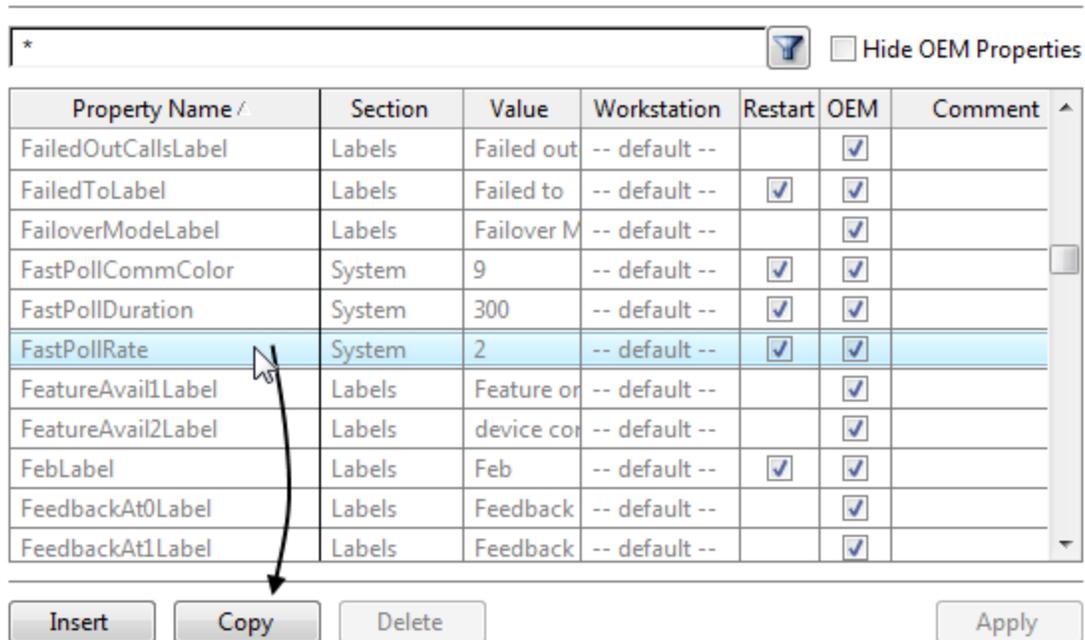
- Property Name:** A text box containing "FastPollRate".
- Section:** A dropdown menu with "System" selected.
- Value:** A text box containing "2".
- Workstation:** A dropdown menu with "-- default --" selected.
- Comment:** A text box containing "Sets the rate (in seconds) of fast polling".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

In the Edit Properties dialog, you will notice that a few properties are shown using a bold font while most are displayed using a faint gray shade. Those shown in a faint gray color are properties whose value has been set in one of the application's underlying OEM layers. (If the Hide OEM Properties option is checked, only local properties are shown.)

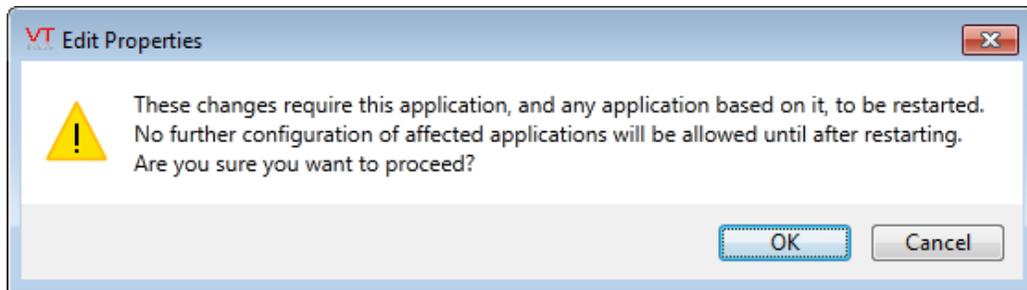
Note: A property set in the current application takes precedence over a property set in an OEM layer. The same property cannot be set twice in the application, within a section and having the same workstation name.

1. Open the Application Configuration dialog.
2. Ensure that the Hide OEM Properties box is not selected.
3. Find and select the property whose value you want to change.
See: Sort and Filter the Application Property List for shortcuts.
4. Click on the Copy button.
The Copy Property dialog will open.



Note: The Copy Property dialog enables you to change all fields. Note that unknown property names are ignored. Properties attached to the wrong section are likewise ignored.

5. Change the Value as required for your application.
6. [optional] If the copied property is meant to be in effect for only a particular workstation, type the name of that workstation in the field provided.
7. [optional] Alter the comment field to provide a reminder note to yourself, explaining the reason for the new value.
8. Click OK.
The dialog closes. Note that the new property will not be saved until you apply your changes.
9. Click Apply.
If the property is one that requires an application restart before it goes into effect, you will see the following warning:



10. Click on OK unless you would like to make other configuration changes before proceeding with this one.
The Comment dialog will appear.
11. Type a comment into the Comments dialog and click OK.
If you later use the VTScada controlled versioning system to review the changes made to your application, this comment will help you remember what changes were made and why.

Troubleshooting:

- The new value has no effect.
Check that the property name is spelled correctly and that a legal value has been assigned.
Check that the property has been declared in the correct section.
Ensure that comments are not included on the same line as the property declaration.
Ensure that the file changes have been imported.
If the property requires a re-start, shut down the application and re-start it.

Related Information:

- ...Sort and Filter the Application Properties Dialog – Save time when looking for a property.
- ...Application Properties Files – Structure and location of the files affecting an application.
- ...Unsaved Configuration Changes – Error dialog description.

Next Steps:

- ...Copy a Property – Make a local copy of an OEM property, with its own value.
- ...Change a Property's Value – Control the appearance or behavior of your application.
- ...Set a Workstation-Specific Property Value – Have a different appearance or behavior from one workstation to another.

Change a Property's Value

You can use the Edit Properties page of the Application Configuration dialog to change the value of a property that is set locally within an application. If the property's value is set in an OEM layer, you must copy that property to the current application layer in order to change it. If the property has not been defined in this application or any underlying layer, you must add it.

Note: The most commonly changed properties may be accessed through one of the three tabs of the basic mode, Display, Alarms, and Other, eliminating the need to use the following steps.

1. Open the Edit Properties page of the Application Configuration dialog.
2. Open the Advanced Mode.
3. Find and select the property whose value you want to change. Only properties that are not flagged as OEM (and displayed in a pale gray color) may be edited.
4. Click in the Value field.

An edit window will open within the field.

[Modify the properties of your application](#)

To add an application property, click the "Insert" button. To delete an application property, select the property to delete and click the "Delete" button. To copy a property (for example, to override a setting for a particular workstation), select the property to copy and click the "Copy" button. To modify an application property, select the property and modify the property fields. You can sort by clicking on the column headings.

The changes you make are not applied until you click the "Apply" button.

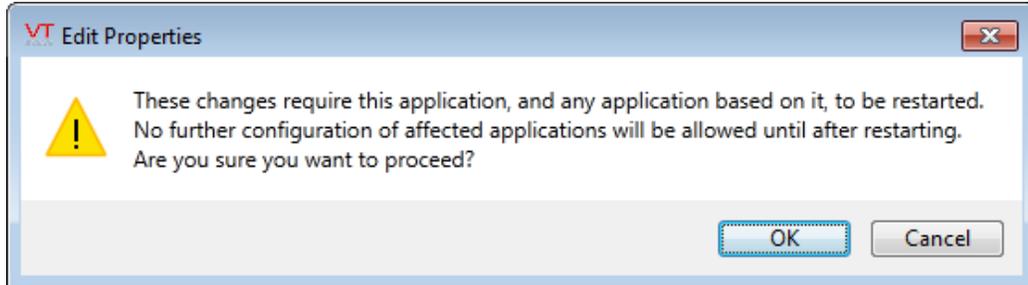
*
 Hide OEM Properties

Property Name	Section	Value	Workstation	Restart	OEM	Comment
DispMgrResizable	System	1	-- default --			Flag - TRUE to allow application to be resized
DispMgrWidth	System		-- default --			Width of window in pixels if not in full screen mode
DispMgrHeight	System		-- default --			Height of window in pixels if not in full screen mode
DispMgrX	System		-- default --			X coordinate of window if not in full screen mode
DispMgrY	System		-- default --			Y coordinate of window if not in full screen mode
AlarmKeySize	System	256	-- default --	<input checked="" type="checkbox"/>		The maximum number of characters in an alarm name
ModiconTypedAddr1Offset	System	<input style="width: 30px;" type="text" value=""/>	-- default --	<input checked="" type="checkbox"/>		Applies offset for "Type specified" Modicon address, e
Name	Application	VTScada Library	-- default --		<input checked="" type="checkbox"/>	Application Name
AutoActivate	Application	0	-- default --		<input checked="" type="checkbox"/>	TRUE to automatically activate this application when th
AutoStart	Application	0	-- default --		<input checked="" type="checkbox"/>	TRUE to automatically start this application when the V
PageNoteAddTip	Labels	Add Page Note	-- default --		<input checked="" type="checkbox"/>	

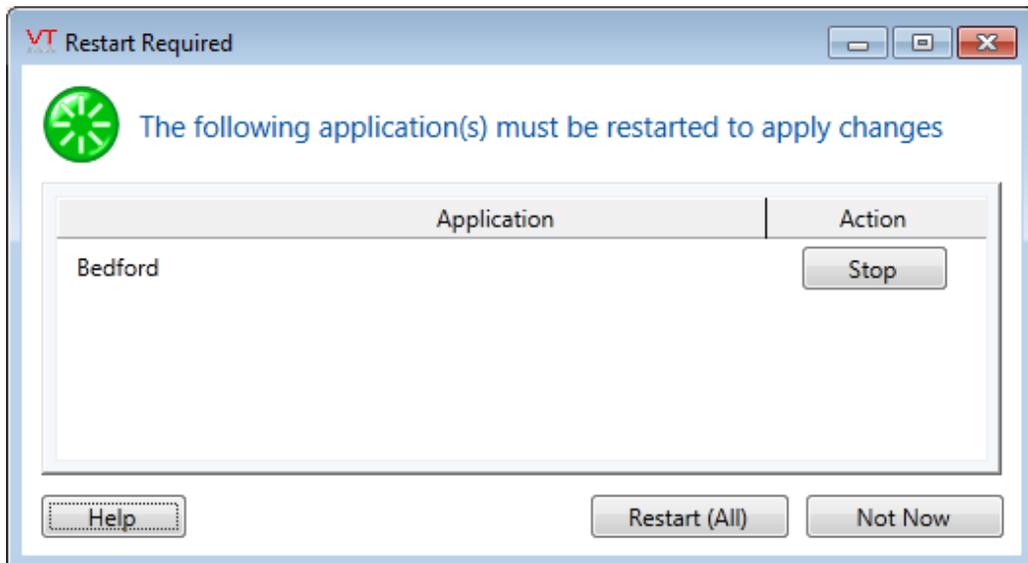
Insert
Copy
Delete

Basic Mode
Apply

5. Type a new value for the property and press Enter.
6. Click on the Apply button.
If the property is one that requires an application restart before it goes into effect, you will see the following warning:

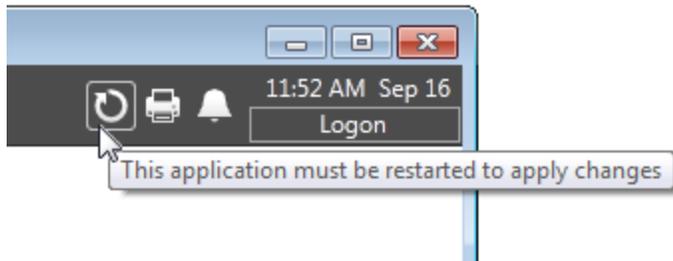


7. Click on OK unless you would like to make other configuration changes before proceeding with this one.
The Comment dialog will open.
8. Type a comment into the Comments dialog and click OK.
If you later use the VTScada version control system to review the changes made to your application, this comment will help you remember why the changes were made.
9. If the property requires a re-start before it takes effect, you will see the following dialog. Choose whether to stop the application, restart now or restart later.



If you choose Not Now, the Restart Required symbol will be added to the application's title bar and further configuration changes will not be allowed.

The buttons for the Idea Studio, Application Properties, Tag Browser and for Page Notes will be hidden.



Troubleshooting:

- The new value has no effect.
Check that the property name is spelled correctly and that a legal value has been assigned.
Check that the property has been declared in the correct section.
Ensure that comments are not included on the same line as the property declaration.
Ensure that the file changes have been imported.
If the property requires a re-start, shut down the application and re-start it.

Related Information:

...Sort and Filter the Application Properties Dialog – Save time when looking for a property.

...Application Properties Files – Structure and location of the files affecting an application.

...Unsaved Configuration Changes – Error dialog description.

Related Tasks:

...Copy a Property – Make a local copy of an OEM property, with its own value.

...Set a Workstation-Specific Property Value – Have a different appearance or behavior from one workstation to another.

Set a Workstation-Specific Property Value

Any property can be assigned a value that will apply only to the instance of VTScada running on a specific workstation. You might use this feature

to set display properties or security features that will be in effect only for a given workstation.

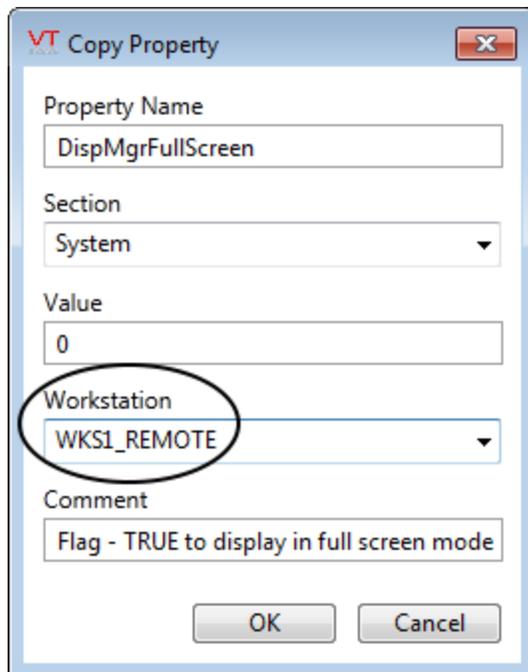
Workstation-specific properties are stored in a file named after the workstation where they will apply and having an extension of either .Startup or .Dynamic. They are located in the WorkstationSettings sub-folder of your application.

To set a workstation-specific property value:

1. Open the Edit Properties page of the Application Configuration dialog.
2. Locate and copy the property.

Property Name	Section	Value	Workstation	Restart	OEM/	Comment
AlarmKeySize	System	256	-- default --	<input checked="" type="checkbox"/>		The maximum number of characters in an
CallOutDelay1	System	300	-- default --			
CallOutDelay2	System	900	-- default --			
CallOutPriority	System	2	-- default --			
DialerConnectDelay	System	5	-- default --			The interval from when a call is initiated u
DialerLocation	System	The VTS System	-- default --			
DispMgrFullScreen	System	1	-- default --			Flag - TRUE to display in full screen mode
DispMgrHeight	System		-- default --			Height of window in pixels if not in full scr
DispMgrResizable	System	0	-- default --			Flag - TRUE to allow application to be resiz
DispMgrWidth	System		-- default --			Width of window in pixels if not in full scre
DispMgrX	System		-- default --			X coordinate of window if not in full screen
DispMgrY	System		-- default --			Y coordinate of window if not in full screen
DNP3LocalTimestampsDe	System	0	-- default --			DNP3 driver default timestamp timezone

3. In the Workstation field of the property, select or type the machine name of the workstation where this property will apply.



4. Set the value that will be used on that workstation, then click OK.
5. Click Apply.
6. Provide a comment when prompted.

If the property is flagged as requiring a restart, you will need to stop and restart the application before the new value goes into effect and before you are able to make any further changes to the list of application properties.

For more information about workstation-specific properties, see: [Workstation-Specific Properties](#).

Apply and Deploy Changes to Application Properties

None of the changes that you make to an application's properties, using the Edit Properties dialog will be saved or put into effect until you click on the Apply Changes button.

If you leave the page without clicking the Apply button, you will see the following warning.

If you click on the Yes button, the Edit Properties page will close and none of your edits will be saved. Clicking on No closes the warning and leaves the Edit Properties dialog open so that you can use the Apply button.

Troubleshooting:

- The new value has no effect.
 - Check that the property name is spelled correctly and that a legal value has been assigned.
 - Check that the property has been declared in the correct section.
 - Ensure that comments are not included on the same line as the property declaration.
 - Ensure that the file changes have been imported.
 - If the property requires a re-start, shut down the application and re-start it.

Related Information:

...Sort and Filter the Application Properties Dialog – Save time when looking for a property.

...Application Properties Files – Structure and location of the files affecting an application.

...Unsaved Configuration Changes – Error dialog description.

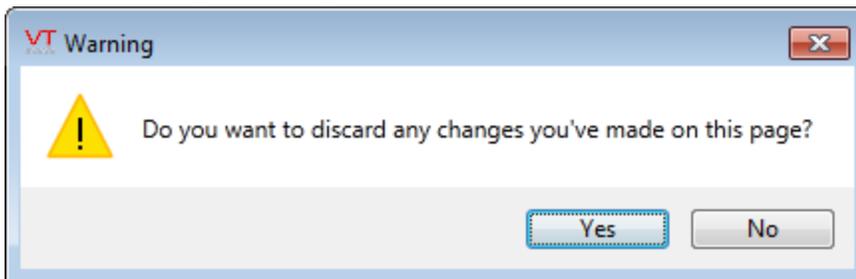
...Add a Property – Used in the rare instance that a property is not already in one of the files.

...Copy a Property – Make a local copy of an OEM property, with its own value.

...Change a Property's Value – Control the appearance or behavior of your application.

Unsaved Configuration Changes

If you make changes in the Application Configuration dialog, then navigate to a different page, or close the configuration window, you will see the following message.



Unsaved changes will be lost if you either close the dialog or navigate to a different page of the Application Configuration screen.

Click Yes to discard the changes and continue navigating or No to retain the changes and continue working on the same page.

Application Properties Files

Most VTScada application properties are stored in one of two files: Settings.Startup and Settings.Dynamic, found in the root directory of your application. Properties that are flagged as workstation-specific are stored in one of Workstation.Startup or Workstation.Dynamic.

Note: In almost all cases it is better to modify application properties using the Edit Properties page of the Application Configuration dialog.

Note: If you must edit one of the property files directly, find it in the application's root directory and after editing it, import it using File Import/Export tool in the Application Configuration dialog. Do not edit any file located in the .sync folder of your application. Any attempt to do so will damage the application.

The exception to the above is the file, Setup.INI. This configuration file is located in the VTScada directory (C:\VTScada\SETUP.INI) and provides system-wide configuration, affecting the behavior and appearance of the VTScada program. You can change values within Setup.INI using any text editor.

All other configuration files, such as AlarmManager.INI, SecurityManager.INI, etc. are obsolete.

Related Information:

- ...Configuration Hierarchy
- ...Editing Application Properties
- ...Import Edited Files
- ...Rules for Application Property Files
- ...Section Names for Property Files
- ...Workstation-Specific Properties

Configuration Hierarchy

Note: Definition: Applications that are not script-based are referred to as "standard applications". All standard applications are ultimately based on the VTScada library layer, regardless of how many OEM layers exist.

When a VTScada application starts, it loads the properties within itself and all of the OEM layers upon which it is based. Properties defined in higher levels take precedence over those defined in lower levels. All standard applications will use the complete set of property definitions found in the VTScada library layer unless those properties are re-defined in an OEM layer or in the application itself.

The exception is the Setup.ini configuration file, which contains system-wide configuration variables that affect the appearance and behavior of the VTScada software. There is only one Setup.ini file.

The process by which VTScada loads application properties is as follows:

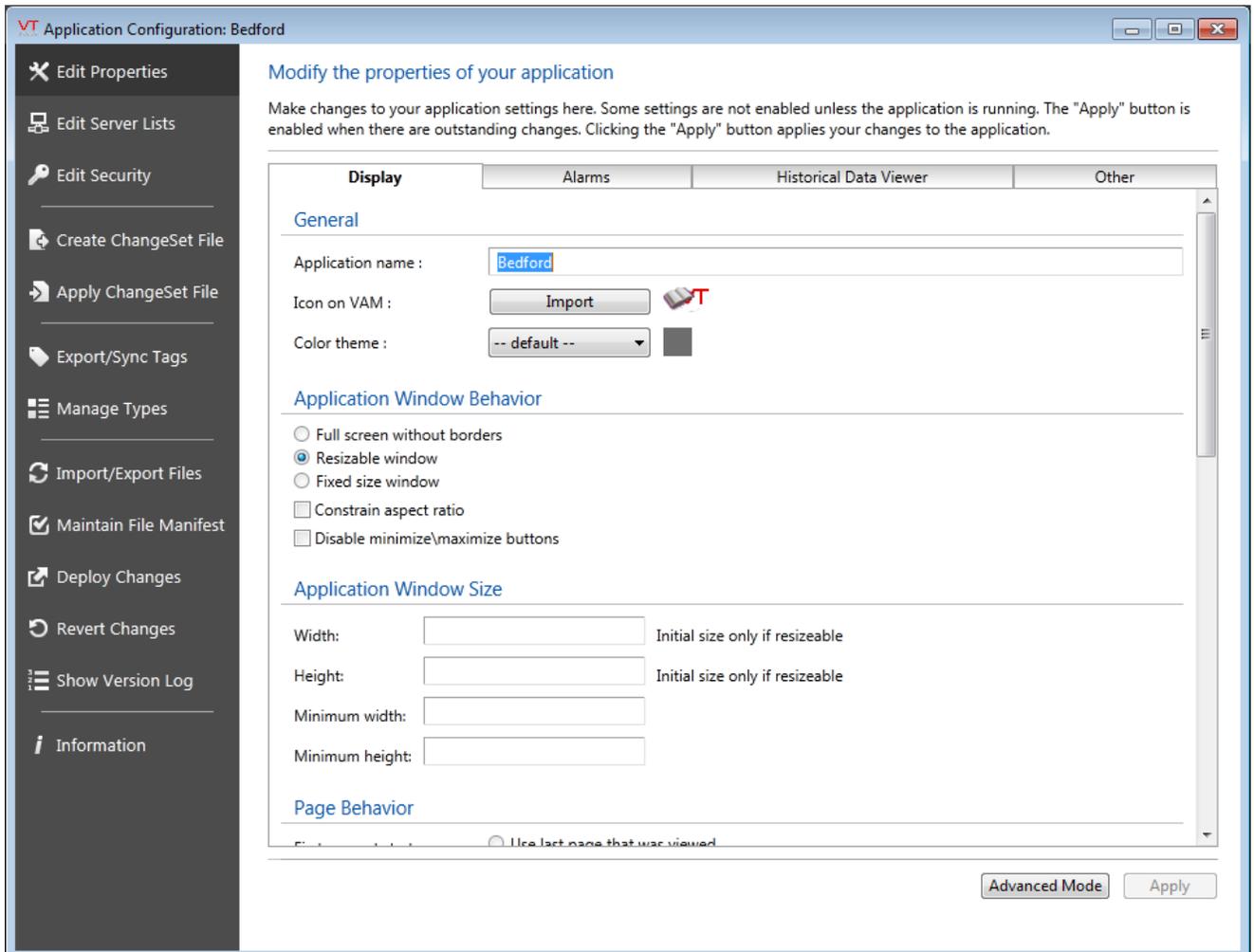
1. Properties that are flagged with the name of the current workstation, will be loaded and used.
2. VTScada loads all the properties defined in the application. All properties that were not already found in the previous step, are loaded.
3. VTScada loads all the properties found in the OEM layer that the application is based on. All properties that were not already found in the previous steps, are loaded. This step repeats for all OEM layers.
4. VTScada loads all the properties found in the VTScada layer. Any that were not already found in the previous step, are now loaded.

Editing Application Properties

Note: Do not edit application properties for the VTScada layer. Changes made to these layers will be ignored. Make all of your edits in either your OEM layer, or in the application.

In versions of VTS prior to release 10, configuration variables were edited within one of the .INI files. This system has been replaced by "application properties" that are controlled using the Application

Configuration dialog. Within this tool, the Edit Properties page gives you access to all of the application's properties.



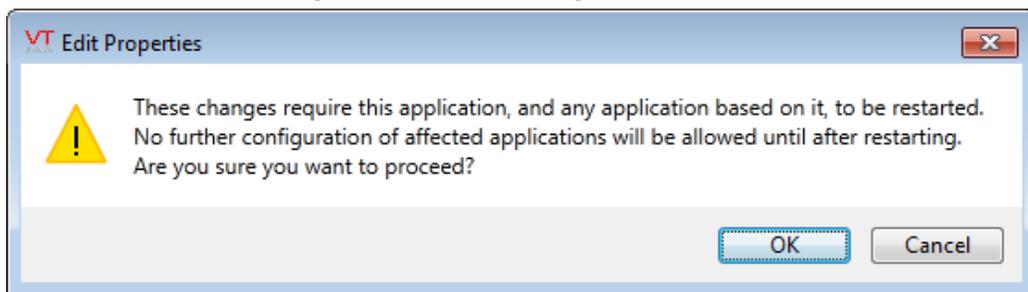
A property that is displayed in bold text is local to your application. Those displayed using a faint text are supplied by an underlying OEM layer. If the property is given different values by multiple underlying OEM layers, only the top-most is shown. With the Hide OEM Properties check box, you can restrict the view to show only those properties whose value is set at the application level.

To set the value of a property for your application, copy that property to the application level, and then set the value of the new copy. The steps are as follows:

1. Open the Edit Properties page of the Application Configuration dialog for your application.

2. Click on the heading, Property Name to sort the table by name.
This makes it easier to find the property you want.
3. Find and select the property that you want to edit.
4. Click on Copy
A local copy of the property will now exist in your application.
5. Click on the Value field for the copied property.
6. Enter a new value.
7. Click on Apply.
8. Provide a reason for the new value, in the dialog box that opens.
All changes are recorded in the application's history. By providing a reason for the edit, you make it easier for yourself or others to understand why changes were made.

If the property requires a restart before it takes effect, the following dialog will appear when you click on Apply Changes. You must restart the application before making any other changes to application properties.



Note: If the AutoDeploy option is not checked (available in the "Other" application properties tab of the Application Configuration dialog), then you will need to Deploy Changes before the new values are put into use throughout your application.

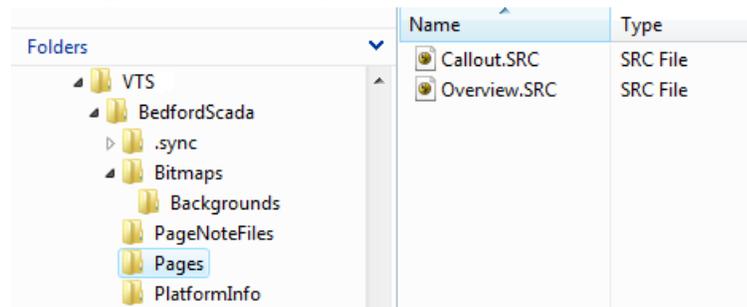
Import Edited Files

All files used by an application are stored within the VTScada version control system. If you make changes to files outside the repository, such as editing a page file, changing a background image, or modifying the configuration files Startup.Settings and Dynamic.Settings, then you must import the edited file into the version control system before it will be used by the application.

The Import/Export Files page of the Application Configuration dialog is used bring manual edits into the running application. 5 separate tasks can be done with this page:

- Import changed files.
- Discard changed files
- Export the contents of the working copy of the file to the off-line copy.
- Compare the contents of the offline source-file to the working copy.
- Reload the display. (Useful if the working copy was edited while the dialog is open.)

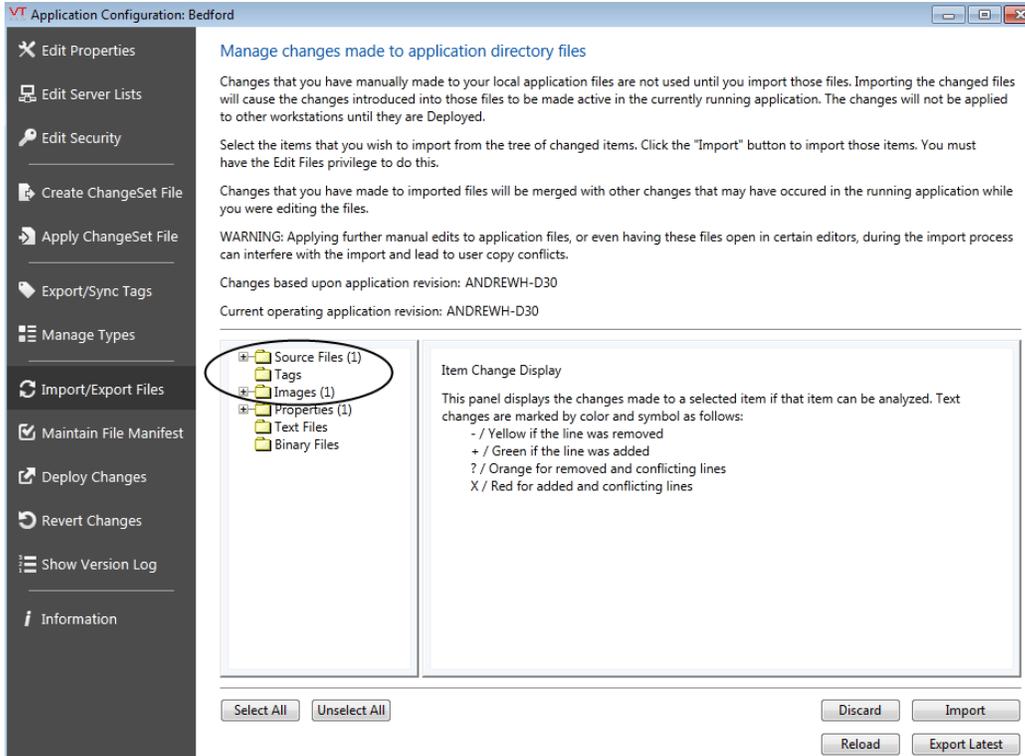
The following image shows the Pages folder for a simple application. In this example, the folder Bitmaps\Backgrounds has been added, containing one file: CityMap.PNG (not shown here).



For this example, a text editor has been used to make an offline change to the file Overview.SRC. A paint program has been used to modify the city map.

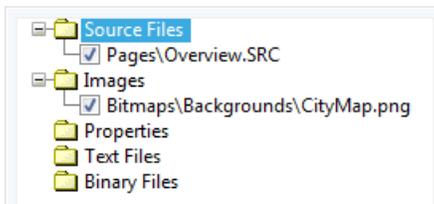
To import the changed files, go to the VAM, select the application and click on the properties button.

In the Application Configuration dialog, select Import/Export Files, as shown:



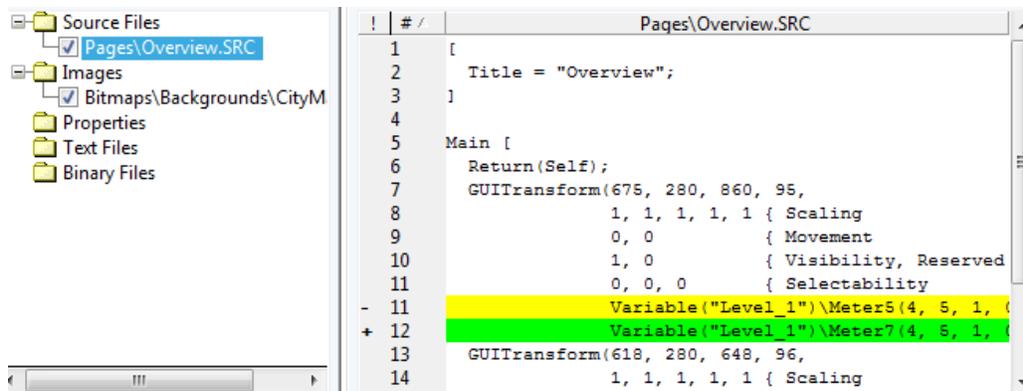
Note the plus signs beside both Source Files and Images. This indicates that VTScada has found files of both these types to which off-line edits have been made.

Clicking on the plus signs expands the tree so that the edited files may be seen:



Selecting an edited source file will result in the edits being displayed for you to review. In the following image, green shows the contents of a line as found in the edited file and yellow shows the version of that code in use in the application. The difference between the two is that an off-line change was made to swap Meter7 for Meter5.

Application Configuration



In the case of image files, differences in the file sizes and last modified dates will be shown.

At the bottom of the Import File Edits dialog are four control buttons:

Discard Replaces the file with the version in the working directory, discarding all off-line edits.

Import Merge the changes in from the off-line file into the working copy.

Reload Refresh the display

Export Changes found in the working copy that are not in the off-line

Latest file are exported. Changes in the off-line file that do not conflict with the working copy are not lost.

You must click on Import for your off-line edits to become part of the working application. All selected files are imported.

Application Property Components

Every application property consists of the following components:

Property component	Description
Name	Identifies the property
Section	Within the property storage files, properties are organized by section. A property assigned to the wrong section will be ignored by VTScada.
Value	The value assigned to a property. Boolean values (TRUE or FALSE) are given values of 1 for TRUE and 0 for FALSE.

Workstation	set to "—default —" if the property is not restricted by workstation. If the property's value is to apply to a given workstation, type the name of that station in the Workstation field.
Restart	Automatically assigned. A checkmark here indicates that the changes to the property will only take effect when the workstation is restarted. If there is no checkmark, the new value for the property will go into effect when the change is deployed.
OEM	Automatically assigned. A check here indicates that the value for the property was defined in an OEM layer that the application is based upon rather than in the application itself.
Comment	Notes to describe the property.

Errors in the application properties table are ignored. If you have misspelled a variable, or have assigned a value of the wrong type (perhaps a word instead of a number) then that line in the table will be ignored and VTScada will find the value in a lower-level properties table.

Rules for Application Property Files

- Section headings and properties **MUST** appear in the appropriate configuration file to be recognized by VTScada.
- Properties must appear under the appropriate section heading to be valid;
- Section headings **MUST** be surrounded by square brackets;
- Section headings and property names **MUST** not have spaces;
- Property names must not include the following characters `[]<>=;`
- Section headings and properties **MUST** be spelled exactly as they appear in this guide;
- Properties and their values **MUST** be separated by an equals sign (=) (unless otherwise specified);
- Values **MUST** be valid values as indicated in this guide. Values may be numeric (either 1 or 0, or another value), a text string, or a path or file name, depending upon the variable. Valid values are specified for each variable in this guide.
- If you wish to add comments throughout a configuration file, each comment line must be prefaced by a semicolon, and comments must appear on a line

Application Configuration

underneath the variable being commented – no comments should appear on the same line as a variable. For example (correct):

```
[SYSTEM]
DispMgrFullScreen = 1
; FALSE if the Display Manager should have a windows title bar.
DispMgrWidth = 700
; Indicates the width of the Display Manager
DispMgrHeight = 500
; Indicates the height of the Display Manager
```

Rather than (incorrect):

```
[SYSTEM]
DispMgrFullScreen = 1 ;FALSE if there should be a windows title bar.
DispMgrWidth = 700 ;Indicates the width of the Display Manager
DispMgrHeight = 500 ;Indicates the height of the Display Manager
```

The following are suggestions, rather than rules:

- Section headings and properties should follow the case conventions displayed in this guide. (For example, "<SECURITYMANAGER-PrivApp>", not "<securitymanager-privapp>".) These case conventions help to clearly distinguish property names making them easier to read
- Properties and their values should follow the spacing conventions displayed in this guide. For example, separate all properties from the equals sign using a tab, and separate the equals sign from the value using a tab. Again, this helps to clearly distinguish and organize properties and values, making them easier to read.

Note: Throughout this section, the documented properties requiring a value of 1 (true) or 0 (false) will also accept and recognize the literal values TRUE or FALSE. However, for the purposes of consistency, the values 1 and 0 will be used in this guide.

Workstation-Specific Properties

Application properties can be configured that take effect only on specified workstations. From within the Application Configuration dialog, this is done by specifying the workstation name beside the property as shown:

- Edit Properties
- Edit Server Lists
- Edit Security
- Create ChangeSet File
- Apply ChangeSet File
- Export/Sync Tags
- Manage Types
- Import/Export Files
- Maintain File Manifest
- Deploy Changes
- Revert Changes
- Show Version Log
- Information

Modify the properties of your application

To add an application property, click the "Insert" button. To delete an application property, select the property to delete and click the "Delete" button. To copy a property (for example, to override a setting for a particular workstation), select the property to copy and click the "Copy" button. To modify an application property, select the property and modify the property fields. You can sort by clicking on the column headings.

The changes you make are not applied until you click the "Apply" button.

Property Name /	Section	Value	Workstation	Restart	OEM	Comment
DefaultPageColor	System	15	-- default --			Default background color of a page
DialerConnectDelay	System	5	-- default --			The interval from when a call is initiated until s
DispMgrFullScreen	System	0	-- default --			Flag - TRUE to display in full screen mode
DispMgrFullScreen	System	1	ANDREWH			Flag - TRUE to display in full screen mode
DispMgrHeight	System		-- default --			Height of window in pixels if not in full screen r
DispMgrResizable	System	1	-- default --			Flag - TRUE to allow application to be resized
DispMgrWidth	System		-- default --			Width of window in pixels if not in full screen m
DispMgrX	System		-- default --			X coordinate of window if not in full screen mo
DispMgrY	System		-- default --			Y coordinate of window if not in full screen mo
DNP3LocalTimestamp	System	0	-- default --			DNP3 driver default timestamp timezone
DriverRPCOptimizatio	System	1	-- default --			Enables generic VTSDriver data handling optim
EchoPhoneThroughSp	System	0	-- default --			
MenuItemsAutoGene	Application	1	-- default --			TRUE indicates that MenuItem tags have already
ModiconTypedAddr1	System	0	-- default --	<input checked="" type="checkbox"/>		Applies offset for "Type specified" Modicon adk
Name	Application	Bedford	-- default --			Application Name
Page	System	PageMenuPage(Ir	-- default --			Initial page to show when application starts
RepeatMenuTime	System	5	-- default --			The interval between speech utterances if no o
RosterDelay	System	0	-- default --			
SimulateIO	System	0	-- default --			

Insert
Copy
Delete
Basic Mode
Apply

In this example, the setting for the variable, DispMgrFullScreen will only apply to the VTScada installation running on the workstation, ANDREWH. Workstation-specific properties are stored in files named after the workstation to which they apply. For the example given, there will be a file named, "ANDREWH.Startup" in the subdirectory "WorkstationSettings". (C:\VTScada\BedfordScada\WorkstationSettings\ANDREWH.Startup") The extension is "Startup" rather than "Dynamic" since this example used a property that takes effect only on application startup. The structure of the Workstation files is identical to that of the Settings.Startup and Settings.Dynamic files. All of the same rules for section names, comments, etc. apply.

Section Names for Property Files

Application properties are organized by section. If you change a property to use a section other than the one it was meant for, then that property

will be ignored by VTScada. Note the shape of the brackets delimiting each section name.

- [] Section names in square brackets will be shown in the Application Configuration dialog.
- <> Section names in angled brackets are hidden from that dialog.

Properties in an hidden section may still be changed, but must be edited directly in the user copy of the Settings file and that file then imported into the application.

The following sections are defined application properties.

Section Name	Used in	Notes
<APPLICATION>	Settings.Startup	Introduced in VTS version 10. The <APPLICATION> section includes information that in previous versions of VTScada was stored in the file GDI.WIF, as well as other application-specific properties such as AutoStart.
[Application]	Settings.Dynamic	Similar to <Application> in the .Startup file, but contains application-level properties that may change dynamically. Examples include AutoActivate, Name and Vamlcon.
<ALARM_MANAGER>	Settings.Startup	The <ALARM_MANAGER. section includes the properties that define the format of alarm records, and the default filter dialog format. See also: <ALARM_MANAGER>
[Areas]	Workstation.Startup	When added to one or more of an application's Workstation.Startup files, the [AREAS] section enables you to perform tag area filtering. See also: [Areas]
[LABELS]	Settings.Startup & Settings.Dynamic	Application properties in the [LABELS] section are used to set the text associated with all the labels related to your application. See also: [LABELS]
<SecurityManager-Admin>	Settings.Dynamic	The hidden section, <SecurityManager-Admin>, contains properties set by the Administrative screen of the security man-

		ager. These include properties controlling the default AutoLogoff time and minimum password length.
<SecurityManager-PrivSys>	Settings.Dynamic	The hidden section, <SecurityManager-PrivSys>, sets the name used for each of the system privileges.
[StandardServerLists]	Settings.Dynamic	The [StandardServerLists] section defines server lists available to choose from when adding a new service in the Edit Server Lists panel.
[SYSTEM]	Settings.Dynamic & Settings.Startup	The [SYSTEM] section contains a list of variables that will determine the attributes of the application while it is running. Any values in the [SYSTEM] section are added or modified in the root system VTScada module. The [SYSTEM] section corresponds to the class 0 variables in AppRoot.src
[SystemAlarmAreas]	Settings.Startup	The [SystemAlarmAreas] section contains a list of predefined areas in use by VTScada. These are used when filtering the alarm history display in order to view only certain system such as "Security" and "OperatorLog". Using the area names from this list will cause no harm ("System" is commonly used for port, driver and other tags), but as a general guideline you may wish to avoid using the area names, "Security", "OperatorLog, " and "Report" for I/O tags.

<ALARM_MANAGER>

File: Settings.Startup

The <ALARM_MANAGER> section includes the properties that define the format of alarm records, and the default filter dialog format.

The <ALARM_MANAGER> section may also be used for filtering alarm tags according to their Area property so that only the alarm tags

belonging to certain areas are loaded on specific workstations. Alarm area filtering on specific workstations can be performed by the workstation name for specific properties.

```
<Alarm_Manager>
; The record fields.
KEYCOUNT = 7
KeyName = Message, 0, 80
KeyName = Priority, 1, -1
KeyName = Type, 2, -1
KeyName = HookPointValue, 3, -3
KeyName = Area, 4, 32
KeyName = HookPointUnits, 5, 15
KeyName = Operator, 6, 32
; The number of extra lists required (see Lists).
LISTS = 0
;The record fields
FILTERCOUNT = 6
FilterName = 0, 1, 0, Message for the alarm
FilterName = 1, 2, 0, Priority
FilterName = 2, 3, 0, Type of Alarm
FilterName = 3, 4, 0, Value
FilterName = 4, 5, 0, Area
FilterName = 5, -2, 0, Alarm Name
```

KeyCount Specifies the number of alarm fields that are stored in the alarm database (Alarms.db), as qualified by the number of KeyName variables that follow it.

Note: For VTScada programmers: If working directly in the Settings.Startup file, the KeyCount property must be defined before any KeyName variables. Any KeyName variables found before the KeyCount variables are ignored. Also, the KeyCount variable must be incremented according to the number of KeyName entries you configure. For example, if you specify 7 KeyName entries, then KeyCount should be set equal to 7.

KeyName Defines the fields in the alarm database (Alarms.db). Each KeyName entry indicates the name of the variable representing each field, the index number for the field in the alarm database, and the data type corresponding to the type of data to be stored in the field. The syntax is as follows:

KeyName = <Name>, <Position>, <Size>

Where:

- Name is the variable name associated with the database field.
- Position is the position of this field within the record (starting at zero and incrementing by one for each subsequent KeyName variable).
- Size is the size of the field.
- A positive size defines the size of a text field.
- A size of zero defines a record of unknown size; any value can be put in the field, but it will not be saved to any file.
- A negative size indicates a numeric data type:
 - 1 for a signed short integer (2 bytes).
 - 2 for a signed long integer (4 bytes).
 - 3 for a signed double-precision floating-point variable (8 bytes).

Lists Used when extra user-defined lists are required within the alarm database (Alarms.db). The number indicates the number of extra lists required over the default lists (i.e. the Active, Unacknowledged, and Disabled lists that are present by default in the Alarms.db).

Note: Changing the Lists variable makes it necessary for you to delete the Alarms.log and Alarms.db files from your application directory.

FilterCount Indicates the number of filterable keys that you wish to be displayed in the Alarm Filtering dialog.

Note: For VTScada programmers: The FilterCount variable must be defined before any FilterName variables. Any FilterName variables found before the FilterCount variables are ignored.

FilterName Used to define the fields displayed in the Alarm Filtering dialog. See: Filter Dialog Button

The syntax is as follows:

FilterName = <Position>, <Field>, 0, <Description>

Where:

- 0 must be entered as the fourth parameter.
- Field is the field number assigned to this filtering item (starting at 1).
- Position is the position of this filtering item in the Alarm Filtering dialog, starting at 0 (from top to bottom in the list of filterable fields).

- Description is the description of this filtering item to be displayed in the Alarm Filtering dialog

[Areas]

File: **Workstation.Startup**

When added to one or more of an application's Workstation.Startup files, the [AREAS] section enables you to perform tag area filtering. In summary, you list the tag areas that you wish to load on a given workstation, followed by an equals sign, followed by a 1.

Example:

```
[AREAS]
AreaA = 1
AreaB = 1
```

The result of this example is that, for the workstation matching the name .Startup file name that these values are stored in, tags configured with AreaA or AreaB as their Area property will be loaded at startup. If the AreaExclude variable is set to 1 in the [System] section of the file, then only tags with these areas will be loaded.

Related Information:

...See: "Tag Area Filtering" in the VTScada Developer's Guide for details and examples.

[LABELS]

File: **Settings.Dynamic & Settings.Startup**

Application properties in the [LABELS] section are used to set the text associated with all the labels related to your application. You may customize the text that appears on dialogs and messages throughout the entire application by modifying these properties.

Possible reasons for doing so include: modifying the application according to the needs of your company, translating the operator interface into another language (English is the default), or to customizing the wording of dialogs to better suit your application.

To change the appearance for each label, simply enter the name of the label, followed by the text you wish to appear.

```
[LABELS]  
AreasLabel = Tag Areas
```

Applying the above example would result in the "Areas" label that appears above the Tag Browser's Areas drop-down list to be labeled "Tag Areas"

Note that a [LABELS] section also exists in the Setup.INI configuration file. Labels in Setup.INI can be used to customize the entire VTScada software product according to your needs. See: Setup.ini [LABELS] Section Variables.

Sections for Realm Area Filtering

The sections, [REALMAREAS], [*-REALMAREAS], and [<Area>-REALMAREAS] are used to perform filtering on tags based on the Area with which they've been configured. This filtering technology works with security groups to enable you to specify:

- What tag areas should be accessible (if any) when no user is logged on to the application.
- What tag areas should be accessible when a group user is logged on to the application.
- What tag areas should be accessible when a super user is logged on to the application.

A group user is one whose account has been assigned to a security group. A super user is one who is not restricted by any security group.

Note: Realm-area filtering affects internet logons. Users may log on to only the realm name matching their security group. Users who are not part of a security group may log on to only the realm specified by the application property, RootNamespace.

Related Information:

...See also: "Realm Area Filtering" in the VTScada Developer's Guide

[REALMAREAS] Section

The application properties in the [REALMAREAS] section are used to indicate the tag areas that should be permissible when no user is logged on to your application. (You may wish to protect your system by preventing view access for users who are not logged on.)

To specify the tag areas that should be permissible to users who are not logged onto your application, follow the syntax shown:

```
[REALMAREAS]
Area = <area>
Area = <area>
...
```

In the example above, <area> indicates the tag areas permissible to users who are not logged on to the application. For example:

```
[REALMAREAS]
Area = Station005
Area = Station006
```

In this example, were a user to access the VTScada application using a VIC, but was not logged on to the application, he/she would only be permitted to view those tags whose area has been configured as "Station005" and "Station006".

If you wish to configure an application so that if users are not logged on, they will not be permitted to view any tag data, set the Area variable equal to nothing, as shown:

```
[REALMAREAS]
Area =
```

Note: The question mark (?) and asterisk (*) wildcard characters are permitted. Area declarations are not case-sensitive, nor is the [REALMAREAS] section heading.

Related Information:

...See also: "Realm Area Filtering" in the VTScada Developer's Guide

[*-REALMAREAS] Section

The [*-REALMAREAS] section enables you to indicate the areas that should be permissible when a super user is logged on to your application

(a super user is one who is not restricted by any group and who has access to all application data).

Note: In addition to configuring the [*-REALMAREAS] section, be sure to set up security groups in order to restrict users to certain tag areas based on the group to which they've logged on. See: Realm Area Filtering.

```
[*-REALMAREAS]
Area = *
```

In this example, the asterisk (*) wildcard character in the section heading (i.e. [*-REALMAREAS]) indicates all realms, and the asterisk wildcard character following "Area" indicates all areas. The result of the above example is that super users will see everything.

Note: The question mark (?) and asterisk (*) wildcard characters are permitted. Area declarations are not case-sensitive, nor is the [REALMAREAS] section heading.

The section that follows discusses setting permissible tag areas for viewing by members of a specific security group.

Note: Detailed information on realm area filtering (including examples) is provided in Realm Area Filtering.

[<Area>-REALMAREAS] Section

The [<Area>-REALMAREAS] section is used to indicate the areas that should be permissible when a group user is logged on to your application. To properly use the [<Area>-REALMAREAS] section, follow the syntax shown:

```
[<Area>-REALMAREAS]
Area = <area>
Area = <area>
...
```

Note: The question mark (?) and asterisk (*) wildcard characters are permitted. Area declarations are not case-sensitive, nor is the [REALMAREAS] section heading.

In the example above, <Area> in the section heading (i.e. [<Area>-REALMAREAS]) indicates the name of the realm or security group, and <area> declarations beneath the section heading indicate the tag areas permissible when a user is logged on to that realm. For example:

```
[NE-REALMAREAS]
Area = Tank
Area = Pump
```

Using the example above, a VIC user logged on to the "NE" realm or security group using his or her user account will be permitted to view all tags whose area is either "Tank" or "Pump".

Note: In addition to configuring the [<Area>-REALMAREAS] section, be sure to set up security groups in order to restrict users to certain tag areas based on the realm to which they've logged on. See: [Realm Area Filtering](#).

Alarm Notification System Properties

The following list of variables belong to the VTScada Alarm Notification System.

See also: [Application Properties for Alarms](#)

- ...AlarmDialerStatusTemplate
- ... AlarmDialerTemplate
- ...AlarmEmailAckSubjectTemplate
- ...AlarmEmailAckTemplate
- ...AlarmEmailStatusTemplate
- ...AlarmEmailSubjectTemplate
- ... AlarmEmailTemplate
- ...AlarmNotifyEmailAcknowledge
- ... AlphaNumericXFormScheme
- ...AlarmPagerStatusTemplate
- ... AlarmPagerTemplate

...AlarmPriorityIndicatorShowNormalUnacked
...AlarmSMSAckTemplate
...AlarmSMSStatusTemplate
...AlarmSMSTemplate
...AnswerAlarmCalls
...AnswerCalls
... DialCancelOnNormal
... DialerLocation
...DialerPort
... DialerSpeechInit
...DialInControl
... DialerVoice
... DialogMoveTime
... DialOnActive
... DialOnClear
... EchoPhoneThroughSpeaker
... EnableLexiconDialog
...GiveUpCallTimeout
... HideMenuOnOutgoing
... MaxCallAlarmPriorityReported
... MaxPagerBaudRate
... MenuRepeatMax
... NoInitialDriverDial
... PINRetries
... PINTimeOut
... RepeatMenuTime
... RosterDelay
... SMTPPort

... UseOldSpeechEngine

... UseSMTPOverTLS

AlarmCheckMail

Used only if the application is configured to accept alarm acknowledgments by email. This sets the frequency with which VTScada will check in inbound email account when there are no unacknowledged alarms. Measured in seconds.

Default: AlarmCheckMail = 600

Section: System

AlarmCheckMailFastPoll

Used only if the application is configured to accept alarm acknowledgments by email. This sets the frequency with which VTScada will check in inbound email account when there are unacknowledged alarms. Measured in seconds.

Note: Some email servers will disable an account that polls too rapidly, as a suspected spam source.

Default: AlarmCheckMailFastPoll = 60

Section: System

AlarmDialerStatusTemplate

Template to be used for the status message of alarms spoken by the Alarm Notification System.

Section: System

Default: AlarmDialerStatusTemplate = Alarm status is %S.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

... AlarmDialerTemplate

AlarmDialerTemplate

Provides a template to use for alarms delivered over the phone via the Alarm Notification System. May be a combination of words and replaceable parameter tokens as chosen from the table in Alarm Message Templates:

Section: System

Default: AlarmDialerTemplate = %T. %A %W %M.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

... AlarmEmailTemplate

... AlarmPagerTemplate

... AlarmSpeechTemplate

Time and date formatting codes:

... AlarmTemplateDateFmt

... AlarmTemplateTimeFmt

AlarmEditEmailAck

Used only if the system is configured to allow alarm acknowledgment by email. When set to TRUE, operators must add the letters "ACK*" before the alarm code when replying. By default, this is not required.

Section: System

Default: AlarmEditEmailAck = 0

AlarmEmailAckSubjectTemplate

Template to be used for the subject line of alarm acknowledgment messages sent through email by the Alarm Notification System.

Section: System

Default: AlarmEmailAckSubjectTemplate = Acknowledged %A

Parameter	Meaning
%A	Area of the Alarm tag.

Application Configuration

%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmEmailAckTemplate

...AlarmEmailStatusTemplate

...AlarmEmailSubjectTemplate

... AlarmEmailTemplate

AlarmEmailAckTemplate

Template to be used for the acknowledge message of alarms sent through email by the Alarm Notification System.

Section: System

Default: AlarmEmailAckTemplate = Acknowledged %N

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm

%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmEmailAckSubjectTemplate

...AlarmEmailStatusTemplate

...AlarmEmailSubjectTemplate

... AlarmEmailTemplate

AlarmEmailStatusTemplate

Template to be used for the status message of alarms sent through email by the Alarm Notification System.

Section: System

Default: AlarmEmailStatusTemplate = %NStatus: %S

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name

%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmEmailAckSubjectTemplate

...AlarmEmailAckTemplate

...AlarmEmailSubjectTemplate

... AlarmEmailTemplate

AlarmEmailSubjectTemplate

Holds the text that will be inserted into the subject line of alarm notifications sent by email.

Default: AlarmEmailSubjectTemplate = The VTScada System: %A | %P Priority Alarm

Section: System

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name

%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmEmailAckSubjectTemplate

...AlarmEmailAckTemplate

...AlarmEmailStatusTemplate

...AlarmEmailSubjectTemplate

... AlarmEmailTemplate

AlarmEmailTemplate

Provides a template to use for alarms delivered to an email address via the Alarm Notification System. May be a combination of words and replaceable parameter tokens as chosen from the table in Alarm Message Templates:

Section: System

Default: AlarmEmailTemplate = %D %T%NArea: %A%NName: %F%NDesc:

%M

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm

%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Developer's Guide

... AlarmDialerTemplate

... AlarmPagerTemplate

... AlarmSpeechTemplate

Time and date formatting codes:

... AlarmTemplateDateFmt

... AlarmTemplateTimeFmt

AlarmNotifyEmailAcknowledge

Controls whether a confirmation email will be sent after an alarm is acknowledged by email. Defaults to 1, meaning that a confirmation will be sent.

Default: AlarmNotifyEmailAcknowledge = 1

Section: System

AlarmNotifySMSAcknowledge

Controls whether an acknowledgment message is sent back to the operator after an alarm was successfully acknowledged via SMS text.

Section: System

Default: AlarmNotifySMSAcknowledge = 1

AlarmPagerStatusTemplate

Template to be used for the status message of alarms sent to a pager by the Alarm Notification System.

Section: System

Default: AlarmPagerStatusTemplate = %S.

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Developer's Guide

... AlarmPagerTemplate

AlarmPagerTemplate

Provides a template to use for alarms delivered to a pager via the Alarm Notification System. May be a combination of words and replaceable parameter tokens as chosen from the table in Alarm Message Templates:

Section: System

Default: AlarmPagerTemplate = %D %T. %A. %F. %M.

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Developer's Guide

...AlarmPagerStatusTemplate

codes:

... AlarmTemplateDateFmt

... AlarmTemplateTimeFmt

AlarmPriorityIndicatorShowNormalUnacked

Controls the behavior of the Alarm Priority Icon and Alarm Priority Box when the unacknowledged linked alarm state is no longer in an active state.

This table assumes that an alarm occurs and later transitions to being either inactive or acknowledged.

Note that "trip" alarms are never in an active state.

Property value	Active	Acknowledged	Icon display
0	Yes	No	Visible and blinking
0	Yes	Yes	Visible but not blinking
0	No	No	Invisible
0	No	Yes	Invisible.
1	Yes	No	Visible and blinking
1	Yes	Yes	Visible but not blinking
1	No	No	Visible and blinking
1	No	Yes	Invisible.

Section: System

Default: AlarmPriorityIndicatorShowNormalUnacked =

AlarmSMSAckTemplate

Template to be used for the acknowledge message of alarms sent to SMS text devices by the Alarm Notification System.

Section: System

Default: AlarmSMSAckTemplate = Acknowledged:%N%A%N%F%N%M

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name

Application Configuration

%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmSMSStatusTemplate

...AlarmSMSTemplate

AlarmSMSStatusTemplate

Template to be used for the status message of alarms sent to SMS text devices by the Alarm Notification System.

Section: System

Default: AlarmSMSStatusTemplate= %N%S

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.

%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmSMSStatusTemplate

...AlarmSMSTemplate

AlarmSMSTemplate

Provides a template to use for alarms delivered to an SMS text device via the Alarm Notification System. May be a combination of words and replaceable parameter tokens as chosen from the table in Alarm Message Templates:

Section: System

Default: AlarmSMSTemplate = %D %T%N%A%N%F%N%M

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm

%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Programmer's Guide

...AlarmSMSTemplate

...AlarmSMSStatusTemplate

AlphaNumericXFormScheme

Enables you to specify the password scheme to be obeyed by users of the VTScada Alarm Notification System.

- **If set to 0**, passwords will be unmapped (i.e. only strictly numeric passwords will be accepted by the Alarm Notification System (e.g. 98443)).
- **If set to 1** (default), letters will be mapped to numbers as per ITU-T E.161 (i.e. the letters Q and Z map to the numbers 7 and 9 respectively).
- **If set to 2**, letters will be mapped to numbers as per legacy scheme (i.e. the letters Q and Z map to the number 0).
- **If set to 3**, both scheme 1 and scheme 2 above will be accepted (i.e. the letters Q and Z and the numbers 7 and 9 map to the number 0). Please note that this scheme is less secure!

Note: By default, the call-out system has been configured to use alphanumeric passwords. If you change the mapping scheme from its default (i.e. if you change the value of AlphaNumericXFormScheme from 1 to 0, 2, or 3), user passwords will have to be re-entered into the system by telephone. See also: ForcePasswordAltIdSync.

Section: System

Default: AlphaNumericXFormScheme = 1

AnswerAlarmCalls

If set to 0, prevents the Alarm Notification System audio discriminator from being registered with the Modem Manager. This would be useful in an application where the Alarm Notification System is not being used for incoming voice calls, but other drivers are registered for incoming data calls. Up to 30 seconds of time can thereby be saved from each inbound call.

AnswerAlarmCalls should not be confused with the ModemManager setting, AnswerCalls. AnswerCalls determines whether the modem will answer at all. AnswerAlarmCalls determines whether the Alarm Notification System discriminator will be registered with the Modem Manager for use by an incoming call.

Section: System

Default: AnswerAlarmCalls = 1

CallOutDelay1

Indicates the amount of time (in seconds) that you wish the system to wait before notifying designated operators of unacknowledged priority 1 (critical) alarms.

Please review the information on the CallOutPriority and MaxCallAlarmPriorityReported variables.

Section: System

Default: CallOutDelay1 = 120

CallOutDelay2

Indicates the amount of time (in seconds) that you wish the system to wait before notifying designated operators of unacknowledged priority 2 (urgent) alarms.

Please review the information on the CallOutPriority and MaxCallAlarmPriorityReported variables.

Section: System

Default: CallOutDelay2 = 600

CallOutPriority

Indicates whether or not the Alarm Notification System should contact operators when alarms have gone unacknowledged for a user-defined period of time. The CallOutPriority variable further permits you the option of selecting the priority of alarms of which designated operators should be notified.

If set to 0, the Alarm Notification System is disabled.

If set to 1, the Alarm Notification System will notify designated operators of only those alarms that have a priority of 1 (critical).

If set to 2, the Alarm Notification System will notify designated operators of only those alarms that have a priority of 1 (critical), or 2 (urgent).

Note: Please review the information on the MaxCallAlarmPriorityReported variable.

Note: This variable correlates to the Dial-out Priority radio buttons on the Alarm Notification Options dialog.

Section: System

Default: CallOutPriority = 2

DialCancelOnAck

Indicates whether or not alarms that have been acknowledged should be dialed out to operators.

If set to 0, then the VTScada call-out system will continue to dial out to designated operators even once the alarm has been acknowledged.

If set to 1 (default), then the VTScada call-out system will cancel call-outs to designated operators once the alarm has been acknowledged.

Section: System

Default: DialCancelOnAck = 1

DialCancelOnNormal

Indicates whether or not unacknowledged alarms, whose condition has become normal, should be dialed out to operators.

If set to 0, then the VTScada call-out system will continue to dial out to designated operators even once the condition that triggered an alarm has returned to normal.

If set to 1 (default), then the VTScada call-out system will cancel call-outs to designated operators once the condition that triggered the alarm has returned to normal.

Section: System

Default: DialCancelOnNormal = 1

DialerConnectDelay

The interval from when a call is initiated until speech starts.

Default: DialerConnectDelay = 1

Section: System

DialerLocation

Sets the text to be spoken by the VTScada Alarm Notification System when contacting designated operators by phone. (This variable correlates to the Spoken Name in Phone Greeting field on the Alarm Notification Options dialog.)

Section: System

Default: DialerLocation = The VTScada System

DialerPort

Obsolete

Indicated the number of the serial port you wish the Alarm Notification System to use to contact designated operators, or the name of the modem you wish the Alarm Notification System to use to contact designated operators.

If you choose to state the name of the modem you wish the Alarm Notification System to use to contact designated operators, you must enter the name of the modem exactly as it appears in the Modem Properties dialog box of the Windows Control Panel. (The Modem Properties dialog

is accessed using the Phone and Modem Options icon (accessed through the Control Panel in Windows 2000), or the Modems icon (accessed through the Control Panel in Windows NT).

(This variable correlates to the Alarm Notification System Modem drop-down list on the Alarm Notification Options dialog.)

Section: System

Default: DialerPort = Modem1

DialerSpeechInit

This is the string to be used to initialize the text-to-speech device for audio calls.

Section: System

Default: DialerSpeechInit = \xPfl=60\

DialerVoice

Should be a voice as listed on the Windows Text to Speech dialog voice droplist. When set to the default "-", the voice used for the Alarm Notification System will be chosen from the Windows Text to Speech control panel.

Changes take effect on the next restart.

Section: System

Default: DialerVoice = -

DialInControl

Enables access to control actions through the Alarm Notification System's phone menu.

Set to FALSE (0) to disable control options.

Default: DialInControl = 1

Section: System

DialOnActive

Indicates whether or not active alarms should be dialed out to operators. If set to 0, then the VTScada Alarm Notification System will not notify designated operators of active alarm conditions.

If set to 1 (default), then the VTScada Alarm Notification System will notify designated operators of active alarm conditions.

Section: System

Default: DialOnActive = 1

DialOnClear

Indicates whether or not acknowledged alarms, whose condition has returned to normal on site, should be dialed out to operators, notifying them when the alarm has been cleared.

If set to 0 (default), then the VTScada Alarm Notification System will not alert designated operators when an alarm has returned to normal.

If set to 1, then the VTScada Alarm Notification System will call out to designated operators when an alarm has returned to normal.

Section: System

Default: DialOnClear = 1

EchoPhoneThroughSpeaker

Enables you to hear the Alarm Notification System's calls through your PC speakers (in addition to the phone) so that others can hear the Alarm Notification System announce alarms. (This setting is typically used for demonstration purposes and for debugging.)

Section: System

Default: EchoPhoneThroughSpeaker = 0

EnableLexiconDialog

Selects whether the VTScada Lexicon should be enabled in the Alarms page of the Application Properties dialog.

Disable when using a 3rd party voice that provides its own lexicon configuration.

Section: System

Default: EnableLexiconDialog = 1

GiveUpCallTimeout

Specifies how long the alarm dialer will wait for an available modem when making a voice call or pager call to a specific roster entry, before going on to the next roster entry. Defaults to 10 minutes. (600 seconds) Because of this behavior, it is good practice to alternate media in the roster. For example, after a voice contact, have an email or SMS contact, so that if all modems are disabled, the alarm will still being sent out in a timely manner.

Default: GiveUpCallTimeout = 600

Section: System

HideMenuOnOutgoing

If set to TRUE, then there is no return to the main menu of the Alarm Notification System for outgoing calls. After hearing the unacknowledged alarms, the operator has the choice of acknowledging the alarms (after which, the dialer will hang up), repeating the list or exiting. If set to the default (0) the third option is to return to the main menu and the fourth is to exit.

Section: System

Default: HideMenuOnOutgoing = 0

IncomingCallSection

Determines which section of the Alarm Notification System menu is first spoken when a call is made.

Section: System

Default: IncomingCallSection = Menu

MaxCallAlarmPriorityReported

Enables you to configure the Alarm Notification System to report lower alarms with priorities lower than 1 or 2 to operators once contact has been established.

Please review the information on the CallOutPriority variable.

Section: System

Default: MaxCallAlarmPriorityReported = 2

MaxPagerBaudRate

Indicates the maximum number of bits per second to be transmitted to the pagers of designated operators by the Alarm Notification System.

Section: System

Default: MaxPagerBaudRate = 2400

MenuRepeatMax

Indicates the number of times a voice menu will be repeated by the Alarm Notification System before it hangs up if the user makes no keypad input from the phone. For example, if MenuRepeatMax is set to 2, the menu will be heard three times (i.e. repeated twice).

Section: System

Default: MenuRepeatMax = 3

DialerAckIndividualAlarms

When set to 1, causes alarms to be spoken, then acknowledged (or ignored) one by one.

Section: System

Default: DialerAckIndividualAlarms =

PhoneKeyFeedback

Obsolete

Indicated whether or not the pressed telephone keys should be spoken back to the user by the Alarm Notification System.

PINRetries

Indicates the number of times that a user may attempt to correctly enter their PIN number when responding to the Alarm Notification System.

Section: System

Default: PINRetries = 3

PINTimeOut

Indicates the amount of time (in seconds) after which an operator's PIN number will time out if the system is idle while the operator is responding to the Alarm Notification System.

Section: System

Default: PINTimeOut = 30

RepeatMenuTime

Indicates the delay (in seconds) between repeats of the menus by the Alarm Notification System if the user makes no keypad input from the phone.

Section: System

Default: RepeatMenuTime = 5

RosterDelay

Once the Alarm Notification System starts calling out, it will wait for "\RosterDelay" seconds before calling out a second time. A new alarm will terminate any "\RosterDelay" based time-out. If the roster fails to send a notification to one contact, no delay is used before attempting the next (if any).

Section: System

Default: RosterDelay = 10

SkipLogonDialout

When set TRUE, the challenge/response for calls that dial out to the user will be disabled. The user will not be able to return to the main menu.

Section: System

Default: SkipLogonDialout = 0

Related variables:

... IncomingCallSection

SMTPPort

Deprecated. The SendMail function now includes an optional Port parameter. This property will be checked if the SendMail parameter is not specified.

Sets the SMTP port that the configured email server will use. The default value of 25 will work for most SMTP servers. If communicating with a server that uses or requires Transport Layer Security (TLS) such as Gmail, port 587 should be used. Other providers may use non-standard port numbers – consult your provider for details.

Section: System

Default: SMTPPort = 25

SpeechEngine

For systems that include the Alarm Notification System option. Selects the voice engine to use. By default, this will be "-", indicating that the Microsoft SAPI engine should be used.

Customers who have the IVONA® Voice engine from an earlier version of VTScada may continue to use it by ensuring that this property is set to "IVONA".

Section: System

Default: SpeechEngine = -

UseOldSpeechEngine

Note: Use of the ETI-Eloquence speech engine with the call-out system is now obsolete. This variable has been preserved for backwards compatibility only.

Enabled you to command the ETI-Eloquence speech engine to run when sending or receiving an audio call (set UseOldSpeechEngine to 1), or to disable the ETI speech engine.

If set to 1, the older ETI-Eloquence speech engine will be run when an audio call is sent or received, and an instance of SAPIWrap will be run.

Section: System

Default: UseOldSpeechEngine = 0

Related Information:

SpeechEngine

UseSMTPOverTLS

Note: As of VTS 10.1, this property is no longer stored in Settings.Dynamic. Use the Email Options dialog to change its value rather than the Applications Properties dialog.

Controls whether Transport Layer Security (aka SSL) is to be used for communications with your SMTP email server. The following options are available:

UseSMTPOverTLS	Meaning
0	Use plain text mode only. No email will be sent if the server requires TLS.
Non-Zero	Use TLS only. If the server does not support TLS, or if the attempt to use TLS fails, the email will not be sent.
Invalid (default)	If TLS is available on the email server and a connection can be made, TLS mode will be used. Otherwise, the connection will be closed and VTScada will request a plain text connection. If the email server required TLS mode, but a connection could not be made, the plain text connection will fail.

Section: System

Default: UseSMTPOverTLS =

Application Properties for Alarms

The following list of application variables relate to alarms.

See also: Alarm Notification System Properties

...AckAllRequiresConfirmation
...ActiveAlarmFlash
... ActiveCommColor
... ActiveFlashRate
...AlarmAutoNavEnable
...AlarmAutoNavHold
...AlarmAutoNavTimeout
...AlarmAutoNavWindowed
... AlarmCheckMail
... AlarmCheckMailFastPoll
... AlarmColor
...AlarmDatabaseGroups
...AlarmDatabasePurgeDelay
...AlarmDatabasePurgeEnable
...AlarmDatabasePurgeRate
... AlarmDisplayDateFormat
... AlarmDisplayTimeFormat
... AlarmEditEmailAck
... AlarmEmailTemplate
... AlarmEventDescWidth
... AlarmEventDesc0 – AlarmEventDesc21
... AlarmFlashTime
...AlarmFlashTitleBar
...AlarmFlashTitleBarOnVIC
... AlarmIndDisable
...AlarmListBGColor
...AlarmMaxPriority
...AlarmMinPriority

... AlarmNotifySMSAcknowledge
... AlarmOperatorVarName
...AlarmPageHistoryRecordHardLimit
...AlarmPageHistoryRecordLimit
... AlarmPopupsEnable
... AlarmPrintDateFormat
...AlarmPrintOn
... AlarmPrintPort
...AlarmPrintTimeFormat
... AlarmPriorityDescWidth
... AlarmRevUnack
... AlarmRPCEnable
... AlarmSeparatorString
...AlarmSnapshotCount
... AlarmSoundDisable
... AlarmSpeechEnable
... AlarmSpeechInit
... AlarmSpeechQuality
... AlarmSpeechTemplate
... AlarmSpeechVoice
... AlarmStateDesc0
... AlarmStatusDesc0 – AlarmStatusDesc5
... AlarmStatusDescWidth
... AlarmStatusField
... AlarmTemplateDateFmt
... AlarmTemplateTimeFmt
... AlarmTimeStampField
... AlarmTxtColClear

... AlarmTxtColDisable
... AlmColumn1
... AlmColumn2
... AlmColumn3
... AlmColumn4
... AlmColumn5
... AlmColumn6
... AlmColumn7
... AlmDBArea
... AlmDBHPUnits
... AlmDBHPValue
... AlmDBMessage
... AlmDBOperator
... AlmDBPointName
... AlmDBPriority
... AlmDBStatus
... AlmDBTimeStamp
... AlmDBType
... AlmHdg1
... AlmHdg2
... AlmHdg3
... AlmHdg4
... AlmHdg5
... AlmHdg6
... AlmHdg7
... AlmPgStartList
... AlmTagsOnly
...ApplyMuteSilencePerComputer

- ...ApplyMuteSilencePerUser
- ... BackupAlarmPriority
- ... ClientAlarmSoundOn
- ... Cycles
- ...FlashUnackedAlarmsOnServer
- ...FlashUnackedAlarmsOnVIC
- ...HighlightUnackedAlarms
- ...MaxMuteDuration
- ...MaxShelveDuration
- ...MinMuteDuration
- ...MinShelveDuration
- ... MuteAlarms
- ...NoteMinLengthForAck
- ...NoteMinLengthForShelve
- ...NoteMinLengthForUnshelve
- ...NoteRequiredForAck
- ...NoteRequiredForShelve
- ...NoteRequiredForUnshelve
- ... SecurityAlarmArea
- ... UnackAlarmFlash
- ... UnackFlashRate
- ... WavAmplitude
- ... WAVType

AckAllRequiresConfirmation

When TRUE (1), operators must click through a confirmation dialog when attempting to acknowledge all the alarms shown in the list.

Section: System

Default: AckAllRequiresConfirmation = 1

ActiveAlarmFlash

Indicates whether active low setpoint or high setpoint alarms should or should not be signaled by a flashing indicator on the related station symbol and on the tag's widget on the related station page.

If set to 1, active alarms will cause the related station symbol and station page to display a flashing alarm indicator.

Station pages are automatically-generated dialogs that display data for a Data Flow RTU and its associated inputs/outputs.

Default: ActiveAlarmFlash = 0

Section: System

ActiveCommColor

Indicates the color displayed for site symbols, input tags, and in the legend when signaling active communications. The default color is 0 (black).

Default: ActiveCommColor = 0

Section: System

ActiveFlashRate

Indicates the rate (in seconds) at which active alarms should flash on station symbols and station pages if the ActiveAlarmFlash variable (see above) is set to 1.

The ActiveFlashRate variable may be set to fractions of a second (e.g. .5) if you desire a faster flash rate.

Default: ActiveFlashRate = 2

Section: System

AlarmAutoNavEnable

If set to 1, automatic alarm page navigation is enabled. New alarms will cause the application to open a page showing the alarm tag or triggering tag subject to the following conditions:

If the alarm tag, tag with a built-in alarm, or tag that triggered the alarm is not visible on any page, then the alarm page will be selected.

If more than one page could be selected, VTScada will make a best-choice.

Automatic navigation will occur after a delay, and only if there has been no operator activity during that delay.

Default: AlarmAutoNavEnable =

Section: System

Related Information:

...AlarmAutoNavEnable

...AlarmAutoNavTimeout

...AlarmAutoNavWindowed

AlarmAutoNavHold

Sets the number of seconds that a page, automatically opened in response to an alarm, will remain visible before another page will be opened by the automatic navigation feature.

This property has no effect on operator navigation.

Default: AlarmAutoNavHold = 10

Section: System

Related Information:

...AlarmAutoNavEnable

...AlarmAutoNavTimeout

...AlarmAutoNavWindowed

AlarmAutoNavTimeout

Auto-navigation will only occur if there has been no operator activity for the given number of seconds prior to the triggering of the alarm. Operator activity is defined as any mouse motion or keyboard input.

Default: AlarmAutoNavTimeout = 300

Section: System

Related Information:

...AlarmAutoNavEnable

...AlarmAutoNavTimeout

...AlarmAutoNavWindowed

AlarmAutoNavWindowed

Associated with the property, AlarmAutoNavEnable. The page that is automatically opened in response to an alarm will be opened as a window, if possible.

If the page has been configured as Never Open in a Window, it won't.

If the maximum number of pop-up windows is already open

(PopupPageLimit) and more pop-ups are prohibited by PopupLim-

itAction, then the standard error message will occur upon automatic navigation attempting to open a new pop-up page.

Default: AlarmAutoNavWindowed =

Section: System

Related Information:

...AlarmAutoNavEnable

...AlarmAutoNavWindowed

...AlarmAutoNavTimeout

AlarmCheckMail

Used only if the application is configured to accept alarm acknowledgments by email. This sets the frequency with which VTScada will check in inbound email account when there are no unacknowledged alarms. Measured in seconds.

Default: AlarmCheckMail = 600

Section: System

AlarmCheckMailFastPoll

Used only if the application is configured to accept alarm acknowledgments by email. This sets the frequency with which VTScada will check in inbound email account when there are unacknowledged alarms. Measured in seconds.

Note: Some email servers will disable an account that polls too rapidly, as a suspected spam source.

Default: AlarmCheckMailFastPoll = 60

Section: System

AlarmColor

Designates the color to be flashed to indicate an alarm (e.g. in the Display Manager's title bar). The default color is red (12).

Default: AlarmColor = 12

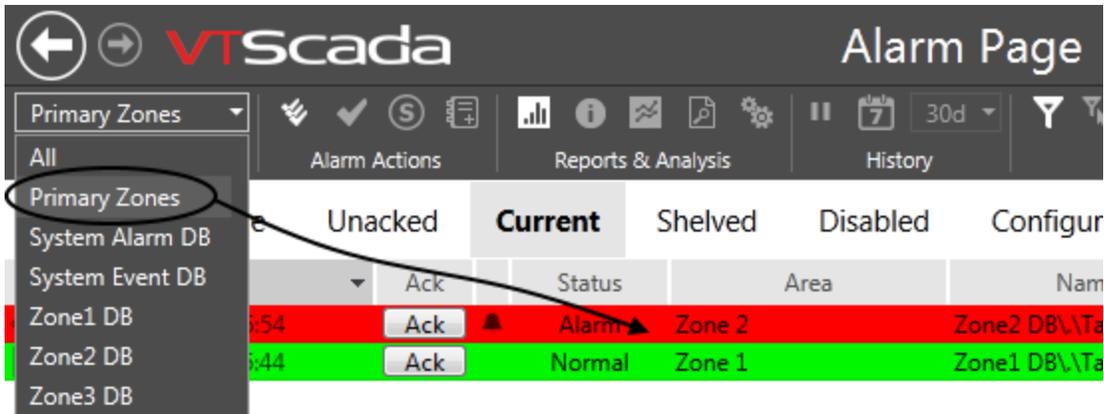
Section: System

AlarmDatabaseGroups

For the majority of applications, there is no need to create extra alarm databases, but a few locations might choose to do so. For those that do, it is possible to create display groups so that alarms from several, but not all, databases can be viewed at once. Database groups are defined in your application properties, system section, by adding a property as follows:

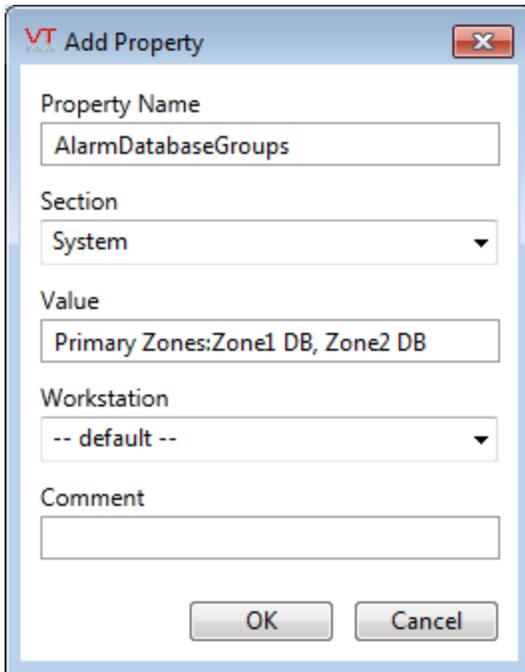
```
Property name: AlarmDatabaseGroups  
Section: System  
Value: Northeast Group:NorEast Database,NorWest Database;Southwest  
Group:SouWest Database, SouEast Database
```

For the preceding, note that each group name is followed by a full colon, then the names of the alarm databases that are to be included in that group, separated by commas. A semi-colon is used between each group name definition. All groups must be defined in the single property, AlarmDatabaseGroups.



The group, Primary Zones, shows alarms from both Zone1 DB and Zone2 DB

Example: Using an alarm database group



The property definition used for this example:

Section: System

Default: AlarmDatabaseGroups =

AlarmDatabasePurgeDelay

It is possible to create orphaned alarms, especially if the tag database is modified outside VTScada. These are purged automatically upon startup, following a delay in seconds specified by this property.

Section: System

Default: AlarmDatabasePurgeDelay = 120

Related Information:

Orphaned Alarms in the VTScada Developer's Guide

AlarmDatabasePurgeEnable

Set TRUE (1) to allow automatic purging of duplicate and orphaned alarm records from alarm databases.

Section: System

Default: AlarmDatabasePurgeEnable = 1

AlarmDatabasePurgeRate

Number of seconds to wait between each alarm record check. Throttles the purge mechanism.

Section: System

Default: AlarmDatabasePurgeRate = 0.01

AlarmDisplayDateFormat

Controls the format in which dates should be displayed on the Alarm page and in Alarm Lists.

predefined Date Codes can be found in the General Reference section of the VTScada Programmer's Guide.

Section: System

Default: AlarmDisplayDateFormat = 30

AlarmDisplayTimeFormat

Controls the format in which times should be displayed on the Alarm page and in Alarm Lists.

predefined Time Formats can be found in the General Reference section of the VTScada Programmer's Guide.

Section: System

Default: AlarmDisplayTimeFormat = 5

AlarmEventDescWidth

Indicates the maximum number of characters in the alarm event descriptions when the alarm list is printed. As alarm events appear only in the History list, this variable will only affect the History list when printed.

Related Variables: The AlarmPriorityDescWidth variable enables you to set the maximum number of characters in the alarm priority descriptions when the alarm list is printed. The AlarmStatusDescWidth variable enables you to set the maximum number of characters in the alarm status descriptions when the alarm list is printed.

Section: System

Default: AlarmEventDescWidth = 11

AlarmEventDesc0 – AlarmEventDesc21

Sets the description to be displayed in the Event column of the History list for custom alarm states.

Section: System

Default: (See following list)

AlarmEventDesc0 = Disable

AlarmEventDesc1 = Enable

AlarmEventDesc2 = Active

AlarmEventDesc3 = Trip

AlarmEventDesc4 = Event

AlarmEventDesc5 = Normal

AlarmEventDesc6 = Off Normal

AlarmEventDesc7 = Normal Trip

AlarmEventDesc8 = Acknowledge

AlarmEventDesc9 = Unknown

AlarmEventDesc10 = Normal Ack

AlarmEventDesc11 = Active Ack

AlarmEventDesc12 = Shelve
AlarmEventDesc13 = Unshelve
AlarmEventDesc14 = Notify
AlarmEventDesc15 = Decommission
AlarmEventDesc16 = Recommission
AlarmEventDesc17 = Commission
AlarmEventDesc18 = Rename
AlarmEventDesc19 = Modify
AlarmEventDesc20 = Rearm
AlarmEventDesc21 = Purge

Related Information:

AlarmStatusDesc0 – AlarmStatusDesc5

AlarmFlashTime

Indicates the frequency (in seconds) between flashes of active alarm indicators (for example, in the Display Manager's title bar).

Related Variables: The AlarmColor variable indicates the color to be flashed.

Section: System

Default: AlarmFlashTime = 0.5

AlarmFlashTitleBar

When set TRUE (1), the entire title bar will flash red while there are unacknowledged alarms that are visible to the logged-on user.

If not checked, only the alarm indicator blinks.

Default: AlarmFlashTitleBar = 1

Section: System

Related Information:

AlarmFlashTitleBarOnVIC

AlarmFlashTitleBarOnVIC

When set TRUE (1), the entire title bar will flash red on VTScada Internet Clients while there are unacknowledged alarms that are visible to the logged-on user.

Note: This feature will consume extra bandwidth when enabled. Use with caution.

Default: AlarmFlashTitleBarOnVIC = 0

Section: System

Related Information:

AlarmFlashTitleBar

AlarmIndDisableOnVIC

AlarmIndDisable

AlarmIndDisable

Enables users to disable and enable the flashing alarm indicator in the Display Manager's title bar.

Related Variables: The AlarmColor variable described above indicates the color to be flashed.

Note: Use extreme caution in using the AlarmIndDisable variable, as operators will not be alerted to the presence of incoming alarms in the system.

Section: System

Default: AlarmIndDisable = 0

Related Information:

AlarmIndDisableOnVIC

AlarmIndDisableOnVIC

If set to TRUE (1) then the unacknowledged alarms indicator will be disabled on VTScada internet clients. Set to FALSE (0) to enable the indicator.

Note: This feature will consume extra bandwidth when enabled. Use with caution.

Default: AlarmIndDisableOnVIC = 1

Section: System

Related Information:

AlarmFlashTitleBarOnVIC

AlarmKeySize

Obsolete, used only to import legacy history into new system.

AlarmListBGColor

Alarm list background color. Defaults to gray. Replaces the now-obsolete AlarmDispBgndColor.

Default: AlarmListBGColor = <282828>

Section: System

AlarmMaxPriority

If sending alarms to a printer (AlarmPrintOn), this property sets the maximum priority level that will be printed.

Default: AlarmMaxPriority = 1

Section: System

AlarmMinPriority

If sending alarms to a printer (AlarmPrintOn), this property sets the minimum priority level that will be printed.

Default: AlarmMinPriority = 1

Section: System

AlarmOperatorVarName

Indicates the name of the variable that stores the operator name.

Section: System

Default: AlarmOperatorVarName = operator

AlarmPageHistoryRecordHardLimit

The maximum number of records that will be shown in any alarm list is limited by the related property, AlarmPageHistoryRecordLimit. If there are more records than that value in the selected time frame, a Load More button will be available at the bottom of the list. Load More will allow you to view successive sets of records (always limited to AlarmPageHistoryRecordLimit at a time), up to the maximum number as controlled by AlarmPageHistoryRecordHardLimit which defaults to 100,000.

Default: AlarmPageHistoryRecordHardLimit = 100000

Section: System

Related Information:

...AlarmPageHistoryRecordLimit

AlarmPageHistoryRecordLimit

Limits the maximum number of records that will be shown in any alarm list. If there are more records than this in the selected time frame, a Load More button will be available at the bottom of the list. Load more will allow you to view successive sets of records (always limited to AlarmPageHistoryRecordLimit at a time), up to the maximum number as controlled by AlarmPageHistoryRecordHardLimit.

Default: AlarmPageHistoryRecordLimit = 1000

Section: System

Related Information:

...AlarmPageHistoryRecordHardLimit

AlarmPopupsEnable

Toggle to control whether alarm pop-up dialogs (if any) are enabled. Disabled by default.

Section: System

Default: AlarmPopupsEnable = 0

AlarmPrintDateFormat

Controls the format with which the alarm's date is recorded. See the Date function for a list of available formats. The default format (2) is "mm/d-d/yy".

Section: System

Default: AlarmPrintDateFormat = 2

AlarmPrintTimeFormat

The format to use when displaying the [time](#) in the alarm message

Default: AlarmPrintTimeFormat = 2

Section: System

AlarmPrintPort

Indicates the port to which the printer you wish to use to print the alarm list is connected. By default, AlarmPrinterPort is set to the default printer as defined in Windows.

Section: System

Default: AlarmPrintPort = DEF:

AlarmPriorityDescWidth

Indicates the maximum number of characters in the alarm priority descriptions when the alarm list is printed.

Related Variables: The AlarmPriorityDescWidth variable enables you to set the maximum number of characters in the alarm priority descriptions

when the alarm list is printed. The AlarmStatusDescWidth variable enables you to set the maximum number of characters in the alarm status descriptions when the alarm list is printed.

Section: System

Default: AlarmPriorityDescWidth = 11

AlarmRevUnack

Obsolete

Enables you to reverse the display color for unacknowledged alarms so that they appear highlighted in the alarm list.

If set to 1 (default), unacknowledged alarms are reversed (i.e. highlighted in the alarm list).

If set to 0, unacknowledged alarms are not reversed (i.e. are not highlighted in the alarm list).

Section: System

Default: AlarmRevUnack = 1

AlarmRPCEnable

Indicates whether remote procedure calls for alarms are enabled or disabled for this application.

If set to 0 (false), remote procedure calls are disabled for this application.

If set to 1 (true), remote procedure calls are enabled for this application (default)

Section: System

Default: AlarmRPCEnable = 1

AlarmSeparatorString

Enables you to specify a string to separate the name of a custom alarm's parent tag from its index in the parent's array of alarms. The default setting for AlarmSeparatorString is a colon, followed by a number hatch, followed by a colon.

Section: System

Default: AlarmSeparatorString = :#:

AlarmSnapshotCount

Maximum number of alarm events until the alarm database saves snapshots of their state

Section: System

Default: AlarmSnapshotCount = 10000

AlarmSoundDisable

When set to TRUE, will completely disable alarm sounds thereby saving on CPU & RAM. This can make a significant difference in systems with a large number of alarms and a large number of operator connections.

Section: System

Default: AlarmSoundDisable = 0

AlarmSpeechEnable

Controls whether the text-to-speech alarm feature will be used. Spoken alarms are disabled by default.

Section: System

Default: AlarmSpeechEnable = 0

AlarmSpeechInit

This variable provides an initialization string to the speech engine to control the voice. It can be any XML string accepted by the voice engine.

Please refer to the documentation for your configured voice engine for the details of this initialization string. The default value sets voice pitch, volume and speed for the Microsoft SAPI engine.

Section: System

Default: AlarmSpeechInit = <PITCH ABSMIDDLE="-2"/><VOLUME LEVEL="100"/><RATE ABSSPEED="-1"/>

AlarmSpeechQuality

Determines the audio quality, and therefore the data transfer required, for speech. The number used for this variable directly corresponds to the SAPI SPStreamFormat enumeration. When set to the default of -1, the quality that is native to the voice engine will be used.

Section: System

Default: AlarmSpeechQuality = -1

Value	Meaning	Value	Meaning
4	SAFT8kHz8BitMono	5	SAFT8kHz8BitStereo
6	SAFT8kHz16BitMono	7	SAFT8kHz16BitStereo
8	SAFT11kHz8BitMono	9	SAFT11kHz8BitStereo
10	SAFT11kHz16BitMono	11	SAFT11kHz16BitStereo
12	SAFT12kHz8BitMono	13	SAFT12kHz8BitStereo
14	SAFT12kHz16BitMono	15	SAFT12kHz16BitStereo
16	SAFT16kHz8BitMono	17	SAFT16kHz8BitStereo
18	SAFT16kHz16BitMono	19	SAFT16kHz16BitStereo
20	SAFT22kHz8BitMono	21	SAFT22kHz8BitStereo
22	SAFT22kHz16BitMono	23	SAFT22kHz16BitStereo
24	SAFT24kHz8BitMono	25	SAFT24kHz8BitStereo
26	SAFT24kHz16BitMono	27	SAFT24kHz16BitStereo
28	SAFT32kHz8BitMono	29	SAFT32kHz8BitStereo
30	SAFT32kHz16BitMono	31	SAFT32kHz16BitStereo
32	SAFT44kHz8BitMono	33	SAFT44kHz8BitStereo
34	SAFT44kHz16BitMono	35	SAFT44kHz16BitStereo
36	SAFT48kHz8BitMono	37	SAFT48kHz8BitStereo
38	SAFT48kHz16BitMono	39	SAFT48kHz16BitStereo

AlarmSpeechTemplate

Provides a template for spoken alarms to use. May be a combination of words and replaceable parameter tokens as chosen from the table in Alarm Message Templates:

Section: System

Default: AlarmSpeechTemplate = %A %W %F %W %M

Parameter	Meaning
%A	Area of the Alarm tag.
%D	Date of the alarm
%F	Full tag name
%H	Short tag name
%M	Alarm description
%N	New sentence for email and pager messages.
%O	Name of the operator logged on at the time the alarm was triggered.
%P	Priority of the alarm.
%S	Status of the alarm
%T	Time of the alarm
%U	Units of the Triggering tag.
%V	Alarm value (this is the value of the alarm trigger at the time that it triggered the alarm)
%W	Pause for ¼ second. Has no effect on email or pager messages.

Related Information:

...Alarm Message Templates – See: VTScada Developer's Guide

... AlarmDialerTemplate

... AlarmEmailTemplate

... AlarmPagerTemplate

Time and date formatting codes:

... AlarmTemplateDateFmt

... AlarmTemplateTimeFmt

AlarmSpeechVoice

Sets which voice in the Microsoft-integrated speech engine is used to speak the alarm. In general, it is best to select the voice using the Microsoft Speech Tools configuration box and set this variable to a dash (-) to indicate "configured Windows voice". If selecting a particular voice, the string must exactly match the desired voice name.

This property is relevant only when SpeechEngine is set to SAPI.

Section: System

Default: AlarmSpeechVoice = -

AlarmStateDesc0**Obsolete**

Indicates the description to be displayed in the Event column for the Trip alarm state.

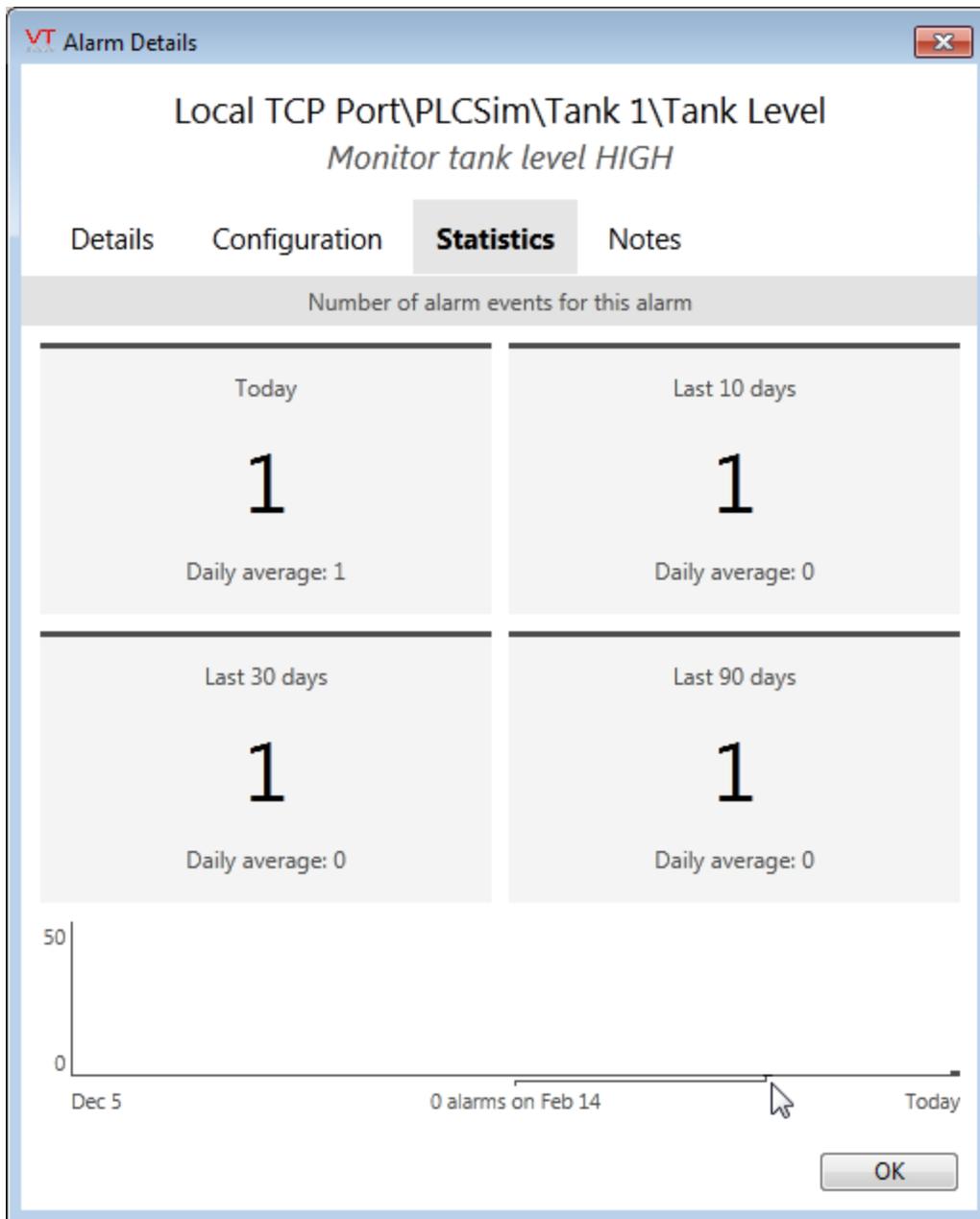
Descriptions of events in the History list are controlled by the AlarmEventDesc0 through AlarmEventDescX variables.

Section: System

Default: AlarmStateDesc0 = Trip

AlarmStatRange0 – AlarmStatRange3

The four AlarmStatRangeN properties control the time period for each of the four statistics in the Alarm Details dialog.



When changing a time range, be certain to also change the related label to match. Each set of properties should be stored in the [SYSTEM] section of your Settings.Dynamic file. The default values are shown here.

Top left box:

AlarmStatRange0 = 1
AlarmStatRange0Label = Last 24 hours

Top right box:

AlarmStatRange1 = 10
AlarmStatRange1Label = Last 10 days

Bottom left box:

AlarmStatRange2 = 30
AlarmStatRange2Label = Last 30 days

Bottom right box:

AlarmStatRange3 = 90
AlarmStatRange3Label = Last 90 days

Example: You wish to display alarm statistics for a seven-day period instead of ten days in the upper right box.

1. Open the Application Configuration dialog.
2. Switch to the Advanced display mode.
3. Click the Insert button.
4. Name the new property, AlarmStatRange1.
5. Leave the section set to System.
6. Set the value to 7.
7. Click OK.
8. Click the Insert button again.
9. Name the new property AlarmStatRange1Label.
10. Leave the section set to System.
11. Set the value to Last 7 days
12. Click OK.

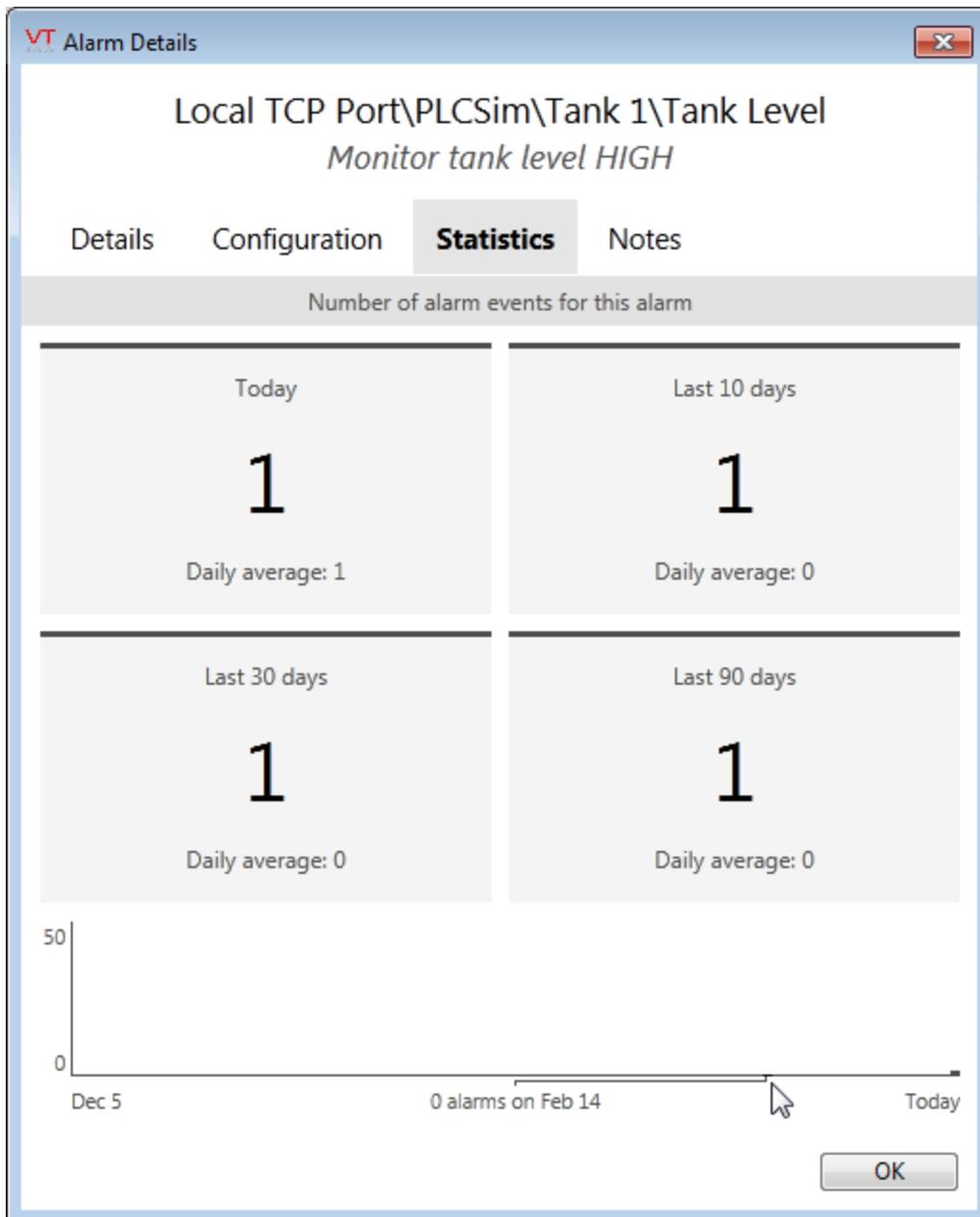
The statistics dialog will now show values for 1, 7, 30 and 90 days.

Related Information:

AlarmStatRange0Label – AlarmStatRange3Label

AlarmStatRange0Label – AlarmStatRange3Label

The four AlarmStatRangeNLabel properties control the label identifying each time period for the four statistics in the Alarm Details dialog.



When changing a time range label, be certain to also change the related time range to match. Each set of properties should be stored in the [SYSTEM] section of your Settings.Dynamic file. The default values are shown here.

Top left box:

AlarmStatRange0 = 1

AlarmStatRange0Label = Last 24 hours

Top right box:

AlarmStatRange1 = 10

AlarmStatRange1Label = Last 10 days

Bottom left box:

AlarmStatRange2 = 30

AlarmStatRange2Label = Last 30 days

Bottom right box:

AlarmStatRange3 = 90

AlarmStatRange3Label = Last 90 days

Example: You wish to display alarm statistics for a seven-day period instead of ten days in the upper right box.

1. Open the Application Configuration dialog.
2. Switch to the Advanced display mode.
3. Click the Insert button.
4. Name the new property, AlarmStatRange1.
5. Leave the section set to System.
6. Set the value to 7.
7. Click OK.
8. Click the Insert button again.
9. Name the new property AlarmStatRange1Label.
10. Leave the section set to System.
11. Set the value to Last 7 days
12. Click OK.

The statistics dialog will now show values for 1, 7, 30 and 90 days.

Related Information:

AlarmStatRange0 – AlarmStatRange3

AlarmStatusDesc0 – AlarmStatusDesc5

Provides the description for the alarm status in all alarm lists except the history list, which uses the AlarmEventDesc0 through the AlarmEventDesc21 variables.

Section: System

Default: See following list

AlarmStatusDesc0 = Trip

AlarmStatusDesc1 = Normal

AlarmStatusDesc2 = Alarm

AlarmStatusDesc3 = Normal

AlarmStatusDesc4 = Alarm

AlarmStatusDesc5 = Disabled

Related Information:

AlarmEventDesc0 – AlarmEventDesc21

AlarmStatusDescWidth

Indicates the maximum number of characters in the alarm status descriptions when the alarm list is printed. The only exception is when the History list is being printed; the History list displays events rather than status.

Related Variables: The AlarmPriorityDescWidth variable enables you to set the maximum number of characters in the alarm priority descriptions when the alarm list is printed. The AlarmStatusDescWidth variable enables you to set the maximum number of characters in the alarm status descriptions when the alarm list is printed.

Section: System

Default: AlarmStatusDescWidth = 14

AlarmStatusField

Indicates the field number in the alarm database (Alarms.db unless the root file name for the alarm database is indicated otherwise by the AlarmFileName variable) for status..

Section: System

Default: AlarmStatusField = 0

AlarmTemplateDateFmt

Controls the date format used in spoken (and other) alarms when the %D formatting variable is used.

predefined Date Codes can be found in the General Reference section of the VTScada Programmer's Guide.

Section: System

Default: AlarmTemplateDateFmt = 30

Related Information:

... AlarmTemplateTimeFmt

AlarmTemplateTimeFmt

Controls the time format used in spoken (and other) alarms when the %T formatting variable is used.

predefined Time Formats can be found in the General Reference section of the VTScada Programmer's Guide.

Section: System

Default: AlarmTemplateTimeFmt = 2

Related Information:

... AlarmTemplateDateFmt

AlarmTimeStampField

Indicates the field number in the alarm database (Alarms.db unless the root file name for the alarm database is indicated otherwise by the AlarmFileName variable) for the time stamp.

Section: System

Default: AlarmTimeStampField = 1

AlarmTxtColClear

Indicates the display color for cleared alarms in the alarm list. The default display color for cleared alarms in the alarm list is light green (10).

Section: System

Default: AlarmTxtColClear = 10

AlarmTxtColDisable

Indicates the display color for disabled (blocked) alarms in the alarm list. The default display color for disabled alarms in the alarm list is light magenta.

Section: System

Default: AlarmTxtColDisable = 13

AlmColumn1

Obsolete

Indicates the position of the last pixel of the first column from the right (the Event column) on the default Alarm page. The width of the first column is therefore the number of pixels from 0 to the value of AlmColumn1.

Section: System

Default: AlmColumn1 = 80

AlmColumn2

Obsolete

Indicates the position of the last pixel of the second column from the right (the Priority column) on the default Alarm page. The width of the second column is therefore the number of pixels from the value of AlmColumn1 to AlmColumn2.

Section: System

Default: AlmColumn2 = 210

AlmColumn3

Obsolete

Indicates the position of the last pixel of the third column from the right (the Time portion of the Time/Date column) on the default Alarm page.

The width of the third column is therefore the number of pixels from the value of AlmColumn2 to AlmColumn3.

Although in appearance, the Time/Date column appears to be a single column, it is actually two columns (one for the time, and one for the date).

Section: System

Default: AlmColumn3 = 285

AlmColumn4

Obsolete

Indicates the position of the last pixel of the fourth column from the right (the Date portion of the Time/Date column) on the default Alarm page. The width of the fourth column is therefore the number of pixels from the value of AlmColumn3 to AlmColumn4.

Although in appearance, the Time/Date column appears to be a single column, it is actually two columns (one for the time, and one for the date).

Section: System

Default: AlmColumn4 = 340

AlmColumn5

Obsolete

Indicates the position of the last pixel of the fifth column from the right (the Area column) on the default Alarm page. The width of the fifth column is therefore the number of pixels from the value of AlmColumn4 to AlmColumn5.

Section: System

Default: AlmColumn5 = 510

AlmColumn6

Obsolete

Indicates the position of the last pixel of the sixth column from the right (the Message column) on the default Alarm page. The width of the sixth column is therefore the number of pixels from the value of AlmColumn5 to AlmColumn6.

Section: System

Default: AlmColumn6 = 1140

AlmColumn7

Obsolete

Indicates the position of the last pixel of the seventh column from the right (the Value column) on the default Alarm page.

Section: System

Default: AlmColumn7 = 1260

AlmDBArea

Obsolete

Indicates the index of the alarm's area in the alarm database.

Section: System

Default: AlmDBArea = 5

AlmDBHPUnits

Obsolete

Indicates the index of the associated trigger tags unit (associated with the tags value) in the alarm database.

Section: System

Default: AlmDBHPUnits = 6

AlmDBHPValue

Obsolete

Indicates the index of the associated trigger tags value in the alarm database.

Section: System

Default: AlmDBHPValue = 4

AlmDBMessage

Obsolete

Indicates the index of the alarms message in the alarm database.

Section: System

Default: AlmDBMessage = 1

AlmDBOperator

Indicates the index of the operator's username in the alarm database.

Alarm database index names correspond to the key name indexes in the [Alarm_Manager] section. To properly configure the alarm database index names, you **MUST** ensure that the index is +1 greater than the number assigned in the [Alarm_Manager] section. For example, if in the [Alarm_Manager] section, Message is given an index of 0, than AlmDBMessage must be given an index of 1.

Section: System

Default: AlmDBOperator = 7

AlmDBPointName

Obsolete

Indicates the index of the position of the alarm tags name in the alarm database.

Section: System

Default: AlmDBPointName = -2

AlmDBPriority

Obsolete

Indicates the index of the alarms priority in the alarm database.

Section: System

Default: AlmDBPriority = 2

AlmDBStatus

Obsolete

Indicates the index of the alarms status in the alarm database.

Section: System

Default: AlmDBStatus = 0

AlmDBTimeStamp

Obsolete

Indicates the index of the alarms timestamp in the alarm database.

Section: System

Default: AlmDBTimeStamp = -1

AlmDBType

Obsolete

Indicates the index of the alarms type in the alarm database.

Section: System

Default: AlmDBType = 3

AlmHdg1

Obsolete

Indicates the title to be displayed over the first column from the left (the Event column) on the default Alarm page.

Section: System

Default: AlmHdg1 = Event

AlmHdg2

Obsolete

Indicates the title to be displayed over the second column from the left (the Priority column) on the default Alarm page.

Section: System

Default: AlmHdg2 = Priority

AlmHdg3

Obsolete

Indicates the title to be displayed over the third column from the left (the Time portion of the Time/Date column) on the default Alarm page. Although in appearance, the Time/Date column appears to be a single column, it is actually two columns (one for the time, and one for the date).

Section: System

Default: AlmHdg3 = Time/Date

AlmHdg4

Obsolete

Indicates the title to be displayed over the fourth column from the left (the Date portion of the Time/Date column) on the default Alarm page. Although in appearance, the Time/Date column appears to be a single column, it is actually two columns (one for the time, and one for the date).

Section: System

Default: AlmHdg4 =

AlmHdg5

Obsolete

Indicates the title to be displayed over the fifth column from the left (the Area column) on the default Alarm page.

Section: System

Default: AlmHdg5 = Area

AlmHdg6

Obsolete

Indicates the title to be displayed over the sixth column from the left (the Message column) on the default Alarm page.

Section: System

Default: AlmHdg6 = Message

AlmHdg7

Obsolete

Indicates the title to be displayed over the seventh column from the left (the Value column) on the default Alarm page.

Section: System

Default: AlmHdg7 = Value

AlmListTextColor

Sets the color to be used for text in the alarm list. If set to Invalid, alarms will be displayed using their priority color. Defaults to white (15).

Section: System

Default: AlmListTextColor = 15

AlmPgLineStyle

Obsolete

Indicated the amount of information to be displayed for each line in the alarm list on the Alarm page.

AlmPgStartList

Indicates the initial list of alarms to be displayed in the alarm list on the default Alarm page. This can be one of seven options, as shown:

Value	Description
AlmPgStartList = -2	Current list (merged active & unacknowledged lists)
AlmPgStartList = -1	Configured list (all registered alarms)
AlmPgStartList = 0	History list (a historical list of all alarms)
AlmPgStartList = 1	Disabled list (all disabled alarms)
AlmPgStartList = 2	Active list (all active alarms)
AlmPgStartList = 3	Unacknowledged list (all unacknowledged alarms)

AlmPgStartList = 4	(or greater) User-defined lists
--------------------	---------------------------------

Section: System

Default: AlmPgStartList = -2

ApplyMuteSilencePerComputer

Controls whether the Mute and Silence controls of the Alarm Page affect only the current computer or whether the settings will affect all computers that the current user logs onto

Default: ApplyMuteSilencePerComputer = 1

Section: System

Related Information:

ApplyMuteSilencePerUser

ApplyMuteSilencePerUser	ApplyMuteSilencePerComputer	Result
1	1	(default) Silence and mute affect only the logged-on user on the current computer.
0	1	Changes to silence and mute will affect only the current workstation, but will remain in effect for all users until changed.
1	0	Changes to silence and mute affect only the current user, but will follow a user who logs out from one computer and in on another.
0	0	Changes to silence and mute will affect all users on all workstations.

ApplyMuteSilencePerUser

Controls whether the Mute and Silence controls of the Alarm Page affect only the current user (resetting when a new user logs on) or whether the settings will affect all users who subsequently log on at the current workstation.

Default: ApplyMuteSilencePerUser = 1

Section: System

Related Information:

ApplyMuteSilencePerComputer

ApplyMuteSilencePerUser	ApplyMuteSilencePerComputer	Result
1	1	(default) Silence and mute affect only the logged-on user on the current computer.
0	1	Changes to silence and mute will affect only the current workstation, but will remain in effect for all users until changed.
1	0	Changes to silence and mute affect only the current user, but will follow a user who logs out from one computer and in on another.
0	0	Changes to silence and mute will affect all users on all workstations.

AlmTagsOnly

Obsolete

Enables you to specify whether you wish modules other than tags to have the ability to generate alarms.

If set to 0 (default), only tags will be able to generate alarms.

If set to 1, modules other than tags may generate alarms.

Section: System

Default: AlmTagsOnly = 0

BackupAlarmPriority

Indicates the alarm priority for the alarm that is triggered when the backup server takes over polling.

Section: System

Default: BackupAlarmPriority = 3

Related Information:

BackupSwitchCount

ClientAlarmSoundOn

Obsolete

Indicates whether alarm sounds will trigger on client workstations running the application, or will be limited to the server.

Section: System

Default: ClientAlarmSoundOn = 0

Cycles

Obsolete

Controls continuous alarm sounds in the system.

The Cycles variable is required to avoid competition for the PC speaker, and should therefore always be set to 0.

Section: System

Default: Cycles = 0

FlashUnackedAlarmsOnServer

When true, unacknowledged alarms, that the current user is able to view, will blink in the alarm list in order to draw operator attention. Does not

affect the alarm display of an internet client.

Default: FlashUnackedAlarmsOnServer = 0

Section: System

Related Information:

FlashUnackedAlarmsOnVIC

FlashUnackedAlarmsOnVIC

Affects the alarm display for Internet Clients. When true, unacknowledged alarms, that the current user is able to view, will blink in the alarm list in order to draw operator attention.

If your internet connection is limited by bandwidth restrictions, Trihedral recommends that you do not enable this option for the VIC display.

Default: FlashUnackedAlarmsOnVIC = 0

Section: System

Related Information:

FlashUnackedAlarmsOnServer

HighlightUnackedAlarms

When checked, unacknowledged alarms in the alarm list will be highlighted with the color matching their priority, in order to draw operator attention.

Separate options exist for the server and VIC displays, which will cause the alarm to flash.

Default: HighlightUnackedAlarms = 1

Section: System

Related Information:

FlashUnackedAlarmsOnServer

FlashUnackedAlarmsOnVIC

MaxMuteDuration

Maximum length of time in seconds, for which an operator may mute an alarm. No default value.

Section: System

Default: MaxMuteDuration =

MaxShelveDuration

Maximum length of time in seconds, for which an operator may shelve an alarm. No default value.

Section: System

Default: MaxShelveDuration =

MinMuteDuration

Minimum length of time in seconds, for which an operator may mute an alarm. No default value.

Section: System

Default: MinMuteDuration =

MinShelveDuration

Minimum length of time in seconds, for which an operator may shelve an alarm. No default value.

Section: System

Default: MinShelveDuration =

MuteAlarms

Indicates whether or not all alarms are to be muted at the start of each user's session.

If set to 1 (true), then all alarms are muted at startup.

Section: System

Default: MuteAlarms = 0

NoteMinLengthForAck

Sets the minimum length for notes that are prompted for when 'Require note when acknowledging alarm' (NoteRequiredForAck) is TRUE. If left at zero, operators may cancel the note entry dialog and acknowledge the alarm without recording a note.

Not relevant unless NoteRequiredForAck is TRUE.

Section: System

Default: NoteMinLengthForAck = 0

Related Information:

...NoteRequiredForAck

...NoteMinLengthForShelve

...NoteMinLengthForUnshelve

NoteMinLengthForShelve

Sets the minimum length for notes that are prompted for when 'Require note when shelving alarm' (NoteRequiredForShelve) is TRUE. If left at zero, operators may cancel the note entry dialog and shelve the alarm without recording a note.

Not relevant unless NoteRequiredForShelve is TRUE.

Section: System

Default: NoteMinLengthForShelve= 0

Related Information:

...NoteRequiredForShelve

...NoteMinLengthForAck

...NoteMinLengthForUnshelve

NoteMinLengthForUnshelve

Sets the minimum length for notes that are prompted for when 'Require note when unshelving alarm' (NoteRequiredForUnshelve) is TRUE. If left at zero, operators may cancel the note entry dialog and unshelve the alarm without recording a note.

Not relevant unless NoteRequiredForUnshelve is TRUE.

Section: System

Default: NoteMinLengthForUnshelve= 0

Related Information:

...NoteRequiredForUnshelve

...NoteMinLengthForAck

...NoteMinLengthForShelve

NoteRequiredForAck

When set TRUE, operators will be prompted to add a note when acknowledging an alarm. The note is not mandatory unless the related property, NoteMinLengthForAck, is set greater than zero.

Notes will be added to the notebook associated with the database that belongs to the alarm being acknowledged.

Section: System

Default: NoteRequiredForAck = 0

Related Information:

...NoteMinLengthForAck

...NoteRequiredForShelve

...NoteRequiredForUnshelve

NoteRequiredForShelve

When set TRUE, operators will be prompted to add a note when shelving an alarm. The note is not mandatory unless the related property, NoteMinLengthForShelve, is set greater than zero.

Notes will be added to the notebook associated with the database that belongs to the alarm being shelved.

Section: System

Default: NoteRequiredForShelve = 0

Related Information:

...NoteMinLengthForShelve

...NoteRequiredForAck

...NoteRequiredForUnshelve

NoteRequiredForUnshelve

When set TRUE, operators will be prompted to add a note when unshelving an alarm. The note is not mandatory unless the related property, NoteMinLengthForUnshelve, is set greater than zero.

Notes will be added to the notebook associated with the database that belongs to the alarm being unshelved.

Section: System

Default: NoteRequiredForUnshelve = 0

Related Information:

...NoteMinLengthForUnshelve

...NoteRequiredForAck

...NoteRequiredForShelve

SecurityAlarmArea

Indicates the area to display in the alarm list for security-related alarms.

Section: System

Default: SecurityAlarmArea = Security

UnackAlarmFlash

Indicates whether unacknowledged low setpoint or high setpoint alarms should or should not be signaled by a flashing indicator on the related station symbol and station page.

If set to 1 (default), unacknowledged alarms will cause the related station symbol and station page to display a flashing alarm indicator.

Section: System

Default: UnackAlarmFlash = 1

UnackFlashRate

Indicates the rate (in seconds) at which unacknowledged alarms should flash on station symbols and station pages if the UnackAlarmFlash variable (see above) is set to 1.

The UnackFlashRate variable may be set to fractions of a second (e.g. ".5") if you desire a faster flash rate.

Section: System

Default: UnackFlashRate = 1

WavAmplitude

Adjusts the volume of alarm tones, ranging from 0 (mute) to 32,768 (full). This value represents the peak of a generated 16-bit signed wave amplitude.

Section: System

Default: WavAmplitude = 12288

WAVType

Indicates the type of waveform produced by the WAVGenerator module. This may be set to one of:

Value	Meaning
0	Sine
1	Square
2	Saw (default)

Section: System

Default: WAVType = 2

Color Properties

The following list of variables pertain to colors.

... BadQualityColor

...ButtonFace

... ButtonHighlight

... ButtonShadow

... ButtonTextColor

... DefaultBGColor

...DefaultPageColor

- ... DefGraphicBColor
- ... DefGraphicPColor
- ... DialogBGColor
- ...DigitalIndicator0Color
- ...DigitalIndicator1Color
- ...DigitalIndicator2Color
- ...DigitalIndicator3Color
- ...DigitalIndicatorAlarmColor
- ...DigitalIndicatorInvalidColor
- ... FieldHighlight
- ... FieldShadow
- ... GrayedText
- ... GridColor
- ... InvalidColor
- ... MenuBgnd
- ... MenuTextColor
- ... NormalColor
- ... OffColor
- ... OnColor
- ... OpaqueBackground
- ... PollDisabledColor
- ... ReceiveColor
- ... SelectedBGnd
- ... SelectedText
- ... State0DefColor
- ... State1DefColor
- ... State2DefColor
- ... State3DefColor

... TransmitColor
... UnselectedBgnd
... UnselectedText
... WindowBgnd
... WindowFrame

BadQualityColor

Controls the color displayed when a tag is experiencing bad data quality. The default display color for bad data quality is orange.

You can associate basic I/O tags with each other in such a way that the quality of one tag is based on the value of another (refer to the I/O tag's Quality tab). If the Quality of the associated tag is non-zero, blank, or invalid, the data quality is assumed to be good; otherwise, the data is assumed to be bad.

Section: System

Default: BadQualityColor = <FF8000>

ButtonFace

Sets the background color for buttons.

If left invalid (which it is by default), ButtonFace uses the GetSystemColor (15) function to return the system colors as defined by the user in Windows.

Section: System

Default: ButtonFace =

ButtonHighlight

Indicates the highlight color for the sides of buttons.

If left invalid (which it is by default), ButtonHighlight uses the GetSystemColor(20) function to return the system colors as defined by the user in Windows.

Section: System

Default: ButtonHighlight =

ButtonShadow

Indicates the shadow color for the sides of buttons.

If left invalid (which it is by default), ButtonShadow uses the GetSystemColor(16) function to return the system colors as defined by the user in Windows.

Section: System

Default: ButtonShadow =

ButtonTextColor

Indicates the color of the text label for buttons.

If left invalid (which it is by default), ButtonTextColor uses the GetSystemColor(18) function to return the system colors as defined by the user in Windows.

Section: System

Default: ButtonTextColor =

DefaultBGColor

Indicates the background color when no page is displayed in the Display Manager. By default, the background color to be displayed is white (15) for VTS applications and black (0) for script applications. For valid color values, please refer to "VTScada Color Palette" in the VTScada Programmer's Guide.

Section: System

Default: DefaultBGColor = 0

DefaultPageColor

Indicates the background color for new pages. By default, the page background color to be displayed is white (15). For valid color values, please refer to "VTScada Color Palette" in the VTScada Programmer's Guide.

Default DefaultPageColor = 15

DefGraphicBColor

Indicates the default fill color used in the Select Brush color palette, and for all geometric drawing tools featuring a brush or fill color. The default brush color is red. For valid color values, please refer to the VTScada Color Palette.

Section: System

Default: DefGraphicBColor = 12

DefGraphicPColor

Indicates the default pen color used in the Select Pen color palette, and for all geometric drawing tools featuring an outline or pen color. The default pen color is black. For valid color values, please refer to VTScada Color Palette.

Section: System

Default: DefGraphicPColor = 0

DialogBGColor

Indicates the background color for dialogs. By default, the background dialog color is obtained from the system using the GetSystemColor(15) function.

Section: System

Default: DialogBGColor =

DigitalIndicator0Color

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag's state is 0. Defaults to light gray.

Section: System

Default: DigitalIndicator0Color = 8

DigitalIndicator1Color

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag's state is 1. Defaults to green.

Section: System

Default: DigitalIndicator1Color = 10

DigitalIndicator2Color

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag's state is 2. Defaults to blue.

Section: System

Default: DigitalIndicator2Color = <0080DD>

DigitalIndicator3Color

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag's state is 3. Defaults to purple.

Section: System

Default: DigitalIndicator3Color = <8000FF>

DigitalIndicatorAlarmColor

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag is in an alarm state. The indicator will also blink while the alarm is unacknowledged. Defaults to red.

Section: System

Default: DigitalIndicatorAlarmColor = 12

DigitalIndicatorInvalidColor

Controls the color of digital indicators, as shown in the I/O listing of a Sites page, when the matching tag's state is Invalid. Defaults to black.

Section: System

Default: DigitalIndicatorInvalidColor= 0

FieldHighlight

Indicates the highlight color for the sides of fields.

If left invalid (which it is by default), FieldHighlight uses the GetSystemColor(15) function to return the system colors as defined by the user in Windows.

Section: System

Default: FieldHighlight =

FieldShadow

Indicates the shadow color for the sides of fields.

If left invalid (which it is by default), FieldShadow uses the GetSystemColor(18) function to return the system colors as defined by the user in Windows.

Section: System

Default: FieldShadow =

GrayedText

Indicates the color for inactive (disabled) text.

If left invalid (which it is by default), GrayedText uses the GetSystemColor(17) function to return the system colors as defined by the user in Windows.

Section: System

Default: GrayedText =

GridColor

Obsolete

Indicated the initial color of the Snap Grid in older versions of VTS.

Section: System

Default: GridColor = 11

InvalidColor

Indicates the color that will be displayed for tag widgets in the event that their value is invalid. By default, the invalid color is set to black (0).

This color can be overridden for some tags on an individualized basis by setting the tag's invalid color property in its widget's settings.

Related Variables: The InvalidColor variable can be used with the State0DefColor, State1DefColor, State2DefColor, and State3DefColor variables in order to make the default settings for different states unique and comprehensive.

Default: InvalidColor = 0

MenuBgnd

Indicates the background color for the shortcut menu that opens when any graphic object representing a tag is right-clicked. The default setting is invalid, and the default color is derived from system settings.

It is recommended that you choose contrasting colors for the MenuBgnd and MenuTextColor variables so that the text on the shortcut menu is not invisible or difficult to read.

If MenuBgnd is set to invalid (as it is by default), then the background color for the shortcut menu is derived from the GetSystemColor(4) function.

Related Variables: The MenuTextColor, SelectedBgnd, and SelectedText variables indicate the colors used for non-selected shortcut menu text, the highlight used for selected shortcut menu text, and the color used for selected shortcut menu text (respectively).

Section: System

Default: MenuBgnd =

MenuTextColor

Indicates the color of the text used to display the menu items on the shortcut menu that opens when any graphic object representing a tag is right-clicked. The default setting is invalid, and the default color is derived from system settings.

It is recommended that you choose contrasting colors for the MenuBgnd and MenuTextColor variables so that the text on the shortcut menu is not invisible or difficult to read.

If MenuTextColor is set to invalid (as it is by default), then the text color for the shortcut menu is derived from the GetSystemColor(7) function.

Related Variables: The MenuBgnd, SelectedBgnd, and SelectedText variables indicate the colors used for non-selected shortcut menu text, the highlight used for selected shortcut menu text, and the color used for selected shortcut menu text (respectively).

Section: System

Default: MenuTextColor =

NormalColor

Indicates the color displayed for site symbols, input tags, and in the legend when experiencing normal conditions. The default color is 10 (light green).

Section: System

Default: NormalColor = 10

OffColor

Specifies the color to be used in the Duplexes widget to indicate an off state for digital control and pump status tags. The default color is 10 (light green).

The available color values are identified in VTScada Color Palette.

Section: System

Default: OffColor = 10

OnColor

Specifies the color to be used in the Duplexes widget to indicate an on state for digital control and pump status tags. The default color is 12 (light red).

The available color values are identified in VTScada Color Palette.

Section: System

Default: OnColor = 12

OpaqueBackground

Indicates the state of the opacity of background images (such as maps). If set to 0 (false), then the background images are drawn onto the background as transparent backgrounds (default).

If set to 1 (true), then background images are to be destructively drawn onto the background (opaque).

It is recommended that you set OpaqueBackground to 1 (true) for faster draw times.

Section: System

Default: OpaqueBackground = 0

PollDisabledColor

Modify the color to be used to indicate when polling has been disabled for a station. The default color is purple (13).

Section: System

Default: PollDisabledColor = 13

ReceiveColor

Specifies the color used to display data received from the I/O devices on the default Communications Data page. The ReceiveColor variable is set to 10 (light green) by default.

By default, the Communications Data page has a black background. If you choose to change the color in which received data is displayed, be sure to choose a color that contrasts well with black.

Please read the information provided for the TransmitColor variable.

Section: System

Default: ReceiveColor = 10

SelectedBGnd

Indicates the color of the highlight used to indicate that a menu item is selected on the shortcut menu that opens when any graphic object representing a tag is right-clicked. The default setting is invalid, and the default color is derived from system settings.

It is recommended that you choose contrasting colors for the SelectedBgnd and SelectedText variables so that the text on the shortcut menu is not invisible or difficult to read.

If SelectedBgnd is set to invalid (as it is by default), then the text color for the shortcut menu is derived from the GetSystemColor(13) function.

Related Variables: The MenuBgnd, MenuTextColor, and SelectedText variables indicate the colors used for the background of the shortcut menu, non-selected shortcut menu text, and the color used for selected shortcut menu text (respectively).

Section: System

Default: SelectedBgnd =

SelectedText

Indicates the color of text when highlighted in the shortcut menu that opens when any graphic object representing a tag is right-clicked. The default setting is invalid, and the default color is derived from system settings.

It is recommended that you choose contrasting colors for the SelectedBgnd and SelectedText Color variables so that the text on the shortcut menu is not invisible or difficult to read.

If SelectedText is set to invalid (as it is by default), then the color for text highlighted in the shortcut menu is derived from the GetSystemColor(14) function.

Related Variables: The MenuBgnd, MenuTextColor, and SelectedText variables indicate the colors used for the background of the shortcut menu, non-selected shortcut menu text, and the highlight color used for selected shortcut menu text (respectively).

Section: System

Default: SelectedText =

State0DefColor

Indicates the default color for state 0 for widgets for digital tags. This setting can be overridden on an individual basis in the tag's widget's settings. By default, state 0 is set to be represented by a light red color (12).

Related Variables: The State0DefColor variable should be used together with the State1DefColor, State2DefColor, State3DefColor and InvalidColor variables in order to make the default settings for different states unique and comprehensive.

Section: System

Default: State0DefColor = 12

State1DefColor

Indicates the default color for state 1 for widgets of digital tags. This variable can be overridden on an individual tag basis in the tag's widget's set-

tings. By default, state 1 is set to be represented by a light green color (10).

Related Variables: The State1DefColor variable should be used together with the State0DefColor, State2DefColor, State3DefColor and InvalidColor variables in order to make the default settings for different states unique and comprehensive.

Section: System

Default: State1DefColor = 10

State2DefColor

Indicates the default color for state 2 for widgets of digital tags. This variable can be overridden on an individual tag basis in the tag's widget's settings. By default, state 2 is set to be represented by a light cyan color (11).

Related Variables: The State2DefColor variable should be used together with the State0DefColor, State1DefColor, State3DefColor, and InvalidColor variables in order to make the default settings for different states unique and comprehensive.

Section: System

Default: State2DefColor = 11

State3DefColor

Indicates the default color for state 3 for widgets of digital tags. This variable can be overridden on an individual basis in the tag's widget's settings. By default, state 3 is set to be represented by a light gray color (7).

Related Variables: The State3DefColor variable should be used together with the State0DefColor, State1DefColor, State2DefColor, and InvalidColor variables in order to make the default settings for different states unique and comprehensive.

Section: System

Default: State3DefColor = 7

TransmitColor

Specifies the color used to display data transmitted to I/O devices on the default Communications Data page. The TransmitColor variable is set to 11 (light cyan) by default.

By default, the Communications Data page has a black background. If you choose to change the color in which transmitted data is displayed, be sure to choose a color that contrasts well with black.

Please read the information provided for the ReceiveColor variable.

Section: System

Default: TransmitColor = 11

UnselectedBgnd

Sets the background color for alarm list items that are not selected in the alarm list.

If set to invalid (as it is by default), the background color for alarm list items not selected in the alarm list is derived from the GetSystemColor(5) function.

Related Variables: The UnselectedText variable sets the color for the text of non-selected alarm list entries.

Section: System

Default: UnselectedBgnd =

*Restart Required (Settings.Startup property)

UnselectedText

Sets the text color for alarm list entries that are not selected in the alarm list.

If set to invalid (as it is by default), the background color for alarm list items not selected in the alarm list is derived from the GetSystemColor(8) function.

Related Variables: The UnselectedBgnd variable sets the background color for alarm list items that are not selected in the alarm list.

Section: System

Default: UnselectedText =

*Restart Required (Settings.Startup property)

WindowBgnd

Sets the background color for windows.

If set to invalid (as it is by default), then the background color is derived from the GetSystemColor(5) function.

Section: System

Default: WindowBgnd =

*Restart Required (Settings.Startup property)

WindowFrame

Sets the border color for windows.

If set to invalid (as it is by default), then the border color is derived from the GetSystemColor(6) function.

Section: System

Default: WindowFrame =

*Restart Required (Settings.Startup property)

Communication Driver Properties

The following list of variables pertain to communication drivers and communications.

...#DataLines

... BackupSwitchCount

... BadQualityColor

... CommFailColor

... CommStatsQualityFactor

... CommStatsUpdateRate

... DataFlowModuleName

... DataFlowStationName
... DemoMode
... DFSimulateOn
... DisableCommStats
... DNP3DataInvalidOnFail
...DNP3DelayedResponseTimeout
... DNP3FailoverCount
... DNP3MaxFileSize
... DNP3SharedRPC
...DriverRPCOptimization
... FastPollCommColor
... FastPollDuration
... FastPollRate
... InactiveCommColor
... ModiconVTSTMaxBlock
... NoSoftDriverFailure
...SNMPAgentEnable
...SNMPAgentInformRetryInterval
...SNMPAgentInformRetryLimit
...SNMPAgentIPListener
...SNMPAgentMaxTCPSize
...SNMPAgentMaxUDPSize
...SNMPAgentReadCommunity
...SNMPAgentSessionTimeout
...SNMPAgentTagNotifyMode
...SNMPAgentTrapCommunity
...SNMPAgentTrapHost
...SNMPAgentTrapPort

...SNMPAgentWriteCommunity
...SNMPAgentWriteEnable
...SQLDataQueryDriverDefaultDBType
...SQLDataQueryDriverDefaultTableName
...SQLDataQueryDriverMaxTagsPerQuery
...VTSDriverClearDataOnServerLossDelay

#DataLines

Indicates the maximum number of communications display lines to be displayed on the VTScada Communications Data page.

Section: System

Default: #DataLines = 100

BackupSwitchCount

Indicates the number of consecutive communication errors that need to occur when polling Data Flow RTUs before switching to the first specified backup server.

Section: System

Default: BackupSwitchCount = 30

BadQualityColor

Controls the color displayed when a tag is experiencing bad data quality. The default display color for bad data quality is orange.

You can associate basic I/O tags with each other in such a way that the quality of one tag is based on the value of another (refer to the I/O tag's Quality tab). If the Quality of the associated tag is non-zero, blank, or invalid, the data quality is assumed to be good; otherwise, the data is assumed to be bad.

Section: System

Default: BadQualityColor = <FF8000>

CIP_O_to_T_RPI

Used in combination with the `CIPTimeoutMultiplier` property. These two values together define the CIP connection timeout value for the connection from the driver to the PLC. If the driver does not send any message within this timeout period, then the session is terminated and the PLC does not respond until a new session is established. The driver monitors this timeout value and if no message is sent within the timeout, a new session is automatically established, thus preventing driver timeouts.

`CIP_O_to_T_RPI` is the originator to target packet interval in microseconds. The actual timeout applied to the connection is `CIP_O_to_T_RPI` * the effective multiplier value. The default values are 0 for the timeout multiplier and 5,000,000 for this value giving a timeout of $4 * 5 \text{ S}$, i.e. 20 S.

This value, and `CIPTimeoutMultiplier` should only be modified with an understanding of the effect of any variation from the defaults

The driver will limit the minimum timeout value to two seconds, regardless of user settings.

Default: `CIP_O_to_T_RPI` = 5,000,000

Section: System

Related Information:

`CIPTimeoutMultiplier`

`CIPTimeoutMultiplier`

Used in combination with the `CIP_O_to_T_RPI` property. These two values together define the CIP connection timeout value for the connection from the driver to the PLC. If the driver does not send any message within this timeout period, then the session is terminated and the PLC does not respond until a new session is established. The driver monitors this timeout value and if no message is sent within the timeout, a new session is automatically established, thus preventing driver timeouts.

This property directly matches the CIP protocol for calculating the timeout and can have values from 0 to 7, resulting in an effective multiplier value of $(1 \ll n) * 4$. The two angle signs are bitwise operators, as described in the list of VTScada Operators.

This value, and CIP_O_to_T_RPI should only be modified with an understanding of the effect of any variation from the defaults

The driver will limit the minimum timeout value to two seconds, regardless of user settings.

Default: CIPTimeoutMultiplier = 0

Section: System

Related Information:

CIP_O_to_T_RPI

See also: List of VTScada Operators in the VTScada Programmer's Guide

CommFailColor

Indicates the color displayed for site symbols, input tags, and in the legend when communications with the site have failed. The default color is 12 (light red).

The available color values are identified in VTScada Color Palette.

Section: System

Default: CommFailColor = 12

CommStatsQualityFactor

Quality of communication is measured by the following formula:

$$Q = Q * qF + (1 - qF) * (1 - !Error)$$

where Error is a Boolean stating whether the driver reported an error state, and the initial value of quality, Q, is defined as 1.

Each time a driver completes a read or write, a new value of the quality is calculated.

qF in this equation stands for QualityFactor and is set by this system variable.

Section: System

Default: CommStatsQualityFactor = 0.99

CommStatsUpdateRate

Sets the frequency, in seconds, of when communication statistics are logged if no error has happened. Statistics are logged whenever an error is encountered regardless of this frequency setting.

Section: System

Default: CommStatsUpdateRate = 60

DataFlowModuleName

Obsolete

Enables you to specify the title for tags representative of installed modules. This title appears in the Tag Browser's Type drop-down list and on the title bar of all tag properties folders for this tag type. By default, tags representative of installed modules are titled, "Data Flow Module".

Modification of the title for the Data Flow Module tags does not affect the title of the corresponding table in the tag properties database (Point-s.mdb). The table for Data Flow Module tags is titled "DFModule".

Section: System

Default: DataFlowModuleName = Data Flow Module

DataFlowStationName

Enables you to specify the title for Data Flow RTU tags. This title appears in the Tag Browser's Types drop-down list, and on the title bar of all tag properties folders of this tag type. By default, Data Flow RTU tags are titled, "Data Flow RTU".

Modification of the title for the Data Flow RTU tags does not affect the title of the corresponding table in the tag properties database (Point-s.mdb). The table for Data Flow Module tags is titled "DataFlow".

Section: System

Default: DataFlowStationName = Data Flow RTU

DemoMode

Enables you to set your VTScada applications to operate in simulation mode, as though a fully-configured system is in operation. Analog Status tags will update to a random value, once every 60 seconds.

If set to 1, the simulation mode is switched on.

The DFSimulateOn variable further enables you to enhance the simulation by mocking the transmission and reception of data from Data Flow RTUs to the application.

Section: System

Default: DemoMode = 0

DFSimulateOn

Enables you to set your VTScada applications to operate in simulation mode, as though data is being transmitted and received from Data Flow RTUs.

If set to 0 (default), then the Data Flow simulation mode is turned off.

Your system must consist of at least one Data Flow RTU driver tag whose selected I/O device is a serial port tag in order for the simulation to work. If the simulation is working properly, data should appear to be transmitted and received on the Communications Data page.

The DemoMode variable further enables you to enhance the simulation by mocking data as if a fully-configured system with multiple I/O tags is in operation.

Section: System

Default: DFSimulateOn = 0

DisableCommStats

Disable the logging of communication statistics for all drivers by setting the value to 1.

You can disable the logging of communication statistics for a specific driver type by prepending the drive type name in front of this variable like so:

```
<DriveTypeName>DisableCommStats = 1
```

For example, to disable logging for the Allen Bradley driver use the following:

```
AllenBradleyDisableCommStats = 1
```

Set to false by default.

Section: System

Default: DisableCommStats = 0

DNP3DataInvalidOnFail

Section: System

Default: .

DNP3DelayedResponseTimeout

The timeout (in seconds) for a delayed file transfer response.

Section: System

Default: 300.

DNP3FailoverCount

Number of consecutive errors required before a server marks itself as bad by calling RecommendAlternate

Section: System

Default: No default – must be added to Settings.Dynamic

DNP3MaxFileSize

The maximum size (in bytes) for a permitted file transfer.

Section: System

Default: DNP3MaxFileSize = 2097152

DNP3SharedRPC

Indicates whether or not the same RPC service will be used for all instances of DNP3.

If set to 0 (false), the same RPC is NOT be used for all instances of DNP3 (default).

Section: System

Default: DNP3SharedRPC = 0

DriverRPCOptimization

Causes drivers to send only what has changed, rather than an entire read block. Introduced with VTS 10.0 – defaults to TRUE for new applications, but FALSE for applications being upgraded. Developers may then set the value to TRUE once all servers have been upgraded.

Section: System

Default: DriverRPCOptimization = 1

FastPollCommColor

Indicates the color to be displayed for site symbols, input tags, and in the legend when a site is being fast polled. The default color is 9 (light blue).

The available color values are identified in VTScada Color Palette.

Section: System

Default: FastPollCommColor = 9

FastPollDuration

Indicates the duration (in seconds) for which fast polling will last once a station page has been opened. The default is 5 minutes (300 seconds).

Section: System

Default: FastPollDuration = 300

FastPollRate

Indicates the rate (in seconds) at which fast polling occurs.

Section: System

Default: FastPollRate = 2

InactiveCommColor

Indicates the color displayed for site symbols, input tags, and in the legend when communications with the site are inactive (i.e. idle, not failed communications). The default color is 10 (light green).

The available colors are identified in VTScada Color Palette.

Default: InactiveCommColor = 10

ModiconVTSMaXBlock

May be added to a Settings.Dynamic file in order to limit the number of blocks included in a read.

Default: ModiconVTSMaXBlock = 125

NoInitialDriverDial

If NoInitialDriverDial is set to 0, drivers using modems will automatically make a call when VTScada starts. If set to 1, they will not do so. The list of affected drivers is:

- AB,
- DNP3
- Modicon,
- Omron

Section: System

Default: NoInitialDriverDial = 1

NoSoftDriverFailure

Controls whether drivers should, or should not, switch to backup on failed communications.

- If set to 0 (false), then the drivers do switch to backup on failed communications (default).
- If set to 1 (true), then the drivers do not switch to backup on failed communications.

If you have two servers, both of which are on the same network/subnet, then the likelihood of the backup being able to reach the equipment when the primary cannot is slim. The problem is most likely a device or communications-chain issue. In this case, there is no need to have the servers failing back and forth.

As a general rule, it is better to set NoSoftDriverFailure to true unless the servers are on completely different networks with separate paths to the devices.

Section: System

Default: NoSoftDriverFailure = 0

SNMPAgentEnable

If set to 1 (true), then the SNMP agent will be enabled. Defaults to 0, disabled.

Default: SNMPAgentEnable = 0

Section: System

Related Information:

SNMPAgentReadCommunity | SNMPAgentWriteCommunity | SNMPAgentWriteEnable

SNMPAgentInformRetryInterval

The number of seconds between InformRequest retries. Defaults to 3.

Default: SNMPAgentInformRetryInterval = 3

Section: System

Related Information:

SNMPAgentInformRetryLimit

SNMPAgentInformRetryLimit

Sets the number of retry attempts for InformRequests. Defaults to 1.

Default: SNMPAgentInformRetryLimit = 1

Section: System

Related Information:

SNMPAgentInformRetryInterval

SNMPAgentIPListener

The SNMP Agent uses the IP Network Listener tag to provide access to the system. This tag provides features such as IP filtering and connection audit logs. This property specifies the name of the IP Network Listener to use for access. Defaults to "SNMP Agent Server Port"

Default: SNMPAgentIPListener = SNMP Agent Server Port

Section: System

SNMPAgentMaxTCPSize

Largest SNMP message size allowed over TCP transport, measured in bytes. Defaults to 8192.

Default: SNMPAgentMaxTCPSize = 8192

Section: System

Related Information:

SNMPAgentSessionTimeout

SNMPAgentMaxUDPSize

SNMPAgentMaxUDPSize

Sets the largest SNMP message allowed over UDP transport, measured in bytes. Defaults to 1472.

Default: SNMPAgentMaxUDPSize = 1472

Section: System

Related Information:

SNMPAgentSessionTimeout

SNMPAgentMaxTCPSize

SNMPAgentReadCommunity

Sets the SNMP community name for read-only access. Defaults to "public".

Default: SNMPAgentReadCommunity = public

Section: System

SNMPAgentEnable | SNMPAgentWriteCommunity | SNMPAgentWriteEnable

SNMPAgentSessionTimeout

Controls the number of seconds until an idle **NMS**¹ session is closed (def: 60)

Default: SNMPAgentSessionTimeout = 60

Section: System

Related Information:

SNMPAgentMaxTCPSize

SNMPAgentMaxUDPSize

SNMPAgentTagNotifyMode

Tag change notifications. This is set numerically as follows:

0 == Disable

1 == Server Only (default)

2 == Enable

Default: SNMPAgentTagNotifyMode = 1

Section: System

Related Information:

SNMPAgentTrapCommunity

SNMPAgentTrapHost

SNMPAgentTrapPort

SNMPAgentTrapCommunity

SNMP community name for notification messages. Defaults to "public".

Default: SNMPAgentTrapCommunity = public

Section: System

Related Information:

SNMPAgentTagNotifyMode

SNMPAgentTrapHost

SNMPAgentTrapPort

¹Network Management System

SNMPAgentTrapHost

The host name or IP address to send traps/informs. Set blank to disable.

Default: SNMPAgentTrapHost =

Section: System

Related Information:

SNMPAgentTagNotifyMode

SNMPAgentTrapCommunity

SNMPAgentTrapPort

SNMPAgentTrapPort

UDP port to send traps/informs. Defaults to 162.

Default: SNMPAgentTrapPort = 162

Section: System

Related Information:

SNMPAgentTagNotifyMode

SNMPAgentTrapCommunity

SNMPAgentTrapHost

SNMPAgentWriteCommunity

Sets the SNMP community name for write access. Defaults to none.

Default: SNMPAgentWriteCommunity =

Section: System

Related Information:

SNMPAgentEnable | SNMPAgentReadCommunity | SNMPAgentWriteEnable

SNMPAgentWriteEnable

Must be set to 1 (true), to enable write access. Defaults to 0, disabled.

Default: SNMPAgentWriteEnable = 0

Section: System

Warning: No not enable write access over an unsecured network.

Related Information:

SNMPAgentEnable | SNMPAgentReadCommunity | SNMPAgentWriteCommunity

VTSDriverClearDataOnServerLossDelay

Seconds without an I/O server before a client will invalidate read values. The default of 1 will be adequate in most instances, but can cause problems in applications with RPC problems or with hundreds of RPC services. In these cases, increasing to longer delay value can be beneficial.

Section: System

Default: VTSDriverClearDataOnServerLossDelay = 1

SQLDataQueryDriverDefaultDBType

Note: The property applies only to the SQL Data Query Driver.

A numeric value, setting the default database type for the SQL Data Query Driver tag.

Value	Default database type
0	MSSQL
1	MS Access
2	Oracle
3	MySQL

Section: System

Default: SQLDataQueryDriverDefaultDBType = 2

SQLDataQueryDriverDefaultTableName

Sets the default table name for use by the SQL Data Query Driver tag.

Section: System

Default: SQLDataQueryDriverDefaultTableName = RealAnalog

SQLDataQueryDriverMaxTagsPerQuery

The SQL Query Driver tag places a limit on the number of tags that can be included per query. Use this setting to adjust that limit as required.

Section: System

Default: SQLDataQueryDriverMaxTagsPerQuery = 25

Display Manager Properties

The following list of variables pertain to the Display Manager.

For example: If you want your application to be inside a standard Windows window, (i.e. a resizable window with a title bar and control buttons) use the following settings:

```
DispMgrResizable      = 1
DispMgrFullScreen     = 0
DispMgrMinMaxDisabled = 0
```

See also:

...Color Properties – (default background and other colors)

...BitmapDirExt

... BMPPath

... DisplayManagerTitle

... DispMgrAspectRatio

... DispMgrBitmap

... DispMgrBMPMarginBottom

... DispMgrBMPMarginLeft

... DispMgrBMPMarginRight

... DispMgrBMPMarginsWin

... DispMgrBMPMarginTop

... DispMgrDateFormat

... DispMgrFullScreen

... DispMgrHeight

- ... DispMgrHoriz
- ... DispMgrMinHeight
- ... DispMgrMinMaxDisabled
- ... DispMgrMinWidth
- ... DispMgrPageStyle
- ... DispMgrResizable
- ... DispMgrTimeFormat
- ... DispMgrTitleBorder
- ... DispMgrVert
- ... DispMgrWidth
- ... DispMgrWPageStyle
- ... DispMgrX
- ... DispMgrY
- ...NumHistoryItems
- ... ScaleDisplayContent
- ...ShowUnlinkedIndicators
- ...SiteDetailsWindowed
- ...TitleLogoTarget
- ... ToolBoxOn
- ... ToolBoxTranslucent
- ... VAMIcon

AutoOpenIdeaStudio

Automatically opens the Idea Studio when a user having configuration privileges logs into an application.

Default: AutoOpenIdeaStudio = 0

Section: System

BitmapDirExt

Controls whether the directory for the images displayed in the Select Bitmap dialog (that is opened when you click the Image palette in the Idea Studio) will be shown in the title bar of the dialog, while the name and extension for each image file being displayed will be shown beneath the image.

Section: System

Default: BitmapDirExt = 0

BMPath

Indicates the path for all images for use in the application (for example, images selected using the Bitmap tool, or images selected using the Image Change widget for digital input tags).

You must specify an existing directory; VTScada does not automatically generate a new directory based on the specified path.

Section: System

Default: BMPath = Bitmaps\

DialogMoveTime

The Network Values Xpos and Ypos of all dialogs are within the script of a steady-state Timeout call. This variable sets the time to wait before saving a dialog's new position.

Section: System

Default: DialogMoveTime = 0.5

DisplayManagerTitle

Sets the title of the application as displayed beside the logo in the window title bar and also on the Windows task bar. The title bar may not be visible if the application is running in full screen mode. If not set, the title will be "Display"

Section: System

Default: DisplayManagerTitle =

DispMgrAspectRatio

Constrain the aspect ratio of a page window when users are changing the window size. With DispMgrAspectRatio set to 1 the ratio of the width to height will not change.

Section: System

Default: DispMgrAspectRatio = 0

DispMgrBitmap

Identifies the image to be displayed on the left side of the Display Manager's title bar.

Note: VTScada is a trademark of Trihedral Engineering Limited, and the SCADA software of Trihedral are copyright protected products, provided to customers under license. Under the terms of license, Trihedral's copyright and trademark notices are required to remain, except to the extent otherwise authorized by Trihedral in writing. To assist customers with custom implementation, we may permit customers to alter notifications and related text that appear on application screens with subject matter created by the customer, provided that reasonable prominence is given to notice of the intellectual property rights of Trihedral. We can provide this for you upon supply of the desired logo file.

Section: System

Default: DispMgrBitmap = TitleBarLogo.png

DispMgrBMPMarginBottom

Indicates the width of the bottom margin for the background image

Related Variables: DispMgrBMPMarginWin, DispMgrBMPMarginLeft, DispMgrBMPMarginRight, DispMgrBMPMarginTop

Section: System

Default: DispMgrBMPMarginBottom = 0

DispMgrBMPMarginLeft

Indicates the width of the left margin for the background image

Related Variables: DispMgrBMPMarginsWin, DispMgrBMPMarginRight, DispMgrBMPMarginBottom, DispMgrBMPMarginTop

Section: System

Default: DispMgrBMPMarginLeft = 0

DispMgrBMPMarginRight

Indicates the width of the right margin for the background image

Related Variables: DispMgrBMPMarginsWin, DispMgrBMPMarginLeft, DispMgrBMPMarginBottom, DispMgrBMPMarginTop

Section: System

Default: DispMgrBMPMarginRight = 0

DispMgrBMPMarginsWin

Enables background image margins for windowed pages

Related Variables: DispMgrBMPMarginTop, DispMgrBMPMarginLeft, DispMgrBMPMarginBottom, DispMgrBMPMarginRight

Section: System

Default: DispMgrBMPMarginsWin = 0

DispMgrBMPMarginTop

Indicates the width of the top margin for the background image, if margins are enabled

Related Variables: DispMgrBMPMarginsWin, DispMgrBMPMarginLeft, DispMgrBMPMarginBottom, DispMgrBMPMarginRight

Section: System

Default: DispMgrBMPMarginTop = 0

DispMgrDateFormat

Specify how the date is to be displayed in the upper corner of the VTScada title bar. You may use one of the VTScada predefined date formats or you may use the VTScada date formatting codes to create

your own format. Defaults to format 20 which is three-character month followed by the numeric day of the month.

Section: System

Default: DispMgrDateFormat = 20

Related Information:

See: predefined Date Codes, in the VTScada Programmer's Guide.

DispMgrFullScreen

Enables you to specify whether the Display Manager should feature a Windows title bar with a title and close buttons. (The additional presence of minimize and maximize buttons is determined by the setting of the DispMgrMinMaxDisabled variable.)

If set to 0 (false), the Display Manager does not display in full screen mode, and has a windows title bar with a default title of "Display" and a close button. (To modify the title displayed in the Windows title bar, use the DisplayManagerTitle variable in the [LABELS] section.)

If set to 1 (true), the Display Manager displays in full screen mode. No Windows title bar is present (default).

Section: System

Default: DispMgrFullScreen = 0

DispMgrHeight

Indicates the height (vertical) of the Display Manager. If set to invalid (which it is by default), DispMgrHeight uses the VStatus(Self(),27) call to determine the default height of the Display Manager based on the video board and screen characteristics of your workstation.

Note: This setting applies to the page area, not the entire VTScada application. Borders, scroll bars and the title bar must all be accounted for in addition to the DispMgrHeight value.

Note: The border of a window can vary in width depending on the value set for your Active Window Border Size (found in the advanced properties of the Windows Desktop Properties: Appearance) If set to 1, the

border will be 4 pixels around the window. Each additional number in the setting adds one pixel. Thus, if your screen resolution is set to 1024x768 and you set the DispMgrHeight to 768, the page will not fit the window, since the page height will exceed the available space by a distance equivalent to the width of two borders, plus the title bar, plus the horizontal scroll bar, if visible.

Note: As a guideline, the DispMgrHeight should be set at least 60 pixels less than the current screen height.

Related Variables: To set the width of the Display Manager, use the DispMgrWidth variable. This variable takes precedence over setting DispMgrFullScreen = 1.

Section: System

Default: DispMgrHeight =

DispMgrHidden

EnableShowHide must be set TRUE.

This property is set only in combination with a workstation name (that is, in a WorkstationSettings file). If EnableShowHide is TRUE, the application will be hidden from view while running.

Note: Do not set this property without a Workstation name unless your intention is for the application to be hidden on all workstations while running. You are strongly advised to change the property only by using the Toggle Visibility icon in the VAM. Doing so will ensure that the change affects only the current workstation.

Default: DispMgrHidden = 0

Section: Layer

Related properties:

...EnableShowHide

...LogOffUponHide

DispMgrHoriz

Enables you to set the Display Manager to tile multiple pages on the screen. DispMgrHoriz indicates the number of pages to display horizontally.

Related Variables: Both the DispMgrHoriz and the DispMgrVert variables must be set in order for the Display Manager to tile multiple windows; setting only one of these variables will have no effect.

Note: To stretch your desktop across two or more monitors, you must also configure the display resolution in the Windows™ control panel. This option is not available to all graphics cards.

Section: System

Default: DispMgrHoriz = 1

DispMgrMinHeight

Sets a minimum height for a window when set to a value other than the default of 0. Users will not be able to change the window height to a size less than the value of this variable. Set this value to 0 to disable it.

Section: System

Default: DispMgrMinHeight = 0

DispMgrMinMaxDisabled

Enables you to control the presence of minimize and maximize buttons in the Windows title bar of the Display Manager if the DispMgrFullScreen variable is set to 0 (indicating that a Windows title bar is present for the Display Manager).

If set to 0 (false), the Minimize or Maximize buttons are present in the Windows title bar (if a Windows title bar has been configured for this application using the DispMgrFullScreen variable) (default).

If set to 1 (true), minimize and maximize buttons are not present in the Windows title bar (if a Windows title bar has been configured for this application using the DispMgrFullScreen variable).

Section: System

Default: DispMgrMinMaxDisabled = 0

DispMgrMinWidth

Sets a minimum width for a window when set to a value other than the default of 0. Users will not be able to change the window width to a size less the value of this variable. Set this value to 0 to disable it.

Section: System

Default: DispMgrMinWidth = 0

DispMgrPageStyle

Controls the page style characteristics of a full screen VTScada page.

This is a bitwise variable with the following meanings for the bits:

Value	Constant	Meaning
0x000001	PSTTB	Show title bar
0x000002	PSBMP	Deprecated. Show title bar bitmap
0x000004	PSLGN	Show title bar logon button
0x000008	PSGFX	Show title bar graphic editor {Btn}
0x000010	PSDTE	Show title bar date & time
0x000020	PSIND	Show title bar alarm indicator
0x000040	PSNOT	Show title bar page notes buttons
0x000080	PSPRN	Show title bar print button
0x010000	PSTAG	Show title bar tag button
0x020000	PSAPP	Show title bar app. properties button
0x040000	PSFBB	Show title bar forward/back buttons
0x080000	PSULI	Show title bar unlinked indicator
0xFF00FF	PSTTT	Show all title bar decorations
0x000100	PSMBR	Show task bar
0x000200	PSMNU	Show menu button and menu
0x000400	PSMPB	Show task bar page buttons
0x000800	PSMFB	Deprecated. Show task bar "<" and ">" buttons

0x001000	PSMPM	Show task bar add/remove buttons
0x002000	PSMHD	Deprecated. Hold page button changes target
0x00FF00	PSMMM	Show all menu bar decorations

Section: System

Default: DispMgrPageStyle = 0xFFFFFFFF

Related Information:

DispMgrWPageStyle

DispMgrResizable

Enables you to indicate whether or not the Display Manager should be horizontally and vertically resizable by dragging the window's borders when in windowed mode (i.e. when the DispMgrFullScreen variable is set to 0).

If set to 0 (false), the Display Manager will not be resizable by dragging its borders horizontally or vertically (if a Windows title bar has been configured for this application by setting the DispMgrFullScreen variable to 0) (default).

If set to 1 (true), the Display Manager will be resizable by dragging its borders horizontally or vertically (if a Windows title bar has been configured for this application by setting the DispMgrFullScreen variable to 0).

Related Variables: The DispMgrFullScreen variable must be set to 0 (i.e. the Display Manager must be configured to display a Windows title bar) in order for DispMgrResizable to take effect. The DispMgrHeight, DispMgrWidth, BrowserHeight, and BrowserWidth variables will apply to the Display Manager only until the window has been re-sized by dragging its borders, after which the Display Manager will retain the newly adjusted size. If DispMgrMinMaxDisabled is set to 1, the Display Manager will not feature Windows minimum and maximize buttons, however, the window will be resizable by dragging its borders.

Section: System

Default: DispMgrResizable = 1

DispMgrTimeFormat

Specifies the format of the time displayed in the Display Manager's upper right corner. The default format for the time will look similar to: "1:38 AM". The available time formats are the same as those for the Time function.

Note that the predefined numeric codes return time in a 24-hour format except for formats 6 and 7 which are in a 12-hour format. You may also provide a text string of time format codes for greater control.

Section: System

Default: DispMgrTimeFormat = h:mm tt

Related Information:

See: predefined Time Formats in the VTScada Programmer's Guide

DispMgrTitleBorder

When set to 0, disables the title bar and borders. When set to 1 or when missing altogether, the title bar and borders are unaffected.

Section: System

Default: DispMgrTitleBorder = 1

DispMgrVert

Enables you to set the Display Manager to tile multiple pages on the screen. DispMgrVert indicates the number of pages to display vertically.

Related Variables: Both the DispMgrVert and the DispMgrHoriz variables must be set in order for the Display Manager to tile multiple windows; setting only one of these two variables will have no effect.

Note: To stretch your desktop across two or more monitors, you must also configure the display resolution in the Windows™ control panel. This option is not available to all graphics cards.

Section: System

Default: DispMgrVert = 1

DispMgrWidth

Indicates the width (horizontal) of the Display Manager. If set to invalid (which it is by default), DispMgrWidth uses the VStatus(Self(), 26) call to determine the default width of the Display Manager based on the video board and screen characteristics of your workstation.

Note: This setting applies to the page area, not the entire VTScada application. Borders, scroll bars and the title bar must all be accounted for in addition to the DispMgrWidth value.

Note: The border of a window can vary in width depending on the value set for your Active Window Border Size (found in the advanced properties of the Windows Desktop Properties: Appearance) If set to 1, the border will be 4 pixels around the window. Each additional number in the setting adds one pixel. Thus, if your screen resolution is set to 1024x768 and you set the DispMgrWidth to 1024, the page will not fit the screen, since the page width will exceed the available space by a distance equivalent to the width of two borders, plus the vertical scroll bar, if visible.

Note: As a guideline, the DispMgrWidth should be set at least 8 pixels less than the current screen width.

Related Variables: To set the height of the Display Manager, use the DispMgrHeight variable. This variable takes precedence over setting DispMgrFullScreen = 1.

Section: System

Default: DispMgrWidth =

DispMgrWPageStyle

Controls the page style characteristics of a windowed VTScada page. This is a bitwise variable with the following meanings for the bits:

Value	Constant	Meaning
0x000001	PSTTB	Show title bar

0x000002	PSBMP	Deprecated. Show title bar bitmap
0x000004	PSLGN	Show title bar logon button
0x000008	PSGFX	Show title bar graphic editor {Btn}
0x000010	PSDTE	Show title bar date & time
0x000020	PSIND	Show title bar alarm indicator
0x000040	PSNOT	Show title bar page notes buttons
0x000080	PSPRN	Show title bar print button
0x010000	PSTAG	Show title bar tag button
0x020000	PSAPP	Show title bar app. properties button
0x040000	PSFBB	Show title bar forward/back buttons
0x080000	PSULI	Show title bar unlinked indicator
0xFF00FF	PSTTT	Show all title bar decorations
0x000100	PSMBR	Show task bar
0x000200	PSMNU	Show menu button and menu
0x000400	PSMPB	Show task bar page buttons
0x000800	PSMFB	Deprecated. Show task bar "<" and ">" buttons
0x001000	PSMPM	Show task bar add/remove buttons
0x002000	PSMHD	Deprecated. Hold page button changes target
0x00FF00	PSMMM	Show all menu bar decorations

Section: System

Default: DispMgrWPageStyle = 0x000000

Related Information:

DispMgrPageStyle

DispMgrX

Indicates the X coordinate (horizontal) of the Display Manager's upper left corner if the Display Manager is not in full screen mode.

Related Variables: To set the Y coordinate of the Display Manager's upper left corner, use the DispMgrY variable. To set the height of the Display Manager, use the DispMgrHeight and DispMgrWidth variables.

By default, the Display Manager is in full screen mode. This behavior can be controlled using the `DispMgrFullScreen` variable.

Section: System

Default: `DispMgrX = 0`

DispMgrY

Indicates the Y coordinate (vertical) of the Display Manager's upper left corner if the Display Manager is not in full screen mode.

Related Variables: To set the X coordinate of the Display Manager's upper left corner, use the `DispMgrX` variable. To set the height of the Display Manager, use the `DispMgrHeight` and `DispMgrWidth` variables.

By default, the Display Manager is in full screen mode. This behavior can be controlled using the `DispMgrFullScreen` variable.

Section: System

Default: `DispMgrY = 0`

Page Indicates the page file name of the first page to be opened in the Display Manager when the application runs.

If set to invalid (as it is by default), the Display Manager displays the last page that was viewed before the application was stopped.

Section: System

Default: `Page =`

NumHistoryItems

Limits the number of items shown in the Recent Pages area of the tile menu.

Default: `NumHistoryItems = 10`

Section: System

ScaleDisplayContent

Indicates whether the contents of the pages shown in the Display Manager should be stretched or shrunk to fit within the Display Manager's display area.

If set to 1 (true), then the contents of the pages shown in the Display Manager are stretched or shrunk to fit within the Display Manager's display area.

Section: System

Default: ScaleDisplayContent = 0

Note: Automated display scaling works reasonably well when enlarging the page. It cannot do as good a job when shrinking a display for a smaller screen. In particular, labels embedded within buttons or widgets are more likely to be truncated than scaled down.

Always design for the smallest screen that the application will be displayed upon.

ShowUnlinkedIndicators

When TRUE, an indicator will be shown on each unlinked tag widget.

Section: System

Default: ShowUnlinkedIndicators = 0

SiteDetailsWindowed

Controls the default behavior of whether a Site Details page will open full screen or in a pop-up window. Has no effect on pages that are set to "Always display in window" or "Never display in window".

- When set TRUE, the details page will be displayed in a pop-up window unless the page is set to "Never display in a window".
- When set FALSE, the site details page will open in the main window, unless the page is set to "Always display in a window".

Section: System

Default: SiteDetailsWindowed = 1

TitleLogoTarget

Sets the page that should be opened when an operator clicks the logo at the top of a page. A list of parameters for the page can be provided in

parentheses following the page name. Set the parameter list to Invalid if there are none.

Default: TitleLogoTarget = PageMenuPage(Invalid)

Section: Labels

ToolBoxOn

Obsolete as of release 11.

Controlled whether the Configuration Toolbox was to be open or closed at startup.

If set to 1 (true), the Configuration Toolbox is not open at startup.

Note: The ToolBoxOn variable works only if the security system for the application has not yet been activated.

Section: System

Default: ToolBoxOn = 0

ToolBoxTranslucent

Obsolete as of release 11.

Indicated whether or not you wish the Configuration Toolbox to be translucent when any of the configuration tools (e.g. Tag Browser, etc.) are open.

If set to 0, then the Configuration Toolbox will not be translucent when any of the configuration tools are open.

If set to 1 (default), the Configuration Toolbox will be translucent when any of the configuration tools are open.

Section: System

Default: ToolBoxTranslucent = 1

Editing and Debugging Properties

The following list of variables pertain to code editing and debugging.

... Language

... NoModal

... NoOpChangeDialog

... NVShowCheckFilesDlgCount

... NVShowDialogs

... OnTop

Language

For use in custom-built code. Not used by VTScada.

In applications that contain custom code for dynamic language change support, this provides a storage location for language selection.

Section: System

Default: Language = 0

Related Information:

The following can be found in the VTScada Programmer's Guide:

...Language Support – Creating a user-interface with a language other than English.

...Using a Non-English Character Set – Configure Windows (and thereby VTScada) to use alternative character sets.

NoModal

Indicates whether or not most modal dialogs are to be made non-modal. If set to invalid (as it is by default), then the application will default to the NoModal flag variable in Setup.INI (or its default if NoModal is not set in Setup.ini)

If set to 0 (false), then most modal dialogs are not made non-modal.

If set to 1 (true), then most modal dialogs are made non-modal.

Warning: Setting NoModal to other than its default can affect your application adversely if users are allowed to click outside of dialogs that were intended to be modal.

Section: System

Default: NoModal =

NoOpChangeDialog

Enables you to suppress or reveal the dialog that is displayed when a user attempts to make an operational change to a tag.

Is set to 0 (false), then the dialog is not suppressed (default).

If set to 1 (true), then the dialog is suppressed.

Section: System

Default: NoOpChangeDialog = 0

NVShowCheckFilesDlgCount

Sets the number of NetworkValues files that are needed before the Check Files dialog will be displayed.

Default: NVShowCheckFilesDlgCount = 5000

NVShowDialogs

If set to TRUE then the Network Values service will show dialogs on start-up. The purpose of these dialogs is to let the operator know that the system is still working when there are a large number of files to check.

Section: System

Default: NVShowDialogs = 1

OnTop

Indicates whether or not the Debugger should appear on top of all other screens.

If set to 0 (false), then the Debugger does not appear on top of all other screens (default).

If set to 1 (true), then the Debugger does appear on top of all other screens.

Section: System

Default: OnTop = 0

General Properties

...AutoActivate

...AutoStart

...DisableGoToPage

...DoNotStart

...HideFromVAM

...LocalScopeSyntax

...SyncOEMLayers

... VAMIcon

AutoActivate

Controls whether the application will activate automatically when VTScada starts.

Defaults to FALSE (0).

Default: AutoActivate = 0

Section: Application

AutoStart

Controls whether the application will start automatically when VTScada starts.

Defaults to FALSE (0).

Default: AutoStart = 0

Section: Application

DisableGoToPage

Deactivates the Go To Page feature in both the Tag Browser and the Alarm Page. Recommended if you rely on restricted access to hotboxes to prevent unauthorized access to certain pages rather than using security privileges within those pages.

Default: DisableGoToPage =

Section: System

DoNotStart

When set TRUE (1) the application cannot be started.

It can and will be activated when needed.

It is common to prevent an OEM layer from starting by setting this property.

Unlike most other properties, this property is local to the application where it is set. Hiding an OEM layer does not cause applications built on that OEM layer to also be hidden.

Default: DoNotStart = 0

Section: Application

Related Information:

HideFromVAM

HideFromVAM

Controls whether the application is visible in the VTScada Application Manager when loaded in the VAM's list. Set to 1 (TRUE) to hide the application. OEM layers, which are not meant to be run, but which must be present in the VAM, are sometimes hidden from view.

Unlike most other properties, this property is local to the application where it is set. Hiding an OEM layer does not cause applications built on that OEM layer to also be hidden.

The application can be displayed again by adding it back into the VAM as an existing application.

Default: HideFromVAM = 1

Section: Application

Related Information:

DoNotStart

HideVAM

LocalScopeSyntax

Must be set TRUE (1) for the "." character to function as a scope operator.

- Will default to 0 for legacy applications (those created prior to VTScada release 11.2).
- Will default to 1 for new applications.

Section: System

Default: LocalScopeSyntax = 1

*Restart Required (Settings.Startup property)

SyncOEMLayers

TRUE to cause all OEM Layers for this application to synchronize their configuration using this layer's configuration server list.

It is often the case that an OEM layer will be distributed to multiple client sites, each with a different network layout. A server list in the OEM layer itself would be difficult or impossible to maintain, therefore it is best to use each dependent application's server list.

If FALSE then an OEM layer would need its own server list for configuration synchronization, or the update would need to be applied to each workstation individually. As a general rule, this property should be managed only in the top-most (aka. dependent) layer.

Default: SyncOEMLayers = 1

Section: Layer

Related Information:

VAMIcon

Identifies the bitmap file (.BMP, .JPG or .PNG) that will be displayed beside the application name in the VTScada Application Manager.

If not set (default), the application's icon will use whatever was defined in the layer that it is based on. This will usually be the VTScada logo.

Images larger than 38x20 pixels will be scaled to fit. In order for the icon to blend smoothly into the VAM, rather than appearing as a rectangle, any pixels in the image file that are not a part of the actual icon should be transparent.

Section: Application

Default: VAMIcon =

Related Information:

Display Tab of the Edit Properties Page

Internet Server and Client Properties

The following list of variables apply to the VTScada internet server & client

... BrowserHeight

... BrowserWidth

... BrowserX

... BrowserY

...CloseSessionOnLogout

... RealmAreasExcludeInvalid

Related Information:

... Mobile Browser Properties

...Sections for Realm Area Filtering

...Setup.ini [REMOTE] Section Variables

BrowserHeight

Indicates the height (in pixels) for the Internet Explorer secondary window that displays the pages of a Browser Client enabled VTScada application on the client PC. If not specified (invalid) then the window height auto sizes. The default setting for BrowserHeight is invalid.

Section: System

Default: BrowserHeight =

BrowserWidth

Indicates the width (in pixels) for the Internet Explorer secondary window that displays the pages of a Browser Client enabled VTScada application on the client PC. If not specified (invalid) then the window width auto sizes. The default setting for BrowserWidth is invalid.

Section: System

Default: BrowserWidth =

BrowserX

Indicates the X coordinate origin for the Internet Explorer secondary window that displays the pages of a Browser Client enabled application on a client PC.

Section: System

Default: BrowserX = 0

BrowserY

Indicates the Y coordinate origin for the Internet Explorer secondary window that displays the pages of a Browser Client enabled application on a client PC.

Section: System

Default: BrowserY = 0

CloseSessionOnLogout

OBSOLETE

Enables you to command VTScada to close a VIC session when a user logs out.

If CloseSessionOnLogout is set to "1", a VIC session will automatically be closed when a user logs out. The user will have to log back in to access the pages of the associated application.

If CloseSessionOnLogout is set to "0", a VIC session will not automatically be closed when a user logs out.

Default: CloseSessionOnLogout = 1

RealmAreasExcludeInvalid

Used when Realm Area Filtering is in effect. When an application uses realm area filtering, it is customary to configure one or more users that do not have a group membership and grant to these users viewing access to all areas. The variable RealmAreasExcludeInvalid controls whether or

not tags that do not have any area defined will be included or excluded from view.

If `RealmAreasExcludeInvalid` is set to 1, then no user will be able to view tags that do not have an associated area.

Section: System

Default: `RealmAreasExcludeInvalid = 1`

RootNamespace

If your applications makes use of realm-area filtering and if you allow remote access to the VTScada Internet Server (VIC or MIC) then you must define a realm for super-user access and declare it in the `RootNamespace` property. Accounts that are not part of any security group (super-users) will not have access to any realm otherwise.

Default: `RootNamespace =`

Section: System

Logging & Reporting Properties

The following list of variables pertain to logging.

- ...`DefaultAnalogDeadbandFractionOfFullScale`
- ...`DefaultCalculationDeadbandFractionOfFullScale`
- ...`DiskFreeSpaceCheck`
- ... `DiskFreeSpaceDrives`
- ... `DiskPcentLogRestart`
- ... `DiskPcentLogStop`
- ... `FileListMax`
- ... `HistorianBroadcastMaxSize`
- ... `HistorianBroadcastMinInterval`
- ... `HistorianConnectionRetryDelay`
- ...`HistorianDataAgeSweepIntervalDivisor`
- ...`HistorianDefaultArchiveInterval`

- ... HistorianFailoverInterval
- ... HistorianWriteBufferMaxLength
- ... HistorianWriteBufferMaxTimeDiff
- ... LegacyHistoryPath
- ... LogPath
- ...SQLQueryHideLegacyTables
- ...SQLQueryHistoryNoOverridesTableName
- ...SQLQueryHistoryNoOverridesTableSupportsTPP
- ...SQLQueryTableTPPs
- ... StorageLocation
- ... StorageType
- ... TraceUserConfigActions
- ... UseLegacyHistoryPriorTo

DiskFreeSpaceCheck

Obsolete. Removed as of version 10.0

DiskFreeSpaceDrives

Obsolete. Removed as of version 10.0

DiskPcentLogRestart

>

Obsolete. Removed as of version 10.0

DiskPcentLogStop

Obsolete. Removed as of version 10.0

FileListMax

Deprecated as of VTS 10. Indicates the maximum number of log files that are accessible per logger tag. The GetLog function will not retrieve more than FileListMax files, and only FileListMax file names will be saved in the .LOG file for the tag.

Section: System

Default: FileListMax = 1000

HistorianBroadcastMaxSize

The maximum number of service updates to send at once.

Section: System

Default: HistorianBroadcastMaxSize = 500

HistorianBroadcastMinInterval

The minimum number of seconds between service updates.

Section: System

Default: HistorianBroadcastMinInterval = 1

HistorianConnectionRetryDelay

The number of seconds that a Historian should wait before retrying a connection.

Section: System

Default: HistorianConnectionRetryDelay = 1

HistorianDataAgeSweepIntervalDivisor

If data age storage limiting mode is used, then the sweep interval will be the data age divided by this value.

Section: System

Default: HistorianDataAgeSweepIntervalDivisor = 4

HistorianDefaultArchiveInterval

If data age storage limiting mode is used, then this value sets default and maximum archive interval in seconds (365 days).

Section: System

Default: HistorianDefaultArchiveInterval= 31536000

HistorianFailoverInterval

The interval between successive Historian server failover attempts.

Section: System

Default: HistorianFailoverInterval = 60

HistorianDataAgeSweepIntervalDivisor

HistorianWriteBufferMaxLength

Sets the maximum number of records per tag name that will be retained in the Historian WriteHistory buffer.

Section: System

Default: HistorianWriteBufferMaxLength = 100

HistorianWriteBufferMaxTimeDiff

Sets the number of seconds for which backup buffer data will be retained. The time difference is relative to the most recent server timestamp

Section: System

Default: HistorianWriteBufferMaxTimeDiff = 15

LegacyHistoryPath

Deprecated. Maintained only for backward compatibility.

Required only on a workstation that does not have its own copy of the data. Typically set to a network path, identifying the machine and the folder (usually "History") where the legacy data is stored.

LogPath

Deprecated as of VTScada 10. If present, should be left unchanged.

Indicated the path at which the data files for tags whose data is being recorded by logger tags are stored. You must append the name of the directory you specify for the LogPath with a backslash (example: LogPath = C:\VTScada\History).

If set to invalid (as it is by default), LogPath will automatically save the data files to the application directory.

This path can be a relative path (e.g. MyData\), or an absolute path (e.g. C:\VTScada\MYData\). If the directory you reference does not exist, VTScada will create it for you. A relative path is recommended, as it enables you to move the application without consequence at a later date. You should decide upon the path to which you wish the data files to be saved prior to creating your application. The name given each data file is, by default, tagname.DAT (i.e. the name of the tag whose data is being logged by the logger tag).

UNC path names (i.e. those of the form ServerName://Path/) may not be used.

Section: System

Default: LogPath =

SoapServicesRealmName

Applies only to installations that include the VTScada ODBC Server as part of the license.

Part of the configuration of an ODBC data source name (DSN) is to specify the VTScada realm to which the ODBC driver will connect. The property, SoapServicesRealmName must be given a value matching this realm or set of realms, where each name is separated by a semicolon.

Default: SoapServicesRealmName =

Section: System

Related Information:

...See: SQL Queries of VTScada Data: The ODBC Server in the VTScada Developer's Guide

Note: Despite what might be suggested by the name, SoapServicesRealmName is not used when configuring VTScada Web Services.

SQLQueryHideLegacyTables

Prior to release 11.1 of VTScada, logged tag data was stored in separate tables. These legacy tables may still be viewed if this application property `SQLQueryHideLegacyTables` is set to 0 (FALSE). If set true, only the History table (and any `History_TPP` tables) will be visible.

Default: `SQLQueryHideLegacyTables = 0`

Section: System

SQLQueryHistoryNoOverridesTableName

May be set to a text value, which VTScada will then use as a table name. SQL Queries that refer to this table will return all values stored with the same tag name and timestamp. A common value to assign for this property is "HistoryWithDuplicates".

(Under normal conditions, when there are multiple values stored for a tag value, all having the identical timestamp, VTScada assumes that the extras are duplicates and will return only a single value per timestamp.)

Default: `SQLQueryHistoryNoOverridesTableName =`

Section: System

Related Information:

`SQLQueryHistoryNoOverridesTableSupportsTPP`

ODBC Interface: Table Structure and Notes – in the VTScada Developer's Guide. Refer to sub-section, "Multiple Values per Time Stamp"

SQLQueryHistoryNoOverridesTableSupportsTPP

In most cases when querying for duplicates from the history table, queries that aggregate data will not be useful. This property may be set to false to direct VTScada to ignore such queries.

Default: `SQLQueryHistoryNoOverridesTableSupportsTPP = 1`

Section: System

Related Information:

SQLQueryHistoryNoOverridesTableName

SQLQueryTableTPPs

Used by the ODBC Server option to group data records by time interval. By adding the application property, SQLQueryTableTPPs, you can retrieve tag data from specific time intervals. The format of the statement is:

```
SQLQueryTableTPPs = <time frame specifier>
```

where the time frame specifier takes the form of a digit and a letter. The letter indicates the units in which time interval is measured (hours: H , weeks: W, etc.) and the digit specifies the number of units of each interval that should pass between each record.

The available time interval units are:

MS – milliseconds

S – seconds (this is the default; the S may be omitted)

M – minutes

H – hours

D – days

W – weeks

Y – years

Default: SQLQueryTableTPPs=

Section: System

StorageLocation

Sets the location for storage of data from a named Historian tag. Must be added to your application. The name of the tag must precede this property name. For example, to specify a storage location for the SystemHistorian tag, add the property "SystemHistorianStorageLocation". Defaults to the Data\History directory under your application. If using the VTScada history database, this value should be a folder name. If using an ODBC database, this should be either the DSN or a valid connection string for the database.

StorageType

Sets the type of storage for a named Historian tag. Must be added to your application. The name of the tag must precede this property name. For example, to specify a storage type for the SystemHistorian tag, add the property "SystemHistorianStorageType".

Defaults to the VTScada proprietary database. The only other valid value is "ODBC" for all other storage types.

TraceUserConfigActions

Adds events to the alarm history whenever a user makes an online configuration change. On by default.

Default: TraceUserConfigActions = 1

UseLegacyHistoryPriorTo

Sets a timestamp marking the latest date and time that legacy data was recorded. This will usually be the moment that the application was converted from one system to the other but, if your application is configured to use a time-delay when logging data, then you may need to adjust the UseLegacyHistoryPriorTo value to account for the offset.

The time should be specified in the UTC timezone. For example, "2012-04-01 12:35:30.304", or the equivalent using a time stamp.

Modem Manager Properties

The following list of variables pertain to the Modem Manager.

- ...AnswerCalls
- ... CallInterval1 Through CallInterval10
- ... CallOutDelay1
- ...CallOutDelay2
- ... CallOutPriority
- ... CycleDelay
- ... CycleLength

- ... DataIdleTime
- ... DialerSpeechInit
- ... DialResetTime
- ... DialWaitTime
- ... GuardTone
- ... HangUpDelay
- ... HelloPacketLength
- ... InitialDataDelay
- ... InitModemsDisabled
- ... MaxHandOffCount
- ... MinModemsFree
- ...MMUnAvailRetry
- ... MMCycleTime
- ... MMLogDateFormat
- ... MMLogLevel
- ... MMLogTimeFormat
- ...MMMaxQTime
- ... MMRPCTimeout
- ... ModemAlarm
- ... ModemAutoReset
- ... ModemManagerLogSize
- ... ModemMmaster
- ... <ModemName>Device
- ... <ModemName>Disabled
- ... ModemRetries
- ... ModemSpeechTO
- ... ModemTCPIPPort
- ... SiteRetries

... SquelchDetectDelay
... SquelchIdleTime
... SquelchPacketLength
... UseSerialAreaInModemCall
... UseUnimodem

AnswerCalls

Controls whether or not you wish the Modem Manager to answer calls. If set to 1 (true), the Modem Manager will answer incoming calls.

Section: System

Default: AnswerCalls = TRUE

CallInterval1 Through CallInterval10

Indicates the number of seconds to wait after a connection attempt in a call cycle fails. The number following CallInterval in the name matches the connection attempt, 1 through 10.

Related Variables: CycleLength indicates the number of times that CallInterval1 through CallInterval10 occurs. CycleDelay indicates the amount of time that the system will wait before beginning the entire call cycle again.

Section: System

Defaults:

CallInterval1 = 5
CallInterval2 = 60
CallInterval3 = 120
CallInterval4 = 120
CallInterval5 = 600
CallInterval6 = 600
CallInterval7 = 600
CallInterval8 = 600
CallInterval9 = 600
CallInterval10 = 600

CallOutDelay1

Indicates the amount of time (in seconds) that you wish the system to wait before notifying designated operators of unacknowledged priority 1 (critical) alarms.

Please review the information on the CallOutPriority and MaxCallAlarmPriorityReported variables.

Section: System

Default: CallOutDelay1 = 120

CallOutDelay2

Indicates the amount of time (in seconds) that you wish the system to wait before notifying designated operators of unacknowledged priority 2 (urgent) alarms.

Please review the information on the CallOutPriority and MaxCallAlarmPriorityReported variables.

Section: System

Default: CallOutDelay2 = 600

CallOutPriority

Indicates whether or not the Alarm Notification System should contact operators when alarms have gone unacknowledged for a user-defined period of time. The CallOutPriority variable further permits you the option of selecting the priority of alarms of which designated operators should be notified.

If set to 0, the Alarm Notification System is disabled.

If set to 1, the Alarm Notification System will notify designated operators of only those alarms that have a priority of 1 (critical).

If set to 2, the Alarm Notification System will notify designated operators of only those alarms that have a priority of 1 (critical), or 2 (urgent).

Note: Please review the information on the MaxCallAlarmPriorityReported variable.

Note: This variable correlates to the Dial-out Priority radio buttons on the Alarm Notification Options dialog.

Section: System

Default: CallOutPriority = 2

CycleDelay

Number of seconds to wait after CycleLength failed attempts occurred to connect to a phone number. After this time interval, the calls are attempted again and failed attempts restart after a time delay of CallInterval1. For BAPT (British Telecom) rules, no more than four cycles may occur in a four-hour period. The default of 55 minutes causes one call cycle every hour.

Section: System

Default: CycleDelay = 3300

CycleLength

Number of attempts for a connection to a single phone number before CycleDelay occurs and call attempts restart with retry intervals starting at CallInterval1 again (assists in support of BAPT (British Telecom) rules). Any CallInterval variables with intervals larger than CycleLength are ignored; if CycleLength is invalid, all retries beyond 10 use CallInterval10.

Section: System

Default: CycleLength = 5

DataIdleTime

Number of seconds to wait after data stops arriving (after initial data starts on an incoming call) before data tested to determine which driver should handle it.

Section: System

Default: DataIdleTime = 1

DialResetTime

A configurable time delay (in seconds or fractions of a second) between the hanging-up of a modem, and its selection for use in a new call. This

delay enables the system driver to reset the modem to a known state. At low baud rates it may be necessary to extend this time.

Section: System

Default: DialResetTime = 10

DialWaitTime

Indicates the delay (in seconds) to wait before retrying a failed modem operation after no dial tone, or no response is received from the modem.

Related Variables: The HangUpDelay variable indicates the number of seconds to wait before hanging up the modem when there are not active attempts to read or write

Section: System

Default: DialWaitTime = 10

GuardTone

Defines a wave file that will be played every \ModemSpeechTO seconds while an audio call is silent. If not defined, then nothing is played.

Section: System

Default: GuardTone =

HangUpDelay

Indicates the number of seconds to wait to hang up the modem when there are no active attempts at communications (i.e. no active attempts to read or write).

Related Variables: The DialWaitTime variable indicates the number of seconds to wait before retrying a failed modem operation.

Section: System

Default: HangUpDelay = 10

HelloPacketLength

Maximum number of bytes to accept as the initial message to be passed on to the drivers to determine the type of protocol and station address initiating the incoming call. The maximum allowable value is 1024.

Section: System

Default: HelloPacketLength = 1024

InitialDataDelay

Indicates the number of seconds the system should wait to receive initial data on an incoming call before proceeding with further attempt at communications.

Section: System

Default: InitialDataDelay = 10

InitModemsDisabled

If this is defined and has a true value (i.e. a non-zero numeric value), then all modems are started in Disabled mode. If this is defined for a workstation, then only the modems owned by that workstation are affected.

Section: System

Default: InitModemsDisabled =

MaxHandOffCount

When Modem Manager answers a call, but no registered VTScada driver accepts it, Modem Manager hands the call off to the next application that handles incoming modem calls. If another application accepts the call, Modem Manager increments a count of concurrent handed-off calls. While this count equals MaxHandOffCount, no further calls are handed off.

If MaxHandOffCount is not defined, then there will be no restrictions on call hand offs.

Section: System

Default: MaxHandOffCount = 0

MinModemsFree

Indicates the minimum number of free modems that must be maintained to handle incoming calls. This parameter enables the Modem Manager to try and keep a free pool of modems available for incoming calls. An

outgoing call will be queued while there are less than MinModemsFree modems unused.

Related Variables: If the AnswerCalls variable has been set to 0 (as it is by default), then the MinModemsFree variable is ignored.

Section: System

Default: MinModemsFree = 0

MMCycleTime

Relevant only when there is more than one modem in a networked application. When MMCycleTime is invalid, only the modem on the primary server will be used by the Alarm Notification System, so long as that modem is available.

If set to zero, the least recently used modem of all those available will be preferred.

If set to a numeric value greater than zero, then only the modem on the primary server will be used (while it is available) until one or more of the other modems has been unused for MMCycleTime seconds, after which the least recently used of those modems will be preferred.

Section: System

Default: MMCycleTime = 86400

MMLogDateFormat

Indicates the date format to be used for the elements in the Modem Manager's event log (see "Modem Manager Programming Interface").

If MMLogDateFormat is set to -1, no time is recorded in the list. (The available date format options are described in the Date function.)

Default: MMLogDateFormat =

Section: System

MMLogLevel

The Modem Manager's event log records events at four levels of detail (0..3). Setting this value to non-zero enables the additional information to be viewed.

Section: System

Default: MMLogLevel = 0

MMLogTimeFormat

Indicates the time format for the elements in the Modem Manager's event log (see "Modem Manager Programming Interface"). The default time format is "hh:mm:ss:dd" (4).

If MMLogTimeFormat is set to -1, no time is recorded in the list. (The available time format options are described in the Time function.)

Section: System

Default: MMLogTimeFormat = 4

MMMaxQTime

Enables you to set a time limit (in seconds) on how long a call will be held in the Modem Manager's queue when the Modem Manager determines that no modems are available (e.g. when no server is running for the defined modems, or modems have failed). The default value is the equivalent to approximately 12 years.

Section: System

Default: MMMaxQTime = 0x18000000

MMRPCTimeout

Indicates the number of seconds to wait before failing an attempt to connect to another workstation. Connections that require multiple RPC hops utilize multiples of this timeout value.

Section: System

Default: MMRPCTimeout = 60

MMUnAvailRetry

If a modem cannot be used due to some reason external to VTScada, the modem manager will poll the modem periodically in case the status changes. MMUnAvailRetry can be added to your Settings.Dynamic file to

control how often the modem will be checked. Defaults to 60 seconds if missing or invalid.

Section: System

Default: MMUnAvailRetry = 60

ModemAlarm

If set to 0, this will override the ModemAlarm module, effectively disabling the recording of modem manager events in the alarm history. This may be useful in applications that otherwise generate a large number of modem manager alarm log entries.

Section: System

Default: ModemAlarm =

ModemAutoReset

Indicates the number of minutes to wait before retrying a modem that has been marked as failed.

Section: System

Default: ModemAutoReset = 60

ModemManagerLogSize

Indicates the number of entries to be stored in the Modem Manager's log file. If one intends to log modem manager events then this value should be set to at least 256.

If the variable is not set, then no logging of modem events will occur until the Event Log is first displayed on the screen. The Event Log modem palette tool permits you to view these log entries.

Section: System

Default: ModemManagerLogSize = 1000.

ModemMmaster

Text GUID of the application that is running the Modem Manager (e.g. ModemMmaster = {05ecfb23-7b5d-4238-b5df-8729a8094062}).

There is normally no need to set this. However, it is necessary when implementing Cross-Application working. A typical scenario would be where more than one VTScada application is run on the same machine and each requires access to the common pool of modem(s). In this case, one application would be designated the Master and would control the pool for all applications.

Section: System

Default: ModemMmaster =

<ModemName>Device

Normally, local modem(s) are allocated to any modem devices on the local machine on a first-available basis. This parameter may be set to force a particular relationship by associating a modem tag name with an explicit modem device name. Since modem device names are not always predictable, this parameter may be set for a workstation.

Section: System

Default: <ModemName>Device =

<ModemName>Disabled

If this is defined and has a true value (i.e. a non-zero numeric value) then the modem identified by ModemName is started in Disabled mode.

Section: System

Default: <ModemName>Device =

ModemRetries

Indicates the number of failed connection attempts that do not get to the ringing/busy signal stage before the modem is declared to have failed.

Section: System

Default: ModemRetries = 10

ModemSpeechTO

Defines the interval (in seconds) between playing the wave file identified by \GuardTone (if any).

Section: System

Default: ModemSpeechTO = 3.5

ModemTCPIPPort

The Modem Manager needs to be able to setup socket-based communications between different PCs in order to stream the modem data. This parameter sets the base port number. The Modem Manager will start with this base and will try to open a socket, incrementing the port number until successful.

Note: For historical reasons, the port actually used for the connection is always at least 1 more than the configured setting. (e.g. if ModemTCPIPPort == 50000, the actual port will be at least 50001). This can be relevant when setting up firewalls, etc

Section: System

Default: ModemTCPIPPort = 50000

SiteRetries

Indicates the number of unsuccessful connection attempts to a specific remote phone number before deeming the connection a failure. If SiteRetries successive connection attempts for the same call fail, then that call is abandoned. These call attempts may be tried via a number of different modems.

Section: System

Default: SiteRetries = 10

SquelchDetectDelay

Indicates the number of seconds to wait for the first byte of noise on the modem line after answering an incoming call.

Related Variables: The SquelchIdleTime variable enables you to set the number of seconds to wait for idle time after squelch noise has been detected, while the SquelchPacketLength variable enables you to set the maximum number of bytes of noise to accept before the modem hangs up on an incoming call.

Section: System

Default: SquelchDetectDelay = 0

SquelchIdleTime

Indicates the number of seconds to wait for idle time after squelch noise is detected to decide that real data is to follow. InitialDataDelay starts counting after this time.

Related Variables: The SquelchDetectDelay variable enables you to set a number of seconds the modem should wait for the first byte of noise on the modem line after answering an incoming call, while the SquelchPacketLength variable indicates the maximum number of bytes of noise to accept before the modem hangs up on an incoming call.

Section: System

Default: SquelchIdleTime = 0.25

SquelchPacketLength

Indicates the maximum number of bytes of noise to accept before the modem is hung up after answering an incoming call.

Related Variables: The SquelchDetectDelay variable enables you to set a number of seconds the modem should wait for the first byte of noise on the modem line after answering an incoming call, while the SquelchIdleTime variable indicates the number of seconds to wait for idle time after squelch noise is detected to decide that real data is to follow.

Section: System

Default: SquelchPacketLength = 65536

UseSerialAreaInModemCall

Controls whether modem selection will rely on the Area property configured for Serial Port tags.

If set to 1, UseSerialAreaInModemCall forces calls to a remote RTU site to use only modems with an area property matching that of the serial port tag. The benefit is that a voice modem, used for the Alarm Notification

System and configured without an area property, would not be used for data calls.

If set to 1 and there is no modem with an area matching the serial port, then the call will simply be canceled.

If UseSerialAreaInModemCall is set to "0", the area configured for serial port tags has no bearing on modem calls. (This is the default, for backwards compatibility issues).

Section: System

Default: UseSerialAreaInModemCall = 0

UseUnimodem

Indicates whether or not you want the UniModem V driver to appear in the list of available modem drivers

Trihedral supplies its own modem driver / TAPI Service Provider (TSP). By default, only Trihedral's driver will appear in the available list. If UseUnimodem is set to "1", the older UniModem V driver will also be available for you to select.

Section: System

Default: UseUnimodem = 0

Port Properties

The following variables affect the functioning of I/O ports.

... SerialShareSemaphore

... SerPortDisconnectDelay

... TCPIPPortMaxRcvLen

... TCPIPPortMaxXmtLen

... UseSerialAreaInModemCall

SerialShareSemaphore

The application property, SerialShareSemaphore has been marked as deprecated. In the unusual event that you have multiple devices attempt-

ing to use the same channel at the same time across multiple ports, you might consider adding Comm Link Sequencer Tags to serialize requests.

Related Information:

See: "Comm Link Sequencer Tags" in the VTScada Developer's Guide. Serialize requests for the same communication channel across ports.

Original description follows:

Enables multiple serial ports to share the same semaphore. Doing so prevents more than one driver from using more than one of the serial ports in the group at a time; thereby preventing two drivers on different serial ports connected to different radios sharing the same frequency from colliding.

To allow serial ports to share the same semaphore, set SerialShareSemaphore to "1" (the default is "0"). The result is that all serial ports with the same Area parameter will use the same semaphore.

Section: System

Default: SerialShareSemaphore = 0

SerPortDisconnectDelay

Controls how long the serial port will wait to return to an idle state after a driver releases the port semaphore. The purpose of this feature is to allow multiple drivers to share a Serial Tag in 'serial' mode (vs. modem mode).

There is a backward compatibility issue (prior to version 7.1) in that older port drivers did not have to acquire the port semaphore to cause the port to open. This will most likely affect drivers that operate in a listen mode, as they will now have to acquire the port semaphore to keep the port open.

To address this issue, set SerPortDisconnectDelay to a negative number. This will disable serial port sharing over the entire application, but will allow legacy driver to use the serial ports.

Section: System

Default: SerPortDisconnectDelay = 1

TCPIPPortMaxRcvLen

Indicates the maximum size of the receive buffer for the TCP/IP Port tag type.

Related Variables: The TCPIPPortMaxXmtLen variable enables you to set the size of the transmit buffer for the TCP/IP Port tag type.

Section: System

Default: TCPIPPortMaxRcvLen = 16384

TCPIPPortMaxXmtLen

Indicates the maximum size of the transmit buffer for the TCP/IP Port tag type.

Related Variables: The TCPIPPortMaxRcvLen variable enables you to set the size of the receive buffer for the TCP/IP Port tag type.

Section: System

Default: TCPIPPortMaxXmtLen = 16384

UseSerialAreaInModemCall

Controls whether modem selection will rely on the Area property configured for Serial Port tags.

If set to 1, UseSerialAreaInModemCall forces calls to a remote RTU site to use only modems with an area property matching that of the serial port tag. The benefit is that a voice modem, used for the Alarm Notification System and configured without an area property, would not be used for data calls.

If set to 1 and there is no modem with an area matching the serial port, then the call will simply be canceled.

If UseSerialAreaInModemCall is set to "0", the area configured for serial port tags has no bearing on modem calls. (This is the default, for backwards compatibility issues).

Section: System

Default: UseSerialAreaInModemCall = 0

Mobile Browser Properties

The following list of application variables relate to the mobile browser:

...ContainerTerm

...EnableMobileMaps

...IdleWebSessionTimeout

... MobileBrowserAutoRefreshPeriod

...MobileBrowserSnapshotRefreshPeriod

...MobileBrowserDisablePageGraphics

... MobilePageMaxRenderTime

...MobileSlippyMapTilesSource1

Related Information:

... Internet Server and Client Properties

ContainerTerm

Specifies the word to be used for containers (stations, context tags, sites, etc) that may be browsed into.

Section: System

Default: ContainerTerm = Sites

EnableMobileMaps

Enables the display of slippy maps in the mobile browser interface. Disabled by default.

See also, the Setup.INI property MobileSlippyMapTilesSource1.

Section: System

Default: EnableMobileMaps=

IdleWebSessionTimeout

Sets the length of time, after which an inactive mobile browser client will be logged out and the session terminated, thereby freeing the license key. Measured in minutes.

Note that this property is part of the <SECURITYMANAGER-ADMIN> section, and therefore can be added only by editing your Settings.Dynamic file.

Section: <SECURITYMANAGER-ADMIN>

Default: IdleWebSessionTimeout = 5

MobileBrowserAutoRefreshPeriod

Specifies the Auto-refresh period for mobile browser pages in list-view mode (measured in seconds). Note that the browser connection must be restarted before a change to this setting will go into effect.

Section: System

Default: MobileBrowserAutoRefreshPeriod = 60

MobileBrowserDisablePageGraphics

If set to TRUE (1), this disables page graphics in the mobile browser display, changing the display to a version that minimizes the required bandwidth to the device, as well as the CPU load on the server.

Has no effect on the number of mobile browser client licences.

Section: System

Default: MobileBrowserDisablePageGraphics =

MobileBrowserSnapshotRefreshPeriod

Specifies the Auto-refresh period for mobile browser pages in graphic-view mode (measured in seconds). Note that the browser connection must be restarted before a change to this setting will go into effect.

Section: System

Default: MobileBrowserSnapshotRefreshPeriod = 600

MobilePageMaxRenderTime

Specifies the Maximum time, in seconds, that a page may run before tags are collected from it for the mobile browser view.

Section: System

Default: MobilePageMaxRenderTime = 2

Object Selection Marquee Properties

A marquee appears around an object that has been selected in a group of objects and whose Style dialog is open for modification.

... MarqueeDashColor

... MarqueeSolidColor

... MarqueeSpeed

MarqueeDashColor

Enables you to set the first of two contrasting colors for the dashes of the marquee that appears when a selected object's properties are being displayed. The default color index is 15 (white).

Section: System

Default: MarqueeDashColor = 15

MarqueeSolidColor

Enables you to set the second of two contrasting colors for the dashes of the marquee that appears when a selected object's properties are being displayed. The default color index is 0 (black).

Section: System

Default: MarqueeSolidColor = 0

MarqueeSpeed

Indicates the speed (in fractions of a second) at which the marquee that appears when a selected object's properties are being displayed moves around the object.

Section: System

Default: MarqueeSpeed = 0.1

Operator Logging Properties

Properties related to the logging of operator actions are:

... OperatorLogArea

... OperatorLogging

... OperatorLogName

... OperatorLogTemplate

OperatorLogArea

Enables you to set the area for logged operator control actions so that operator control action entries in the History list can be conveniently sorted.

Section: System

Default: OperatorLogArea = OperatorLog

Related Information:

VTScada Event Logging

See: VTScada Event Logging, in the VTScada Programmer's Guide.

OperatorLogging

Operator logging is a feature in VTScada that logs any value changes made to output tags and their related equipment via tag widgets such as SetValue Button, SetValue Hotbox, Numeric Entry field, and Slider. Data recorded includes the operator's username, the name and description of the tag, the new value, and the workstation from which the change was made. See: Operator Control Action Logging.

The OperatorLogging variable enables you to turn operator control action logging to the Alarms.log file on or off. By default, operator control action logging is turned on (OperatorLogging = 1).

If set to 0 (false), then control actions performed by operators are not logged to Alarms.log, and so cannot be displayed in the History list on the Alarm page.

Section: System

Default: OperatorLogging = 1

Related Information:

See: VTScada Event Logging, in the VTScada Programmer's Guide.

OperatorLogName

Enables you to set the name to be displayed for all logged operator control action events (for example, the setting of a digital output tag via a SetValue button to 1).

Section: System

Default: OperatorLogName = OperatorLog

Related Information:

See: VTScada Event Logging, in the VTScada Programmer's Guide.

OperatorLogTemplate

Default format for operator log entries. This variable affords customers more flexibility in the format of the operator log message that is added to the alarm history when an operator performs a control operation. The default value for OperatorLogTemplate contains a series of elements whose meanings are as follows. Note that these elements are case-sensitive.

^M = machine name (Deprecated. Workstation name will be included in all cases.)

^U = user name (Deprecated. Account name will be included in all cases.)

^T = tag name

^D = quoted tag description

^d = unquoted tag description

^A = tag area

^O = old value

^N = new value

^C = OperatorLogChangedLabel

^F = OperatorLogFromLabel (if valid old value)

^I = OperatorLogToLabel (if valid new value)

The order of the above elements may be modified according to the user's needs.

Section: System

Default: OperatorLogTemplate = OperatorLogTemplate = ^C ^F ^O ^I ^N

Related Information:

See: VTScada Event Logging, in the VTScada Programmer's Guide.

Page Properties

The following list of variables pertain to application pages.

- ... AnalogInputWidth
- ... DefaultPage
- ...DefaultPageColor
- ... DefaultBGColor
- ... DigitalInputWidth
- ... DisableUSDialog
- ... DOWidth
- ... IODrawGap
- ... IODrawHeight
- ... MaxWinPage
- ... OpaqueBackground
- ... Page
- ... PageButtonToolTipBalloonStyle
- ... PageButtonToolTipDelay
- ... PageButtonToolTipEnable
- ... PageButtonToolTipFont
- ... PageToolTipLabel
- ...PopupCloseOnPageClose
- ...PopupLimitAction
- ...PopupPageLimit
- ... ProgSpawnTitle
- ... StretchBackground
- ... TPPath

... UseOldSiteDialog

AnalogInputWidth

Indicates the width (in pixels) of the analog input column (the analog status/pulse input column (i.e. first column from the left)) for station pages.

Please refer to IODrawHeight and IODrawGap variables to set the height and width of the I/O buttons on station pages.

Section: System

Default: AnalogInputWidth = 200

DefaultPage

Indicates the page file name that the Display Manager should open if the current page being viewed is deleted. For example, if DefaultPage is set to Page5, you are viewing Page2, and you delete it, Page5 will open.

Section: System

Default: DefaultPage =

DefaultPageColor

Indicates the background color for new pages. By default, the page background color to be displayed is white (15). For valid color values, please refer to "VTScada Color Palette" in the VTScada Programmer's Guide.

Default DefaultPageColor = 15

DialogBGColor

Indicates the background color for dialogs. By default, the background dialog color is obtained from the system using the GetSystemColor(15) function.

Section: System

Default: DialogBGColor =

DigitalInputWidth

Indicates the width (in pixels) of the digital input column (the digital status/pump status column (i.e. second column from the left)) for station pages.

Please refer to the `IODrawHeight` and `IODrawGap` variables to set the height and width of the I/O buttons that appear on station pages.

Section: System

Default: `DigitalInputWidth = 200`

DisableUSDialog

When set to true (1) disables the dialog that prompts for parameter values when opening an under-specified parametrized page.

Section: System

Default: `DisableUSDialog = 0`

DOWidth

Indicates the width (in pixels) of the digital output column (the digital control column (i.e. the last two columns from the left)) for station pages.

Please refer to `IODrawHeight` and `IODrawGap` variables to set the height and width of the I/O buttons on station pages.

Section: System

Default: `DOWidth = 150`

IODrawGap

Indicates the space (in pixels) between each I/O tag's button, displayed on the station pages in your system.

Please refer to `AnalogInputWidth`, `DigitalInputWidth`, and `DOWidth` variables to set the width of the I/O buttons on the station pages.

Section: System

Default: `IODrawGap = 2`

IODrawHeight

Indicates the height (in pixels) of each I/O tag's button displayed on the station pages in your system.

Please refer to AnalogInputWidth, DigitalInputWidth, and DOWidth variables to set the width of the I/O buttons on the station pages.

Section: System

Default: IODrawHeight = 24

MaxWinPage

Indicates the maximum number of instances of windowed pages that can be opened at one time for any given page.

This variable does not apply to the Trends page or the Alarm page. Only one instance of these pages can be open at one time.

Section: System

Default: MaxWinPage = 1

OpaqueBackground

Indicates the state of the opacity of background images (such as maps). If set to 0 (false), then the background images are drawn onto the background as transparent backgrounds (default).

If set to 1 (true), then background images are to be destructively drawn onto the background (opaque).

It is recommended that you set OpaqueBackground to 1 (true) for faster draw times.

Section: System

Default: OpaqueBackground = 0

Page

Tells VTScada which page to open in the Display Manager when the application starts.

If set to invalid, the Display Manager will show the last page that was viewed before the application was stopped.

Section: System

Default: Page = **PageMenuPage**¹

PageButtonToolTipBalloonStyle

Gives the option of having larger, balloon style tool tips that can display large amounts of text.

When set to 0, displays normal tool tip. When set to 1, displays a balloon tool tip.

Section: System

Default: PageButtonToolTipBalloonStyle = 0

PageButtonToolTipDelay

Specifies a time delay in seconds before the tool tip is initially displayed. Re-show and time on screen delays are left as default. The value set here will apply to all tooltips in a window. If set to 0 then only the standard delay used with VTScada tool tips will be in effect.

Section: System

Default: PageButtonToolTipDelay = 2

PageButtonToolTipEnable

Controls display of tool tip on page buttons in the task bar according to the following table of values:

Value	Description
0	Does not display tooltips over page buttons
1	Displays the page title only, but not as a tool tip, thereby being consistent with other VTScada tooltips on the taskbar.
2	Displays the page description or the PageToolTipLabel specific to the page.

¹A page module that will show all the pages in the menu as a series of tiles. Each tile is a live view of the matching page and can be clicked to open that page.

- 3 Displays both the page title and PageToolTipLabel value in the tool tip, with the page title showing in bold. If no value has been provided for the PageToolTipLabel, then an empty gap will be present after the page title.

Section: System

Default: PageButtonToolTipEnable = 3 (page title and tool tip)

PageButtonToolTipFont

This provides a way to select the font that the tool tip is to be displayed in. Most Windows fonts are available for use. If not specified then the default system font will be used. The height will be set to 8pts unless specified in WinToolTipCtrl.

Section: System

Default: PageButtonToolTipFont =

PageSnapshotCacheThresholdCount

Controls whether the tiled page menu shows a live image of each page, based on a count of tiles displayed.

When the number of tiles exceeds this count, a cached view will be shown for each tile instead of a live view.

Default: PageSnapshotCacheThresholdCount = 12

Section: System

Related Information:

PageSnapshotCacheThresholdCount

PageSnapshotCacheThresholdPct

PageSnapshotsMaxInMemory

PageSnapshotCacheThresholdPct

Controls whether the tiled page menu shows a live image of each page, based on a comparison of the width of each tile to the overall width of the VTScada window.

When the width of any tile is less than this percentage of the overall window, a cached view will be shown for each tile instead of a live view.

Default: PageSnapshotCacheThresholdPct = 0.20

Section: System

Related Information:

PageSnapshotCacheThresholdCount

PageSnapshotsMaxInMemory

PageSnapshotsMaxInMemory

Limits the number of images retained for use by the tiled menu page when displaying a cached view of pages rather than a live view. Images are retained in memory, therefore it is important to consider the effect on your system resources before increasing this value.

Default: PageSnapshotsMaxInMemory = 10

Section: System

Related Information:

PageSnapshotCacheThresholdCount

PageSnapshotCacheThresholdPct

PageToolTipLabel

A long description of a page may be stored in this variable. The text will be displayed in a tool tip, visible when the pointer is held over the page name, displayed in the task bar. PageButtonToolTipBalloonStyle should be set to 1 to provide space for long descriptions and PageButtonToolTipEnable should be set to 2 or 3 to enable the display of the text.

The value may be set either online via the PageManager Properties dialog, or offline via the page source.

Section: System

Default: PageToolTipLabel =

PopupCloseOnPageClose

Causes all pop-up pages to close instantly and automatically when the page in the main display changes. The one exception to this rule is that

moving from one folder to another in the tiled page menu will not cause pop-up pages to close.

If zero, (the default) then pop-up pages will remain open while an operator changes the pages in the main display.

Default: `PopupCloseOnPageClose = 0`

Section: System

Related Information:

PopupPageLimit

PopupLimitAction

PopupLimitAction

Controls what will happen when the operator attempts to open more pages than allowed by the property, `PopupPageLimit`. The following options are possible:

PopupLimitAction	Action to take
Not set / 0	Allow all pop-up pages to open.
1	Warn, but allow the page to open if the operator chooses. (default)
2	Prevent the page opening, and display an error message.
3	Close the oldest pop-up page before proceeding to open the requested page.
4	Close the newest pop-up page before proceeding to open the requested page.

Default: `PopupLimitAction = 1` (Warn, but allow on confirmation)

Section: System

Related Information:

PopupPageLimit

PopupCloseOnPageClose

PopupPageLimit

Sets the maximum number of pop-up pages that can be open at any time. Trend pop-ups, launched by clicking on a tag do not count towards this total.

May be any positive number from zero up. Defaults to eight.

Negative numbers are treated as zero. Decimal values are rounded down to the nearest integer.

Default: `PopupPageLimit = 8`

Section: System

Related Information:

`PopupLimitAction`

`PopupCloseOnPageClose`

ProgSpawnTitle

Indicates the label to be displayed in the title bar (and under the button in the site tools palette) for the program spawn drawing object belonging to the site tools palette.

Section: System

Default: `ProgSpawnTitle = Program Spawn`

StretchBackground

Indicates whether or not background images should be stretched to fit the pages on which they appear.

If set to 1 (true), then background images are stretched to fit the pages on which they appear.

Section: System

Default: `StretchBackground = 0`

TPPath

Indicates the path for background images for pages.

If `TPPath` is set to invalid (as it is by default), then the path for background images defaults to the Backgrounds directory within the applic-

ation directory's Bitmaps directory (i.e. \Ap-
plicationDirectory\Bitmaps\Backgrounds)..

Section: System

Default: TPPath = Invalid

UseOldSiteDialog

When set to 1 (true) the older VTScada station page will be shown when an operator clicks on a Site Draw widget that is associated with a Polling Driver or DataFlow RTU tag.

Must be added to Settings.Dynamic – no default entry is provided.

Section: System

Default: (none)

Report Generation Properties

The following list of variables pertain to report generation.

...AnalogSummaryReportTimeUnits

... DefaultEmailSubject

... EmailServer

... EmailSubject

... ReportBrowseDir

... ReportDateFormat

... ReportOutputDir

... ReportTempDir

... ReportTemplateDir

... ReportTimeZoneAware

... ReportXPos

... ReportXSize

... ReportYPos

... ReportYSize

... ScreenReportsInExcel

... StartOfWeek

AnalogSummaryReportTimeUnits

Sets the time unit to be used when summarizing flow data. If flow is measured in units per second, set this value to 1. If flow is measured in units per minute, set this value to 60.

Section: System

Default: AnalogSummaryReportTimeUnits = 60

DefaultEmailSubject

Sets the default text to be placed in the subject line of an emailed report if a subject is not defined by the user.

Section: System

Default: DefaultEmailSubject = Trihedral VTScada System

EmailServer

Deprecated. If present in an application that is ported to 10.1 or later, the value will be transferred to the new storage format. Subsequent changes to this property will be ignored.

Indicates the name or IP address of the email server for emailed reports (e.g. mail.trihedral.com).

Section: System

Default: EmailServer =

EmailSubject

Indicates the text to be entered in the subject line of emails sent to designated operators by the VTScada Report System.

Section: System

Default: EmailSubject = The VTScada System:

ReportBrowseDir

Indicates the default directory in which to start browsing when selecting a destination for report output files.

Section: System

Default: ReportBrowseDir =

ReportDateFormat

Sets the date format to be used in reports and report names. For report filenames, the slash character (/), will be replaced by a dash (-).

Section: System

Default: ReportDateFormat = 30(YYYY-MM-DD)

Related Information:

See: predefined Date Codes, in the VTScada Programmer's Guide.

ReportOutputDir

Indicates the default directory in which to store automatically generated reports.

Section: System

Default: ReportOutputDir =

ReportTempDir

Indicates the default directory to use for temporary file storage during report generation.

Section: System

Default: ReportTempDir =

ReportTemplateDir

Indicates the default directory to use to browse for Excel screen report templates.

Section: System

Default: ReportTemplateDir =

ReportTimeZoneAware

Makes the report page time zone aware. If an operator, located in another time zone, connects to the application via a VTScada Internet Client and runs a report, this variable controls whether that report will be

displayed using the time zone of the operator (ReportTimeZoneAware = 1) or of the server (ReportTimeZoneAware = 0)

Reports must be configured to use this variable in their calls to GetLog

Section: System

Default: ReportTimeZoneAware = 1

ReportXPos

Obsolete

Indicates the horizontal position (number of pixels from the upper left corner) or the on-screen window that displays report data when Screen Display is selected as the output format.

This variable only applies if Microsoft Excel is not configured to display data when Screen Display is selected, or is not installed on the PC in question.

Section: System

Default: ReportXPos = 10

Related Information:

ScreenReportsInExcel

ReportXSize

Obsolete

Indicates the width of the on-screen window that displays report data when Screen Display is selected as the output format.

This variable only applies if Microsoft Excel is not configured to display data when Screen Display is selected, or is not installed on the PC in question.

Section: System

Default: ReportXSize = 900

Related Information:

ScreenReportsInExcel

ReportYPos

Obsolete

Indicates the vertical position (number of pixels from the upper left corner) of the on-screen window that displays report data when Screen display is selected as the output format.

This variable only applies if Microsoft Excel is not configured to display data when Screen Display is selected, or is not installed on the PC in question.

Section: System

Default: ReportYPos = 10

Related Information:

ScreenReportsInExcel

ReportYSize

Obsolete

Indicates the height of the on-screen window that displays report data when Screen Display is selected as the output format.

This variable only applies if Microsoft Excel is not configured to display data when Screen Display is selected, or is not installed on the PC in question.

Section: System

Default: ReportYSize = 800

Related Information:

ScreenReportsInExcel

ScreenReportsInExcel

Indicates whether VTScada reports whose chosen output format is "Screen Display" should be displayed in a window, or in a Microsoft Excel spreadsheet.

If set to 0 (false), then the report data is displayed in a window.

If set to 1 (true), then the report data is displayed in a Microsoft Excel spreadsheet.

This variable is maintained for backwards compatibility only. VTS version 6.6 and later use a "Use Excel to display report" check box that can be selected to display a screen report using Excel.

Section: System

Default: ScreenReportsInExcel = 1

StartOfWeek

Enables you to specify the starting day of the week for previous week report generation (i.e. when "Previous Week" is the selected time period for a report).

The available options are:

1 Monday (default), 2 Tuesday, 3 Wednesday, 4 Thursday, 5 Friday, 6 Saturday, 7 Sunday

Section: System

Default: StartOfWeek = 1

Application Settings for RPC

The following list of variables pertain to remote procedure calls and the RPC Manager.

Related Information:

...ABSharedRPC

... CIPENIPSharedRPC

... DataradioSharedRPC

... DDESharedRPC

... DNP3SharedRPC

... DriverSetupDelay

... MDSSharedRPC

... ModiconPortSharedRPC

... ModiconSharedRPC

... OmronSharedRPC

... OPCClientSharedRPC

... RemCfgTransLog
... SiemensS7PortSharedRPC
... SiemensS7SharedRPC

ABSharedRPC

Indicates whether the same RPC service should be used for all instances of the Allen–Bradley tag type.

If set to 1 (true), then the same RPC service will be used for all instances of the Allen–Bradley tag type.

Default: ABSharedRPC = 0

Section: System

CIPENIPSharedRPC

Indicates whether or not the same RPC service will be used for all instances of the CIPENIP driver.

If set to 1 (true), the same RPC service is used for all instances of CIPENIP.

Section: System

Default: CIPENIPSharedRPC = 0

DataradioSharedRPC

Indicates whether or not the same RPC service will be used for all instances of Dataradio.

If set to 0 (false), the same RPC is NOT be used for all instances of Dataradio (default).

Section: System

Default: DataradioSharedRPC = 0

DDESharedRPC

Indicates whether or not the same RPC service will be used for all instances of DDE.

If set to 0 (false), the same RPC is NOT be used for all instances of DDE (default).

Section: System

Default: DDESharedRPC = 0

DNP3SharedRPC

Indicates whether or not the same RPC service will be used for all instances of DNP3.

If set to 0 (false), the same RPC is NOT be used for all instances of DNP3 (default).

Section: System

Default: DNP3SharedRPC = 0

DriverSetupDelay

Indicates the number of seconds a VTScada driver waits before trying to resend data once an attempt has failed.

Section: System

Default: DriverSetupDelay = 60

MDSSharedRPC

Indicates whether or not the same RPC service will be used for all instances of MDS.

If set to 1 (true), the same RPC service is used for all instances of MDS.

Section: System

Default: MDSSharedRPC = 0

ModiconPortSharedRPC

Controls whether or not the same RPC service should be used for all instances of the Modbus Plus tag type that are connected to the same serial port or TCP/IP connection.

ModiconPortSharedRPC enables Modbus devices that share the same serial port or TCP/IP connection to be grouped with the same device, enabling Modbus I/O that uses different radio channels to be polled from separate PCs.

If set to 0 (false), then the same RPC service is not used for all instances of the Modicon tag type that are connected to the same serial port or TCP/IP connection (default).

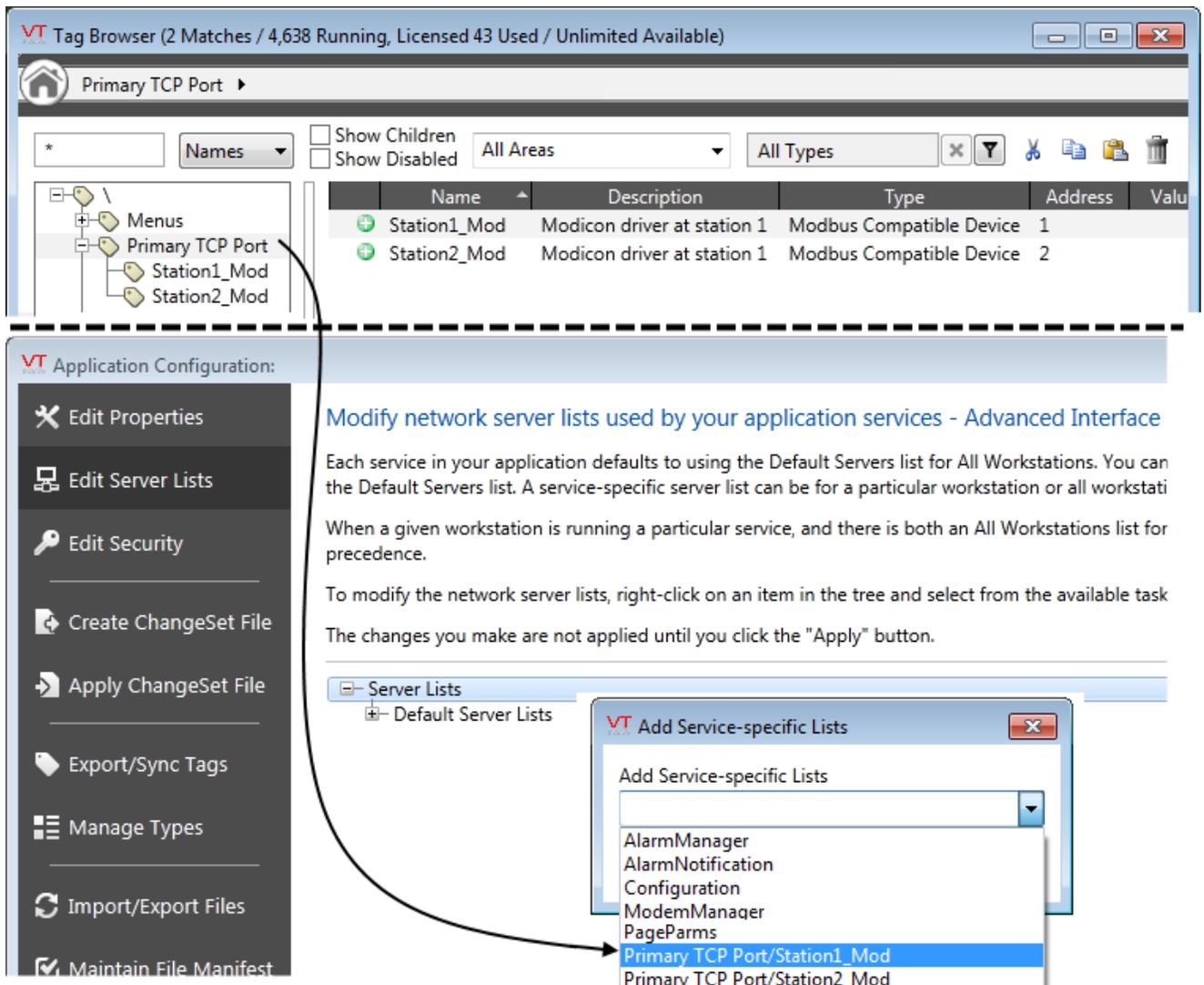
Section: System

Default: ModiconPortSharedRPC = 0

Related Variables: the behavior of the [ModiconSharedRPC](#) will be overridden when this property is equal to 1 (true).

Note for multi-server applications using advanced server lists: If ModiconPortSharedRPC is set to 1, each Modbus-compatible driver service will be renamed to a combination of "ModiconServer" followed by the port name.

For example, if the Modbus Plus tags are attached to a driver named "PrimaryTCPPort" in an application where ModiconPortSharedRPC has been set to 1, then the driver service will be named "Modicon-ServerPrimaryTCPPort".



ModiconSharedRPC

Controls whether or not the same RPC service should be used for all instances of the Modicon tag type.

If your networked application uses a polling driver, then it is recommended that this variable be set to 1.

If set to 0 (false), then the same RPC service is not used for all instances of the Modicon tag type (default).

Section: System

Default: ModiconSharedRPC = 0

Related Variables: This property will be overridden when [Modicon-PortSharedRPC](#) property is set TRUE (1).

OmronSharedRPC

Indicates whether or not the same RPC service should be used for all instances of the Omron tag type.

If set to 0 (false), then the same RPC service is not used for all instances of the Omron tag type (default).

Section: System

Default: OmronSharedRPC = 0

OPCClientSharedRPC

Indicates whether or not the same RPC service should be used for all instances of the OPC Client Driver tag type.

If set to 0 (false), then the same RPC service is not used for all instances of the OPC Client Driver tag type (default).

Section: System

Default: OPCClientSharedRPC = 0

RemCfgTransLog

Indicates whether or not configuration database transactions should be logged.

If set to 0 (false), then remote configuration database transactions are not logged.

Section: System

Default: RemCfgTransLog = 0

SiemensS7PortSharedRPC

Indicates whether or not the same RPC service will be used for all instances of the SiemensS7 tag type connected to a common TCP/IP/Serial port. If set to 0 (false), the same RPC is not used for all instances of SiemensS7Port (default).

If set to 1 (true), the same RPC service is used for all instances of SiemensS7Port.

Section: System

Default: SiemensS7PortSharedRPC = 0

SiemensS7SharedRPC

Indicates whether or not the same RPC service will be used for all instances of the SiemensS7 driver.

If set to 1 (true), the same RPC service is used for all instances of Siemens.

Section: System

Default: SiemensS7SharedRPC = 0

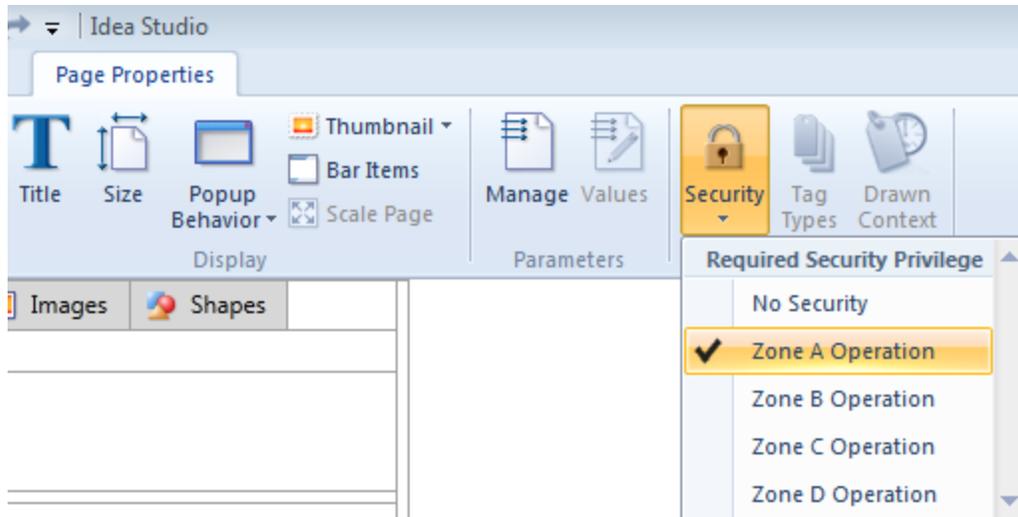
Security-Related Settings

Certain configuration settings related to security are stored in the file, Settings.Dynamic. Many of these variables can be changed only by directly editing this file in your application's root directory, and then importing the edited file using the Application Configuration dialog. Only authorized accounts may import a file that has been edited.

All application privileges that you create in an application are named according to the pattern PrivDescN where N is a number starting at 0. For example, if you have added 4 custom application privileges to your application, they would appear as follows:

```
<SECURITYMANAGER-PRIVAPP>
PrivBitsTotal = 4
PrivDesc0 = Zone A Operation,0
PrivDesc1 = Zone B Operation,1
PrivDesc2 = Zone C Operation,2
PrivDesc3 = Zone D Operation,3
```

The label is used for display purposes, including the selection drop-down in each output tag's Merit tab and the security property of each page.



The number following the property sets its value, which is to be used in code. Note that this value is an offset from 16. Referring to the preceding example, where the page has been protected with the application privilege "Zone A Operation", the first few lines of the source code of that page will look like the following:

```
[
  Title = "Overview";
  Color = "<FFFFFFF>";
  SecBit = 16;
]
```

PrivDes0, having number 0 in the list above, means that its actual value to be used in code is $16 + 0 = 16$.

Note: For the following list, take careful note of each property's section. Three distinct sections are used for security-related properties. A property will be ignored if it is associated with the wrong section.

... AccountLockoutTime
 ...AccountRateWindow
 ...ADGroupPrefix
 ...ADRefreshPeriod
 ...AutoAddADUsers
 ... AutoLogOff

- ... AutoLogOffMax
- ... AutoLogOffMin
- ...ForcePasswordAltIdSync
- ... GroupLogin
- ...IdleWebSessionTimeout
- ... MaxFailedLoginAttempts
- ...MaxRateFailedLoginAttempts
- ... NamespaceDelimiter
- ... OEMEncryptKey
- ... PasswordDisplay
- ... PasswordMinLen
- ... PasswordTimeLimit
- ... PasswordWarningTime
- ...pcProxBaudRate
- ...pcProxConnectCheckTO
- ...pcProxDatabits
- ...Security-Related Settings
- ...pcProxExcludePortx
- ...pcProxParity
- ...pcProxPortNum
- ...PcProxPortScanHigh
- ...pcProxPortScanLow
- ...pcProxStopBits
- ... PrivBitsTotal
- ... PrivDescX
- ... PromptForBadAltID
- ... ReadOnlyStation
- ...RootNamespace

- ... SecurityAlarmArea
- ... SharedContexts
- ... SharedSecurity
- ... SysPrivDefault
- ... SysPrivSuppress
- ... UserName

AccountLockoutTime

Indicates the minutes (or fractions of a minute) for which the user will be locked out after supplying an incorrect password MaxFailedLoginAttempts times, or MaxRateFailedLoginAttempts within the AccountRateWindow time frame.

Section: SecurityManager-Admin

Default: AccountLockoutTime = 1

Application restart required before changes will take effect.

Related Information:

- ...AccountRateWindow
- ... MaxFailedLoginAttempts
- ...MaxRateFailedLoginAttempts

AccountRateWindow

The window of time, measured in seconds, used to distinguish between logon attempts made by a person and those made by an automated attack.

If the number of consecutive unsuccessful logon attempts set by MaxRateFailedLoginAttempts are made within this time period, the account is locked.

If there are MaxFailedLoginAttempts consecutive failed attempts within any time frame, the account will be locked.

Section: SecurityManager-Admin

Default: AccountRateWindow = 15

Application restart required before changes will take effect.

Related Information:

AccountLockoutTime

MaxFailedLoginAttempts

MaxRateFailedLoginAttempts

ADGroupPrefix

The prefix to be added to a VTScada role name for the equivalent Active Directory Security Group.

Default: ADGroupPrefix = VTScada-

Section: <SecurityManager-Admin>

ADRefreshPeriod

The interval in seconds between checks for changes to the accounts in the Active Directory for the logged-on users.

Default: ADRefreshPeriod = 900

Section: <SecurityManager-Admin>

AutoAddADUsers

Controls whether authorized Windows accounts are automatically added to the VTScada Security Manager upon initial successful logon.

Must be added to the application's Settings.Dynamic file.

Default: FALSE

Section: <SecurityManager-Admin>

AutoLogOff

Indicates the minutes (or fractions of a minute) of inactivity after which the logged on user is logged off.

Section: SecurityManager-Admin

Default: AutoLogOff = 15

AutoLogOffMax

Indicates the highest amount of time that can be selected for the AutoLogoff variable.

This variable represents the maximum value that can be selected from the Minutes of Inactivity spinbox in the Administrative Settings Security Manager dialog.

Section: SecurityManager-Admin

Default: AutoLogOffMax = 720

AutoLogOffMin

Indicates the lowest amount of time that can be selected for the AutoLogoff variable.

This variable represents the minimum value that can be selected from the Minutes of Inactivity spinbox in the Administrative Settings Security Manager dialog.

Section: SecurityManager-Admin

Default = 0

ForcePasswordAltIdSync

By default, SecurityManager keeps encrypted passwords and alternate ids in sync during user update, but only if they were in sync to begin with. If this variable is 1, it will always keep them in sync.

If you intend to use an alternate ID for purposes other than for alarm dialler support, this value should be set to FALSE. See also: AlphaNumericXFormScheme

Section: SecurityManager-Admin

Default: Set to 1 in all new applications by the application template.

GroupLogin

Enables the group name field in the Please Logon dialog that is launched when the Logon button in the Display Manager's title bar is clicked.

Accounts that have been assigned a group name will be able to enter it in that field.

The `NameSpaceDelimiter` property is also part of security group configuration, and must be specified before you can assign group names to accounts.

Section: `System`⁽¹⁾

Default = 0

⁽¹⁾In legacy applications, this property was defined in the `<SecurityManager-Admin>` section. It will work in either section, but the `System` definition takes precedence.

Related Information:

... `NameSpaceDelimiter`

MaxFailedLoginAttempts

Sets the number of times in a row that a user may attempt to log on with an incorrect password before being locked out of the system for `AccountLockoutTime` minutes. Defaults to twenty-five (25) consecutive attempts will result in the account being locked.

Note: Attempts made within a user-defined time span are subject to a lower threshold before lockout. See related information.

Section: `SecurityManager-Admin`

Default: `MaxFailedLoginAttempts` = 25

Application restart required before changes will take effect.

Related Information:

... `AccountLockoutTime`

...`AccountRateWindow`

...`MaxRateFailedLoginAttempts`

MaxRateFailedLoginAttempts

Sets the number of times in a row that a user may attempt to log on with an incorrect password, and within the time span defined by `AccountRateWindow`, before being locked out of the system for `AccountLockoutTime` minutes. This value is lower than `MaxFailedLoginAttempts`

on the assumption that an automated attack will make repeated attempts much faster than would a person.

Defaults to three (3)

Section: SecurityManager-Admin

Default: MaxRateFailedLoginAttempts = 3

Application restart required before changes will take effect.

Related Information:

...AccountRateWindow

... AccountLockoutTime

... MaxFailedLoginAttempts

NamespaceDelimiter

Required in order to specify the characters that will be used to separate security groups from account names. If NamespaceDelimiter has a valid value, then group security accounts are enabled for your application (see "Security Namespaces").

Security groups enable the subdivision of the user base into "super users" and "group users,". The primary application is for realm-area filtering.

The GroupLogin property is also part of security group configuration, and must be enabled before users will be able to enter a group name while logging on.

Section: System⁽¹⁾

Default =

⁽¹⁾In legacy applications, this property was defined in the <SecurityManager-Admin> section. It will work in either section, but the System definition takes precedence.

Related Information:

... GroupLogin

NoteAddRequiresAuthentication

When set, a logon prompt will be displayed whenever an attempt is made to save a note, requiring the author to prove that he or she is authorized to create notes. The note will be attributed to account used to log on, even though another account is the logged-on user.

Logging-on to save a note does not change the logged-on user account.

This challenge is used only for saving the note.

It is expected that security will be enabled and operator accounts created before notes are added. The challenge resulting from NoteAddRequiresAuthentication will be displayed regardless of whether you have actually enabled security.

Default: NoteAddRequiresAuthentication = 0

Section: System

OEMEncryptKey

Enables you to enter an encryption key for this application.

If left invalid (as it is by default), then no encryption key is required.

Section: SecurityManager-Admin

Default: OEMEncryptKey =

PasswordDisplay

Indicates the display that users view when entering their passwords in the Please Log on dialog (that appears when the Logon button is clicked) to help protect password entries from detection.

This variable can be set to one of three values:

Value	Description
0	Displays the characters in the password as they are entered by the user.
1	Displays asterisks equal to the password length as the characters are entered by the user (default).
2	Displays a number of asterisks that vary in length as the password is entered by the user.

Section: SecurityManager-Admin

Default: PasswordDisplay = 1

PasswordMinLen

Indicates the minimum number of characters that can appear in any user's password.

Section: SecurityManager-Admin

Default: PasswordMinLen = 1

PasswordTimeLimit

If the application is configured for automatic expiration of passwords, this variable stores the number of days that passwords will be valid for. For each user, the time of their last password reset is stored within SecMgr.DAT.

Section: SecurityManager-Admin

PasswordWarningTime

This variable stores the number of days prior to password expiration during which the user will be warned upon logon.

This feature applies only if the application is configured for automatic expiration of passwords, and also to provide a warning prior to password expiration.

Section: SecurityManager-Admin

pcProxBaudRate

The default baud rate for communication with the proximity card reader connection.

Default: pcProxBaudRate = 9600

Section: System

pcProxConnectCheckTO

Period at which the connection to the proximity card reader should be re-checked. Disabled when set to zero (the default).

Default: pcProxConnectCheckTO = 0

Section: System

pcProxDataBits

The default data bit setting for communication with the proximity card reader connection.

Default: pcProxDataBits = 8

Section: System

pcProxEnable

Controls whether ports will be scanned for a proximity card reader.

Defaults to off (0). Scanning will begin from the last port used.

Default: pcProxEnable = 0

Section: System

Related Information:

pcProxExcludePortx

pcProxPortNum

PcProxPortScanHigh

pcProxPortScanLow

pcProxExcludePortx

If it is known that devices other than a proximity card are on various ports, you should exclude those port numbers.

"x" should be replaced by the port to be excluded from scanning, and the value of the property should then be set to 1 to exclude that port.

For example, if an auxiliary input device is installed on port 3, you would set:

pcProxExcludePort3 = 1

Ports that are associated with modems are automatically excluded from scanning.

Default: no defaults.

Section: System

All port numbers from pcProxPortScanLow to PcProxPortScanHigh will be scanned, excepting those associated with modems, if pcProxEnable is set to true.

Related Information:

pcProxExcludePortx
pcProxPortNum
PcProxPortScanHigh
pcProxPortScanLow

pcProxParity

The default parity bit setting for communication with the proximity card reader connection.

Default: pcProxParity = 0

Section: System

pcProxPortNum

Set this value if you know the port number to which the proximity card reader will be attached. Not set by default.

Use with caution: the port number may change if the USB device is unplugged temporarily. In general, it is better to allow VTScada to search for the device.

Default: pcProxPortNum =

Section: System

Related Information:

pcProxPortNum
pcProxExcludePortx
PcProxPortScanHigh
pcProxPortScanLow

PcProxPortScanHigh

Specifies the highest port number to scan for a proximity card reader.

Defaults to 16.

Default: PcProxPortScanHigh = 16

Section: System

Related Information:

PcProxPortScanHigh

pcProxExcludePortx

pcProxPortNum

pcProxPortScanLow

pcProxPortScanLow

Specifies the lowest port number to scan for a proximity card reader.

Defaults to 3.

Default: pcProxPortScanLow = 3

Section: System

Related Information:

pcProxPortScanLow

pcProxExcludePortx

pcProxPortNum

PcProxPortScanHigh

pcProxStopBits

The default stop bit setting for communication with the proximity card reader connection.

Default: pcProxStopBits = 1

Section: System

PrivBitsTotal

Indicates the total number of application privileges that have been configured for this application.

PrivBitsTotal should not be set to invalid, or errors will occur in your application. If there are no application privileges for your application, you should set PrivBitsTotal to 0, as it is by default.

Each time you add a new application privilege using the PrivDescX variables (that is PrivDesc0 through to PrivDesc239), you must remember to increment PrivBitsTotal by 1. For example, if you've specified 5 application privileges using the PrivDesc0 through to PrivDesc4 variables, then you should set PrivBitsTotal to 5. It should be noted that this process is only necessary if you are manually adding application privileges. If you use the Administrative Settings dialog to add application privileges, VTScada automatically updates the PrivBitsTotal and PrivDescX variables.

Section: SecurityManager-PrivApp

Default: PrivBitsTotal = 0

PrivDescX

Where "X" is the number of the privilege starting at 0. Each PrivDescX variable is set equal to the name of the privilege.

If no application privileges have been added to your application, the PrivDescX variables are invalid.

Related Variables: The PrivBitsTotal variable represents a running total of the application privileges you have configured. PrivBitsTotal must always have a value matching the number of PrivDescX variables present for your application.

Section: SecurityManager-PrivApp

Default = Invalid

Note that when referred to by code, application privilege numbers are offset by 16. 0 -> 16, 1 -> 17, etc.

Example:

```
<SECURITYMANAGER-PrivApp>
PrivBitsTotal = 2
AppPrivDefault =
PrivDesc0 = Station 1 Access,0
PrivDesc1 = Station 2 Access,1
```

PromptForBadAltID

Indicates whether or not users should be prompted if validation of their alternate ID fails during user management. The purpose is to avoid passwords that will be the same on touchtone keypads.

If set to 1 (default), prompt user if validation of their alternate ID fails during user management. Duplicate passwords are disallowed.

If set to 0, do not prompt user if validation of their alternate ID fails during user management. Duplicate passwords are allowed

Section: SecurityManager-Admin

Default: PromptForBadAltID = 1

ReadOnlyStation

When set to true (1), tag write operations on the named workstation will be prevented.

Intended for use with named workstations, therefore this property should be added to a Workstation.Dynamic file rather than Settings.Dynamic.

Section: System

Default: ReadOnlyStation = 0

RootNamespace

If your applications makes use of realm-area filtering and if you allow remote access to the VTScada Internet Server (VIC or MIC) then you must define a realm for super-user access and declare it in the RootNamespace property. Accounts that are not part of any security group (super-users) will not have access to any realm otherwise.

Default: RootNamespace =

Section: System

SharedContexts

Matches the field "Enable Shared User Logins" of the security manager's Administrative Options dialog. When set, a user need only log in once on

a workstation for all application contexts that share a security database. This applies to applications that share security with an OEM layer and to the separate contexts of the application and its control buttons in the VAM.

Section: SecurityManager-Admin

Default: SharedContexts = 1

SharedSecurity

Matches the field, "Enable Shared Security" of the security manager's Administrative Options dialog. Enables shared security if set to 1 in an OEM layer.

Section: SecurityManager-Admin

Default: SharedSecurity = 0

SysPrivDefault

Indicates the default system privileges available to those users who are not logged on to the application. The defined system privileges will also be granted to newly-created user accounts by default.

Related Privileges: AppPrivDefault

You may also define default application-specific privileges to those users who are not logged on to the application. The defined application privileges will also be granted to newly-created user accounts by default.

Section: SecurityManager-Admin

Default: SysPrivDefault =

SysPrivSuppress

Indicates whether system privileges have been suppressed or revealed. Each digit following the SysPrivSuppress variable represents a system privilege, each of which can be turned on or off using a "0", a "1", or a "2" respectively. Digits have meaning according to their placement counting from the right. Leading zeros are not required. If set to "0", the associated system privilege is revealed.

If set to "1", the associated system privilege is suppressed in all security dialogs, except the Administrative Settings dialog.

If set to "2", the associated system privilege is suppressed in all security dialogs, including the Administrative Settings dialog.

By default, all system privileges are revealed in all security dialogs. A table showing the index of each system privilege in the SysPrivSuppress variable can be found in: Suppress and Reveal System Privileges Using the SysPrivSuppress Variable.

Section: SecurityManager-Admin

Default: SysPrivSuppress = 000000000000000000000000000000000000

UserName

Indicates the registered username of the logged on user. If no user is logged on to the application, UserName will be invalid.

Section: n/a

Default = Invalid

Snap Grid Properties

The following list of variables pertain to the snap grid. Most are no longer used as of version 11.

... GridColor

... GridDense

... GridShiftX

... GridShiftY

... GridVis

... SnapOn

... XGrid

... YGrid

GridColor

Obsolete

Indicated the initial color of the Snap Grid in older versions of VTS.

Section: System

Default: GridColor = 11

GridDense

No longer used.

Indicated the initial density of the snap grid (i.e. the ratio of visible points to actual snap points).

The Every X Points field of the Grid Options dialog can also be used to temporarily set GridDense while the application is running.

Section: System

Default: GridDense = 1

GridShiftX

No longer used.

Indicates the number of pixels along the X-axis (horizontal) by which to offset the snap grid origin (i.e. the number of pixels from the left of the screen before the grid starts).

Section: System

Default: GridShiftX = 0

GridShiftY

No longer used.

Indicates the number of pixels along the Y-axis (vertical) by which to offset the snap grid origin (i.e. the number of pixels from the top of the screen before the grid starts.)

Section: System

Default: GridShiftY = 0

GridVis

No longer used.

Indicates whether the snap grid should initially be visible each time the application runs.

If set to 0 (false), the snap grid is not initially visible when the application is run (default).

If set to 1 (true), the snap grid is initially visible when the application is run.

Section: System

Default: GridVis = 0

SnapOn

No longer used.

Indicates whether the snap grid should be turned on each time the application runs.

If set to 1 (true), then the snap grid is initially turned on each time the application is run (default).

Section: System

Default: SnapOn = 1

XGrid

No longer used.

Indicates the initial spacing (in pixels) of the snap grid's points along the X-axis (horizontal) when the application runs.

Related Variables: The YGrid variable enables you to change the initial spacing of the snap grid's Y-axis.

Section: System

Default: XGrid = 4

*Restart Required (Settings.Startup property)

YGrid

No longer used.

Set the initial spacing (in pixels) of the snap grid's points along the Y-axis (vertical) when the application runs.

Related Variables: The XGrid variable enables you to change the initial spacing of the snap grid's X-axis.

Section: System

Default: YGrid = 4

*Restart Required (Settings.Startup property)

Tag Properties

The following list of variables pertain to tags.

- ...AnalogControlName
- ...AnalogScaledMaxDefault
- ...AnalogScaledMinDefault
- ... AnalogStatusName
- ...AnalogUnscaledMaxDefault
- ...AnalogUnscaledMinDefault
- ... AreaExclude
- ... AreaFilter
- ...CanRedefineOEMType
- ...DefaultAnalogDeadbandFractionOfFullScale
- ...DefaultCalculationDeadbandFractionOfFullScale
- ... DigitalControlName
- ... DigitalStatusName
- ...HelpFile
- ... InvalidText
- ... ParmChangedColor
- ... ParmInfoCreatedByLabel
- ... ParmInfoCreatedOnLabel
- ...ParmInfoDateFormat
- ... ParmInfoHistoryEnabled
- ... ParmInfoLastModByLabel
- ... ParmInfoLastModOnLabel
- ... ParmInfoTimeFormat
- ... ParmOverrideColor

- ... PulseInName
- ... RateOfChangeTagRPCInterval
- ... RateOfChangeTagRPCThreshold
- ... RememberNewTagParameters
- ... SiteToolsConfirmOutput
- ... SQLLoggerDefaultLogInterval
- ... SQLLoggerDefaultMaxDataAge
- ... SQLLoggerDefaultTagDataTableName
- ... SQLLoggerDefaultTagIdTableName
- ... SQLLoggerDeleteInterval
- ... SQLLoggerDeleteOffset
- ... SQLLoggerGroupSharedRPC
- ... SQLLoggerLogInvalids
- ... TagField1Name
- ... TagField2Name
- ... TagField3Name

AnalogControlName

Indicates the label to be displayed in the title bar of the tag properties folder for analog control tags. This label also determines the label displayed in the Tag Browser for the analog control tag type.

Section: System

Default: AnalogControlName = Analog Control

AnalogScaledMaxDefault

Holds the default value for the maximum scaled value, corresponding to the maximum unscaled value as read from hardware. This value will be used in the scaling tab when configuring new analog tags.

Default: AnalogScaledMaxDefault = 100

Section: System

AnalogScaledMinDefault

Holds the default value for the minimum scaled value, corresponding to the minimum unscaled value as read from hardware. This value will be used in the scaling tab when configuring new analog tags.

Default: AnalogScaledMinDefault = 0

Section: System

AnalogStatusName

Indicates the label to be displayed in the title bar of the tag properties folder for analog status tags. This label also determines the label displayed in the Tag Browser for the analog status tag type.

Section: System

Default: AnalogStatusName = Analog Status

AnalogUnscaledMaxDefault

Holds the default value for the maximum unscaled value (raw equipment value) as read from hardware. This value will be used in the scaling tab when configuring new analog tags.

Default: AnalogUnscaledMaxDefault = 4095

Section: System

AnalogUnscaledMinDefault

Holds the default value for the minimum unscaled value (raw equipment value) as read from hardware. This value will be used in the scaling tab when configuring new analog tags.

Default: AnalogUnscaledMinDefault = 0

Section: System

AreaExclude

Indicates whether tags belonging to any area not listed in the [AREAS] section of the Workstation.Startup configuration file will be excluded from being loaded at startup, or will be loaded at startup (see: Tag Area Filtering).

If AreaExclude is set to 0 (false), then all tags belonging to areas not listed in the [AREAS] section of Settings.Startup are loaded at startup.

If AreaExclude is set to 1 (true), then all tags belonging to areas not listed in the [AREAS] section of Settings.Startup are not loaded at startup.

Related Variables: The AreaFilter variable must be set to 1 (true – which it is by default) in order for area filtering to work.

Section: System

Default: AreaExclude = 0

AreaFilter

Indicates whether the settings of the [AREAS] section and the AreaExclude variable of the Settings.Startup file will be ignored or observed.

If set to 1 (true), then both the [AREAS] section and the AreaExclude variable in Settings.Startup are observed.

Section: System

Default: AreaFilter = 1

CanRedefineOEMType

The security privilege, Manage Tag Types must be granted to your account before you can edit any tag type, whether user-defined or OEM. This property must be set to TRUE (1) before you will be able to redefine OEM tag types, including those that come with VTScada. You are advised to use caution if setting this property to TRUE. The act of redefining an OEM type, especially a commonly used one such as a driver, can have effects that are both undesirable and difficult to reverse.

Default: CanRedefineOEMType = 0

Section: System

DefaultAnalogDeadbandFractionOfFullScale

Use this to set a default deadband for the value of Analog Status tags. The deadband will be calculated as the High Scale Value minus the Low Scale Value, multiplied by this value.

The default value of this property is zero, resulting in no deadband. This ensures consistency for legacy systems being upgraded to the current version of VTScada.

Default: DefaultAnalogDeadbandFractionOfFullScale = 0

Section: System

DefaultCalculationDeadbandFractionOfFullScale

Use this to set a default deadband for the display and logging of Calculation tags. The deadband will be calculated as the High Scale Value minus the Low Scale Value, multiplied by this value.

The default value of this property is 0.0025, resulting in a default deadband value of 0.25 being applied to all calculation tags that are not otherwise configured. (Default values for High Scale and Low Scale are 100 and zero, respectively.)

Default: DefaultCalculationDeadbandFractionOfFullScale = 0.0025

Section: System

DigitalControlName

Indicates the label to be displayed in the title bar of the tag properties folder for digital control tags. This label also determines the label displayed in the Tag Browser for the digital control tag type.

Section: System

Default: DigitalControlName = DigitalControl

DigitalStatusName

Indicates the label to be displayed in the title bar of the tag properties folder for digital status tags. This label also determines the label displayed in the Tag Browser for the digital status tag type.

Section: System

Default: DigitalStatusName = Digital Status

HelpFile

Identifies the name of the help file with which all tags are to be associated. VTScada then uses the identified help file, along with a specified topic ID to locate and open specific help topics that pertain to the selected tag, or possibly to the tag's type. (For example, a help topic that pertains specifically to digital input tag "DI20_1", or a help topic that pertains to digital input tags in general.)

Once a help file is associated with an application via the HelpFile variable, it is necessary to identify the help topic (within that help file) to access for a selected tag. This is done using a "topic ID" - a unique index number assigned to each topic in the help file by the help author.

Topic IDs can be entered into the Help Search Key property that appears on the ID tab of the tag properties folder for all tag types. This enables developers to associate each tag with specific help topics existing within the help file specified by the HelpFile variable.

Once each tag has had a topic ID entered into its Help Search Key property, the associated help topic can be accessed by users in one of two ways:

- By right-clicking the tag's widget and selecting the Help option from the shortcut menu.
- By clicking the Help button that appears between the OK and Cancel buttons on each tag's properties folder.

Section: System

Default: HelpFile = VTSGuides

InvalidText

Enables you to set the text to be displayed for tags whose data value is invalid.

Section: System

Default: InvalidText = ??

ParmChangedColor

Sets the background color to be used in configuration panels when tag parameters are changed. Defaults to a light green.

Section: System

Default: ParmChangedColor = 63

ParmInfoCreatedByLabel

Used only when ParmInfoHistoryEnabled is set to TRUE and there is a record of who created the value. Controls the format of the tool tip that displays information about the creation of the configuration panel variable being pointed to. Accepts up to three string parameters of the format %s, in the following order: creator name, creation date, creation time.

Section: Labels

Default: ParmInfoCreatedByLabel = Created by %s on %s at %s

ParmInfoCreatedOnLabel

Used only when ParmInfoHistoryEnabled is set to TRUE and there is no record of who created the value. Controls the format of the tool tip that displays information about the creation of the configuration panel variable being pointed to. Accepts up to two string parameters of the format %s, in the following order: creation date, creation time.

Section: Labels

Default: ParmInfoCreatedOnLabel = Created on %s at %s

ParmInfoDateFormat

Sets the format of the date displayed in the tag creation/modification history tooltips.

Section: Labels

Default: ParmInfoDateFormat = ddd MMM dd, yyyy

ParmInfoHistoryEnabled

Default: ParmInfoHistoryEnabled = 1

ParmInfoLastModByLabel

Used only when ParmInfoHistoryEnabled is set to TRUE and there is a record of who modified the value. Controls the format of the tool tip that displays information about the modification of the configuration panel variable being pointed to. Accepts up to three string parameters of the format %s, in the following order: name of the user who modified the value, modification date, modification time.

Section: Labels

Default: ParmInfoLastModByLabel = Modified by %s on %s at %s

ParmInfoLastModOnLabel

Used only when ParmInfoHistoryEnabled is set to TRUE and there is no record of who modified the value. Controls the format of the tool tip that displays information about the modification of the configuration panel variable being pointed to. Accepts up to two string parameters of the format %s, in the following order: modification date, modification time.

Section: Labels

Default: ParmInfoLastModOnLabel = Modified on %s at %s

ParmInfoTimeFormat

Sets the format of the time displayed in the tag creation/modification history tooltips.

Section: Labels

Default: ParmInfoTimeFormat =

PulseInName

Indicates the label to be displayed in the title bar of the tag properties folder for pulse input tags. This label also determines the label that is displayed in the Tag Browser's Types drop-down list for the pulse input tag type.

Section: System

Default: PulseInName = Pulse Input

ParmOverrideColor

Sets the color to be used in configuration panels when child tag properties are overridden. Defaults to pale orange.

Section: System

Default: ParmOverrideColor = 183

RateOfChangeTagRPCInterval

In a remote application, Rate of Change Tag information is distributed from the server to workstations at regular intervals, as set by this value. The update frequency is measured in seconds.

Section: System

Default: 60

RateOfChangeTagRPCThreshold

In a remote application, Rate of Change Tag information is distributed from the server to workstations at regular intervals (see: RateOfChageTagRPCInterval) or when the tag's value has changed by at a relative amount.

This variable sets the percentage amount by which the rate of change value must change before it will be distributed from the server to client workstations.

Section: System

Default: 5

RememberNewTagParameters

When set to the default value of 1 (true), new tags will initialize to the same parameters as the last tag created. This behavior can be disabled by setting the value to 0, thus causing all new tags to initialize as if they were the first ones being created in the application.

Section: System

Default: RememberNewTagParameters = 1

SiteToolsConfirmOutput

Used by the automatically-generated output controls in a Site Details page. When set to TRUE, operators must confirm all control actions sent from the Site Details page.

If set FALSE, no confirmation is required.

Default: SiteToolsConfirmOutput = 1 (TRUE)

Section: System

SQLLoggerDefaultLogInterval

Indicates the interval between log entries.

Default: SQLLoggerDefaultLogInterval = 60

SQLLoggerDefaultMaxDataAge

Controls the default for the "Auto-Delete Records Older than (days)" parameter of the SQLLoggerGroup.

Section: System

Default: SQLLoggerDefaultMaxDataAge = 365

SQLLoggerDefaultTagDataTableName

Indicates the table name the logger expects to find in the log database, to use for writing tag value information.

Section: System

Default: SQLLoggerDefaultTagDataTableName = VTS_TAGDATA

SQLLoggerDefaultTagIdTableName

Indicates the table name the logger expects to find in the log database, to use for writing tag ID information.

Section: System

Default: SQLLoggerDefaultTagIdTableName = VTS_TAGID

SQLLoggerDeleteInterval

Indicates in seconds, how often to purge old records. By default, this runs daily.

Section: System

Default: SQLLoggerDeleteInterval = 86400

SQLLoggerDeleteOffset

Indicates, in seconds for each logger delete interval, how long after the beginning of the interval the purge should occur. Taken with the default of 86400 for SQLLoggerDeleteInterval, this sets the purge to take place at 30 seconds past midnight each day.

Section: System

Default: SQLLoggerDeleteOffset = 30

SQLLoggerGroupSharedRPC

If set to TRUE then the same RPC service will be used for all instances of SQLLoggerGroup, making it easier to specify which server to use for all SQL Logger Groups.

Section: System

Default: SQLLoggerGroupSharedRPC = 0

SQLLoggerLogInvalids

Indicates whether invalid values should be logged by the SQL logger.

Section: System

Default: SQLLoggerLogInvalids = 1

TagField1Name

Indicates the field name for the first field in the tag properties folders for all tag types.

Note: It is NOT recommended that you modify this variable, as doing so may adversely affect remote configuration.

Related Variables: The TagField2Name and TagField3Name variables enable you to configure the field names for the second and third fields in the tag properties folders for all tag types.

Section: System

Default: TagField1Name = Name

TagField2Name

Indicates the field name for the second field in the tag properties folders for all tag types.

Note: It is NOT recommended that you modify this variable, as doing so may adversely affect remote configuration.

Related Variables: The TagField1Name and TagField3Name variables enable you to configure the field names for the first and third fields in the tag properties folders for all tag types.

Section: System

Default: TagField2Name = Area

TagField3Name

Indicates the field name for the third field in the tag properties folders for all tag types.

Note: It is NOT recommended that you modify this variable, as doing so may adversely affect remote configuration.

Related Variables: The TagField1Name and TagField2Name variables enable you to configure the field names for the first and second fields in the tag properties folders for all tag types.

Section: System

Default: TagField3Name = Description

Time Synchronization Manager Properties

The following list of variables apply to the Time Synchronization Manager.

... TimeSyncEnable

... TimeSyncMicroAdjust

... TimeSyncRPCQMax

... TimeSyncUpdtltrlvl

TimeSyncEnable

Enable or disable the Time Synchronization Manager.

Related Variables: TimeSyncMicroAdjust, TimeSyncUpdtltrlvl, TimeSyncRPCQMax.

Section: System

Default: TimeSyncEnable = 1

TimeSyncMicroAdjust

Enables the clock to be adjusted incrementally instead of instantly.

Related Variables: TimeSyncEnable, TimeSyncUpdtltrlvl, TimeSyncRPCQMax.

Section: System

Default: TimeSyncMicroAdjust = 1

TimeSyncRPCQMax

Enter the maximum size for the RPC queue on the server. If the RPC queue exceeds this size, no time synchronization will occur.

Related Variables: TimeSyncEnable, TimeSyncMicroAdjust, TimeSyncUpdtltrlvl.

Section: System

Default: TimeSyncRPCQMax = 500

TimeSyncUpdtltrlvl

Enter the time synchronization update interval in seconds.

Related Variables: TimeSyncEnable, TimeSyncMicroAdjust, TimeSyncRPCQMax.

Section: System

Default: TimeSyncUpdtltrlvl = 900

Tooltip Properties

The following list of variables pertain to Tool Tips.

... NoBalloonTips

... ShowTip

... TipBack

... TipFore

... TipOff

... TipOn

NoBalloonTips

Indicates the style of tooltips for an application.

If set to 0, then tooltips will be displayed in the balloon style.

If set to 1, then tooltips will be displayed in the textbox style.

Section: System

Default: NoBalloonTips =

ShowTip

Enables or disables tooltips.

If set to 1 (true), then all tooltips are enabled (default).

Section: System

Default: ShowTip = 1

Related Information:

... TipOff – Sets the duration of the tooltip's display time.

... TipOn – Sets the length of the pause before the tooltip will be displayed.

TipBack

Sets the background color for the tooltip displayed when setting a value using a rotary control or a slider.

Affects other tooltips only when visual themes are disabled in Windows.

When changing the TipBack variable, take into consideration the text and outline colors set by the TipFore variable to ensure clear contrast between colors.

Section: System

Default: TipBack =

Related Information:

...See "VTScada Color Palette" in the General Reference section of the VTScada Programmer's Guide.

... TipFore – Sets the contrasting foreground color

... ShowTip – If it is set to false (0), then all other tooltip variables are ignored.

TipFore

Sets the foreground (text and outline) color for the tooltip displayed when setting a value using a rotary control or a slider.

Affects other tooltips only when visual themes are disabled in Windows.

When changing the TipFore variable, take into consideration the background color set by the TipBack variable, as the background, text, and outline of tooltips must be set in such a way that they can be clearly read.

Section: System

Default: TipFore =

Related Information:

...See "VTScada Color Palette" in the General Reference section of the VTScada Programmer's Guide.

... TipBack – Sets the contrasting background color

... ShowTip – If it is set to false (0), then all other tooltip variables are ignored.

TipOff

Sets the number of seconds for which a tooltip will be displayed once activated.

Section: System

Default: TipOff = 10

Related Information:

... ShowTip – If it is set to false (0), then all other tooltip variables are ignored.

... TipOn – Sets the length of the pause before the tooltip will be displayed.

TipOn

Sets the time, measured in seconds, for which the pointer must hover over an object before any tooltip linked to that object will be shown.

Section: System

Default: TipOn= 1

Related Information:

... ShowTip – If it is set to false (0), then all other tooltip variables are ignored.

... TipOff – Sets the duration of the tooltip's display time.

Trending and Historical Data Viewer Properties

The following list of variables pertain to trending and the Historical Data Viewer page.

...AITrendEnable

... DITrendEnable

... DontLogTrendPens

... HDVAnalogAlarmsVisibility

... HDVAnalogLegendAverage

... HDVAnalogLegendDescription
... HDVAnalogLegendHighScaleValue
... HDVAnalogLegendLowScaleValue
... HDVAnalogLegendMax
... HDVAnalogLegendMin
... HDVAnalogLegendValue
... HDVAnalogPenAverageVisibility
... HDVAnalogPenMinMaxVisibility
... HDVAnalogPenScale
... HDVAnalogPenStyle
... HDVAnalogPenVisibility
... HDVAnalogPenWidth
... HDVAnalogScalesVisibility
... HDVDataRetrievalMsg
... HDVDataRetrievalMsgColor
... HDVDataRetrievalWaitTime
... HDVDateFormat1
... HDVDateFormat2
... HDVDigitalGridColor
... HDVDigitalLegendAverage
... HDVDigitalLegendDescription
... HDVDigitalLegendHighScaleValue
... HDVDigitalLegendLowScaleValue
... HDVDigitalLegendMax
... HDVDigitalLegendMin
... HDVDigitalLegendNumberOfStarts
... HDVDigitalLegendOnTime
... HDVDigitalLegendValue

- ... HDVDigitalPenStyle
- ... HDVDigitalPenVisibility
- ... HDVDigitalPenWidth
- ... HDVDigitalScalesVisibility
- ... HDVDisplayTimeSelectionScrollBar
- ... HDVDisplayToolBar
- ... HDVGridCellColor
- ... HDVGridLineColor
- ... HDVGridViewColor
- ... HDVGridViewSortOrder
- ... HDVHorizontalGridColor
- ... HDVLayoutBGColor
- ... HDVLegendVisible
- ...HDVMaxNoteWindows
- ... HDVNotesLegendDescription
- ... HDVNotesLineVisibility
- ... HDVNotesPenStyle
- ... HDVNotesPenVisibility
- ... HDVNotesPenWidth
- ... HDVPlotBGColor
- ... HDVPlotViewColor
- ... HDVShowAllScales
- ... HDVShowTimeScales
- ... HDVTimeCursorColor
- ... HDVTimeFormat1
- ... HDVTimeFormat2
- ... HDVVerticalGridColor
- ... TrendOnTop

AITrendEnable

Indicates whether the widgets for analog input tags or analog status tags can be clicked to open a windowed version of the Trends page that plots the selected tag's data when the application is in operation mode.

If AITrendEnable is set to 1 (true), then a windowed version of the Trends page will open when an analog input tag's (or analog status tag's) widget is clicked while the application is in operation mode (default).

Related Variables: To configure your application to open a windowed version of the Trends page that automatically plots digital input tag data when the widget for a digital input is clicked, please refer to the DITrendEnable variable, or Application Properties for Trending and the Historical Data Viewer Page.

Default: AITrendEnable = 1

Section: System

DITrendEnable

Indicates whether the widgets of digital input tags can be clicked to open a windowed version of the Trends page that plots the selected tag's data when the application is in operation mode.

If set to 1 (true), then a windowed version of the Trends page will open when a digital input tag's widget is clicked while the application is in operation mode.

Related Variables: To configure your application to open a windowed version of the Trends page that automatically plots analog input tag data when the widget for an analog input is clicked, please refer to the AITrendEnable variable.

Section: System

Default: DITrendEnable = 0

DontLogTrendPens

Enables you to disable logging to disk of live trend data.

If set to 0 (false), VTScada will log live trend data to disk (default).

Section: System

Default: DontLogTrendPens = 0

HDVAnalogAlarmsVisibility

Enables you to indicate whether or not you wish the alarm setpoint value for any alarms related to analog tags to be indicated on the graph on the Historical Data Viewer page using horizontal line markers. If set to 1, the setpoint value for any alarms related to analog tags that are being plotted on the graph will be visible. If set to 0 (default), the setpoint value for any alarms related to analog tags that are being plotted on the graph will be invisible.

Section: System

Default: HDVAnalogAlarmsVisibility = 1

HDVAnalogLegendAverage

Enables you to indicate whether or not you wish the average value of analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the average value of analog tags will be indicated in the pen legend. If set to 0 (default), then the average value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendAverage = 0

HDVAnalogLegendDescription

Enables you to indicate whether or not you wish the description configured for analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1 (default), then the description of analog tags will be indicated in the pen legend. If set to 0, then the description of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendDescription = 1

HDVAnalogLegendHighScaleValue

Enables you to indicate whether or not you wish the high scale value of the analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the high scale value of analog tags will be indicated in the pen legend. If set to 0 (default), then the high scale value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendHighScaleValue = 0

HDVAnalogLegendLowScaleValue

Enables you to indicate whether or not you wish the low scale value of the analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the low scale value of analog tags will be indicated in the pen legend. If set to 0 (default), then the low scale value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendLowScaleValue = 0

HDVAnalogLegendMax

Enables you to indicate whether or not you wish the maximum value of analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the maximum value of analog tags will be indicated in the pen legend. If set to 0 (default), then the maximum value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendMax = 0

HDVAnalogLegendMin

Enables you to indicate whether or not you wish the minimum value of analog tags whose value is being plotted on the graph on the Historical

Data Viewer page to be displayed in the pen legend. If set to 1, then the minimum value of analog tags will be indicated in the pen legend. If set to 0 (default), then the minimum value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendMin = 0

HDVAnalogLegendValue

Enables you to indicate whether or not you wish the value of analog tags whose value is being plotted on the graph to be displayed in the pen legend on the Historical Data Viewer page as the mouse pointer is moved across the plot on the graph. If set to 1 (default), then the value of analog tags will be indicated in the pen legend. If set to 0, then the value of analog tags will not be indicated in the pen legend.

Section: System

Default: HDVAnalogLegendValue = 1

HDVAnalogPenAverageVisibility

Enables you to indicate whether or not you wish the average value of analog tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the legend. If set to 1 (default), then the average values for analog tags will be displayed in the legend. If set to 0, then the average values for analog tags will not be displayed in the legend.

Section: System

Default: HDVAnalogPenAverageVisibility = 1

HDVAnalogPenMinMaxVisibility

Enables you to indicate whether or not you wish the minimum and maximum value of analog tags to be indicated on the graph on the Historical Data Viewer page. If set to 1, then the minimum and maximum values for analog tags will be displayed on the graph. If set to 0 (default), then the

minimum and maximum values for analog tags will not be displayed on the graph.

Section: System

Default: HDVAnalogPenMinMaxVisibility = 0

HDVAnalogPenScale

Enables you to specify the pen scale to be used for analog plots on the Historical Data Viewer page. This can be one of:

- Linear
- Square Root
- Logarithmic

Section: System

Default: HDVAnalogPenScale = Linear

HDVAnalogPenStyle

Enables you to indicate the style of the plot line for analog pens on the Historical Data Viewer page. HDVAnalogPenStyle can be set to one of the following values:

0 - Invisible Plot

1 -Solid

2 -Dashed

3 -Dotted

4 -Dot-dashed

5 -Dot-dot-dashed

Section: System

Default: HDVAnalogPenStyle = 1

HDVAnalogPenVisibility

Enables you to indicate whether or not you wish the value of analog tags to be plotted on the graph on the Historical Data Viewer page. If set to 1 (default), then analog plots will be visible on the graph once added to the legend. If set to 0, then analog plots will not be visible on the graph once added to the legend.

Section: System

Default: HDVAnalogPenVisibility = 1

HDVAnalogPenWidth

Sets the pen width to be used for analog plots in the historical data viewer. If left blank, the default width will be 1.

Section: System

Default: HDVAnalogPenWidth = 1

HDVAnalogScalesVisibility

Enables you to indicate whether or not the value scales should be displayed to the left of the analog plot area on the Historical Data Viewer page. If set to 1, the value scales will be displayed to the left of the analog plot area (default). If set to 0, the value scales will not be displayed to the left of the analog plot area.

Section: System

Default: HDVAnalogScalesVisibility = 1

HDVDataRetrievalMsg

Displays the set message while retrieving data

Section: System

Default: HDVDataRetrievalMsg = Data retrieval in progress ...

HDVDataRetrievalMsgColor

Sets the text color of HDVDataRetrievalMsg

Section: System

Default: HDVDataRetrievalMsgColor = 0

HDVDataRetrievalWaitTime

Defines the number of seconds to wait before displaying the message stored in HDVDataRetrievalMsg

Section: System

Default: HDVDataRetrievalWaitTime = 2

HDVDateFormat1

Set the date format to be displayed beneath the plot areas on the Historical Data Viewer page when the duration is set to low increments. For valid date formats, please refer to the Date function.

Section: System

Default: HDVDateFormat1 = 20

HDVDateFormat2

Set the date format to be displayed beneath the plot areas on the Historical Data Viewer page when the duration is set to high increments. For valid date formats, please refer to the Date function.

Section: System

Default: HDVDateFormat2 = 12

HDVDigitalGridColor

Enables you to indicate the color to be displayed for the vertical grid lines on the digital plot area on the Historical Data Viewer page. The default color is pale grey.

Section: System

Default: HDVDigitalGridColor =

HDVDigitalLegendAverage

Enables you to indicate whether or not you wish the average value of digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the average value of digital tags will be indicated in the pen legend. If set to 0 (default), then the average value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendAverage = 0

HDVDigitalLegendDescription

Enables you to indicate whether or not you wish the description configured for digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1 (default), then the description of digital tags will be indicated in the pen legend. If set to 0, then the description of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendDescription = 1

HDVDigitalLegendHighScaleValue

Enables you to indicate whether or not you wish the high scale value of digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the high scale value of digital tags will be indicated in the pen legend. If set to 0 (default), then the high scale value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendHighScaleValue = 0

HDVDigitalLegendLowScaleValue

Enables you to indicate whether or not you wish the low scale value of digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the low scale value of digital tags will be indicated in the pen legend. If set to 0 (default), then low scale value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendLowScaleValue = 0

HDVDigitalLegendMax

Enables you to indicate whether or not you wish the maximum value of digital tags whose value is being plotted on the graph on the Historical

Data Viewer page to be displayed in the pen legend. If set to 1, then the maximum value of digital tags will be indicated in the pen legend. If set to 0 (default), then the maximum value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendMax = 0

HDVDigitalLegendMin

Enables you to indicate whether or not you wish the minimum value of digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the minimum value of digital tags will be indicated in the pen legend. If set to 0 (default), then the minimum value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendMin = 0

HDVDigitalLegendNumberOfStarts

Enables you to indicate whether or not you wish the number of starts for digital tags whose value is being plotted on the graph on the Historical Data Viewer page to be displayed in the pen legend. If set to 1, then the number of starts for digital tags will be indicated in the pen legend. If set to 0 (default), then the number of starts for digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendNumberOfStarts = 0

HDVDigitalLegendOnTime

Enables you to indicate whether or not you wish the amount of time that a digital tag has been "on" (reading a value of 1) to be displayed in the pen legend when the tag's data is being plotted on the graph on the Historical Data Viewer page. If set to 1, then the on time for digital tags will

be indicated in the pen legend. If set to 0 (default), then the on time for digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendOnTime = 0

HDVDigitalLegendValue

Enables you to indicate whether or not you wish the value of digital tags whose value is being plotted on the graph to be displayed in the pen legend on the Historical Data Viewer page as the mouse pointer is moved across the plot on the graph. If set to 1 (default), then the value of digital tags will be indicated in the pen legend. If set to 0, then the value of digital tags will not be indicated in the pen legend.

Section: System

Default: HDVDigitalLegendValue = 1

HDVDigitalPenStyle

Enables you to indicate the line style for digital pens on the Historical Data Viewer page. HDVDigitalPenStyle can be set to one of the following values:

0 - Invisible Plot

1 -Solid

2 -Dashed

3 -Dotted

4 -Dot-dashed

5 -Dot-dot-dashed

Section: System

Default: HDVDigitalPenStyle = 1

HDVDigitalPenVisibility

Enables you to indicate whether or not you wish the value of digital tags to be plotted on the graph on the Historical Data Viewer page. If set to 1 (default), then digital plots will be visible on the graph once added to the

legend. If set to 0, then digital plots will not be visible on the graph once added to the legend.

Section: System

Default: HDVDigitalPenVisibility = 1

HDVDigitalPenWidth

Sets the pen width to be used for digital plots in the historical data viewer. If left blank, the default width will be 1.

Section: System

Default: HDVDigitalPenWidth = 1

HDVDigitalScalesVisibility

Enables you to indicate whether or not the value scales should be displayed to the left of the digital plot area on the Historical Data Viewer page. If set to 1, the value scales will be displayed to the left of the digital plot area (default). If set to 0, the value scales will not be displayed to the left of the digital plot area.

Section: System

Default: HDVDigitalScalesVisibility = 1

HDVDisplayTimeSelectionScrollBar

Controls whether or not the Date/Time scrollbar on the Historical Data Viewer page should be visible. If set to 1, the Date/Time scrollbar will be visible. If set to 0, the time selection scrollbar will be invisible.

Section: System

Default: HDVDisplayTimeSelectionScrollBar = 1

HDVDisplayToolbar

Controls whether or not the toolbar on the Historical Data Viewer page should be visible. If set to 1, the toolbar will be visible. If set to 0, the toolbar will be invisible.

Section: System

Default: HDVDisplayToolbar = 1

HDVGridCellColor

If set, this value provides a default color for the grid cells in the Historical Data Viewer

Section: System

Default: HDVGridViewColor =

HDVGridLineColor

If set, this value provides a default color for the grid lines in the Historical Data Viewer

Section: System

Default: HDVGridViewColor =

HDVGridViewColor

If set, this value provides a default color for the grid view in the Historical Data Viewer

Section: System

Default: HDVGridViewColor =

HDVGridViewSortOrder

Enables the sorting of the Historical Data Viewer Grid by timestamp in either ascending or descending order. If set to 0 (the default) the order will be ascending. If set to 1, the order will be descending.

Section: System

Default: HDVGridViewSortOrder = 0

HDVHorizontalGridColor

Enables you to indicate the color to be displayed for the horizontal grid lines on the analog plot area on the Historical Data Viewer page. The default color is pale grey.

Section: System

Default: HDVHorizontalGridColor =

HDVMaxNoteWindows

Controls the number of note dialogs that may be opened at once by clicking on an arrow at the bottom of an HDV plot. Defaults to 10.

Default: HDVMaxNoteWindows = 10

Section: System

HDVPlotTextColor

Controls the color used for text in the Historical Data Viewer, within the area of the graph or grid.

Defaults to 0 (Black)

Default: HDVPlotTextColor = 0

Section: System

HDVLayoutBGColor

Enables you to indicate the background color to be used in the area surrounding the Date/Time scroll bar at the bottom of the Historical Data Viewer page.

Section: System

Default: HDVLayoutBGColor =

HDVLayoutTextColor

Controls the color used for text in the Historical Data Viewer, outside the area of the graph or grid.

Defaults to 0 (Black)

Default: HDVLayoutTextColor = 0

Section: System

HDVLegendVisible

Controls whether or not the legend pane on the Historical Data Viewer page should be visible. If set to 1, the legend will be visible. If set to 0, the legend will be invisible.

Section: System

Default: HDVLegendVisible = 1

HDVNotesLegendDescription

Enables you to indicate whether or not you wish the description configured for notebook tags to be displayed in the pen legend on the Historical Data Viewer page. If set to 1 (default), then the description of notebook tags will be indicated in the pen legend. If set to 0, then the description of notebook tags will not be indicated in the pen legend.

Section: System

Default: HDVNotesLegendDescription = 1

HDVNotesLineVisibility

Controls whether or not vertical lines should be drawn on the graph on the Historical Data Viewer page to indicate the presence of a note. If set to 1, a vertical line will be displayed on the graph to indicate the presence of a note. If set to 0, vertical lines will not be displayed on the graph to indicate the presence of notes.

Section: System

Default: HDVNotesLineVisibility = 1

HDVNotesPenStyle

Enables you to indicate the style for note pens on the Historical Data Viewer page. HDVNotesPenStyle can be set to one of the following values:

0 - Invisible Plot

1 -Solid

2 -Dashed

3 -Dotted

4 -Dot-dashed

5 -Dot-dot-dashed

Section: System

Default: HDVNotesPenStyle = 1

HDVNotesPenVisibility

Controls whether or not arrows should be drawn on the graph on the Historical Data Viewer page to indicate the presence of a note. If set to 1, an arrow will be displayed on the graph to indicate the presence of a note. If set to 0, arrows will not be displayed on the graph to indicate the presence of notes.

Section: System

Default: HDVNotesPenVisibility = 1

HDVNotesPenWidth

Sets the pen width to be used for notes in the historical data viewer. If left blank, the default width will be 1.

Section: System

Default: HDVDigitalPenWidth = 1

HDVPlotBGColor

Enables you to change the background color of the plot area of the graph on the Historical Data Viewer page. The default color is pale yellow (31).

Section: System

Default: HDVPlotBGColor =

HDVPlotViewColor

Enables you to indicate the background color to be displayed around the legend (if the legend is present (see HDVLegendVisible above), and the analog and digital plot areas on the Historical Data Viewer page. The default color is the system grey.

Section: System

Default: HDVPlotViewColor =

HDVShowAllScales

Controls whether or not the value scales should be displayed to the left of the plot areas on the Historical Data Viewer page.

Section: System

Default: HDVShowAllScales = 1

HDVShowTimeScales

Controls whether or not the time scales should be displayed beneath the analog and digital plot areas on the Historical Data Viewer page.

Section: System

Default: HDVShowTimeScales = 1

HDVSimpleLegend

Used by the Historical Data Viewer's plot legend to select between a full legend with all statistics, or a simplified legend.

If set to TRUE (1) the number of columns displayed in the legend will be reduced.

Default: HDVSimpleLegend =

Section: System

HDVTimeCursorColor

Set the color of the horizontal time line attached to the mouse pointer when it is resting on the plot areas on the Historical Data Viewer page.

The default color is a dark grey.

Section: System

Default: HDVTimeCursorColor = 28

HDVTimeFormat1

Set the time format to be displayed beneath the plot areas on the Historical Data Viewer page when the duration is set to low increments. For valid time format values, please refer to the Time function.

Section: System

Default: HDVTimeFormat1 = 5

HDVTimeFormat2

Set the time format to be displayed beneath the plot areas on the Historical Data Viewer page when the duration is set to high increments. For

valid time format values, please refer to the Time function.

Section: System

Default: HDVTimeFormat2 = 2

HDVVerticalGridColor

Enables you to indicate the color to be displayed for the vertical grid lines on the analog plot area on the Historical Data Viewer page. The default color is pale grey.

Section: System

Default: HDVVerticalGridColor =

TrendOnTop

Indicates whether or not an open, windowed version of the Trends page always remains on top of your system pages.

If TrendOnTop is set to 1 (true), then an open, windowed version of the Trends page always appears on top of system pages (default).

Section: System

Default: TrendOnTop = 1

Wizard Engine Properties

Related Information:

... WizardFinishText1

... WizardFinishText2

... WizardFinishText3

... WizardFinishTitle

... WizardWelcomeLabel

WizardFinishText1

First line displayed in the Finish screen of a wizard. The full screen is the concatenation of WizardFinishText1 + WizardFinishText2 + WizardFinishText3 plus whatever other text you wish to add.

Section: System

Default: WizardFinishText1 = The Wizard has acquired all necessary information.

WizardFinishText2

Second line displayed in the Finish screen of a wizard. The full screen is the concatenation of WizardFinishText1 + WizardFinishText2 + WizardFinishText3 plus whatever other text you wish to add.

Section: System

Default: WizardFinishText2 = Press FINISH to complete the operation, BACK to change parameters or

WizardFinishText3

Third line displayed in the Finish screen of a wizard. The full screen is the concatenation of WizardFinishText1 + WizardFinishText2 + WizardFinishText3 plus whatever other text you wish to add.

Section: System

Default: WizardFinishText3 = CANCEL to abort the operation without making any changes.

WizardFinishTitle

Title used for the Finish screen of a wizard. The two letter sequence ^W will be replaced by the name of the wizard.

Section: System

Default: WizardFinishTitle = The ^W is ready.

WizardWelcomeLabel

Sets the Welcome label for the wizard engine. The two letter sequence ^W will be replaced by the name of the wizard.

Section: System

Default: WizardWelcomeLabel = Welcome to the ^W.

System Properties – Setup.ini

Note: This chapter includes properties that affect VTScada as a whole and which are set in Settings.INI. Refer also to the chapter, Application Properties, for properties that affect an application and can be set in Settings.Dynamic or Settings.Startup.

The Setup.ini configuration file is used to establish system-wide properties that customize the appearance and behavior of the VTScada software. Unlike the application properties that affect individual applications, the Setup.ini variables affect the performance of the VTScada software overall.

Because the Setup.ini variables apply to the VTScada software, changes will not take effect until VTScada has been restarted.

Note: You are able to use the application properties files to override many of the settings within Setup.ini. This enables you change (some) values without re-starting VTScada.

The following sections are available in the Setup.ini configuration file. Each is described in more complete detail in the sub-topics of this chapter.

[APPS]	A list of the paths to all applications that have been added to the VTScada Application Manager's Available Applications list.
[Clients-AdditionalAllowedOrigins]	Add any domain names or IPs that are used in Anywhere Client URLs that are not already included in the server list for the VTScada Internet Client and set to 1.
[CriticalConfigurationFiles]	A list of files that cannot be removed from using an application's file manifest
[FileExtensionClasses]	A list of file categorizations used for display formatting by the Diff Viewer in the Properties panel
[LABELS]	A list of all text labels appearing in the system.

	<p>These text labels may be used to customize VTScada according to your company's wishes, or perhaps to customize the VTScada software in a language other than English (which is the default).</p> <p>Also includes the property, TRUELabel – used to set the list of strings that will be taken to mean "TRUE" (non-zero) for Boolean variables.</p>
[LINKTOLERANCE-...]	<p>A [LINKTOLERANCE-...] section may be added to the Setup.ini configuration file when dealing with remote or networked applications. The [LINKTOLERANCE-...] section can be used to handle the differing response times from one workstation to another, which is often experienced due to CPU loading, but mostly due to link throughput limitations.</p>
[OEM]	<p>Variables used by an original equipment manufacturer (OEM), or system integrator to customize VTScada for their company</p>
[REMOTE]	<p>Variables applicable to the Internet Browser (VIC).</p>
[RPCMANAGER-EXCLUDEIP]	<p>Used to limit RAS clients to specific workstations by excluding the workstations that you do not wish the RAS client to access.</p>
[RPCMANAGER-NETPRIORITY]	<p>Used in multi-homed situations to resolve the issue of prioritizing communications when dealing with multiple networks.</p>
[SQL_Excel_Types]	<p>An SQL conversion table for MS Excel.</p>
[StandardServerLists]	<p>Server lists to choose from when adding a new service in the Edit Server Lists panel.</p>
[SQL_ODBC_Classes]	<p>Used to match driver types (as reported by the ODBCsources function) to SQL conversion tables</p>
[SYSTEM]	<p>A list of variables that will determine the attributes of VTScada as it is running.</p>
[THEMES]	<p>The definition strings for each of the VTScada</p>

	color themes. You may alter a theme, or create your own.
[TextFileExtensions]	A list of file extensions for files to be interpreted as text by Configuration Management.
[TRACE]	A series of variables that can be used to specify which VTScada activities you wish to trace. These variables are associated with the Trace VTScada Actions utility described in "Trace VTScada Actions Application".

Related Information:

...Application Properties

...Setup.ini [APPS] Section Variables

...Setup.ini [LABELS] Section Variables

...Setup.ini [LAYER] Section Variables

...Setup.ini [LINKTOLERANCE-...] Section Variables

...Setup.ini [OEM] Section Variables

...Setup.ini [REMOTE] Section Variables

... Setup.ini [RPCManager-AllowIP] Section Variables

... Setup.ini [RPCManager-ExcludeIP] Section Variables

...Setup.ini [RPCMANAGER-NETPRIORITY] Section Variables

...Setup.ini [SYSTEM] Section Variables

...Setup.ini [Themes] Section Variables

...Setup.ini [TRACE] Section Variables

Setup.ini [APPS] Section Variables

The [APPS] section of the Setup.ini configuration file consists of a list of the paths to all the applications that you have added to the VTScada Application Manager's list of available applications.

An example of the syntax of the variables in the [APPS] section:

```
[APPS]
0 XY\
0 Example\
```

```
0 TUTSIM\  
1 TUTORIAL\  
0 D:\Backups\HydroSCADAApplication
```

The application directory for each application appears under the [APPS] section. If the application exists within the VTScada directory, a relative path to the application is listed; however, if the application exists outside the VTScada directory, and absolute path (including the drive letter) is given (e.g. the last application in the example above has an absolute path, indicating that this application directory exists outside the VTScada installation or product directory).

Auto Start

Each variable in the [APPS] section is prefaced by either a "0" or a "1", indicating whether the application is an auto start application; those applications prefaced by a "1" will start automatically when the VTScada program is run.

Setup.ini [LABELS] Section Variables

The [LABELS] section of the Setup.ini configuration file contains a list of variables that can be used to change the wording of dialogs, messages and text labels according to your needs.

This lengthy list of over 600 labels includes the labels that appear on buttons, as well as those that appear in message boxes and dialogs, and can easily be changed to suit the needs of your company. One such use would be to replace the labels with text in a language other than English. The list is displayed in alphabetical order and by topic, with error messages and dialog labels appearing at the end of the list.

Due to the large number of label settings that appear in Setup.ini, it is not practical to include them in this guide.

Setup.ini [LAYER] Section Variables

The [LAYER] section of the Setup.ini configuration file contains layer-specific, inheritable settings. It functions similarly to the "SYSTEM" section, with the major differences being that all layer settings are dynamic and

they are stored internally in the "LayerSettings" object within each layer. This means that unlike "SYSTEM", these values are properly inherited and available to each layer even when the application associated with the layer isn't running.

You can create application-specific overrides of add any of the following properties by adding them to your application's Settings.Dynamic file.

...AutoExportToUCDelay

...AutoExportToUserCopy

...AutomaticDeploy

...AutoRecover

...ConfigListBroadcastWait

...NolconFile

...RepositoryCommentDisable

...RepositoryCommentMinLen

...RepositoryShowCloneHistory

...ScriptIconFile

...SyncOEMLayers (links to the property found in Settings.Dynamic)

In VTScada version 11, SyncOEMLayers was added to Settings.Dynamic of the VTScada layer. Since that time, changes to SyncOEMLayers in the file Setup.INI have no effect.

...SyncServAuditDeferTime

...SyncServConnectTimeout

...SyncServSyncTimeout

AutoExportToUCDelay

Time period in seconds between a repository notification and a User Copy export. This delay reduces redundant exports.

Default: AutoExportToUCDelay = 1

Section: Layer

AutoExportToUserCopy

Toggles automatic export of application changes to the user copy

Default: AutoExportToUserCopy = 1

Section: Layer

AutomaticDeploy

All changes are automatically deployed when this flag is non-zero

Default: AutomaticDeploy = 1

Section: Layer

AutoRecover

Automatically reload Layer working copies from Repository if Layer did not stop safely.

Default: AutoRecover = 1

Section: Layer

ConfigListBroadcastWait

Time (in seconds) that a machine waits before sending directed notification of a change in the Configuration server list.

Default: ConfigListBroadcastWait = 10

Section: Layer

NolconFile

Icon to display in the Information panel when no icon is yet selected

Default: NolconFile = Resources\Icons\Nolcon.bmp

Section: Layer

RepositoryCommentDisable

TRUE to disable prompting for repository comments

Default: RepositoryCommentDisable = 0

Section: Layer

RepositoryCommentMinLen

Sets a minimum length for the user comments, stored with version changes, thereby enforcing the use of comments.

Default: RepositoryCommentMinLen =

Section: Layer

Related Information:

See: Commenting Changes in the VTScada Developer's Guide

RepositoryShowCloneHistory

TRUE enables showing version history for branches that existed prior to cloning an application

Default: RepositoryShowCloneHistory = 0

Section: Layer

ScriptIconFile

Icon to display in the VAM for script applications

Default: ScriptIconFile = Resources\Icons\Script.png

Section: Layer

SyncServAuditDeferTime

Time that a server will coalesce audit-only updates before sending them to clients

Default: SyncServAuditDeferTime = 10

Section: Layer

SyncServConnectTimeout

On Layer Activation, time that VTScada will wait for a client to acquire a connection to a server

Default: SyncServConnectTimeout = 10

Section: Layer

SyncServSyncTimeout

On Layer Activation, time that VTScada will wait for a client to finish synchronizing with a server

Default: SyncServSyncTimeout = 60

Section: Layer

Setup.ini [LINKTOLERANCE-...] Section Variables

In networked or remote situations, when two workstations connect, the response time from one workstation to the other can vary, partly due to CPU loading, but mostly due to link throughput limitations. The solution to this matter is to set up link tolerances for particular workstations so that other workstations can link them using the specified tolerance values, thereby solving the response time variance.

The purpose is to apply a safety factor to the RPC timeout values.

RPCResendDelay, RPCReconnectTime and RPCPingInterval all specify an amount of time to wait before assuming that there has been a communication error and taking action.

A "tolerance factor" is specified as a percentage value, applied to each of the three RPC properties listed above, on a workstation-by-workstation basis. A tolerance factor of "100" is unity, "300" is 3 times the value, and "50" is half of the value. This enables the specification of a set of base and system default values and tolerances for each peer-to-peer connection that requires them.

You ultimately have a series of choices in how you set up the link tolerance values for a particular workstation; in each of the instances described here, you must use "[LINKTOLERANCE-" followed by one of the suffixes in the following table:

Suffix	Description	Example
Workstation Name	Specify the name of the local workstation or a remote workstation (e.g. "FREDSPC").	[LINKTOLERANCE-FREDSPC]
Workstation IP	Specify the IP address of the local workstation or a remote workstation (e.g. "192.168.5.50").	[LINKTOLERANCE-198.168.5.50]

Note: Having stated that it is possible to use IPs, it should be noted that we strongly recommend that you use workstation names over IP addresses wherever possible, especially in networks where the workstations may be dual-homed, or where dynamic IPs are assigned. This will help to avoid any miscommunication that could occur in the event that an IP is reassigned to a third workstation while transmissions between two workstations are in progress. Since workstation names are unique, it is good practice to condition yourself to use workstation names, rather than IP addresses, even if your system configuration does not require the use of workstation names.

Once you've established the [LINKTOLERANCE-...] section for a given workstation, you can list the names or IPs of the workstations that will connect to this workstation, followed by the specific link tolerance value each workstation listed should use. Further, you can specify a default tolerance for all workstations (not otherwise specified) to use when connecting to this workstation.

Example:

```
[LINKTOLERANCE-JOESPC]
Default = 200
[LINKTOLERANCE-FREDSPC]
TARASPC = 300
Default = 150
BILLSPC = 100
```

This example will cause workstation JOESPC to have a 200% tolerance of all workstations connected to it. FREDSPC will have a 300% tolerance of workstation TARASPC, a 100% tolerance of BILLSPC, and a 150% tolerance of all other workstations.

To resolve ambiguity and provide flexibility, each workstation uses a set of methods and rules to extract the tolerance variable from the Setup.ini file when a connection is established. For further information on these methods and rules, link tolerances, and RPC, see "Link Tolerances".

Setup.ini [OEM] Section Variables

The [OEM] section of the Setup.ini configuration file contains variables that can be used by an original equipment manufacturer (OEM), or

system integrator to customize the VTScada software for their company. The following is a complete list of variables belonging to the Setup.ini configuration file's [OEM] section.

- ... HideVAM
- ... HideWAM
- ... NoSplash
- ... OEMHelp
- ... OEMPath
- ... OEMRestrict
- ... OEMVersionNum

HideVAM

Indicates whether the VTScada Application Manager (VAM) is displayed when the VTScada program runs. At least one application must be set to auto-run in order for this variable to take effect.

Note: HideWAM has been replaced by HideVAM. HideWAM will still work in Setup.INI, but is checked only on startup, at which time its value is used to set the newer HideVAM. Run-time code that needs to hide the VAM must use HideVAM instead of HideWAM.

If set to 0 (false), the VAM is not hidden and is displayed when VTScada is run.

If set to 1 (true), the VAM is hidden when VTScada is run.

Default: HideVAM = 0

HideWAM

Indicates whether the VTScada Application Manager (VAM) is displayed when the VTScada program runs. At least one application must be set to auto-run in order for this variable to take effect.

Note: HideWAM has been replaced by HideVAM. HideWAM will still work in Setup.INI, but is checked only on startup, at which time its

value is used to set the newer HideVAM. Run-time code that needs to hide the VAM must use HideVAM instead of HideWAM.

If set to 0 (false), the VAM is not hidden and is displayed when VTScada is run.

If set to 1 (true), the VAM is hidden when VTScada is run.

Default: HideWAM = 0

NoSplash

When set to TRUE (1) the initial splash screen animation will not run when VTScada starts.

Default: NoSplash = 0

OEMHelp

Indicates the name of a custom Windows help file (.hlp or .chm file) to display for your custom applications.

This help file is launched from the VAM's Help button when "All" or the name of a custom application is selected in the VAM's Application Type drop-down list. If "Standard Application" or "Script Application" is selected in the Application Type drop-down list, the Help button accesses the default VTScada help guides.

Default: OEMHelp =

OEMPath

Enables you to indicate a customized application to be displayed in the VTScada Application Manager's Application Types drop-down list when VTScada runs. This application will also be selected in the Type field of the New Application Properties dialog that opens when you choose to create a new VTScada application, so that the new application is based on your custom OEM application layer.

Related Variables: You must also set the OEMRestrict variable in order for the OEMPath variable to take effect.

Default: OEMPath =

OEMRestrict

Enables you to set VTScada to restrict the creation of new applications to a customized application type as specified in the OEMPath variable (see above).

If set to 0 (false), then users are not restricted to creating new applications of the type specified in the OEMPath variable.

If set to 1 (true), the users are restricted to creating new applications of the type specified in the OEMPath variable.

Default: OEMRestrict = 0

OEMVersionNum

Enter a version number for your customized VTScada version. This version number is displayed in the About VTScada dialog that opens when the VTScada Application Manager's About VTScada button is clicked.

Default: OEMVersionNum = Invalid

Setup.ini [REMOTE] Section Variables

The Setup.ini [REMOTE] section variables apply to the VTScada Internet server. The server enables remote access to applications using the Internet.

Related Information:

... ClientCabPath

...HTTPServerMaxHeaderLength

...HTTPServerMaxHeaders

... HTTPServerThreads

... ManualVICServerLists

... RefreshRate

... VICMonitorLogFileName

ClientCabPath

Identifies the path to the VTSX.cab file on the VTScada server. This .cab file is automatically installed when you install the VTScada Browser Support component from the VTScada installation CD. By default, the path to the VTSX.cab file is "VTSX\Distribution\VTSX.cab".

It is unlikely that you will have occasion to change the path identified by ClientCabPath, unless you have a valid reason for storing the VTSX.cab file in a location other than its installation location.

Default: ClientCabPath = vtsx/distribution/vtsx.cab

HTTPServerMaxHeaderLength

Limits the amount of work that will be done on malformed (possibly malicious) HTTP request headers. Use this property to set the maximum number of characters (including the terminating CR/LF) in a header line. Any request in excess of this limit will be met with error response 413.

Default: HTTPServerMaxHeaderLength = 8192

Section: Remote

Related Information:

...HTTPServerMaxHeaders

HTTPServerMaxHeaders

Limits the amount of work that will be done on malformed (possibly malicious) HTTP request headers. Use this property to set the maximum number of headers that will be permitted in a request. Any request in excess of this limit will be met with error response 413.

Default: HTTPServerMaxHeaders = 100

Section: Remote

Related Information:

...HTTPServerMaxHeaderLength

HTTPServerThreads

The HTTPServerThreads variable enables you to configure the number of consecutive threads that may run simultaneously without interfering with one another.

Default: HTTPServerThreads = 10

ManualVICServerLists

Enables manual configuration of each server within a VTS/IS cluster. Set to 1 to switch from automatic configuration of all servers to manual configuration of individual servers.

Default: ManualVICServerLists =

See also: Browsing VTScada Applications on the Web.

RefreshRate

Enables you to designate how often (in seconds) the list of applications will automatically refresh following an AppsList request.

Entering a value of 0 indicates that the AppsList display will not be refreshed.

Default: RefreshRate = 60

VICMonitorLogFileName

Sets the name of the file to which the VTScada Internet Client Monitor application will save log information.

Default: VICMonitorLogFileName = VICMonitorLog.txt

Setup.ini [RPCManager-AllowIP] Section Variables

If present, then only the IP addresses listed will be permitted to connect to this machine, and this machine will only issue connection attempts to the IP addresses listed.

Note: If this section is present and empty, no RPC connections are attempted or permitted.

The [RPCManager-AllowIP] section is evaluated before the [RPCManager-ExcludeIP] section (see following topic), therefore, any IP addresses found in the Exclude section will only have effect if they are also in the Allow section – in effect, first being permitted, then finally, being denied. The effect of the AllowIP section is to provide security by only permitting connections to and from a set of known (static) IP addresses. This also provides the benefit of allowing you to exclude connections between a development system and a live system.

Example:

```
[RPCManager-AllowIP]  
IP = 192.168.0.150
```

Setup.ini [RPCManager-ExcludeIP] Section Variables

As described in RAS Clients (see "RAS Clients"), from VTS 5.1502 onwards, a workstation running VTScada can accommodate RAS clients on any subnet, including one already used by a LAN connection. You can achieve this by adding an [RPCMANAGER-EXCLUDEIP] section to Setup.ini, and instructing the RPC Manager via this section to not create a connection to specific IP. This is not intended to be used as a security feature, but rather to block fruitless connection attempts by the RPCManager on IP addresses that should not or cannot be reached. By specifying the IP that the RAS host presents as its own IP to the RAS client, the RAS client will not create a connection to the RAS host IP, but will only connect to the other IPs by which the host workstation is known. For example, if a workstation running VTScada had an IP of 192.168.0.40, and that workstation was configured to support a RAS client, such that the RAS client would see the host workstation as 192.168.0.150, and the RAS client would be assigned an IP address from a pool of addresses from the range of 192.168.0.151 to 192.168.0.155, then the following section should appear in the RAS client's Setup.ini file, so that the RAS client will only make a connection to 192.168.0.40 (which will be done over the RAS link), and not to 192.168.0.150:

```
[RPCMANAGER-EXCLUDEIP]  
IP = 192.168.0.150
```

Note that this is not necessary if the RAS IP address pool is on a different subnet from any other IP of the RAS host, so long as no routing exists between the two subnets.

From VTScada version 5.18 onwards, it is not necessary to exclude any IP addresses on the server; however, if the IP cannot be accessed by a connecting client VTScada system, it is advisable to exclude it from the RPC Manager's view using the method exemplified above.

Setup.ini [RPCMANAGER-NETPRIORITY] Section Variables

In multi-homed situations, RPC Manager will help with communications where multiple network interfaces appear on a workstation.

You can configure the RPC Manager to use the available networks in two ways:

- Prioritized; or
- Round-robin.

These two methods can be described as follows:

Prioritized

The available networks are arranged in an order of priority. The RPC Manager always uses the highest priority available network for transmission.

Round-robin

All network interfaces are treated equally, and RPC Manager traffic is sent using each interface in turn. This method could be used to improve the tolerance of the distributed system for network failures, and is the default behavior.

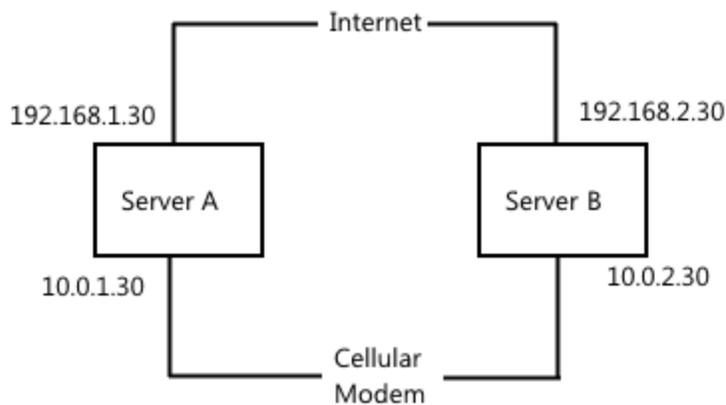
The above two methods can be combined where there are two or more networks, such that some of the networks can be prioritized and the others left as round-robin. RPC Manager traffic will always be sent over the prioritized network first, using the remaining two networks in round-robin mode if the prioritized network link to a workstation fails.

To establish the prioritized mode, you can enter the a subnet mask identifying the subnet that the remote machine is on for each network that the local server should communicate with in order of priority, using CIDR notation as follows:

```
<IP address>/<number of bits specifying the subnet mask>
```

Where, the number of bits specified is applied to the IP address from the most significant end. A mask value of 24 specifies the first three numeric parts of the IP address (8-bits per number) and is otherwise equivalent to a subnet mask of 255.255.255.0. A mask of 16, the first two numeric parts (subnet mask 255.255.0.0), and so forth.

For example, you have two routes of communication between Server A and Server B as shown.



You would prefer to have traffic use the Internet routing when available, in order to reduce communication costs.

On Server A, configure the Setup.INI file as follows:

```
[RPCManager-NetPriority]
IP = 192.168.2.0/24
```

On Server B, configure the Setup.INI file as follows:

```
[RPCManager-NetPriority]
IP = 192.168.1.0/24
```

This example specifies that for Server A, IPs on subnet 192.168.2 are to be given priority over IPs to the same workstation on all other subnets.

Likewise, for Server B, IPs on subnet 192.168.1 are to be given priority over IPs to the same workstation on all other subnets.

If an IP on the preferred subnet becomes unusable, any available IPs on other subnets will have RPCs transmitted to them in round-robin fashion.

For further information on these methods and multi-homed systems and RPC, see "Multi-homed Systems".

Setup.ini [SYSTEM] Section Variables

The following variables are set in the [SYSTEM] section of the Setup.ini configuration file.

Related Information:

- ... AccountsChangeDlgWait
- ... ActivateProgressDelay
- ...AutoLogon
- ... CompileProgressDelay
- ... ConvertProgressDelay
- ... DbTraceDaysToPreserve
- ... DbTraceFileSize
- ...DialogServiceFailoutTime
- ... ErrorLogFileName
- ...HelpServerPath
- ...HTTPAllow
- ...HTTPODeny
- ...LowBatteryPercent
- ...LowBatteryTime
- ...MinAltIDLength
- ...MobileSlippyMapTilesSource1
- ...OrderlyShutdown

... PrintWidth
...QuickAddTypeGUID
... ReloadWCProgressDelay
...RepoClashWait
...RPC Manager Properties
...ShutdownOnLowBattery
...SlippyMapRemoteTileSource1
... TagNameDelimiter
... UseXPCompatibleFont
... VICAutoAddDebugTools

AccountsChangeDlgWait

If the user doesn't respond to an accounts modify (from file change) check within this many seconds the original accounts file is retained.
Default: AccountsChangeDlgWait = 60

ActivateProgressDelay

Suppress activation progress dialog for this many seconds
Default: ActivateProgressDelay = 0.5

AutoLogon

Format: AutoLogon_<Realm> = <u>:<p>

Where "AutoLogon_", "=", and ":" are literal, <Realm> is the name of the realm for which you wish to create an autologon, <u> is the username, and <p> is the password.

Example:

```
AutoLogon_MyRealm = Guest:GuestPass
```

Enables you to create a predefined user account for a specific realm to allow guests to automatically logon without entering a username and password. You may configure multiple realms with auto logons by listing them on separate lines in Setup.INI's [SYSTEM] section (e.g. AutoLogon_

MyFirstRealm = Guest:GuestPass, AutoLogon_MySecondRealm = Demo:Enter).

If a namespace delimiter is used (see: Realm Area Filtering), the username defined in the AutoLogon_<Realm> = <u>:<p> setting MUST NOT include the realm. For example, if the username is Demo.Guest, enter AutoLogon_Demo = Guest:Pass, NOT AutoLogon_Demo = Demo.Guest:Pass.

Note: Warning: Use of this Setup.ini variable will allow users to bypass the Enter Network Password dialog that requests a username and password before allowing the user to logon. It is intended only for closed intranet use where VIC security is not an issue, or for demonstration purposes only.

CompileProgressDelay

Suppress compilation progress dialog for this many seconds
Default: CompileProgressDelay = 1

ConvertProgressDelay

Suppress conversion progress dialog for this many seconds
Default: ConvertProgressDelay = 0.5

DbTraceDaysToPreserve

Enables you to set the number of days that a trace file will be kept for use by the Trace Viewer application, after which the trace file will be deleted.

Default: DbTraceDaysToPreserve = 30

DbTraceFileSize

Enables you to set the maximum number of records to be stored in a single trace file (for use by the Trace Viewer application).

Default: DbTraceFileSize = 40000

DialogServiceFailoutTime

If VTScada is running as a service it will wait this many seconds for an undisplayable user query before defaulting the result. It will attempt to display the query on a VIC if one is available.

Default: DialogServiceFailoutTime = 10

Section: System

EnableShowHide

When set to TRUE(1), all application entries in the VAM will have a Toggle Visibility icon. While this property will normally be set from within an individual application's Edit Properties dialog, it does affect all applications

Default: EnableShowHide = 0

Section: System

Related properties:

...LogOffUponHide

...DispMgrHidden

ErrorLogFileName

Name of the file used to log error information

Default: ErrorLogFileName = Errors.log

HelpServerPath

Indicates the URL for the location of the web server to enable you to access help files for VTScada Internet Clients. When a VIC user presses the "F1" key on their keyboard, if the required help file is not present on the user's workstation, VIC will automatically request the help file from the location specified by the HelpServerPath variable. If this variable is not defined, then the default value is used, resulting in VIC requesting

the help file from the VTScada HTTP server to which the user first connected.

The value for HelpServerPath should be set to an absolute URL, including the protocol prefix (e.g. `http://some.server.com/help/files`", "`https://some.server.com/help/files`"). VIC will then add the uppercase name of the required help file to the request (e.g. "DEVELOPERSGUIDE.CHM").

HTTPAllow

Use to permit a single IP address or a range of IP addresses using the CIDR format. Other than using a range, you cannot define multiple addresses.

If HTTPDeny is also set, then note that rules set using HTTPDeny take precedence over HTTPAllow.

Allowing a single address:

```
HTTPAllow = 192.168.1.32
```

Allowing a range of addresses:

```
HTTPAllow = 192.168.1.0/24
```

Default: No default.

Section: System

HTTPDeny

Use to deny access to a single IP address or a range of IP addresses using the CIDR format. Other than using a range, you cannot define multiple addresses.

If HTTPAllow is also set, then note that rules set using HTTPDeny take precedence over HTTPAllow.

Deny a single address:

```
HTTPDeny = 192.168.1.32
```

Denying a range of addresses:

```
HTTPDeny = 192.168.1.0/24
```

Default: No default.

Section: System

LogOffUponHide

Used only when EnableShowHide has been set to TRUE (1).

When LogOffUponHide is TRUE (1 – the default), users will be logged off automatically when the application is hidden. The default setting is recommended for most situations.

Default: LogOffUponHide = 1

Section: System

Related properties:

...EnableShowHide

...DispMgrHidden

LowBatteryPercent

Used by the OrderlyShutdown feature. Sets the threshold for the percentage of battery power remaining, below which VTScada will undergo an orderly, automatic shutdown.

VTScada monitors the Windows provided GetSystemPowerStatus API call to obtain the status of the system power supply. The status indicates whether the system is running on AC or DC power, whether the battery is charging, and how much battery life remains.

Any UPS driver that provides updates to Window's view of the power state of the system should work with this in-built ability.

Default: 10

See Also: ShutdownOnLowBattery, LowBatteryTime, OrderlyShutdown

LowBatteryTime

Used by the OrderlyShutdown feature. Sets the threshold for the estimated number of minutes of remaining battery power remaining, below which VTScada will undergo an orderly, automatic shutdown.

VTScada monitors the Windows provided `GetSystemPowerStatus` API call to obtain the status of the system power supply. The status indicates whether the system is running on AC or DC power, whether the battery is charging, and how much battery life remains.

Any UPS driver that provides updates to Window's view of the power state of the system should work with this in-built ability.

Default: 15

See Also: `ShutdownOnLowBattery`, `LowBatteryPercent`, `OrderlyShutdown`

MinAltIDLength

Sets the minimum number of characters required for an alternate ID value. Defaults to four if not otherwise set.

Note: Trihedral Engineering strongly discourages any reduction in the number of characters required for identification. Any reduction in the number of possible combinations makes it easier for an attacker to compromise your system.

Default: `MinAltIDLength = 4`

Section: System

MobileSlippyMapTilesSource1

May be used to specify an alternate source for map tiles to be used by the mobile browser interface. You might choose the default,

`http://c.tile.openstreetmap.org/`, or you may create your own cache of map tiles and pull tiles from there. (e.g.

`http://www.MySite.Com/MyTilesFolder`)

Default: `MobileSlippyMapTilesSource1 =`

OrderlyShutdown

Enables VTScada to do an automatic shutdown if it detects that the work-station is relying on a UPS power supply that is failing. Detection uses one of the three related variables: `ShutdownOnLowBattery`, `LowBatteryPercent` or `LowBatteryTime`.

VTScada monitors the Windows provided GetSystemPowerStatus API call to obtain the status of the system power supply. The status indicates whether the system is running on AC or DC power, whether the battery is charging, and how much battery life remains.

Any UPS driver that provides updates to Window's view of the power state of the system should work with this in-built ability.

Default: OrderlyShutdown = 1

PrintWidth

Enables you to set the width of Alarm page and Operator Notes printouts. Measured in printed characters.

Default: PrintWidth = 80

QuickAddTypeGUID

When creating an application with the Quick Add function, the application will be based on the OEM layer with this GUID.

Defaults to the current GUID of the VTScada layer.

Section: System

ReloadWCProgressDelay

Suppress working copy reload progress dialog for this many seconds

Default: ReloadWCProgressDelay = 0.5

RememberLoginDuration

Sets the maximum length of time for which the Anywhere client logon credentials will be stored when the Remember Me option is selected during connection. Units are minutes.

Default: RememberLoginDuration = 20160

Section: System

RepoClashWait

Time (in seconds) that Repository Clash dialog will be displayed before the layer is automatically reloaded.

Default: RepoClashWait = 300

Section: System

RPC Manager Properties

The following Setup.INI properties are documented within the RPC Manager chapter of the VTScada Programmer's Guide.

...RPCBufferLength – This is the maximum TCP/IP buffer length to use for RX and TX buffers.

...RPCConnectPort – The TCP/IP port that RPC Manager tries to connect to.

...RPCMaxPacketSize – Specifies the maximum size of an encoded remote procedure call before the call will be fragmented over a number of transmissions.

...RPCMaxStartDelay – Controls startup behavior if the workstation name is not valid.

...RPCPingInterval – Specifies the time that a socket can have no data transmitted before a "ping" packet will be sent to all the receiving end to determine that the socket is still good.

...RPCReconnectTime – Specifies the seconds to wait for data on a socket before disconnecting the socket.

...RPCResendDelay – Specifies the time to wait for an acknowledgment after sending a packet before resending the packet

...RPCSktConnectAttemptMax – Specifies the number of attempts to open a socket before it is declared to be closed.

...RPCSktResendAttempts – Specifies the maximum number of attempts to send an RPC packet.

...RPCServerPort – The TCP/IP port that RPC Manager "listens" on.

...RPCSocketDeadTime – Specifies the number of seconds that a session will remain alive with no socket connection.

...RPCSocketResendAttempts – Specifies the number of packet re-sends that will occur without acknowledgment, before the socket is closed.

...RPCTrace– Set to a non-zero value to log all RPC activity to the disk file "RPCTRACE.TXT", in the VTScada installation directory.

...RPCUseBuffered – When non-zero this will cause RPC to read the TCP/IP IP and Name once only from the low-level socket stream and cache this information.

ShutdownOnLowBattery

Used by the OrderlyShutdown feature. Monitors a status parameter for the battery and enables VTScada to do an automatic shutdown if it detects that the battery state has reached the defined "Low" level. VTScada monitors the Windows provided GetSystemPowerStatus API call to obtain the status of the system power supply. The status indicates whether the system is running on AC or DC power, whether the battery is charging, and how much battery life remains.

Any UPS driver that provides updates to Window's view of the power state of the system should work with this in-built ability.

Default: ShutdownOnLowBattery = 0

See Also: OrderlyShutdown, LowBatteryPercent, LowBatteryTime

SlippyMapRemoteTileSource1

Sets the URL, from which Site Map tiles are loaded. Defaults to:
SlippyMapRemoteTileSource1 = <http://c.tile.openstreetmap.org/> // © [OpenStreetMap Contributors] (www.openstreetmap.org/copyright).

TagNameDelimiter

Sets the closing delimiter to be used for the short name (display name) of tags. May be changed to an alternative character if a legacy application is to be used in the current version of VTScada and tags in that application used the "]" as part of their name..

Default: TagNameDelimiter =]

UseXPCompatibleFont

Obsolete.

Solved the problem of text clipping when a VTScada Internet Server is using VTScada 10 or later and the VIC is using an older version of windows than the VTScada Internet Server computer.

VICAutoAddDebugTools

Indicates whether or not VTScada system tools (such as the Source Debugger, Profiler, etc.) should be accessible from VICs.

If set to 1, the VTScada system tools will be accessible by VIC users (default).

Default: VICAutoAddDebugTools = 1

Setup.ini [Themes] Section Variables

The color themes available to the VAM are defined in this section of Setup.INI. Each takes the following form:

Theme = ThemeName, Hue, Saturation, Brightness, Contrast

For example:

```
[Themes]
Theme = Grey,0,0,1.1,1
Theme = Navy,-15,2,0.7,1
Theme = Burgundy,110,2,0.5,1
```

Setup.ini [TRACE] Section Variables

The following list identifies a number of Setup.ini variables that are used for the purposes of tracing data transmissions of a variety of different VTScada services.

Note: The following variables can be set using the Trace VTScada Actions utility, which enables you to trace VTS' actions to a text file.

Related Information:

... TraceBrowser

... TraceCM

... TraceDispMgr

... TraceDlg
... TraceELM
... TraceMenuEd
... TraceModem
... TraceNav
... TracePageMgr
... TracePLimit
... TraceRamRecs
... TraceRPC
... TraceSQL
... TraceSS
... TraceTagCfg
... TraceToFile
... TraceTool
... TraceUserConfigActions
... TraceVAM

TraceBrowser

Indicates whether or not to trace the Tag Browser.
If set to 1 (true), the Tag Browser is traced (default).
Default: TraceBrowser = 1

TraceCM

Trace Configuration Management actions (adds ReportError data to the trace)
Default: TraceCM = 1

TraceDispMgr

Indicates whether or not the Display Manager should be traced.
If set to 1 (true), the Display Manager is traced (default).

Default: TraceDispMgr = 1

TraceDlg

Indicates whether or not system dialogs (i.e. 4BtnDialog, ODBCErr, ErrList, Err Queue), should be traced.

If set to 1 (true), then system dialogs are traced (default).

Default: TraceDlg = 1

TraceELM

Indicates whether or not the Edit Lockout Manager service should be traced.

If set to 1 (true), then the Edit Lockout Manager is traced (default).

Default: TraceELM = 1

TraceMenuEd

Indicates whether or not the Menu Editor should be traced.

If set to 1 (true), then the Menu Editor should be traced (default).

Default: TraceMenuEd = 1

TraceModem

Indicates whether or not the Modem Manager service should be traced.

If set to 1 (true), then the Modem Manager should be traced (default).

Default: TraceModem = 1

TraceNav

Indicates whether or not the Navigator (shortcut menus) should be traced.

If set to 1 (true), the navigator is traced (default).

Default: TraceNav = 1

TracePageMgr

Indicates whether or not the Page Manager should be traced.

If set to 1 (true), then the Page Manager is traced (default).

Default: TracePageMgr = 1

TracePLimit

Indicates the maximum number of bytes of data saved for a traced module's parameter.

Default: TracePLimit = 256

TraceRamRecs

Indicates the number of trace records to store in RAM.

Default = 256

TraceRPC

Indicates whether or not the RPC Manager should be traced.

If set to 1 (true), then the RPC Manager is traced (default).

Default: TraceRPC = 1

TraceSQL

Indicates whether or not SQL calls should be traced.

If set to 1 (true), then SQL calls should be traced.

Default: TraceSQL = 0

TraceSS

Indicates whether or not startup synchronization should be traced.

If set to 1 (true), then startup synchronization should be traced.

Default: TraceSS = 1

TraceTagCfg

Indicates whether or not tag properties folders should be traced.

If set to 1 (true), then tag properties folders are traced (default).

Default: TraceTagCfg = 1

TraceToFile

Indicates whether or not to trace to file.

If set to 1 (true), then tracing data is saved to a text file named "VTSTrace.txt".

Default: TraceToFile = 0

TraceTool

Indicates whether or not tracing should be done for VTScada libraries, and drawing objects.

If set to 1 (true), then VTScada libraries, and drawing objects are traced (default).

Default: TraceTool = 1

TraceVAM

Indicates whether or not to trace the VTScada Application Manager (VAM).

If set to 1 (true), then the VAM is traced (default).

Default: TraceVAM = 1

Backups

Note: Warning: The use of imaging (cloning) software to restore a lost VTScada server can cause significant configuration damage, not just on the machine being restored, but on all machines in your VTScada network.

Trihedral strongly advises you to avoid using such software for your VTScada backups.

Your VTScada application and your application data should be considered separately when designing a backup system.

If your application runs on two or more workstations, where one is designated the primary server and one or more others are designated as backup servers, then your application and your logged data are automatically stored and updated on all configured servers continuously. If one server were to fail, install a replacement, do a Get From Workstation to load the application on it, and let VTScada synchronize the data from the current primary server. All of this can be done without interrupting the application. This is the most reliable method available for maintaining a backup of your logged data including operator notes and retained variables and is strongly recommended.

In this configuration, DO NOT use a copy or backup of the data directory to restore data to one server. Doing so will create a discontinuity between the computer that is being restored and the one(s) on which VTScada has been continuing to run. A ChangeSet should not be used to restore a single computer that is part of a VTScada network – always use Get From Workstation to obtain a current copy from another server instead.

DO NOT re-install VTScada and your application on a server using a backup created using imaging software.

If you are running VTScada on a single computer only, or if there is a chance that all servers could be lost in an event such as a fire, then you should do the following:

Create a full (standard) ChangeSet of your application on a regular basis and store that ChangeSet file in a secure location, preferably off-site. If you do not have a copy of the VTS or VTScada installation program, a copy matching your last version can be obtained from Trihedral. Snapshot ChangeSets are not suitable for this purpose.

Note: Warning: A ChangeSet should not be used to restore one workstation within a networked application.

Unless otherwise configured(*), VTScada stores logged data in a folder within your application. For example, if you have installed VTScada in the folder, C:\VTScada and are running an application named MyApp, then the history can be found in:

C:\VTScada\MyApp\Data\

Copy the Data folder and all of its sub-folders.

(*If you have configured your system to use a 3rd party database program for your logged data instead of the VTScada history system, follow the instructions in that program for creating and restoring backups.

Warning: If at all possible, VTScada should be stopped before the data folder backup is made. There are three reasons for this:

- Write-access to the files will be blocked while they are being copied, potentially resulting in the loss of data or damage to the integrity of the system.
- Since VTScada is continually writing data, the backup you create will be out of date by the time the process is complete. Worse, files copied earlier may be out of sync with files copied later during the backup.
- The backup process can be demanding on system resources, possibly interfering with normal VTScada operations.

Again, your best solution for maintaining a backup of the application and all data files is to have primary and backup VTScada servers.

Related information that you may need:

...ChangeSets – An Application in One File – A way to keep a copy of your application itself (excluding logged data).

...Cloning a VTScada Workstation

ChangeSets – An Application in One File

A ChangeSet file contains the instructions required to re-create an application. That is, the set of changes that went into making the application. Depending on how it was created, a ChangeSet may have the extension .ChangeSet, .Snapshot, or .Template. The extension makes it clear what type of ChangeSet you have, when viewed in a folder. In this chapter, all are referred to as "ChangeSets".

In general, ChangeSets are used to distribute new applications, distribute updates to an existing application, or add extra features to OEM layers. They can also be used to create a clone of an application, for purposes of experimentation or testing.

The details of what will happen in each case depend on the type of ChangeSet you use – standard or snapshot, and if snapshot, with or without source files. It also matters whether the application runs on one or multiple servers. An incorrect choice may have undesirable results. Templates are a distinct type of ChangeSet, used only to enhance an OEM layer. These will be discussed in a separate topic.

Important:

Note: ChangeSets do not include logged data or alarm history. The information in this chapter applies to only the application code, including tags, pages, custom drivers, etc.

Note: A ChangeSet is not a backup. (Although, in special circumstances, it may be used as part of a backup strategy.)

Note: ChangeSets do not include OEM layers. If your application was built on a layer other than VTScada, then for purposes of distribution, a separate ChangeSet must be created for that OEM application and distributed with your application's ChangeSet file.

Note: Excepting template ChangeSets, do not store ChangeSet files in the application directory.

Standard ChangeSets

These can include a full development history or just the history since a revision file was created. They are used for the following tasks:

- Initial installation of an application on a machine, but only if that workstation does not have a network connection to other workstations running that application.
- Applying changes to an existing application, where those changes were made on a workstation that does not have a network connection. Changes within the ChangeSet will be merged into the current version. Note that one application's ChangeSet cannot be applied to other applications, including clones of the original.
- Sending a copy of the application for technical support.
- Creating a clone (identical copy) of an application in order to test changes without harming the running application or accidentally distributing your test to other workstations.

The version history, stored in the ChangeSet, will not be visible unless you set the application property, `RepositoryShowCloneHistory` to 1. This property must be part of the section, "Layer" rather than "System".

- Application recovery, using a recently created ChangeSet. You might choose to create a standard ChangeSet on a regular basis as part of a disaster recovery plan. If the application is still running on another server, do not use a ChangeSet to restore the lost workstation. Use "Get from workstation" instead. Remember that data is not included in a ChangeSet and must be managed separately.

Limited ChangeSets and Revision Files

When sending updates for a larger application, it can become cumbersome to include the entire version history with each new update. You can limit a ChangeSet to include only the changes that are not already present on the target machine.

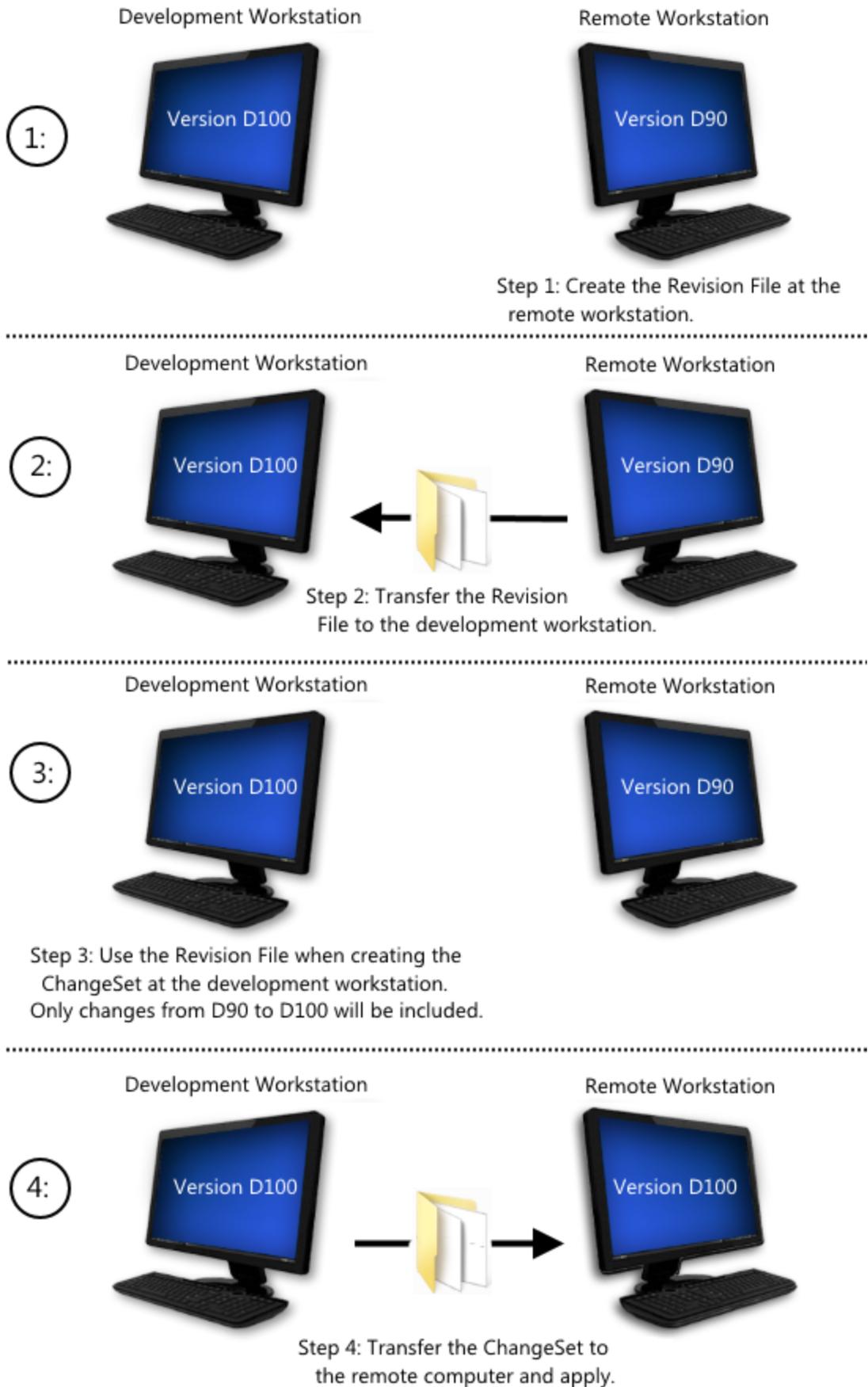
Note: Revision files will typically be created on the workstation that the ChangeSet is destined for, not on the machine where the ChangeSet is being created. The point is to find out what's already at the destination

before creating the set of changes required to bring that workstation up to date.

Note: Another use is to create a revision file immediately after creating each ChangeSet. (Both are created on the same machine.) When the time comes to send updates to the remote machine, you can use the revision file dating from the last ChangeSet in order to include and send only changes made since the previous update.

VTScada will compare the version information of the remote computer, as contained within the revision file, to the local version log to choose what new revisions need to be included in the ChangeSet being created. As a best practice, you should obtain an updated revision file from the remote computer immediately before generating a ChangeSet destined for that computer. The following example illustrates the process, where changes need to be transferred from a development workstation to a remote workstation. The steps would be the same, but on opposite computers if the transfer needed to go the other direction.

ChangeSets – An Application in One File



Snapshots

These do not include version history. They hold only the current state of development of the application. Snapshots may or may not include source files, according to your choice. If source files are not included, it will not be possible to edit the pages, widgets or other components on the workstation where the Snapshot is installed.

Note: When a Snapshot is applied to an application, it replaces the current version of the application, rather than being merged into it. Local changes will be lost.

Snapshots are used for the following:

- Installation of OEM layers, where the development work that went into that layer is proprietary knowledge.
- Installation of applications on workstations that are licensed as run-time only.
- Distribute changes to an application on a run-only workstation.
If local changes exist, they will be lost when the snapshot is applied. This includes operational changes such as disabled alarms.
- Return an application to a earlier state.
In general, it is better to use the Version Control system for this purpose.
Do not use a ChangeSet for this purpose if your application runs on multiple servers. Damage to the application on all servers may result.

Before using ChangeSets, you should understand the VTScada Distributed Version Control system and how changes are deployed. If Auto-Deploy has been disabled on your workstation while making the changes that are included in the ChangeSet, then when applied to the destination computer, those changes will exist only in a local branch. Auto-Deploy relates to changes made to the application, not to the making of the ChangeSet.

If you switch Auto-Deploy off just before making the ChangeSet, the changes made while Auto-Deploy was on will be included and deployed at the destination. On the other hand, deployed changes within the ChangeSet will be deployed on the destination workstation, regardless of whether Auto-Deploy is Off or On at that workstation.



You can install a ChangeSet by double-clicking the file on your desktop or in Windows Explorer™. If VTScada is not running, it will start.

Note that ChangeSets have a distinctive icon to help you distinguish these files from the shortcut to the VTScada executable file.

Related Information:

...See also: "Version Control" in the VTScada Developer's Guide

Related Tasks:

...Create a ChangeSet File – Steps to create.

...Apply a ChangeSet File – Transfer configuration changes between workstations when you don't have a network.

...Create a Template ChangeSet – Predefined settings and other components in OEM layers.

Create a ChangeSet File

Note: When sending an update to a remote computer for a larger application, it may be helpful to limit the size of the ChangeSet by including only revisions that are not on the remote computer. To do so, generate a revision file on the remote computer, and send that file for use when generating ChangeSet . This applies only to standard ChangeSets, being used to update remote workstations.

Note: ChangeSets do not include OEM layers. If your application is based on an OEM layer, you must create a ChangeSet for that as well.

Note: Do not store ChangeSet files in the application directory. (With the exception of OEM Template ChangeSets.)

To create a standard or snapshot ChangeSet:

1. Open the Application Configuration dialog to the Create ChangeSet File page.

2. Select the type of ChangeSet to create.
If creating a snapshot ChangeSet, choose whether or not to include source files.
3. Click, Create.
A dialog box will open, prompting you for a file name. You can also select the directory where the ChangeSet will be stored. The extension ".change-set", ".snapshot" or ".template" will be added to whatever file name you provide.
4. Type a file name for the ChangeSet.
5. Click OK.

Optional step:

If you intend to send further updates to a remote workstation, you may wish to create a revision file on the same machine immediately after creating the ChangeSet. This can be used when generating the next ChangeSet to ensure that it includes only changes made since the previous one.

Next Steps:

...Apply a ChangeSet File – Transfer configuration changes between workstations when you don't have a network.

Apply a ChangeSet File

Use the Apply ChangeSet page of the Application Configuration dialog when you want to import changes from another workstation that is running the same application, and is not visible via a network connection.

Note: You cannot apply a ChangeSet file from one application to another.

Configuration privileges are required in order to apply a ChangeSet to a secured application.

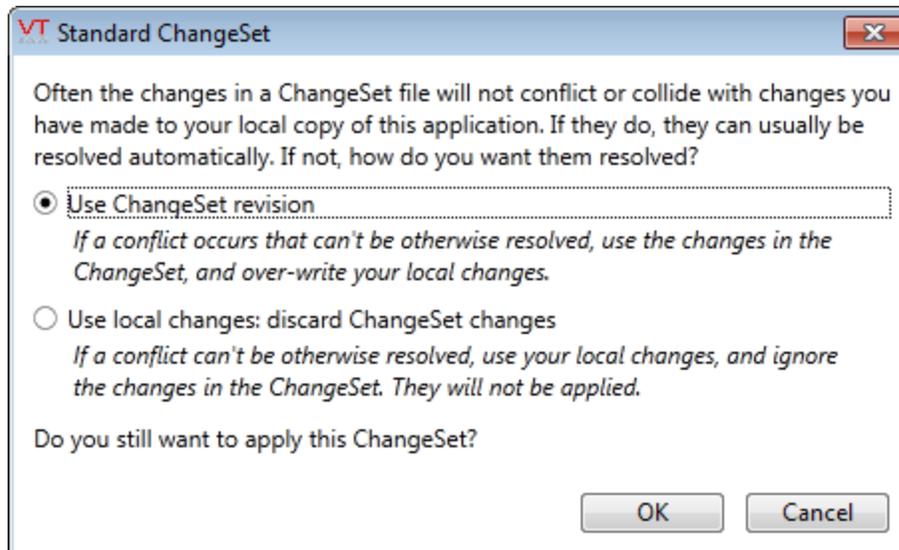
If the ChangeSet is standard, then its contents will be merged into the application. If snapshot, then it will replace the application.

Do not attempt to apply a snapshot that does not include source files to an application that does.

It is possible that the changes coming from the ChangeSet may conflict with changes that have been made to the application on this machine. The Apply ChangeSet menu enables you to choose in advance, whether to use or discard the ChangeSet file's version in the event of a conflict.

The steps to apply a ChangeSet file are:

1. Open the Application Configuration dialog.
2. Select the Apply ChangeSet File option from the menu.
3. Click on the Select button
A browse window will open, allowing you to find and select the .ChangeSet file.
4. Select the file and click Open
A dialog will prompt you to confirm that you wish to apply the changes.



5. Click "Yes"
The changes will be applied.

In the event of a conflict between versions, an error message will tell you which version was used and which ignored.

Related Information:

...See: "Distribute OEM Layer Updates" in the VTScada Developer's Guide

Create a Template ChangeSet

Template ChangeSets are very seldom required in the current version of VTScada.

If you have a legacy OEM layer that made use of this technology, please consult with Trihedral Technical Support. It is likely that newer options exist, which will allow you to move away from the use of a Template ChangeSet.

The steps to create a Template ChangeSet are complex and may vary depending on your application. Please consult Trihedral Technical Support before attempting to use this feature.

Related Information:

...Layers – Describes OEM layers including inheritance of objects across layers.

...Maintain the File Manifest – Manage the files that are considered part of the application.

...See also: "ChangeSets – An Application in One File" in the VTScada Developer's Guide

File Management Tools

A VTScada application is stored in a set of files within a folder. The details for all of your pages, tags, configuration settings, etc. can be found here.

If your VTS license is for a run time only release and does not include configuration options, then only the run time version of your application files will have been distributed to you. These cannot be viewed or edited. If you have a configuration license for your VTScada installation, you will be able to review pages and configuration settings directly in files, and may perform configuration by editing those files.

VTScada is able to detect when files of the recognized types have been added, removed or edited in the application folder. These will be flagged, but not used until an authorized person uses either the Import File Changes button or the Import/Export Files dialog.

Note: VTScada makes a distinction between "user files" – those that can be read by humans, "working files" – compiled versions of the user files, and "repository files" – working files that are part of the version control system. Work only with the user files. Any attempt to modify a working file or repository file will either be ignored, or cause irreparable damage to your application.

Related Tasks:

...Maintain the File Manifest – Control the set of files that is under version control.

...Import/Export Files – Review changed and added files, choosing whether to import or discard on a file by file basis.

...Import File Changes – Import File Changes – Import changed files and re-compile the application with one click, without review.

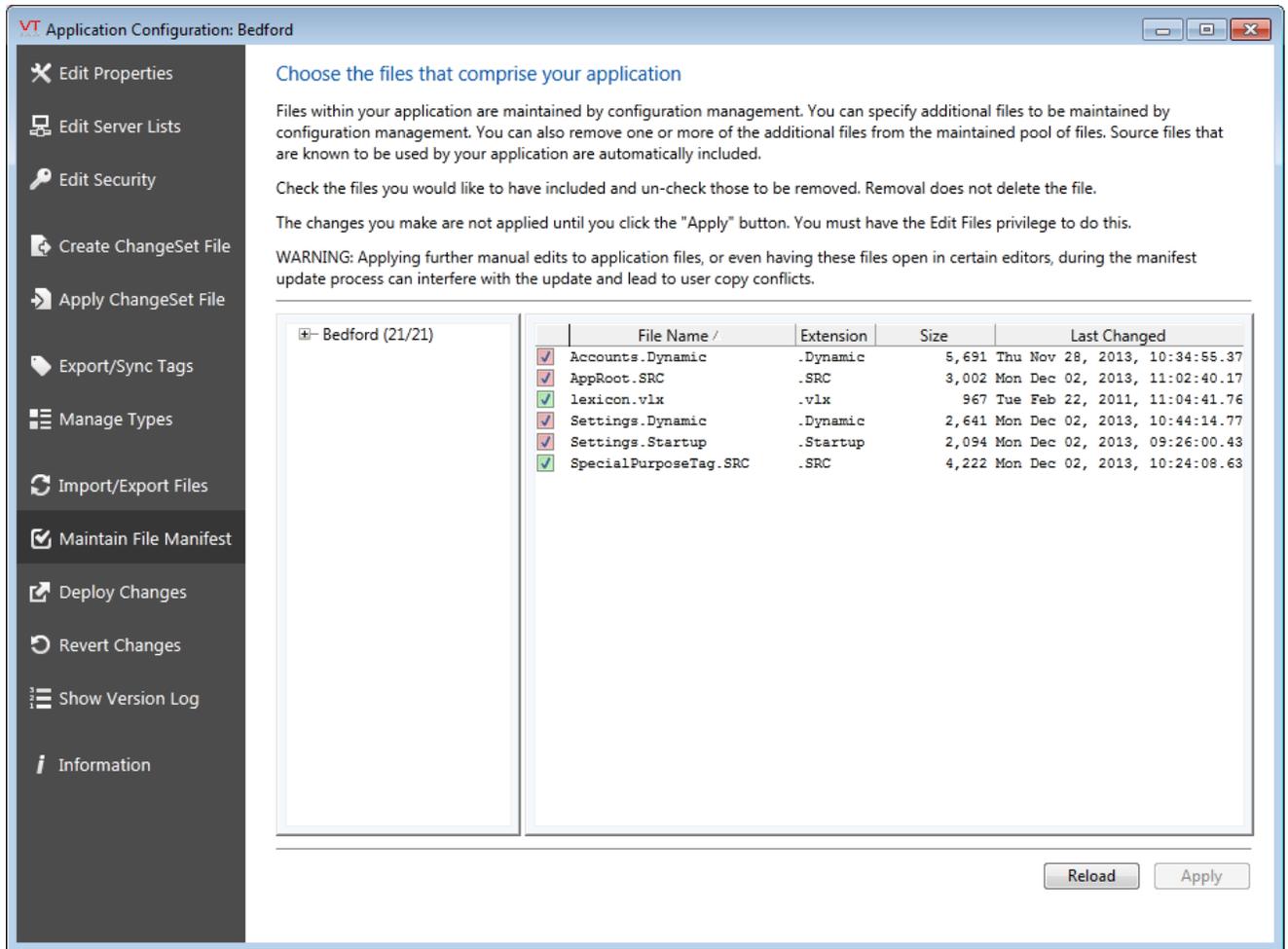
Maintain the File Manifest

The File Manifest, a page of the Application Configuration dialog, lists those user files that are monitored and maintained by the VTScada version control system. You may wish to add files to the list if they should be distributed with the application and maintained under change-control. You may also wish to remove files from the list, although in the case of the VTScada-created files this is usually not advised. Files that you can remove are marked with green. Certain VTScada files cannot be removed from version control and are indicated by red check boxes.

The File Manifest will not include empty files.

Note: Removing a file from version control does not delete the file. A file that has been marked to be ignored must be added back in using the Maintain File Manifest tool before it will be recognized by the Import/Export Files page.

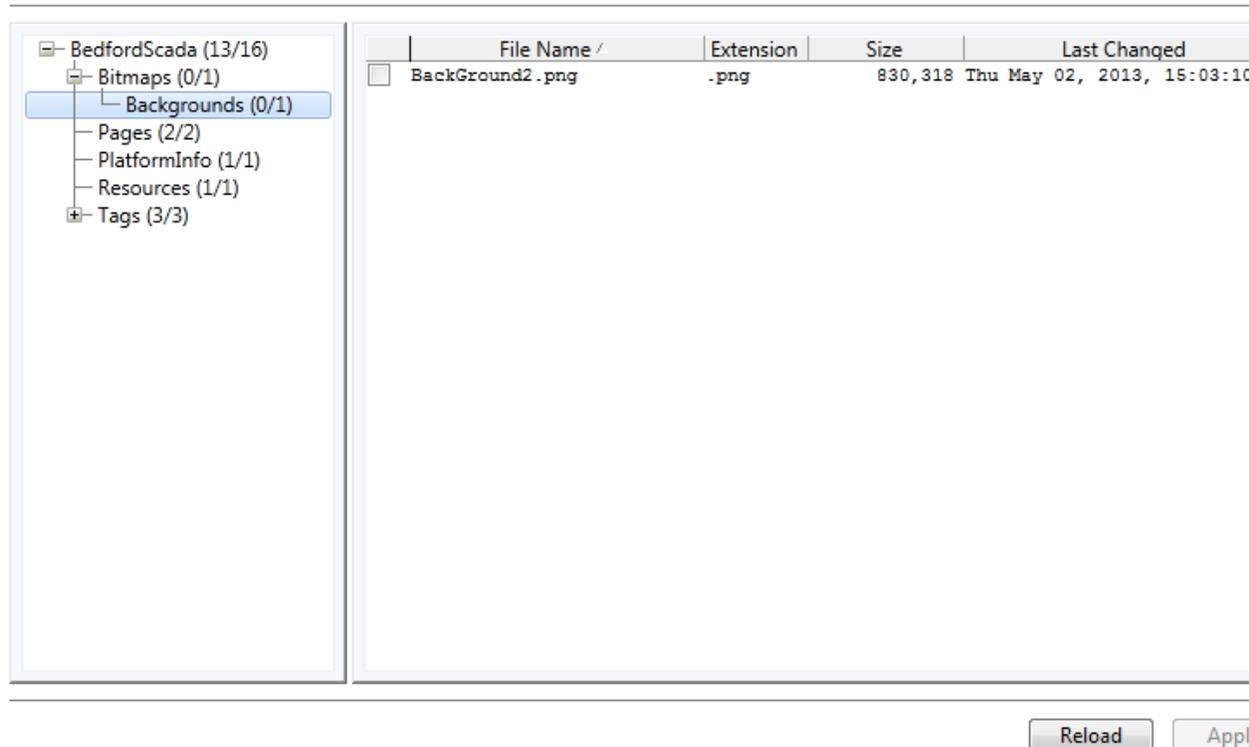
Ensure that files are not open in an editor before applying changes made using the File Manifest. Failure to follow this rule may result in version control conflicts.



Add a new file to your application using the File Manifest:

In this example, a new background image is copied to the Bit-maps\Backgrounds folder of the application. It will be ignored by VTScada until made a part of the application, as follows:

1. Open the Application Configuration dialog.
2. Click Maintain File Manifest.
3. Expand the folder tree to view the contents of the Bitmaps\Backgrounds folder.



Note: If you copy or move files while this dialog is open, click Reload to refresh the display.

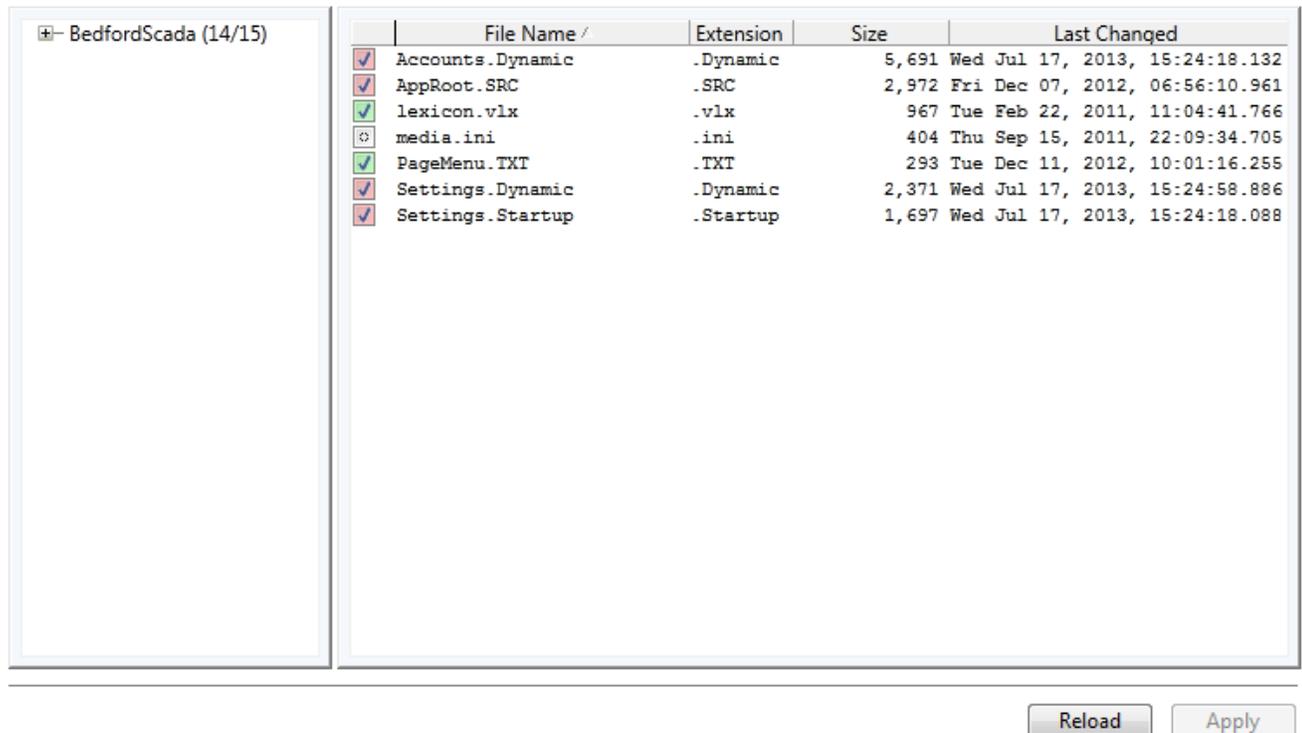
4. Click on the check box beside the name of the file that is to be added to version control.
5. Click Apply.
6. Provide a comment when prompted, and click OK.

The selected file(s) will now be considered part of the application. They will be subject to version control and will be included in a ChangeSet.

Remove a file using the File Manifest:

It may be that files that were useful during development, should not be included in a ChangeSet shipped to a customer. Remove them from the application (without also deleting them) as follows:

1. Open the Application Configuration dialog.
2. Click Maintain File Manifest.
3. Expand the folder tree if required to view the contents of folder where the file resides.



Note: If you copy or move files while this dialog is open, click Reload to refresh the display.

4. Click on the check box beside the name of the file that is to be removed from version control, thereby clearing the check mark.
5. Click Apply.
6. Provide a comment when prompted, and click OK.
The selected file(s) will no longer be considered part of the application. They will still exist in the application folder, but will not be included in a ChangeSet.

Troubleshooting:

- The file isn't shown in the File Manifest.
Empty files will be ignored by VTScada. Ensure that this file is not empty.
If the file was recently copied, click Reload to refresh the display.

Related Tasks:

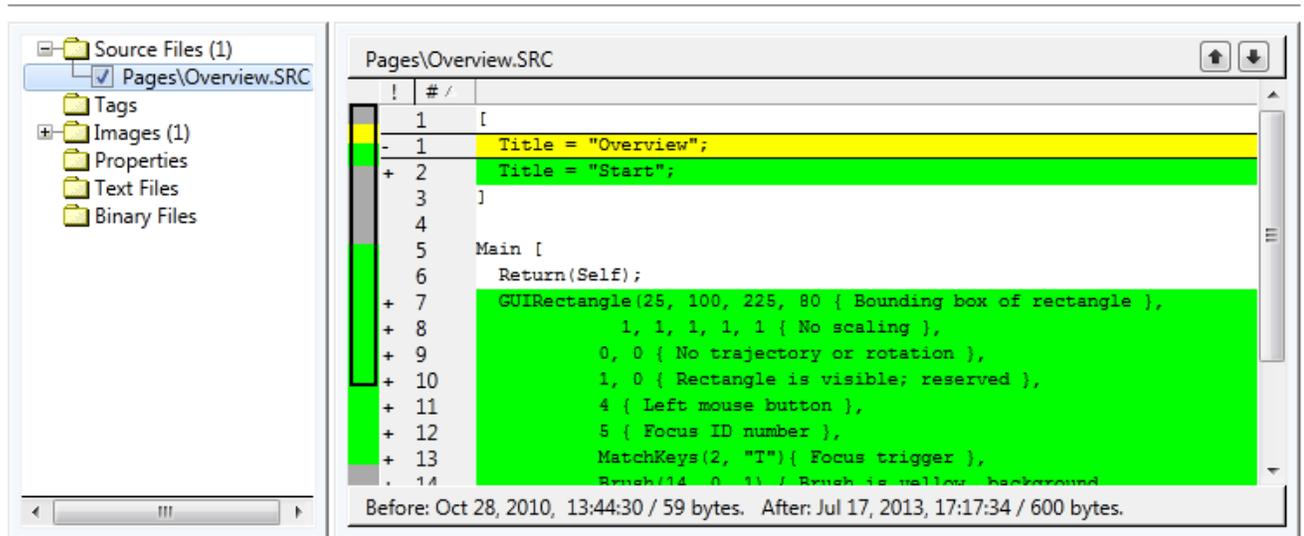
...Import/Export Files – Review changed and added files, choosing whether to import or discard on a file by file basis.

...Import File Changes – Import File Changes – Import changed files and re-compile the application with one click, without review.

Import/Export Files

Changes made outside of VTScada to the files that are part of your application will be ignored. An authorized operator (one who possesses the Configure and the Edit Files security privileges) must import the changed file before VTScada will use it.

For source code and text files, you may review the changes, line by line before importing them. The new version of the line (in the file to be imported) is marked in green and the old version (the current version in change control) is marked in yellow.

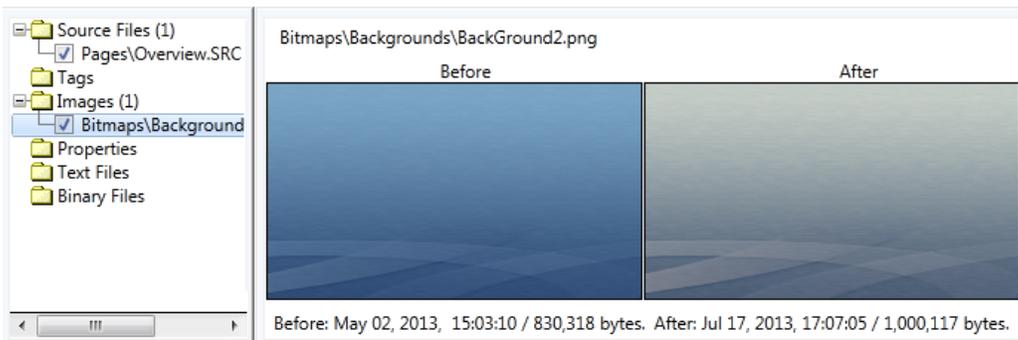


Select All Unselect All

Discard Import

Reload Export Latest

Image files are compared on a side-by-side basis.



Select All Unselect All

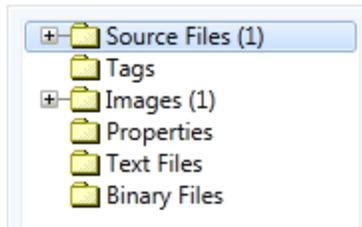
Discard Import

Reload Export Latest

Note: You should always review all the changes within a file before importing it into your application.

Review changes before importing:

1. Open the Application Configuration dialog.
2. Click Import/Export Files.
3. Look for categories of files with plus signs.

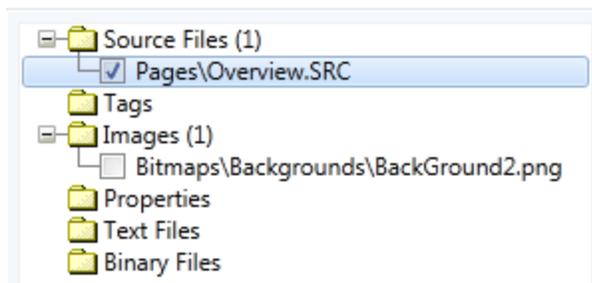


The plus sign and the number beside the category name indicate that changed files were found.

4. Expand the category to view the file(s).
5. Click on the name of a file to examine. Changes will be highlighted as shown at the beginning of this topic.

Import changed files:

Check marks beside the file names indicate which files will be included in this operation.



1. Open the Application Configuration dialog.
2. Click Import/Export Files.
3. Examine the changes within the files you intend to import.
4. Click to select each file to be imported. You may use Select All to speed this process.
Only files marked with a check will be imported.
5. Click Import.

Discard changes in files:

After reviewing changes, you may decide to not import them. In this case you may wish to replace the contents of the file with whatever is in use within your application.

1. Open the Application Configuration dialog.
2. Click Import/Export Files.
3. Click to select each file to be discarded. You may use Select All to speed this process.
Only files marked with a check will be discarded.
4. Click Discard
The file on disk will be replaced by the current version in the application's repository.

Export latest (VTScada changes to files):

Export Latest will merge changes from VTScada into the file on disk. In normal operation, this will be done automatically, but the button exists to allow you to force a merge.

The user copy file will not be overwritten by VTScada, but changes made in VTScada will be merged into that file. Changes within that file that have not yet been imported will be preserved. Conflicts will be reported on a line by line basis if they occur.

1. Open the Application Configuration dialog.
2. Click Import/Export Files.
3. Click to select each file to be discarded. You may use Select All to speed this process.
Only files marked with a check will be discarded.
4. Click Export Latest
The file on disk will be updated with current version in the application's repository.

Troubleshooting:

- Your edited file is not listed in the Import/Export files menu.
Ensure that edits have been saved.
Click Reload to refresh the display.
- An error message reports a conflict.

Review the conflict using the Version Log and a text editor. Depending on whether the changes in VTScada or in the file should have priority, you may edit the file to resolve conflicts, use the Import button, or use the Discard button.

Related Tasks:

...Maintain the File Manifest – Control the set of files that is under version control.

...Import File Changes – Import File Changes – Import changed files and re-compile the application with one click, without review.

Import File Changes

Clicking this button causes a series of events to occur in your application. Only operators who possess the Configure privilege and the Edit Files privilege may use this feature.



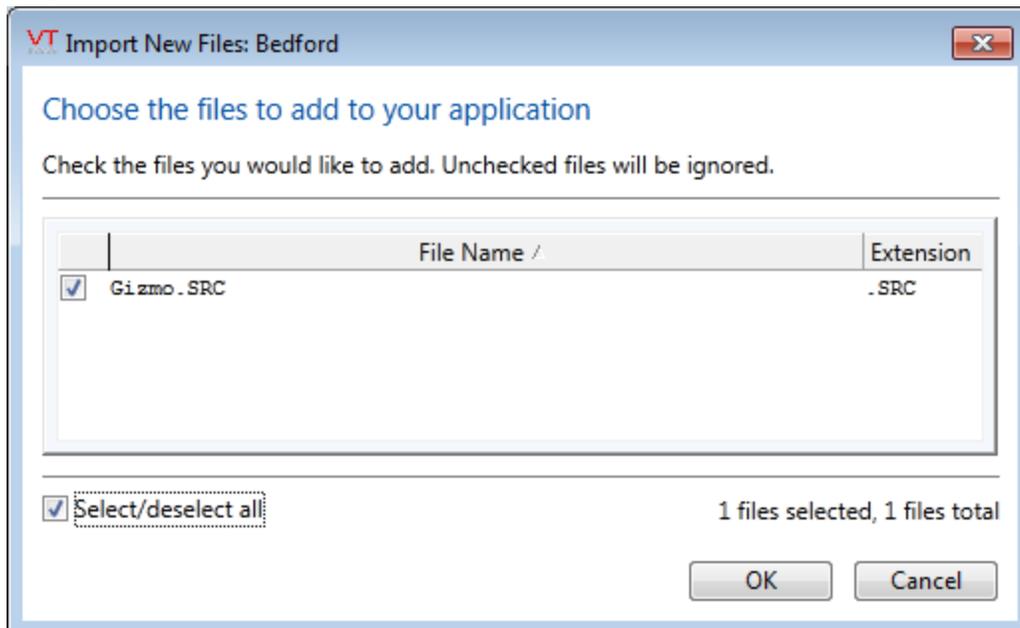
- a. The application will be activated if it is not already. This activates the version control system for the application.
- b. VTScada will scan for new files in your application folder and prompt you to confirm which ones you want to import (put under version control).
- c. All changes to files under version control will be imported. You will not be given a chance to review those changes.
- d. All source code will be recompiled if changes were found.
If no changes were found, and the application is not running, then you will have an opportunity to force a recompile. If the application is running, then the process ends with the "no changes detected" dialog.

The Import File Changes button provides a convenient method for developers who are working directly with source code files to import their changes. (Changes and additions to source code files are ignored

by VTScada until imported). Note however that the lack of an opportunity to review changes carries a certain degree of risk. If there is any chance that someone else may have edited the user files, then you are advised to use the Import/Export Files dialog, where changes may be reviewed before being imported.

Dialogs associated with the Import File Changes operation:

Import New Files

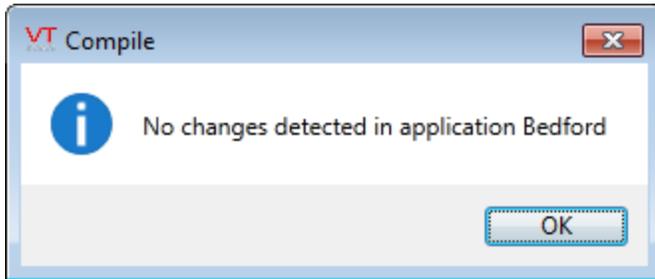


VTScada has found new files in application folder. All will be selected for inclusion if you click OK. You may choose to deselect any of the files before clicking OK, or you may click Cancel to abort the Import File Changes operation.

Note that all files that are deselected before you click OK to finish the Import File Changes operation will be added to VTScada's "ignore" list. If you click Import File Changes a second time, you will see the message, "No changes detected". There will not be a second opportunity to select the files using this button.

Use the File Manifest in the Application Configuration dialog if you wish to add those files to the application at a later time.

Compile – No changes detected



If you had expected changes, ensure that the files you edited were saved using their original names and folders. Files that were not imported the last time this button was clicked are now being ignored. You can use the File Manifest page of the Application Configuration menu to add them now.

Related Tasks:

...Maintain the File Manifest – Control the set of files that is under version control.

...Import/Export Files – Review changed and added files, choosing whether to import or discard on a file by file basis.

Monitor...

VTScada includes several tools designed to monitor both internal (VTScada) and external (hardware) processes and components.

Related Information:

...Monitor Internet Client Connections – Describes both the Internet Client Monitor application and the Internet Client Monitor page.

...Driver Statistics – Monitor device errors and messages.

...ODBC Statistics – Monitor statistics for your ODBC connection.

...Instance Count Application – See the VTScada Programmer's Guide. Count the instances (or copies) of modules that are running .

...Profiler Application – See the VTScada Programmer's Guide. Discover statements that are placing an excessive load on system resources.

...Trace Viewer Application – See the VTScada Programmer's Guide. Monitor the content and parameters of driver messages and VTS-related network traffic.

Monitor Internet Client Connections

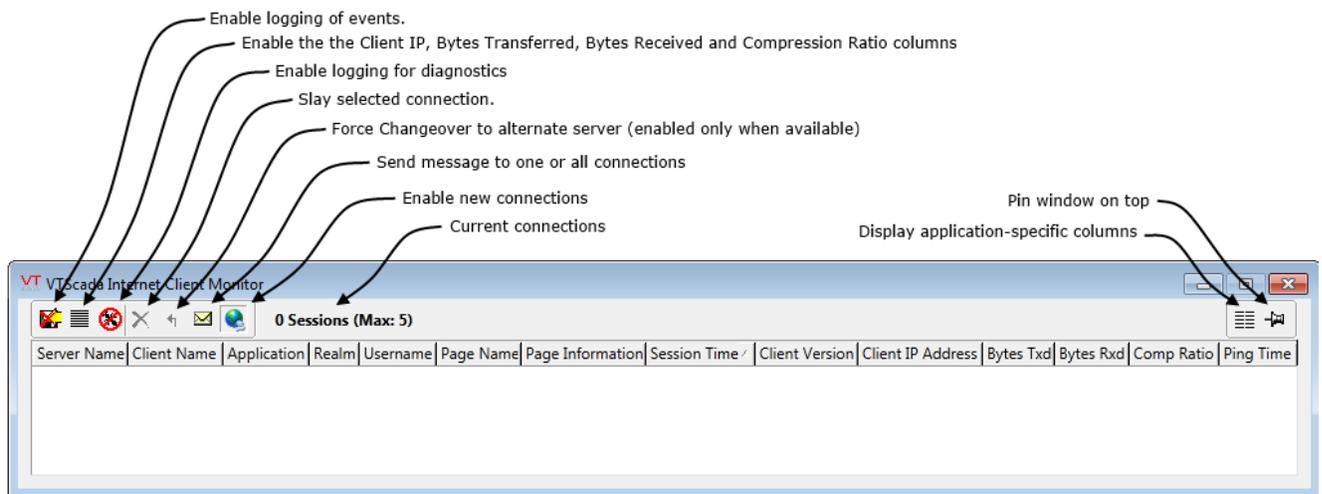
Use the Internet Client Monitor to view active connections, disable or enable access to an application, send messages and slay connections. Technical details for each connection are displayed, and options exist to log connections and to diagnose problems.

There are two versions of Internet Client Monitor. The first is a script application, accessible from the VAM. The second is a page that is a standard part of all new applications. (In applications that have were originally created in VTScada version 8.0 or before, you may add the Internet Client Monitor page to the menu.)

There are three differences in the feature set of these two applications:

Monitor...

- The application version will show all connections to all accessible applications. The page version will show only the connections to the application it is within.
- The application version has a "pin on top" button, to ensure that it is not hidden behind other windows.
- The application version includes three optional columns. VTScada programmers can create customized code to display extra information in these columns.



If the Internet Client Monitor application does not appear in the VAM, you may have to add it. The application directory for the Internet Client Monitor application is named "BrowserMon" and is stored in the VTScada installation directory.

All of the columns can be sorted in either ascending or descending order. Click on a column title to sort by that column – the first click will sort the rows in ascending order and the next will sort by descending order. An arrow will appear beside the column title to indicate the sort order.

Double-clicking on the edge of a column heading will cause the column to the left to re-size to match the data displayed within it.

Controls:

Button	Function
Logging	Enables VTS/IS event logging. The output file is stored in the

	VTScada installation directory as "VICMonitorLog.txt". This file contains the logged data as comma-separated values.
Detail	Controls whether or not information is displayed for the Client IP, Bytes Transferred, Bytes Received and Compression Ratio columns. By default, detail is not displayed.
Diagnostics	Turns on diagnostic logging for subsequent VIC connections. Should you experience problems with your VIC connections, this log may help engineers at Trihedral Engineering Ltd. discover the source. Details follow within this topic.
Slay Connection	Terminates the highlighted VIC session from the VTS/IS.
Force Changeover	Force VIC clients to disconnect from this server. If you have configured for Redundant VIC, the client will automatically connect to the next highest ranked available server as defined by the VTScada Internet Server List. An intended use for this button and the following one is to allow you to take the current server off-line for maintenance without interrupting any client sessions.
Send Message	Send a message to a selected connection, or to all connections.
Enable New Clients	Enable or disable new connections to this server. Note: Use of the Disable New Clients button while you are remotely connected is a risky thing to do. Should your own connection be broken before you have re-enable new client connections, you will have to travel to a VTScada workstation.
The following buttons are available only to the application version.	
Application Specific Columns	Available only to the script application. When selected, three more columns will be displayed, containing data that you program your application to show. The code required to populate these columns goes beyond the scope of the Developer's Manual.
On Top	Available only to the script application. The Pin button enables you to set the Internet Client Monitor on top of all other windows.

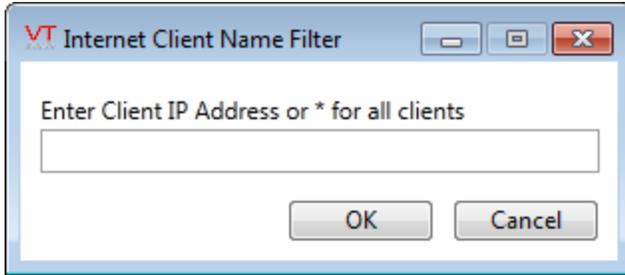
Columns

Server Name	Since the internet client monitor displays information from all servers in the VTS/IS cluster, it is important to know which server a particular client is connected to.
-------------	--

Monitor...

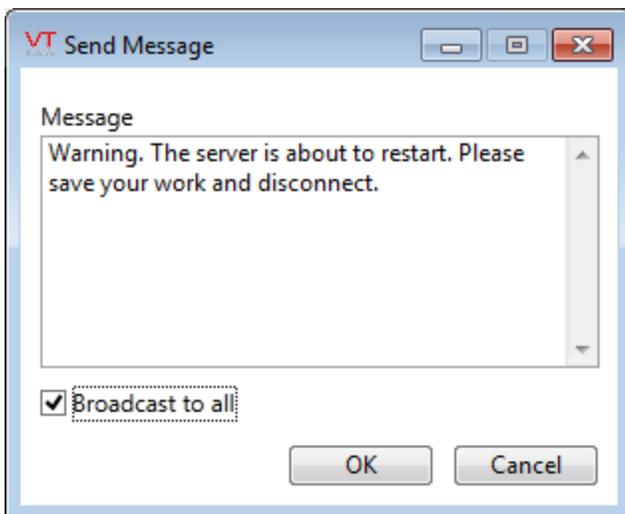
Client Version	Displays the version number of each ActiveX program each client is using to connect.
Client Name	The name of the computer that is viewing the application.
Application	The name of the VTScada application that is being viewed by each connection.
Realm	The name of the realm that each VIC is connected to.
UserName	The UserName column displays the name of the user account for each logged on user.
Page Name	The name of the page within the VTScada application that is being viewed (does not apply to script applications).
Page Information	Additional information about page may be displayed. The source of the information must be coded into the page by a developer. For example, if the client is viewing the Historical Data Viewer page, the Page Information column will show which named pen group is being viewed. Page information is stored into a variable named "VICMonitorPageInfo", which is updated in the page's main state.
Session Time	The length of time that the session has been connected.
Client IP Address	Displays the IP address corresponding to each connection. (Shown only when detail view is enabled)
Bytes Txd	The number of bytes transmitted from the server to the client. (Shown only when detail view is enabled)
Bytes Rxd	The number of bytes received by the server from the client. (Shown only when detail view is enabled)
Comp Ratio	The compression ratio (i.e. the percentage that data has been compressed). (Shown only when detail view is enabled)
Ping Time	An approximation of the time (in milliseconds) taken to communicate between the server and the client. (Shown only when detail view is enabled)

Clicking the Diagnostics button will cause the VTS Internet Client Name Filter dialog to open:



Enter an asterisk, * to enable logging for all clients. The log file will be named VTSDiag.TXT and will be saved to the connected user's My Documents directory.

The Send Message dialog:



Select a connection before clicking the Send Message button in order to send that message to only one connection. Check the Broadcast to all box to send the message to all connections.

Related Information:

...Data Logged by the Internet Client Monitor

Data Logged by the Internet Client Monitor

Only one log file will be maintained, regardless of how many backup servers have been configured. This file will be located on the current primary server.

If change-over occurs to another server, two messages will be recorded in the log: a Connection Closed message, followed by a Changeover mes-

sage. The log will not show which server the client is connected to (or was disconnected from in the event of a change-over).

The following is the information that can be found in the VICMonitorLog.txt file, stored in the VTScada installation folder.

- Time stamp, recorded as date and time.
- The action that initiated the event being logged. Some of the possible actions include:
 - Connection Opened
 - Connection Closed
 - VIC changed servers ("change-over")
 - Page Changed
 - User Changed
- GUID (Globally Unique Identifier) of the connection
- IP address of the connected client
- Number of bytes sent
- Number of bytes received
- Round trip time. The time required to send a packet of information from the server to the client and then receive a response packet back.
- Connected client's computer name
- The name of the application to which the client is connected
- The name of the realm to which the client is connected
- The name of the logged-in user
- The current page being displayed on the connection.

Driver Statistics

A widget named Show Stats (show statistics) exists for every driver. In addition, many drivers have a Show Comms (show communication messages) widget, which can be used to monitor live communications.

For any particular driver, please refer to the widgets that were designed specifically for it.

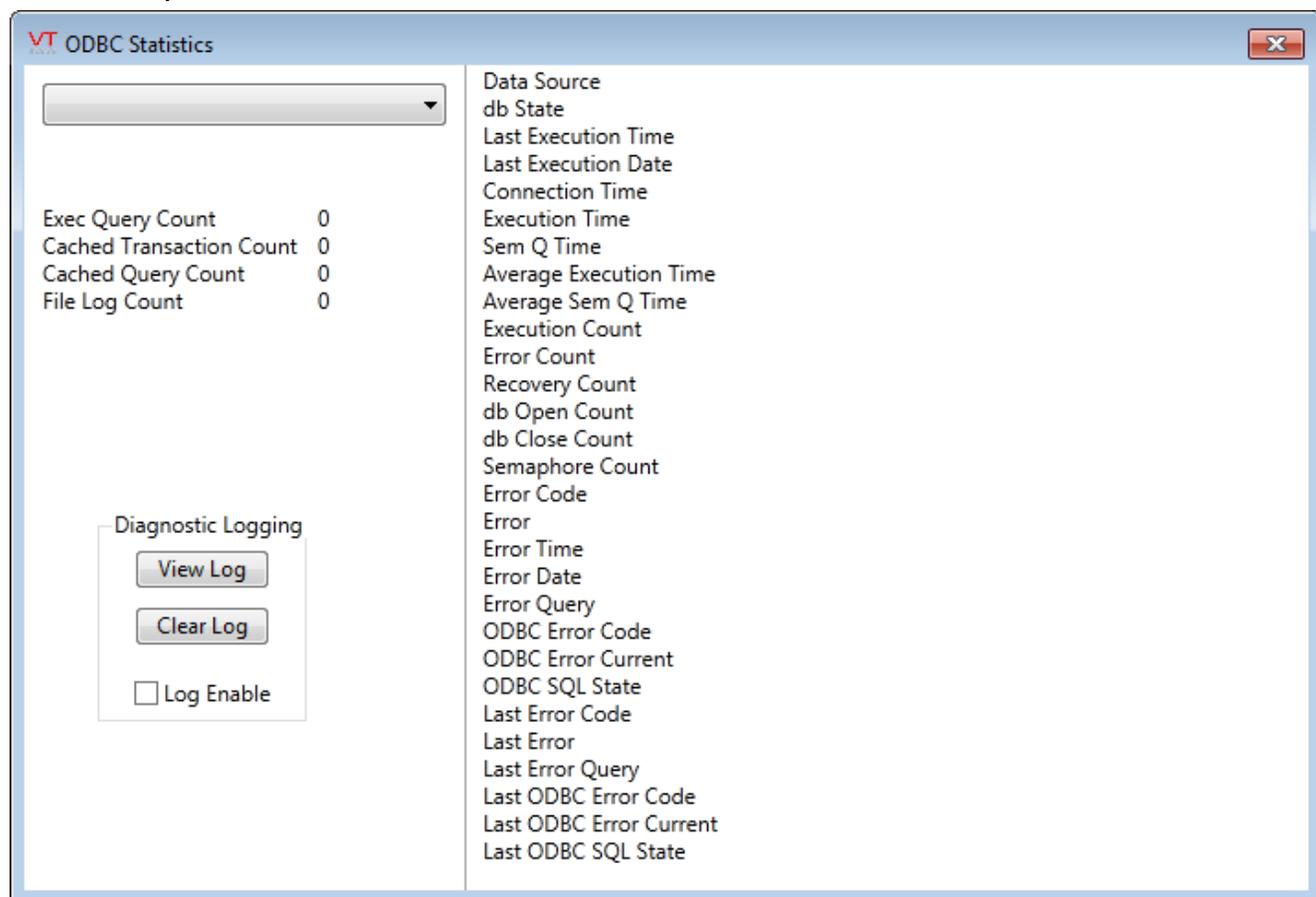
Related Information:

Further information can be found in the VTScada Developer's Guide – Communication Messages Dialog and Communication Statistics Dialog.

ODBC Statistics

Not linked to any tag.

The Show Stats widget for the ODBC manager provides a click-able button that operators can use to view connection statistics.

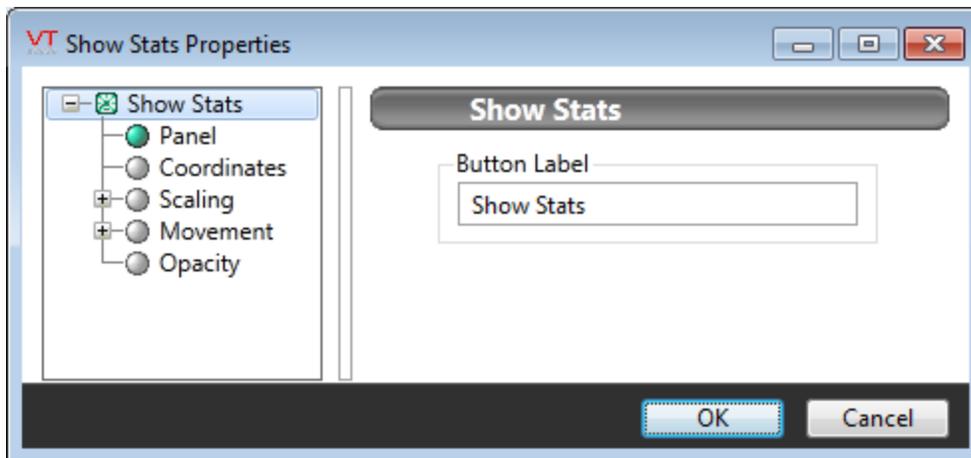


The drop-down menu will include a list of all ODBC connections used by this application.

Note that you cannot view a saved history of diagnostic information until you disable logging, using this dialog.

The properties dialog for the ODBC Manager Show Stats widget:

Monitor...



Button Label

You are advised to change the label to describe which statistics will be shown.

Secure Your Application

You can manage user accounts with either VTScada or Windows.

- If using VTScada authentication and authorization, all accounts and security privileges are managed within VTScada. The SCADA manager has full control over all aspects of each account.
- If using Windows authentication, VTScada privileges are assigned only to roles, which are then associated with Windows accounts. The Domain Administrator has control over creating and managing accounts, including which accounts are associated with which VTScada roles. The VTScada manager controls roles and the privilege set associated with each role.

The account and privilege system provides all the security required. If you enable outside connections to your SCADA system, using the VTScada Internet Server to allow **VIC**¹ or **MIC**² connections, then you must also take steps to secure the communication between the remote site and your server. This is done by implementing a Virtual Private Network (VPN) or by purchasing and installing an SSL Certificate.

Privileges built into VTScada can be used to restrict access to VTScada features such as the Alarm Page and the ability to add Page Notes. To control access to your own pages and to operator controls, then you must create new privileges and apply them to the features that are to have restricted access.

To simplify account management, roles are provided. A role is a named set of privileges and can be thought of as a job description. Any operator account may be assigned individual privileges, or it may be assigned one or more roles, thereby granting a set of privileges needed to perform a job function. Changes made to a role's privilege set are automatically applied to the operators who have been assigned to that role.

¹VTScada Internet Client. Allows you to connect to an application over the Internet with many of the features of a full VTScada workstation.

²Mobile Internet Client. Allows you to connect to a minimized version of the application, suitable for mobile devices.

Note: If realm area filtering is in effect, managers who members of a realm can see only those accounts and roles that are within the same realm.

It is normal practice to wait until you have finished designing and configuring your application before activating security.

Certain functions within the security manager are available to programmers, allowing them to check who is logged in or what privileges are in effect for the logged in user. With this information they can design their custom modules to enable or disable features for the logged-on user.

Note: The VTScada Internet Client, Anywhere Client, and the Mobile Browser Client cannot access any application that is running in an unsecured state.

Only a secured application will allow remote access and alarm acknowledgment via phone, email or text message, and then only to authorized accounts.

An application must be secured before you can make use of the ODBC interface to query the VTS database.

Terms:

System Privilege

A permission to access or use one of the VTScada system tools. Access to the Idea Studio, the ability to acknowledge alarms, etc., are controlled by system privileges.

Alternate ID

A numeric identification associated with an account. Used to verify an account when logging in via the Alarm Notification System, or a proximity card reader. There can be only one alternate ID associated with any account.

Application Privilege

A permission created by a VTScada developer. Application privileges can be applied to pages and to output tag widgets in order to restrict access to these user-created items.

Security Role

A named set of permissions. One or more security roles may be assigned to a user account in order to grant common privileges to people with similar job descriptions.

Security Rule

Any combination of the above that has been applied to a user. Security rules may be qualified by association with a tag or a workstation or both.

Related Information:

...Best Practices for Security – Essential tasks for securing your application.

...Windows Security Integration – Prerequisites and configuration steps.

...Accounts and Roles – Creating and managing.

...Proximity Card Readers – Configure alternate identification for accounts.

...Protect Pages and Output Tags – Create your own privileges for protection.

...Rules for Privilege Scope – Make privileges local rather than global across your application.

...Options for Security Settings – General Configuration

...Read-Only Workstations – Deny write access to equipment from designated stations.

...Technical Reference for Security – Privilege lists, features not covered by built-in privileges, configuration settings and storage.

...Realm Area Filtering, See the Developer's Guide. – Create user-groups. Control access to tag-lists and alarm information based on membership in a security group and the area property of tags.

Related Tasks:

...Activate Security

...Deactivate Security – Stop security checks, with or without removing accounts.

...Securing a VTScada Internet Server – Security when allowing remote connections.

...The following can be found in the VTScada Developer's Guide:

...Securing a VTScada Internet Server – Security when allowing remote connections.

...Locating the Security Dialogs – How to find and open the security tools.

...

...See also: Logon to Your Account in the VTScada Operator's Guide.

Best Practices for Security

- Design your pages and tag structures with security in mind.
You can save a large amount of work, and greatly reduce the number of application privileges you will need by creating a well-organized set of Roles and corresponding Rule Scopes.
- Enforce strong passwords.
Use the available options to enforce strong passwords (minimum length, combination of letters, numbers and other characters). Advise operators against re-using passwords for multiple applications.

- If there is ever a security update for your version of VTScada, apply it as soon as possible.
- Protect your control objects with application privileges so only designated operators may use them.
This will limit the number of operators who will have access to controls and pages.
- Place operator controls on pop-up pages.
By placing controls on a pop-up page, you reduce the chances of an operator accidentally issuing a control action. Also, since access to a pop-up page can be restricted using an application privilege, it is possible to restrict access to many output tags with one privilege on one page rather than many privileges on many tags.
- Use care when granting the Internet Client Access privilege and configuring a VTScada Internet Server.
VTScada cannot secure the networks between the remote client and the server.
VIC/MIC clients transmit the user logon credentials (username and password) using Basic Authentication, which is a simple non-encrypted Base 64 encoding of "username:password", and which is easily decoded by capturing network traffic.
It is essential that you use an SSL certificate to secure the communications from packet sniffing software connected to a local machine or switch. Do not overlook the possibility that attacks might originate from within your trusted network.
The use of a VPN is a reasonable second choice.
- If allowing internet client access, test the SSL connection using 3rd party tools, looking for weak ciphers, etc.
- Do not grant privileges to the Logged Off account. (Exceptions apply.)
Do not grant unnecessary privileges to any account or role.

- Configure the VAM to be hidden.
This can be done through a Setup.INI variable (see Configuring the VAM to be Hidden).
- Before running the Import File Changes tool in the VAM, review the list of changes that will be imported, using the Import/Export files tool of the Application Configuration dialog.
- Use Windows™ security techniques to prevent unauthorized persons from accessing the VTScada program directory. Keep the workstations that are running VTScada in a secure location.
All security measures are in vain if someone can destroy your application, simply by deleting files.

Windows Security Integration

You can choose to use Windows® security integration in place of, or in addition to, VTScada user accounts. The VTScada Security system has three basic elements: Accounts, Roles & Privileges. When using Windows Security Integration, accounts (users) are managed in Windows. The privileges that are related to VTScada functionality are managed within the VTScada Security Manager, via assignment to roles. Windows accounts are linked to VTScada roles using Active Directory Groups that are named for the VTScada roles.

Benefits and differences:

- External account control.
- Fewer passwords for users to remember.
- Privilege sets are created only for roles, which are then assigned to accounts. It is not possible to assign privileges directly to Windows-based accounts.
- Rule-Scope can be applied to privileges within a role, but not to roles assigned to accounts.

- Limited control over domain account configuration within VTScada. Passwords cannot be changed and privileges cannot be granted

When Windows Security Integration (WSI) is in effect, VTScada managers (accounts with both the Manager privilege and the Administrator privilege) retain responsibility for granting privileges to roles. They may also disable individual accounts and can set the automatic log-out time for each account.

Alternative ID values, for the Alarm Notification system and other purposes, are still controlled within the VTScada interface.

Using Both Windows and VTScada Authentication

It is possible to have both VTScada accounts and Windows accounts. Accounts that existed prior to the enabling of WSI will continue to exist, but it is expected that many sites will prefer to disable or delete some or all of those accounts. If there are users who should have access to the SCADA system but not have an account on the domain, they should be given a VTScada account within the application. This feature might be used to send out application ChangeSets to someone who is trusted to work on the application, but who will not be given access to the corporate network.

A feature of WSI is that authorized users may logon with their full account name (myname@company.com) or with their user name (myname). If that user name matches a valid VTScada account name, then it will be assumed that the user intends to logon with the VTScada account. A dialog will open during the logon process to remind you of this.

Related Tasks:

...Enable Windows® Authentication

Related Information:

...Windows Authentication Notes

Enable Windows® Authentication

All VTScada accounts will continue to exist when Windows Security Integration (WSI) has been enabled. You may choose to disable some or all local accounts in favor of domain accounts.

Windows security groups map to VTScada roles with the addition of "VTScada-" before the role name. Thus, the role "Operator" maps to the security group, "VTScada-Operator" and the role, "SuperUser" maps to the group, "VTScada-SuperUser".

The prefix "VTScada-" is stored in the application property, ADGroupPrefix, and may be changed if required. VTScada roles, including role names and assigned privilege sets, are under the control of anyone with the Manager security privilege.

Review the related notes before proceeding: [Windows Authentication Notes](#)

Preparation

1. Ensure that the VTScada workstation is running as a member of a Windows domain.
The "Enable Windows Security Integration" check box will be disabled if VTScada is started on a machine that is not a member of a Windows domain.
2. Ensure that you are a Windows Domain Administrator, or that you have access to one who is available to assist with certain steps in the following procedure.

Enable Windows Security Integration

1. Enable VTScada Security and create an account with the Manager and Administrator privileges.
2. You are advised to set up preliminary VTScada roles and application privileges at this time.
Windows accounts will be associated with VTScada roles as described above. New roles can be added, and privilege sets adjusted at any time.
3. Have your Windows Domain Administrator create security groups that are named for the roles in your application.

The Active Directory Security Group names should follow the form "VTScada-RoleName".

4. Ensure that your Windows user account is given membership in the appropriate Active Directory Security Groups from the previous step.
5. Decide whether to set the property AutoAddADUsers to be enabled. If enabled, domain accounts will be created within VTScada with each successful logon. If not enabled, you must create a domain account in VTScada, using the form "username@company.com" for each user.
6. Open the VTScada Administrative Settings dialog. ("Options" in the security menu.)
7. Select the option, Enable WSI.
8. Read, then acknowledge the warning.
9. Click, Apply.

Test by logging out, then log on using your Windows account and password.

Note: It is not possible to assign privileges or passwords to domain accounts. Privileges for these accounts are determined by their membership in domain groups, matching VTScada roles.

Troubleshooting:

- Unable to log on with your Windows account.
Ensure that your Windows account is associated with a Security Group, named correctly for the VTScada role.
You may need to allow the domain controllers several minutes for the change to propagate.
- Upon logging on with just your user name, you are now logged on with a VTScada account rather than your Windows account.
Both a Windows account and a VTScada account exist with a matching user name. If this is by intent, use care to log on with your full Windows account name, "User@company.com" when using your Windows account, and just "User" when using your VTScada account.

Related Information:

...Windows Authentication Notes

Windows Authentication Notes

- Authentication ensures that you are who you say you are.
- Authorization relates to the privileges accorded to your account, once authenticated.
- WSI = Windows Security Integration
- LDAP = Lightweight Directory Access Protocol
- AD = Active Directory
- SG = Security Group
- The prefix "VTScada-" is set by the property, ADGroupPrefix.

When enabled, VTScada uses Windows® Authentication services, which connect to the domain controllers over a secure channel. Windows Security Integration is enabled through the VTScada Security Manager's Administrative Settings dialog.

Once an account has been authenticated, the privileges accorded to that account are determined by its membership in Active Directory Security Groups that are named for VTScada roles. VTScada privileges are assigned to roles, not to domain accounts. The queries are performed using the default settings for the machine, which are set in the domain group policy.

Windows accounts that do not have membership in at least one of these security groups will not be able to log on to VTScada.

WSI mode uses the LDAP default naming context for the host machine as a basis for the AD account query operations. This is the LDAP equivalent of the domain to which the host machine is joined and thus does not support user accounts from a domain other than that of the host machine.

Upon logon, and at regular intervals while an account is logged on, VTScada will check that the domain account is still enabled and the list of active directory groups it is a member of, updating the logged-on account's privileges as needed.

Active Directory Security Groups

Active Directory Security Groups must be created by someone who has permission to modify AD security groups. To work with VTScada, these

must be named by prepending the letters "VTScada-" before the VTScada role name. For example, "VTScada-Operator" and "VTScada-Configurer". The prefix "VTScada-" is set in the application property, ADGroupPrefix. Role names are under the control of the VTScada manager, and so may vary from these examples.

Accounts are accorded privileges in VTScada according to their role (SG) membership. It is not possible to grant privileges to accounts directly. The title bar will display the Windows account "displayname" attribute rather than the Windows logon name, e.g. "Another User" rather than "another.user@company.com".

Running Multiple Applications

In the situation where two or more VTScada applications are running, it may be necessary to distinguish between them for logons. The recommended practice is to set a different ADPrefix value for each application. For example, if a site has both a water treatment application and a power generation application, then instead of using "VTScada-" for both, they might use "Power-" for one and "Water-" for the other. It would then be clear whether an account was a member of the "Power-Operators" security group, "Water-Operators" security group, or both.

Account caching

For accounts that have been added to the VTScada Security Manager, either automatically or manually, the VTScada host machine will cache Windows logon credentials (if permitted by AD Group Policy) such that if the machine is temporarily isolated from the domain, e.g. a laptop out in the field, then user logons will succeed for those logons that have been cached.

Account roles will not be updated when isolated from the domain.

Attempts to logon with an account that has not been cached on the host machine will fail.

Credentials are stored in a manner that meets current industry best practice.

You can configure the VTScada Security Manager to add Windows accounts automatically upon first successful log-on. By default, automatic storage is enabled. To change the configuration of automatic storage of domain accounts on, add the property, `AutoAddADUsers`, to the `<SecurityManager>` section of your application's `Settings.Dynamic` file. If Windows domain accounts are not being stored automatically, then a user with the Manager privilege must add accounts to VTScada individually.

When connected to the domain, the Security Manager's cached set of account rules are updated on each domain logon. A periodic check (default 15 minutes) is made to ensure that each logged-on Windows account is still enabled, updating its assigned roles if necessary.

Note: If the WSI option is deselected, cached domain users remain in the cache and may continue to logon using their domain accounts until those accounts are deleted from within VTScada.

Application Properties

The following privileges in `Settings.Dynamic` are used when Windows Authentication and Active Directory Authorization are in effect:

- `ADGroupPrefix` – The prefix to be added to a VTScada role name for the equivalent AD Security Group.
- `ADRefreshPeriod` – The interval in seconds between checks for changes to the logged on users account in Active Directory.
- `AutoAddADUsers` – Add and set `TRUE` if you want VTScada to automatically add domain accounts to the local cache upon successful logon. If a domain account is not cached in VTScada, logon is not possible when the workstation is disconnected from the domain.

Note: If using Windows Security Integration and Realm Area Filtering, you must add the realm name and prefix to the account using the VTScada accounts dialog. (e.g. `realm:username@company.com`) If a user needs multiple realm logons, they will require multiple Windows accounts.

VTScada as a Windows service

Windows Security Integration can be used when VTScada is run as a service, but the account that the service is run under must allow the COM operations required for the AD queries. The "Local Service" account may not have sufficient permissions. In most cases, the "Local System" account will.

Warning for Internet and Mobile Client Connections

VIC/MIC clients transmit the user logon credentials (username and password) using Basic Authentication, which is a simple, non-encrypted, Base 64 encoding of "username:password", and which can be decoded by network snooping tools if they can capture the message content. Wireshark as one example, will show the decoded credentials if it connected to a local machine or switch that performs the communications (Since switches don't broadcast network traffic for all to hear, the "listener" must be local to the communications path versus being anywhere on the network.) If Windows Security Integration mode is enabled, then the potential consequences will extend beyond the SCADA system should the operator's Windows credentials be stolen.

To secure user credentials against listeners that may have access to switches or workstations carrying this traffic, it is essential that you encrypt VIC/MIC sessions with SSL by installing an SSL certificate on the VTScada Internet server. The SSL certificate can be obtained from a 3rd party issuer such as Verisign, Thawte, GoDaddy, from an organization's own Certificate Authority (CA) infrastructure, or via local ad-hoc creation. (e.g. By using Open SSL tools.) To allow clients (browsers) to verify the certificate and not display an untrusted warning, they need the "root" certificate from the CA to be installed. The root certificate for most third-party issuers is already installed in most Web browsers.

VTScada maintains a salted, key-stretched, SHA2-512 hash of the Windows Logon password in the same manner as Security Manager logon passwords and this meets current industry best practice.

Related Tasks:

...Enable Windows® Authentication

Related Information:

...AutoAddADUsers

...ADGroupPrefix

...ADRefreshPeriod

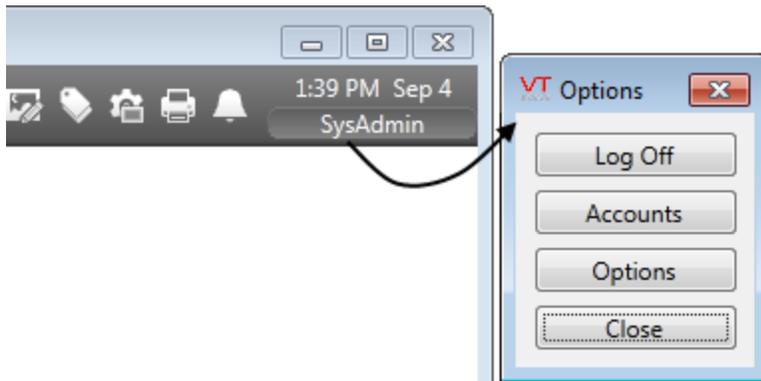
...VTScada as a Windows® Service

Locating the Security Dialogs

There are two methods by which you can access the security-related dialogs. Functionality will be almost the same⁽¹⁾ but, the appearance will differ slightly.

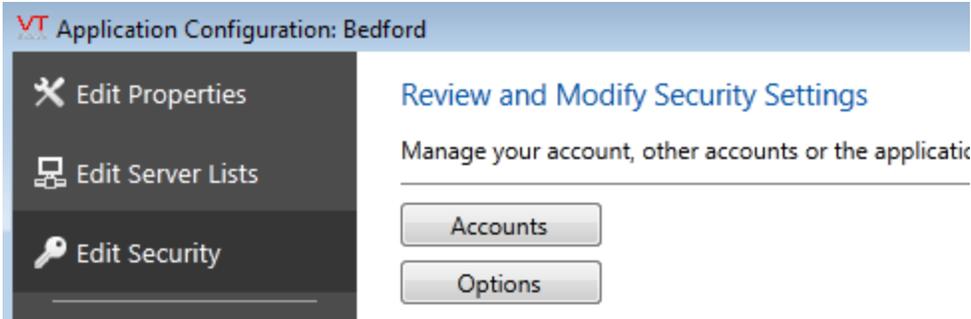
Within an application, click on the Logon button at the upper-right of the screen. After you have logged on, this button will display your user name, rather than the word, "Logon".

The examples within this chapter use this method to access VTScada's security features.



From the VTScada Application Manager (VAM), select the application and click on Properties.

In the Application Configuration dialog that opens, select the Security entry in the menu.



Not all users will see the same list of buttons. The "Options" button is available only to users who possess the Administrator privilege. The Accounts button will be available to a user who possesses any of Manager privilege, View Accounts privilege or Modify Accounts privilege, but what they can do within the Accounts dialog will vary depending on which privileges they possess.

Two buttons that do not appear in the Application Configuration dialog's version are "Log Out" and "Close". Both are relevant only within a running application, where they are available to all users.

⁽¹⁾There are two differences between these methods of accessing the security-related dialogs:

- The Application Configuration dialog may be used even when the application itself is not running.
- Tag and workstation-related security rules will not be available if the application is not running.

Related Information:

...Accounts and Roles – Creating and managing.

...Protect Pages and Output Tags – Create your own privileges for protection.

...Options for Security Settings – General Configuration

Related Tasks:

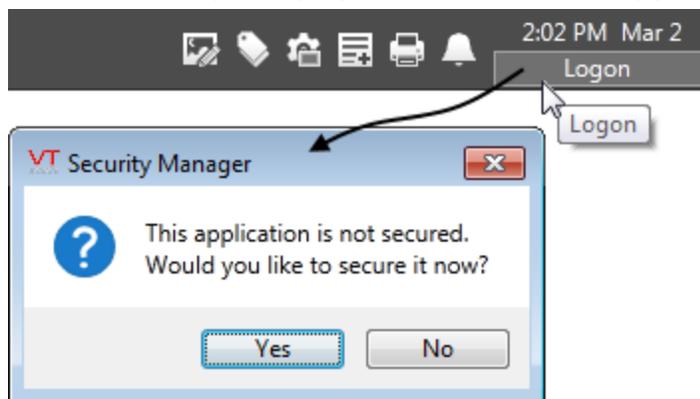
...Activate Security

...Deactivate Security– Stop security checks, with or without removing accounts.

Activate Security

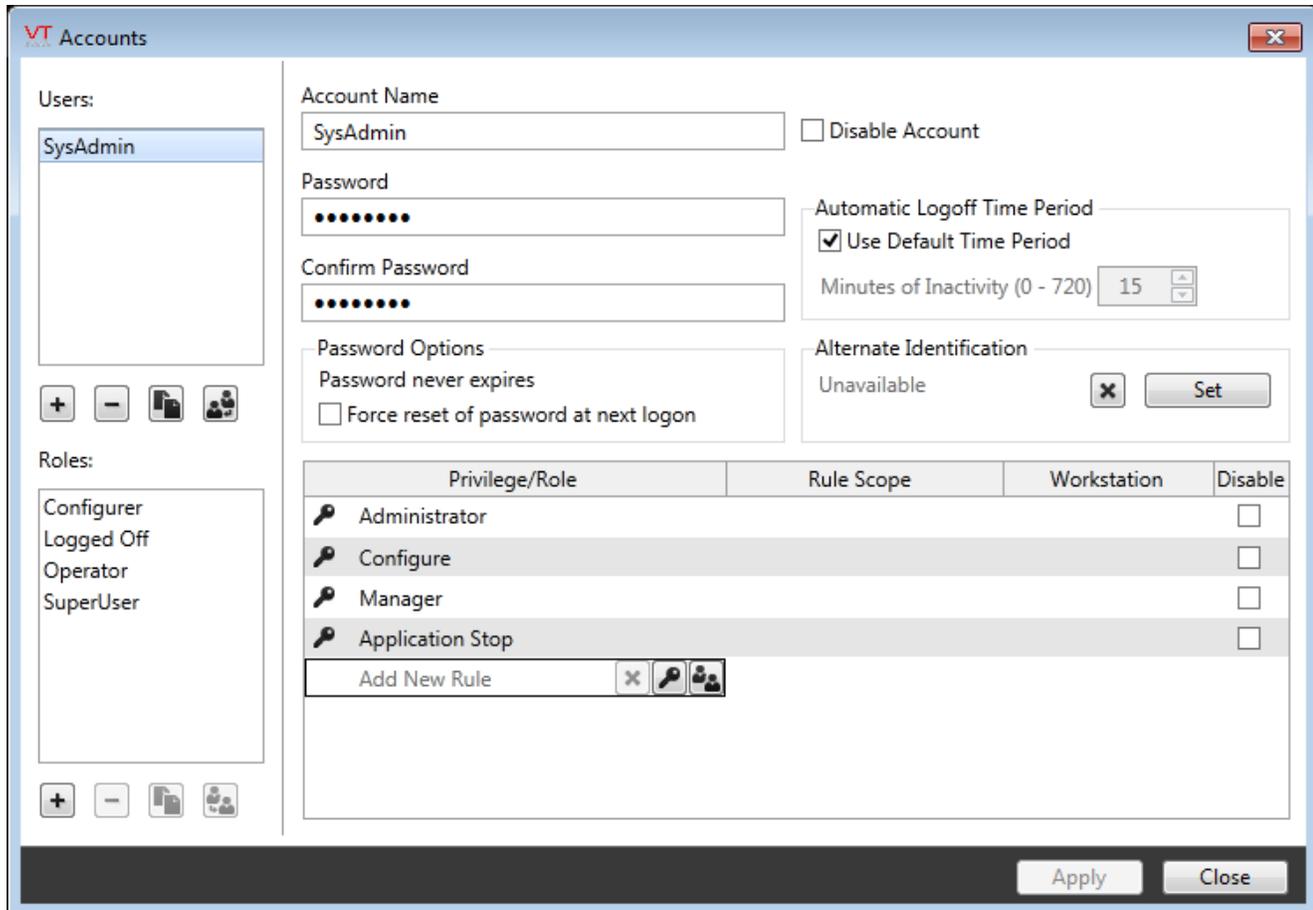
The following steps will both activate security, and create the first user account. A secured application, by definition, is one that has at least one account possessing the Manager privilege.

The process begins by opening the security dialogs for the first time. VTScada will prompt you to secure the application.



Click on the Yes button to proceed.

A secured application is one with at least one active user account, to which the Manager privilege has been granted. For this reason, the Add Account dialog will open immediately after you choose to secure the application. Use this to create an administrative account that you will then use each time you want to create or modify other user accounts. You may configure the initial account with any username, password and privilege set that you want, but VTScada will ensure that the Manager privilege is granted at a minimum. The privileges Administrator, Configure and Application Stop are also suggested (and initially configured) for this account.



Use care when granting privileges. In general, it is safest to grant only the privileges that are absolutely required.

Troubleshooting:

- The Apply button is not enabled. The new account cannot be saved
An account name must be entered, and the password entered and verified. Ensure that you have pressed Enter or Tab after typing the password a second time.
- After creating the account, I see more (or fewer) dots than characters that I entered for the password.
This is by design, to hide the number of characters in your password.
- I've forgotten my password.
A manager can reset an operator's password.
Do not forget the password for the manager account.

Related Information:

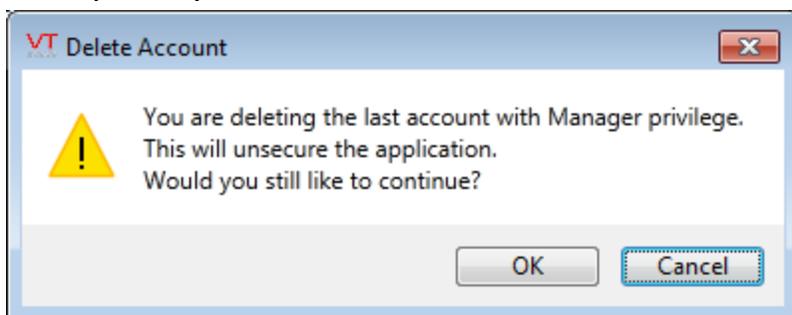
...Deactivate Security– Stop security checks, with or without removing accounts.

Deactivate Security

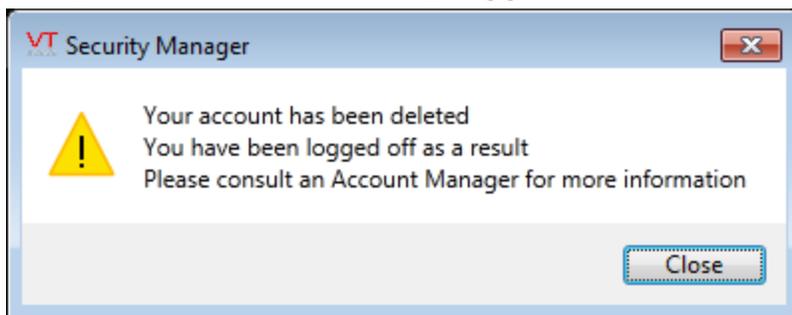
If an application does not have an active account, holding the Manager privilege, then it will be returned to the unsecured state.

Note: If your application uses Windows Authentication, then deselecting that option in the Administrative Settings dialog will deactivate security.

You can return an application to the unsecured state by removing or deactivating all the accounts that have the Manager privilege. Warning messages will be displayed before the application is unsecured. For example, if you delete the final account the following dialog will appear:



Click OK to continue. The application will return to the unsecured state and you will be immediately logged out.



Security can be re-activated as described in Activate Security.

If you deactivated the manager accounts rather than deleting them, then create a new account to re-activating security. Following this, the deactivated accounts will be visible in the Accounts dialog, and may be reactivated.

Troubleshooting:

- I deactivated the manager account, but security is still enabled.
There is still at least one account having the manager privilege.
- After deactivating security, I cannot use the VTScada Internet or Mobile browser client.
Remote access is allowed only to an application that is secured.

Related Information:

...Activate Security

Accounts and Roles

Note: If your application uses Windows Security Integration, refer to implementation notes in the topic: Windows Security Integration

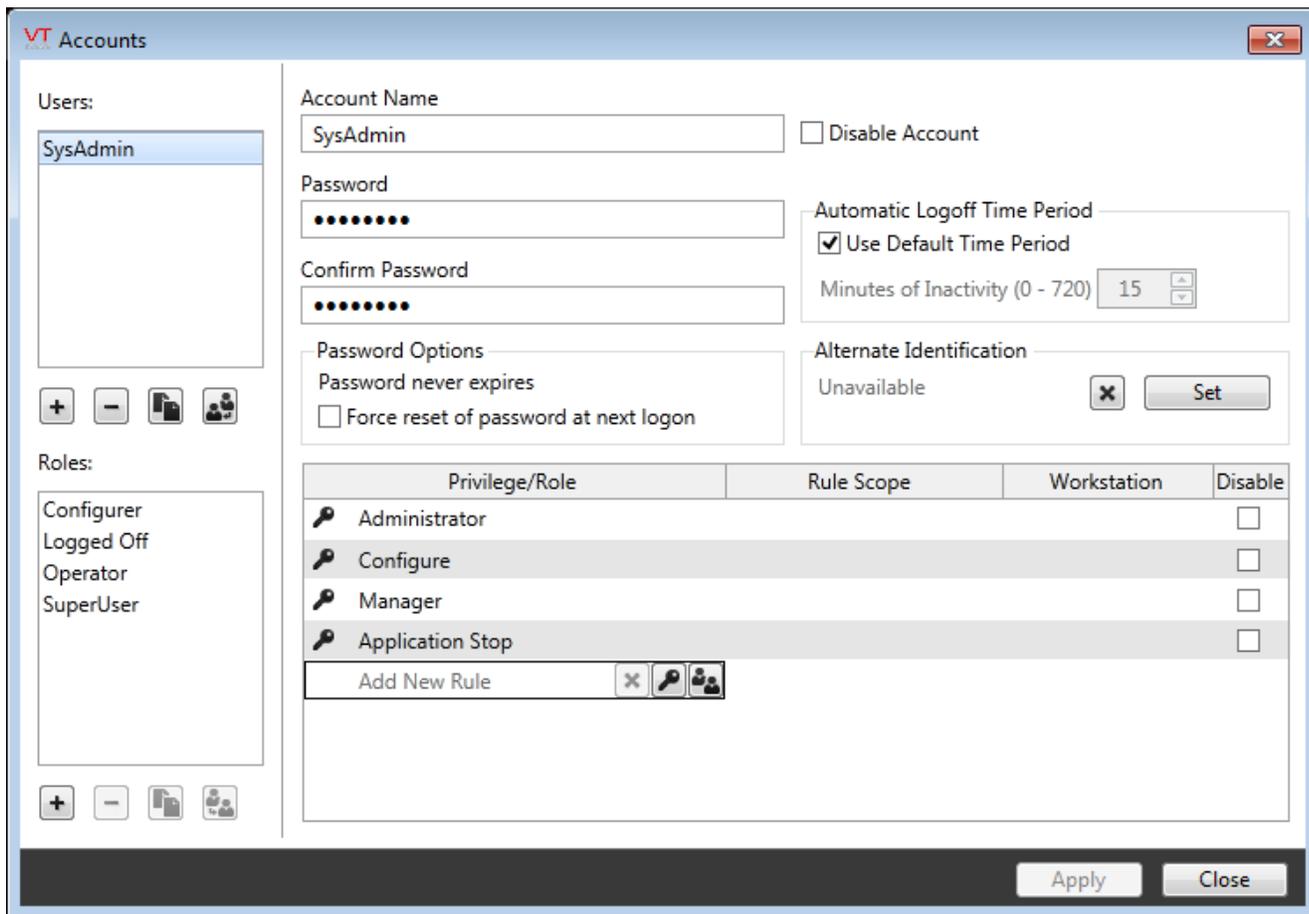
Accounts

When security has been enabled, everyone who uses the application must have an account. The account is used to identify and authenticate the user, hold the list of granted privileges, and store features that may be unique to the user such as a custom automatic log-off period.

Features of an account:

- *Name:* Identifies the user.
- *Password:* Used to authenticate the user.
- *Alternate ID:* For installations that include the Alarm Notification System. The numeric password they will use when logging in by phone.
- *Disable option:* Prevent logons using an account, without deleting that account.
- *Automatic Logoff time period:* May be set between 0 and 720 minutes if the default time period does not apply to this user.
- *Password Expiration:* Often when assigning new accounts, managers will provide a simple password and require the user to change it upon first logon.
- List of assigned privileges and roles, and the tag or workstation scope that those apply within.

Recommended practice is to assign privileges to roles, then assign roles to accounts.



Note: If realm area filtering is in effect, managers who members of a realm can see only those accounts and roles that are within the same realm.

Roles:

Similar to an account, but defines the privileges required by a job description rather than defining an individual. Account management is greatly simplified by defining roles for tasks, then assigning those roles to accounts. Changes made to a role will be applied immediately to the accounts that hold the role.

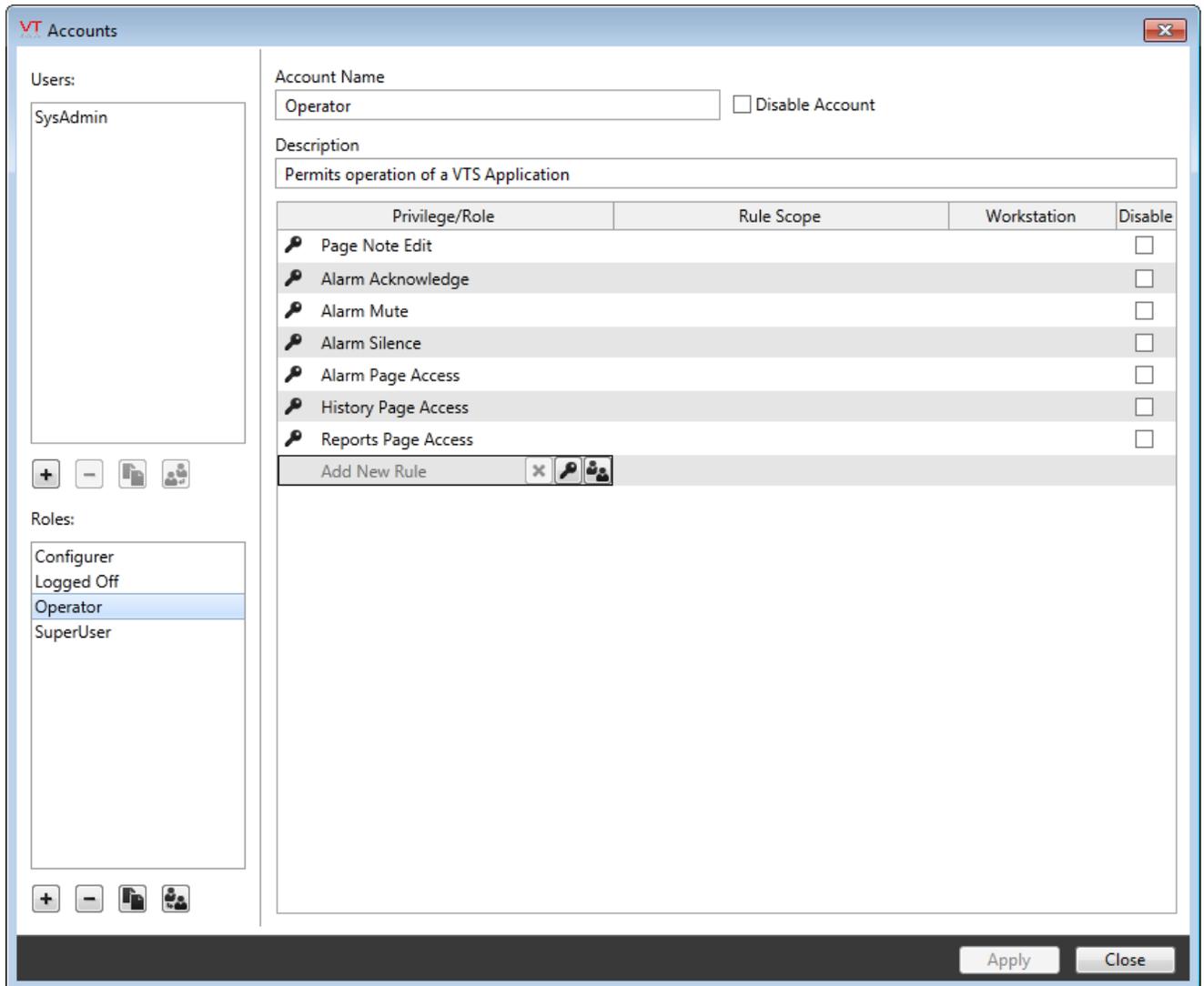
Roles may be assigned to other roles, and multiple roles may be assigned to an account. Privileges are additive, meaning that the account will gain all privileges defined in all assigned roles.

It is not possible to log on to an application using a role.

To help you configure a new application, several roles are built in. These are examples, containing sets of permissions for various possible roles. While these are useful to help you start your security configuration, you should plan to modify or remove the built-in roles and add your own as required.

Features of a role:

- *Name*: Identifies the role. Roles have no other authentication information.
- *Description*: Contextual information about the role. May be used to describe the role's intended use.
- *Disable option*: Immediately removes the privilege set from all accounts that have this role, without needing to delete it. Disabled roles may not be assigned to accounts.
- List of assigned privileges and roles, and the tag or workstation scope that those apply within.



Related Information:

...Built-In Roles – The privilege set assigned to each role.

Related Tasks:

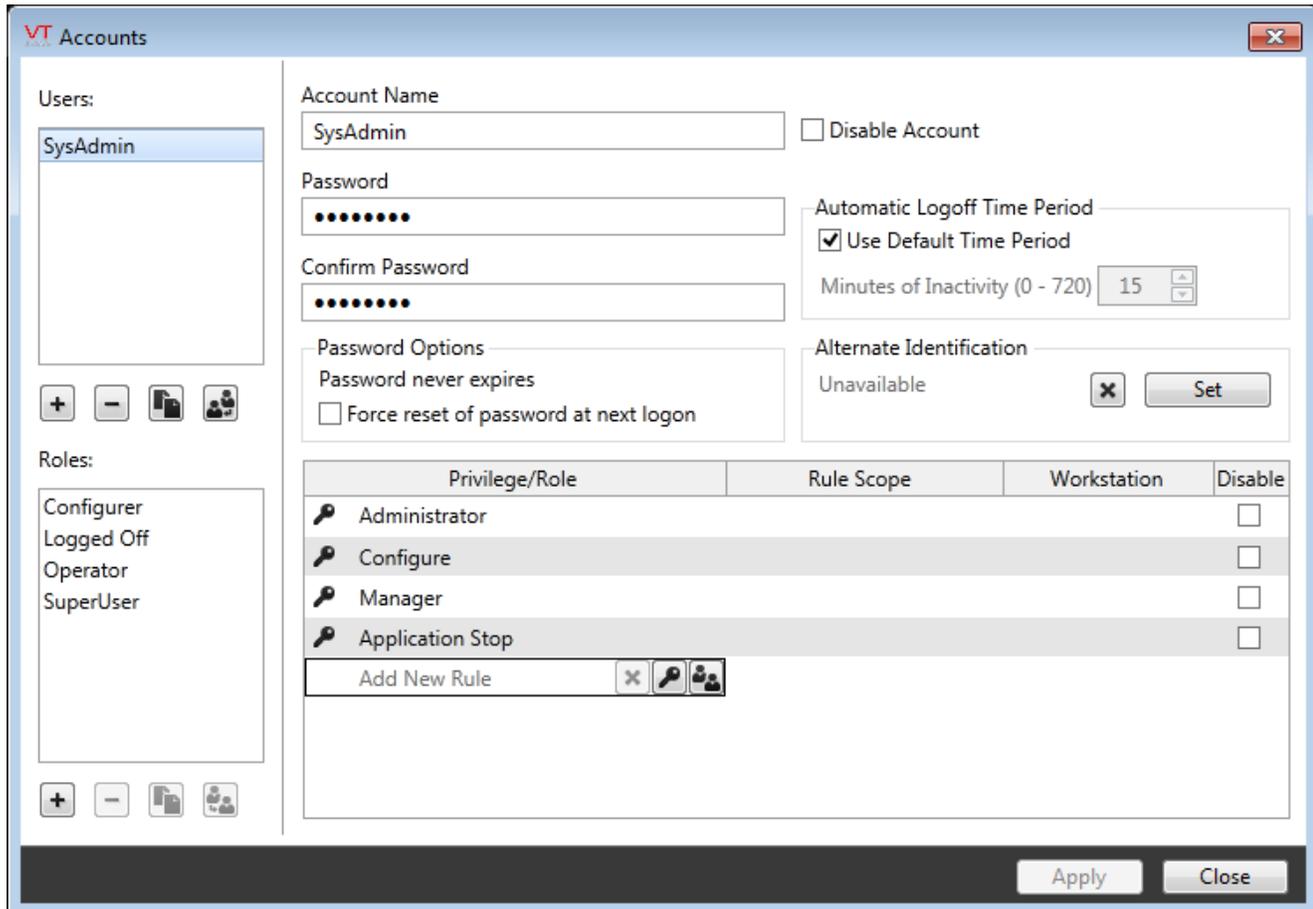
...Create Accounts – Three methods of creating an account.

...Add Privileges to Accounts – The process to add privileges to roles, then roles to accounts.

Create Accounts

Note: If your application uses Windows Security Integration, refer to implementation notes in the topic: Windows Security Integration

All accounts and roles are created and modified using the Accounts dialog. The following instructions are for creating an account, but apply identically to creating a role, excepting that roles do not have passwords. Recommended practice is to assign privileges to roles, then assign roles to accounts.



There are several ways to create an account or role.

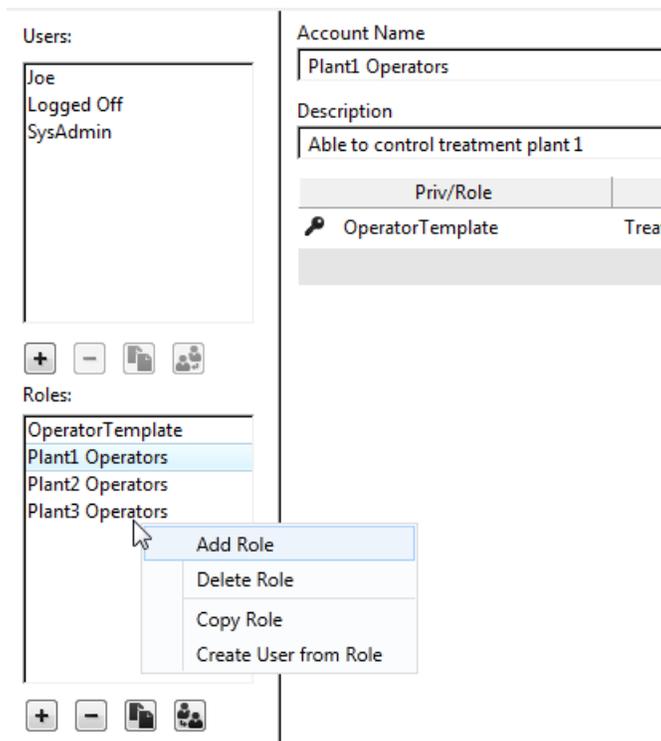
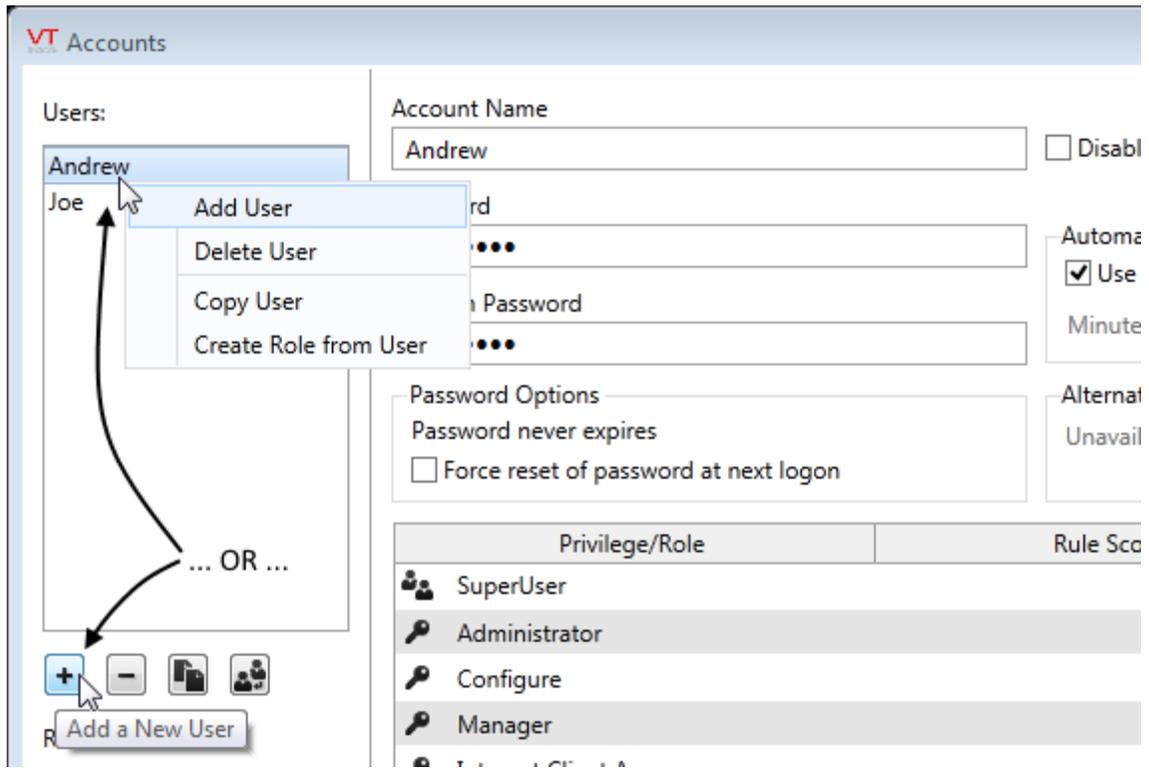
Note: If a manager is a member of a user group, any new user accounts created by that manager will automatically belong to the same user group. In this case, you must enter new user names as simply "User-Name" rather than "GroupDelimiterUserName".

The manager will be able to see (and assign to users) only those roles that are also part of the same group. It is recommended that a manager with global access create roles for each group.

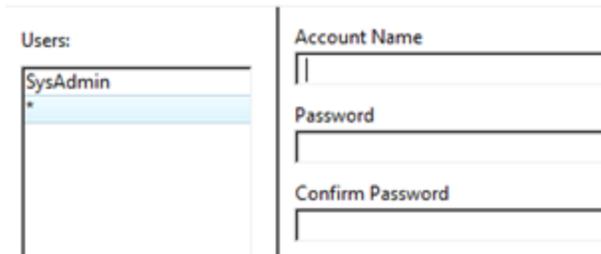
Create a new account or role:

Secure Your Application

1. Right-click in the list of accounts and select "Add User," or click the Plus button below the list of accounts.



An asterisk will appear in the user list, marking the place where the new account is being added.



The screenshot shows a user management interface. On the left, there is a list titled "Users:" containing one entry, "SysAdmin", which has a small asterisk next to it. On the right, there is a form with three input fields: "Account Name", "Password", and "Confirm Password".

The asterisk is used to mark any account that has unsaved changes. You can switch between accounts to compare settings without losing changes made so far, and without losing track of which account has unsaved changes.

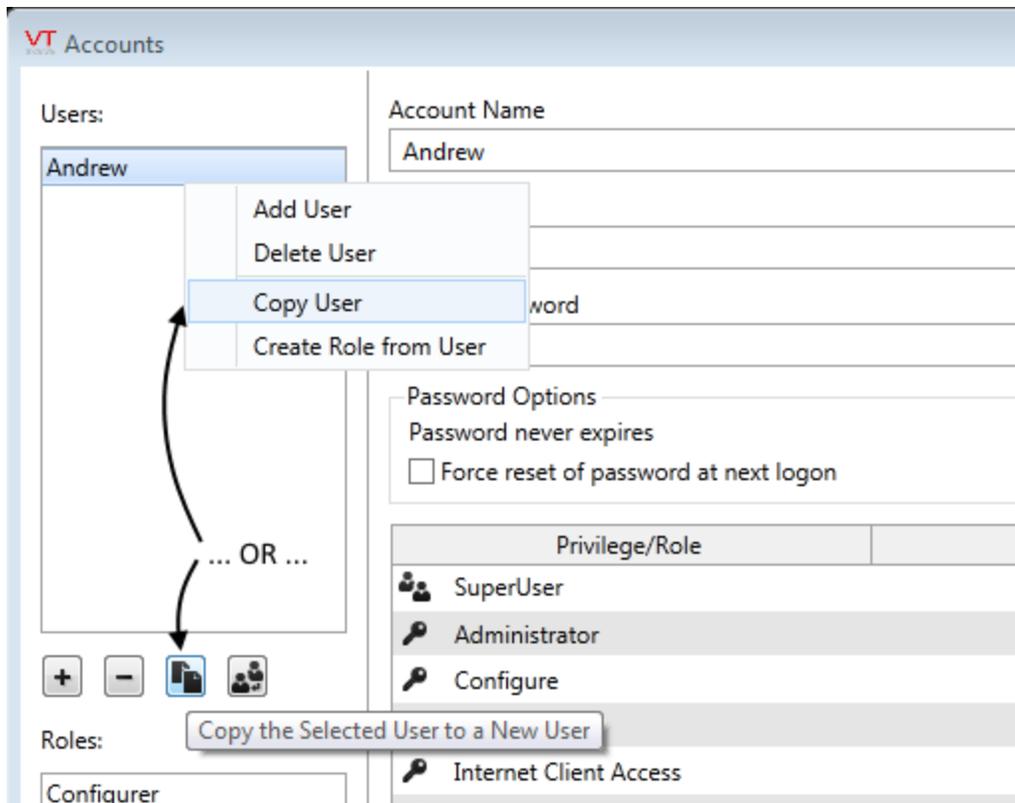
2. Enter an Account Name for the new user.
3. Enter and confirm a password.

You might wish to make this password a temporary, generic password and have the user customize it after the first time he/she logs on. Users do not need the Account Modify privilege to change an expiring password, but they will need that privilege to change their password at other times.

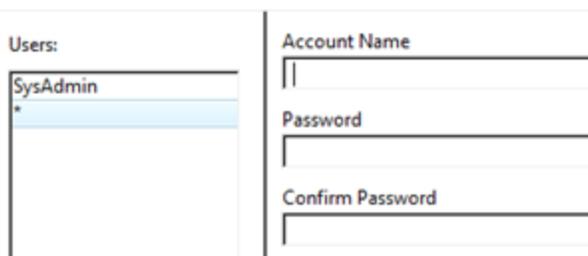
Copy an existing account or role:

Creates a clone of the account or role, differing only in name and password. Useful when creating a series of similar accounts.

1. Click once to select the account to be copied.
2. Right-click to open the menu, then click "Copy User," or click the Copy button.



An asterisk will appear in the user list, marking the place where the new account is being added.



The asterisk is used to mark any account that is being edited – you can switch between accounts to compare settings without losing changes made so far, and without losing track of which account has unsaved changes.

3. Enter an Account Name for the new user.
4. Enter and confirm a password.

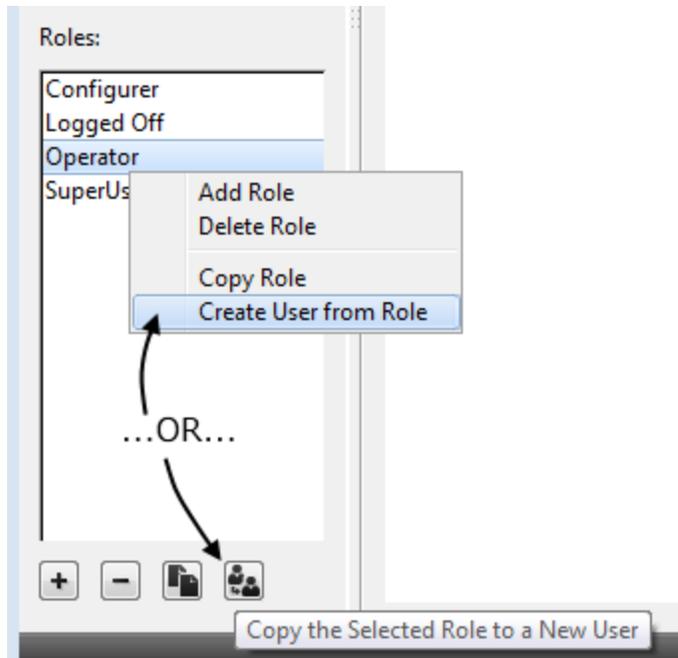
The new account will have all the privileges and other settings that the old account.

If the original account used Alternate Identification, you will need to create a unique password for the new account.

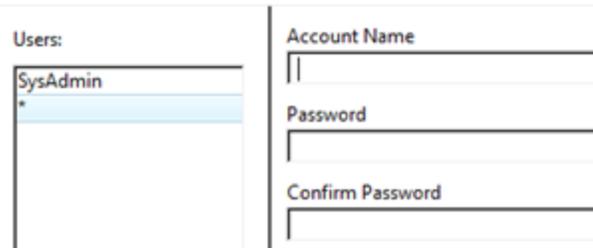
Copy a role to an account

Creates a new account having all the privileges that belonged to the role. In general, it is far more efficient to create a new account using one of the preceding methods, then assign the role.

1. Click once to select the role to be copied.
2. Right-click on the role to be copied and from the menu, select "Create User From Role," or, select the role then click the Copy button at the bottom of the list.



An asterisk will appear in the user list, marking the place where the new account is being added.



The asterisk is used to mark any account that is being edited – you can switch between accounts to compare settings without losing changes made so far, and without losing track of which account has unsaved changes.

3. Enter an Account Name for the new user.
4. Enter and confirm a password.

Copy an account to a role

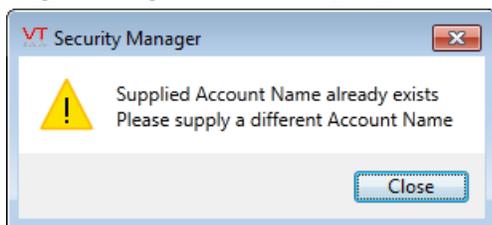
Creates a new role, having all the privileges that belonged to the account. This is a useful step to efficiently expand your list of accounts. New accounts can be granted the role that is created, thereby gaining all the privileges of the original account. The advantage of this method over simply copying an old account to new accounts is that changes made to the role will be applied to all accounts that have that role. (You may wish to modify the original account, substituting the new role for its privilege set.)

1. Click once to select the account to be copied.
2. Right-click on the account to be copied and from the menu, select "Create Role From User," or, select the account then click the Copy button at the bottom of the list.
An asterisk will appear in the user list, marking the place where the new role is being added.
3. Enter an Account Name for the new role.

Note: If the asterisk remains beside the name, the changes have not yet been saved. If the Accounts dialog is closed while an asterisk remains, you will lose all unsaved changes in the marked account(s).

Duplicate User Names

VTScada will not allow you to have two accounts with the same name. In the event that you attempt to create two accounts with the same user name (either by adding, copying or modifying) then the following warning dialog will be displayed and your changes will not be saved.



Troubleshooting:

- Unable to open the Accounts dialog.
Your account does not include the privileges required to use this feature.

- The New and Copy features will not work
Your account does not include the privileges required to use these features.
- A "Discard Changes" dialog appears whenever I try to close the dialog.
Click Apply before trying to close the dialog
- Wrong name given to the account or role.
Click on the Name field, type a new name, then click, "Apply".

Related Information:

...User Groups

Add Privileges to Accounts

While it is possible to add privileges directly to accounts, you are advised to add privileged to roles instead, then add roles to accounts. Working this way, roles define job descriptions. If you later decide to add a new application privilege for a job description, you need only add it to a role in order to grant that privilege to all users whose job description includes that role.

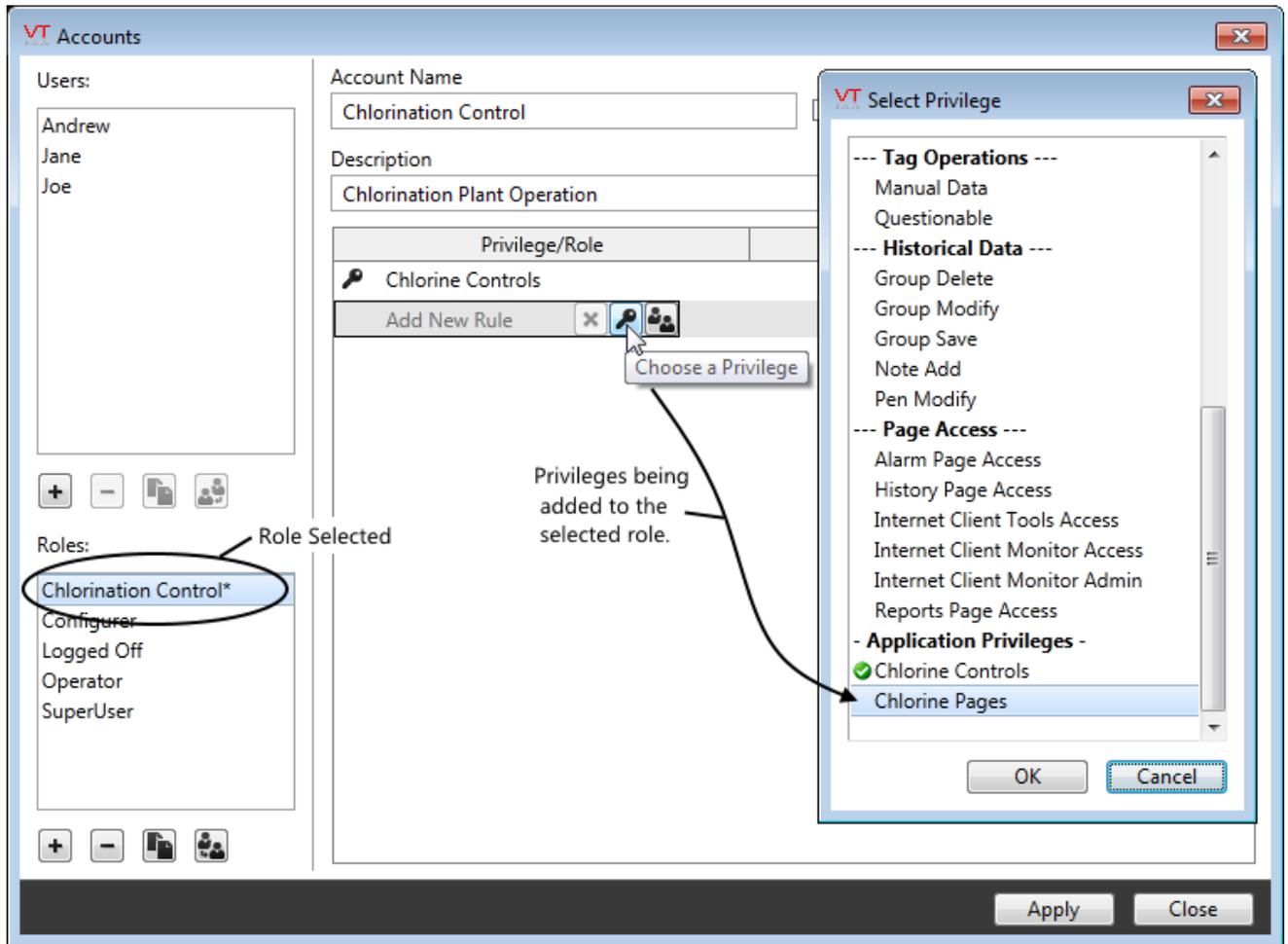
Privileges control what each user is allowed to do within VTScada. By default, all new accounts other than the very first one created, start with no privileges. A user who possesses the Manager privilege can choose what privileges to add (or grant) to each account.

The four roles that come with VTScada are intended to be used as examples. You are advised to modify these and to create your own roles. The process for creating new roles is identical to the process for creating new accounts.

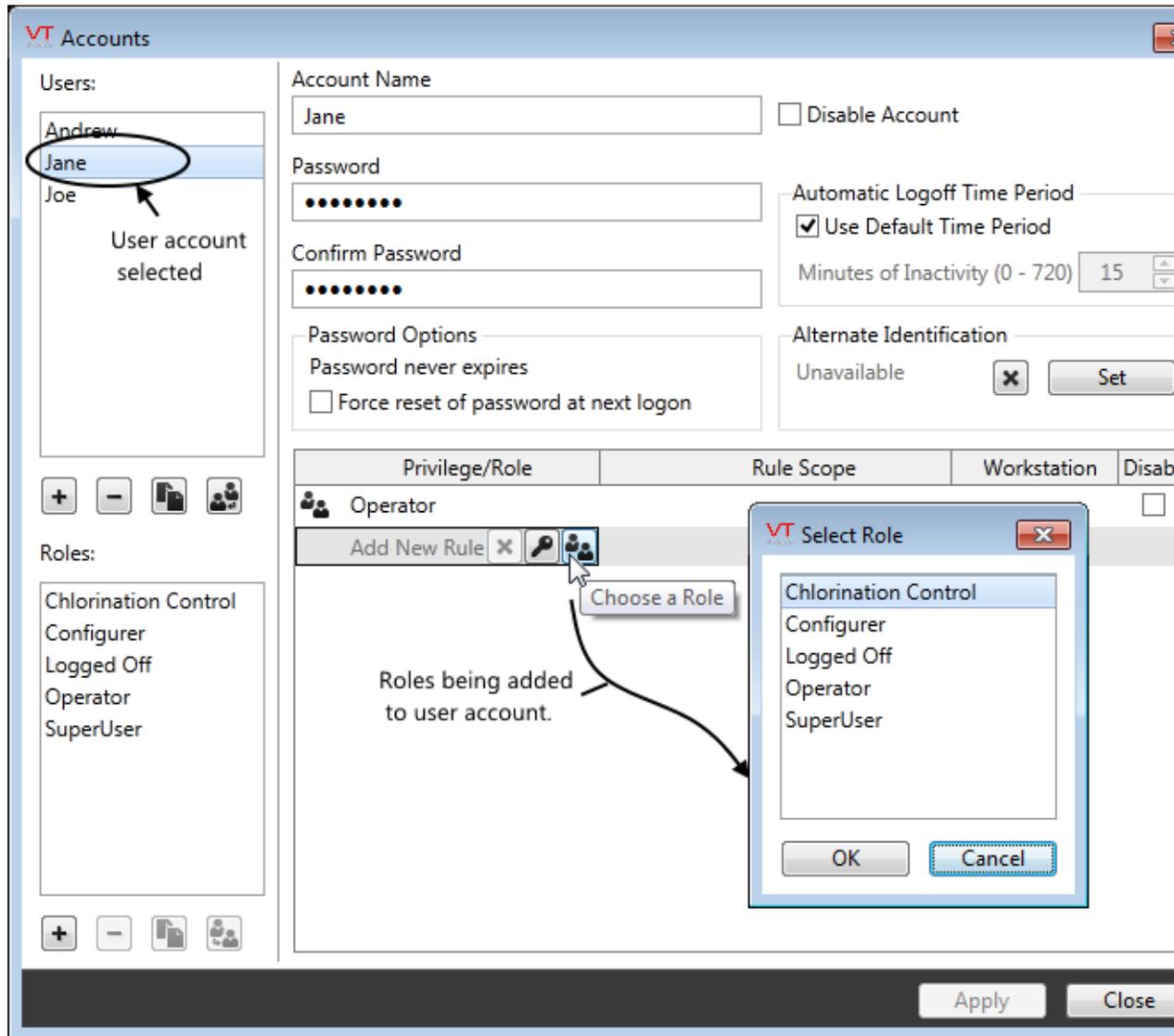
The recommended process for adding privileges to accounts is therefore:

1. Create one or more new roles, named for job descriptions in your operation.
See: Create Accounts.
2. Create application privileges as required. See: Protect Pages and Output Tags.

3. Add privileges to roles by selecting the role, then clicking the Add Privilege button in the next available Add New Rule line, as shown:



4. Add roles to accounts by selecting the account, then clicking the Add Role button in the next available Add New Rule line, as shown:



Accounts will have all the privileges in the set of roles that are assigned to it.

Related Information:

...Rules for Privilege Scope

...System Privilege Reference for Developers

Configure Alternate Identification

Note: Alternate Identification is the same, whether your system uses VTScada authentication or Windows® authentication.

Alternate identification will be required by accounts that may log in over the telephone using the Alarm Notification System, or if you intend to use a proximity card reader.

Any account can have only one alternate ID. The identification used by a proximity card reader could be used for phone verification, but may be long and may include letters as well as numbers. If you intend to use both systems for some users, you may need to create two accounts for those users.

Log on using an account that has the Manager privilege in order to configure user accounts.

Set an Alternate ID for the Alarm Notification System

1. Open the Accounts dialog and select the user.
2. Click Set in the Alternate Identification section.
3. Type a series of numbers into the Alternate Identification field.
These will be the numbers that the user will press on their phone to verify their identity to the Alarm Notification System.
The status field will update to tell you whether the identification can be used.
No two users may share the same alternate identification.
4. Type the same series of numbers into the confirmation field and press enter or tab.
5. Click OK to save and exit.

Set an Alternate ID for a proximity card reader:

1. Install a proximity card reader.
2. Set the application property, pcProxEnable to 1.
VTScada will scan for the device.
3. Open the Accounts dialog and select the user.

4. Open the Alternate Identification dialog.
5. Swipe that user's proximity card through the card reader.

You may want to log out, then swipe the card again in order to verify that it will work to allow the user to log into their account.

Related Information:

...Create Accounts – Describes the Accounts dialog.

...Proximity Card Readers – Installation details.

Built-In Roles

Note: The built-in roles are provided as examples to help you begin security configuration. It is expected that you will modify these and create your own roles.

Logged Off – The privileges available at a workstation when no user is logged in.

No privileges

A VTScada application continues to run whether an operator is logged in or not. While running, any control action that is not protected by an application privilege can be used and that action is recorded to the alarm history. All actions occurring while no one is logged in are attributed to a role named "Logged-Off". This is a role that is built into and standard with every VTScada application.

Use care in granting privileges to the Logged Off account. If you wish to allow certain access to the application for all, then it is better to create a public user account with a carefully restricted set of privileges and publish that user name and password than to grant those privileges to the Logged Off user account.

Operator – Permits basic operation of a VTScada application.

- Page Note Edit
- Alarm Acknowledge
- Alarm Mute
- Alarm Shelve

- Alarm Silence
- Alarm Page Access
- History Page Access
- Reports Page Access

Configurer – Permits development of a VTScada application

- Includes the Operator role, plus:
- Configure
- Account View
- Application Stop
- Advanced Version Control
- Deploy Changes
- Revert Changes
- Edit Files
- Page Add
- Page Modify
- Page Delete
- Page Note Hide
- Parameter View
- Tag Add/Copy
- Tag Modify
- Tag Delete
- Alarm Disable
- Manual Data
- Questionable
- Group Delete
- Group Modify
- Group Save
- Note Add
- Pen Modify
- Internet Client Tools Access
- Internet Client Monitor Access

SuperUser – Configuration and security management

Includes the Configurer role (and therefore, the Operator role), plus:

- Administrator
- Manager
- Account Modify
- Internet Client Monitor Admin
- Revert Changes

Privileges not granted to any built-in role:

- Internet Client Access
- Application Manager View
- Manage Types
- User-created application privileges

Related Information:

...Accounts and Roles – Concepts and tasks.

...Add Privileges to Accounts – The process to add privileges to roles, then roles to accounts.

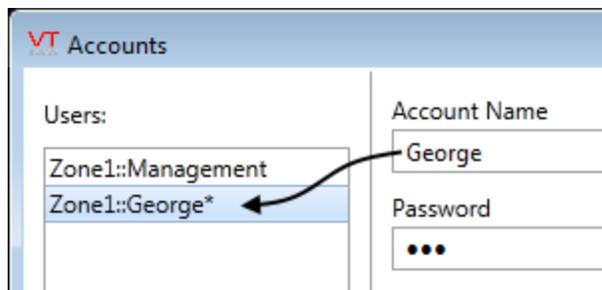
...System Privilege Reference for Developers – Detailed reference for each privilege.

User Groups

VTScada provides the ability to create user groups (sometimes referred to as a "security groups"). These are one part of Realm Area Filtering, which is a VTScada feature that:

- Restricts the display of alarms to those in tag areas assigned to the user's group.
- Restricts the tag browser, limiting the list of tags displayed to those in tag areas assigned to the user's group.
- Restricts the selection of tags available for reports to those in tag areas assigned to the user's group.
- Restricts the selection of tags available for the Historical Data viewer to those in tag areas assigned to the user's group.

- Restricts VTScada Internet Client access for the application, forcing group members to log into a realm that matches the name of their user group.
- Security Manager accounts that are members of a user group will see only user accounts in the same user group.
- If a manager, whose account is a member of a group, adds a new user account, that new account will automatically be made a member of the same group.



Note: If realm area filtering is in effect, managers who members of a realm can see only those accounts and roles that are within the same realm.

As an example, assume that you have a VTScada application named "Umbrella" that serves two plants: "Western" and "Eastern". Western operators should not see or acknowledge Eastern alarms, and vice-versa. However, a third group of users must see both Eastern and Western tags and alarms for administrative purposes. The application can be configured to have three different groups of users: an Eastern group, a Western group, and a set of administrators without group membership.

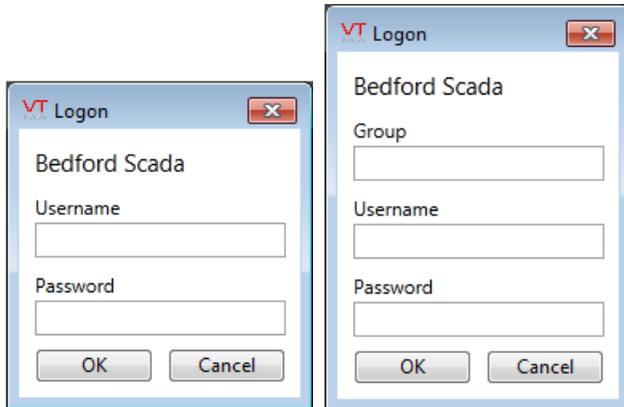
When user groups are enabled, login names are created using the following syntax:

```
<GroupName><GroupDelimiter><Username>
```

where <GroupName> is the name of the group to which the user belongs, <GroupDelimiter> is one or more user-defined characters that separate the group from the username, and <Username> is a typical VTScada security account user name.

The logon dialog will change from the example shown here on the left to that on the right. Note the addition of the Group field at the top of the

dialog. (This is an optional feature – groups can still be configured and used without the extra field. Users would then logon using their full GroupDelimiterUsername designation.)



Using our Umbrella application scenario, the security account for a user from the administrative group might be:

`RPeters` (no group name should be used)

The security accounts for operators for the Western plant might be similar to:

`western:JSmith`

And, the security account for operators for the Eastern plant might be similar to:

`Eastern:MDonaldson`

Note: Groups are useful only when used in conjunction with Realm Area Filtering. Without a Realm Area, a group is little more than a naming convention applied to sets of operators.

Related Information:

...Realm Area Filtering, See the Developer's Guide. – Create user-groups. Control access to tag-lists and alarm information based on membership in a security group and the area property of tags.

...Configure User Groups

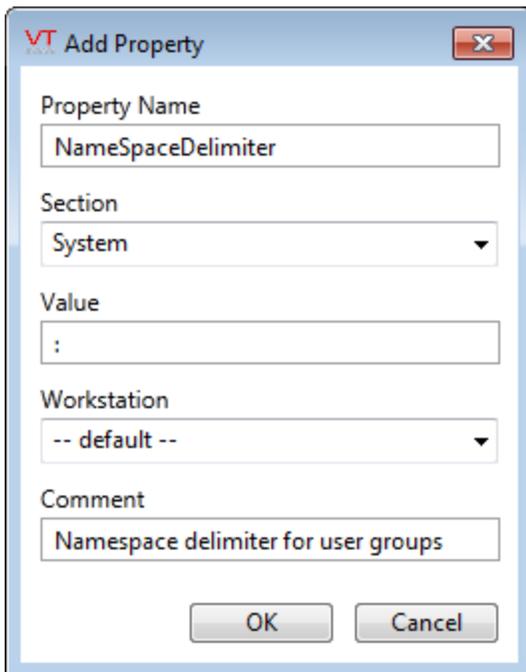
Configure User Groups

User groups are enabled by changing two application properties.

- **NamespaceDelimiter** This property defines the character that will separate the group name from the user name when adding new user accounts. The existence of a delimiter will activate the user-group feature.
- **GroupLogin** Controls whether the Group field will appear in the Logon dialog. It is standard practice to set this to true (1) when user groups are in use.

Add these properties to the [SYSTEM] section of your application's Settings.Dynamic file.

1. Open the Application Configuration dialog.
2. Select the Advanced Mode viewing option.
3. Click, "Insert".
4. Configure the dialog as follows. The use of a colon for the value is suggested, but not required.



5. Click, OK to save the new property.
6. Repeat these steps to add the property, GroupLogin, setting its value to 1.
7. Open the Security Accounts dialog to add a new user.
This instruction assumes that security has been enabled and you have an account with Manager privileges.
8. Add or rename user accounts to have the form, GroupDelimiterUsername
For example, Western:JSmith

These instructions activate the user group feature and create user accounts that are members of groups.

Note: If a manager is a member of a user group, any new user accounts created by that manager will automatically belong to the same user group. In this case, you must enter new user names as simply "User-Name" rather than "GroupDelimiterUserName".

The manager will be able to see (and assign to users) only those roles that are also part of the same group. It is recommended that a manager with global access create roles for each group.

To obtain a practical benefit from the user group feature, you will also need to configure Realm Area Filtering.

Related Information:

...Realm Area Filtering, See the Developer's Guide. – Create user-groups. Control access to tag-lists and alarm information based on membership in a security group and the area property of tags.

Protect Pages and Output Tags

The system privileges can restrict access to native VTScada features, such as the Alarm Page and the ability to do configuration.

To restrict access to your output tags and pages, create new privileges and apply them to the objects to be protected. These privileges are referred to as "application privileges" since they are always custom-built for an application. An application privilege applied to an output tag will prevent an unauthorized user from operating the associated controls, but still allow them to see the tag. An application privilege applied to a page will prevent an unauthorized user from opening the page, thereby hiding its contents from view.

You can create thousands of your own application privileges if necessary. But, before creating large numbers of privileges, you should consider

whether rules that limit a privilege by scope or workstation might help you keep the number to a manageable level.

For programmers: Every application privilege will have an index number, starting at 16. Also, every application privilege is enumerated in the configuration file, Settings.Dynamic with values starting at zero. When writing expressions that check privileges, add 16 to the enumerated value in Settings.Dynamic.

Related Tasks:

...Add New Application Privileges – Instructions for adding application privileges.

...Restrict Access to a Page – Instructions for applying a privilege to a page.

...Restrict Access to Output Controls – Instructions for applying a privilege to an output tag.

Related Information:

...Accounts and Roles– Granting privileges to users.

...Rules for Privilege Scope – Make privileges local rather than global.

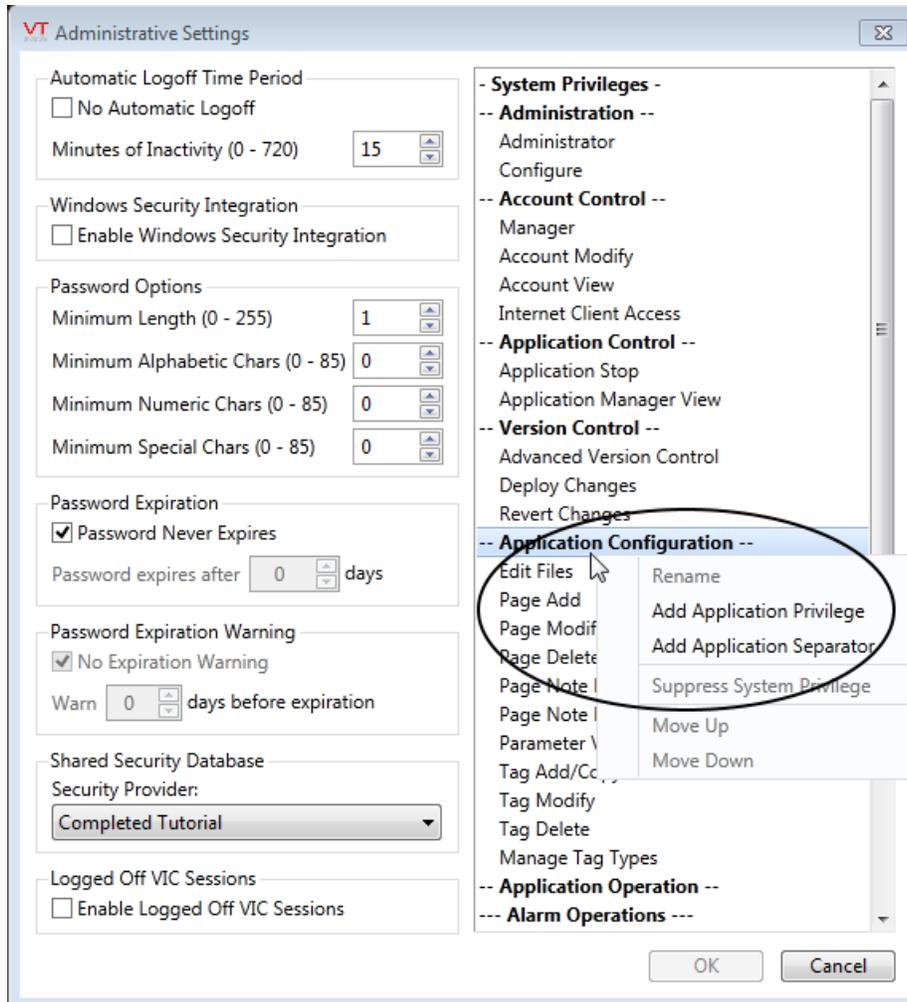
...See "Examples of Expressions" in the Programmer's Guide. Includes an example, showing the use of an application privilege in an expression that controls the push button widget's confirmation dialog.

Add New Application Privileges

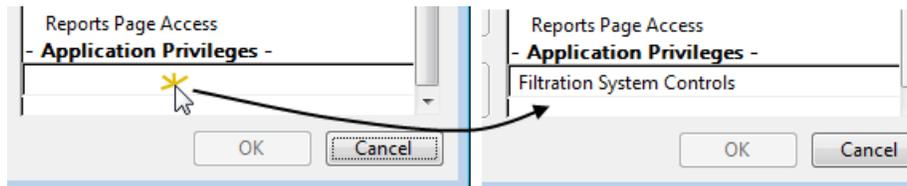
Only users who possess the Administrator privilege can add new application privileges.

To create or change application privileges:

1. Log in to the application using an account that has the Administrator privilege.
2. Click your name (formerly labeled "Logon").
3. The Security Options dialog opens.
4. Click Options to open the Administrative Settings dialog.
5. Right-click anywhere within the list of privileges.



Regardless of where you click in the window, application privileges are always added at the bottom of the list. A space will appear for the new privilege name:



6. Click in the data entry field, then type a name for the new privilege (e.g. "Filtration System Controls").
7. Press the Enter key to save the new privilege name.
8. You may repeat these steps for as many new privileges as are required.

After creating application privileges, you can link them with the objects you wish them to protect and grant them to those accounts or roles that

should have access to the protected objects. *Privileges are not granted automatically to any user account, including your own.*

An application privilege can be renamed by right-clicking on it, within the Administrative Settings dialog, and selecting "Rename" from the context menu that opens. Since applications privileges are tied to tags, pages and accounts by an identifying number, changing the name has no other effect.

For programmers: Every application privilege will have an index number, starting at 16. Also, every application privilege is enumerated in the configuration file, Settings.Dynamic with values starting at zero. When writing expressions that check privileges, add 16 to the enumerated value in Settings.Dynamic.

Troubleshooting:

- Difficulty entering the new privilege name.
Ensure that you click within the name entry field before starting to type, and press <Enter> or <tab> after typing the name.

Next Steps:

...Restrict Access to a Page

...Restrict Access to Output Controls

Related Information:

...

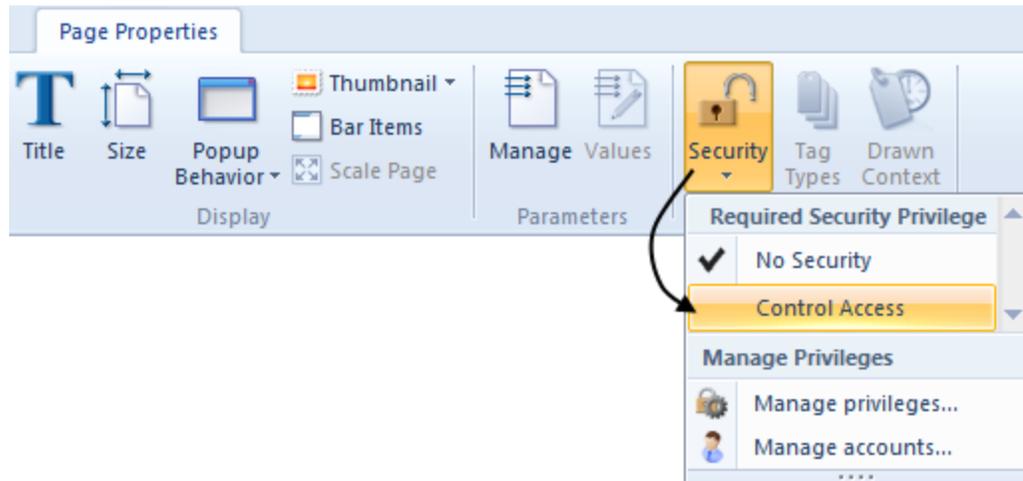
...See "Examples of Expressions" in the Programmer's Guide. Includes an example, showing the use of an application privilege in an expression that controls the push button widget's confirmation dialog.

Restrict Access to a Page

You can deny access to pages for unauthorized users by applying an application privilege to the page. Only users who have been granted that privilege will be able to open the page. Further, users with configuration privileges will not be able to access the page's properties if they do not also have the required privilege for that page.

Note: When assigning privileges: In the operator's account (or role) definition, the privileges required to open a page (or perform any other native VTScada operation) must not be limited by tag scope rules. Pages are independent of tags, therefore if the privilege has a tag-scope rule applied, the result is to deny access to the page for that account.

1. In the Idea Studio, open the page and its associated Page Properties toolbar.
2. Click the Security tool.
3. Select the privilege, which you created earlier for this purpose.



If you have not yet created an application privilege, you may click Manage Privileges to do so.

Troubleshooting:

- There is no privilege to apply.
Create an application privilege, to be applied to the page.
- The page was open, but closed immediately after the privilege was selected.
Your account does not possess this application privilege. You will need that privilege in order to open or make any further changes to the page.
- Operators have been granted the matching privilege to open the page, but cannot do so.
Ensure that the privilege has not been limited by a tag-scope rule in the operator's account or the role that provides the privilege to the operator.

Related Information:

...Refer to the VTScada Admin Guide for "Accounts and Roles" – Creating and managing. Also, "Protect Pages and Output Tags" – Create your own privileges for protection.

Restrict Access to Output Controls

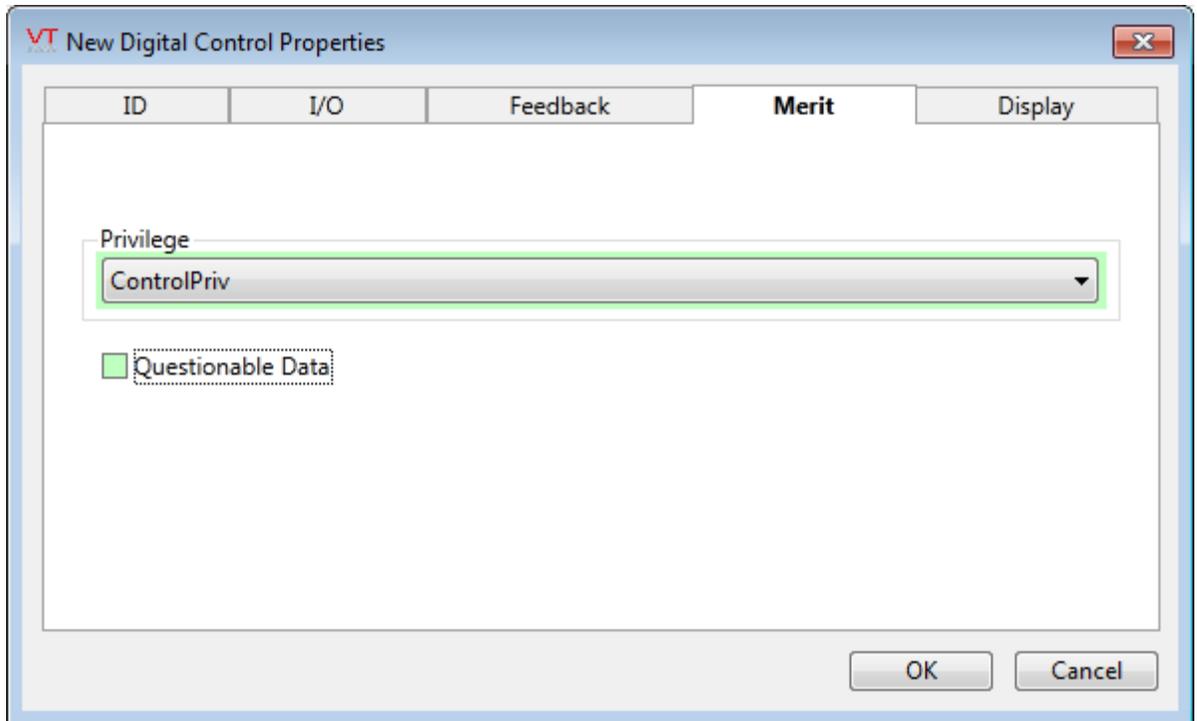
All tags that can be used to write values to equipment can have an application privilege assigned to them. Anyone may view the control, but only users who have the correct privilege will be able to use it to write a value to the PLC or RTU.

Certain operational tags may also be protected with an application privilege. These include Modem, SMS Appliance and Trigger tags.

When used with tags, application privileges may be further defined by a rule scope. Under this system, an operator who has the matching privilege will be able to use it only for tags in a defined scope. For example, the operator may be allowed to operate eastern-zone pumps, but not western-zone pumps even though the same privilege protects both.

To restrict access to output controls:

1. Open the tag's configuration dialog.
2. If the dialog has a Merit tab, open that.
If the dialog has a Quality tab, open that.
3. In the Privilege drop-down control, select the application privilege that was created earlier for this tag.
4. Click OK to save your work.

**Troubleshooting:**

- There is no privilege to apply.
Create an application privilege, to be applied to the tag.

Related Information:

...Protect Pages and Output Tags – Create your own privileges for protection.

...Accounts and Roles– Creating and managing.

...Rules for Privilege Scope– Make privileges local rather than global across your application.

Rules for Privilege Scope

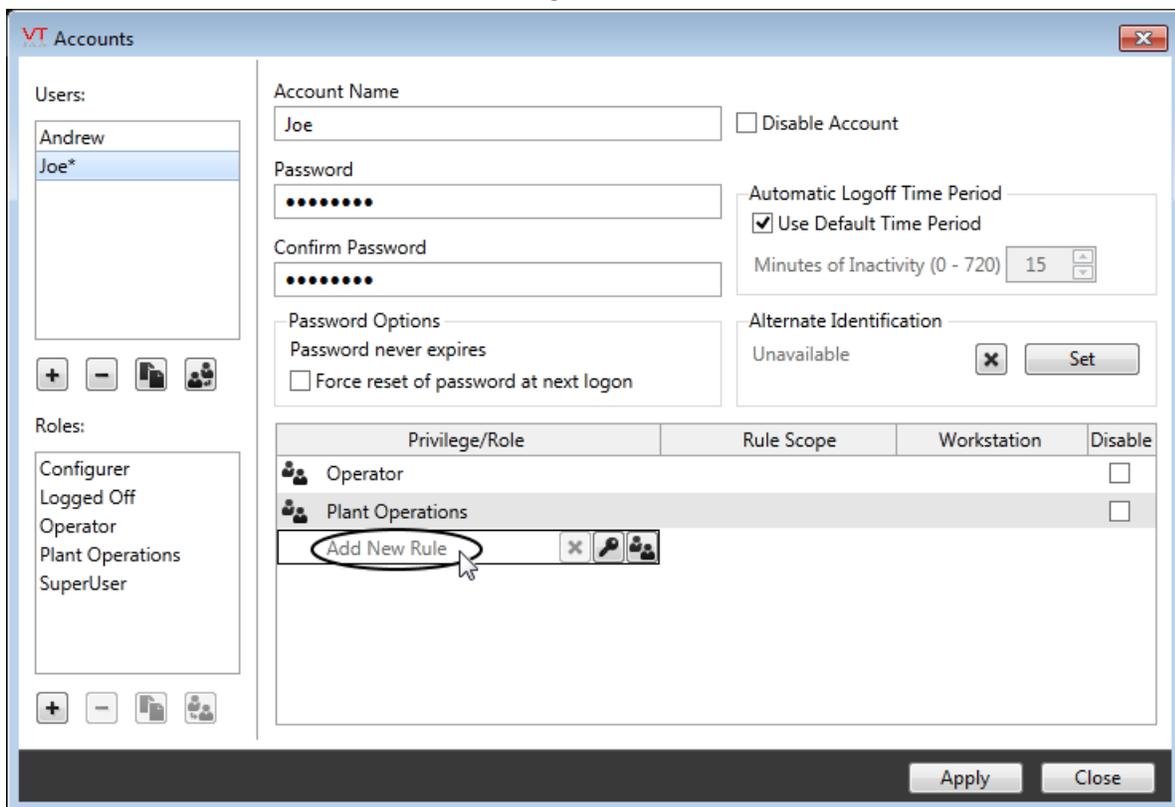
A "rule" is defined as a privilege granted to an account or to a role. Adding a **role**¹ to a user's account also counts as a rule since roles

¹A named set of security permissions, typically encompassing the set required for a defined task or job.

contain privileges.

The word "rule" is used, rather than simply "privilege" because you can control the scope of the privilege by associating it with a tag structure or a workstation. The privilege will then apply only for controls within the associated tag structure, or only when the user is logged on at a particular computer.

Security rules are especially useful when you have organized your tags into parent-child hierarchies that group similar parts of the application together. For example, a city utility may have grouped all of the wells, pumps and other water supply tags for the eastern half of the city under one Context tag named EasternZone. All of the tags for the western side are grouped under a Context tag named WesternZone. For individual operators who work with the EasternZone, you can restrict their job description role to apply only to tags in the EasternZone.



In the example shown, the Operator role and the Plant Operations role have been assigned to Joe's account. The Plant Operators role includes a

number of application privileges for process control, but in Joe's case, those apply only within the scope of tags in the Eastern Zone hierarchy.

Note: Warning: Scope rules should be applied only to application privileges or to the tag-related system privileges, Questionable and Manual Data. Limiting a system privilege by a tag scope is the same as denying the privilege. Applying a scope-rule to a role that has system privileges is also the same as denying that role's privileges.

You can also create a rule such that the privilege is valid only when the user is logged in on a named workstation. For example, if you have created a Manager role, with permissions to modify user accounts, you may wish to restrict that rule so that it may only be used at a given workstation. Even if someone were to guess the password of a user with the Manager role, they would not be able to modify accounts unless they were also at that person's workstation.

Note: Take care that the workstation you select is or will be available. If used carelessly, this feature makes it possible for you to restrict your own Manager privilege to a workstation that is not available, thus making it extremely difficult to further modify any accounts.

Workstation rules are not intended for use with Internet or Mobile client connections. It is not always possible to determine the name of the remote machine, especially if the client is connecting from behind a firewall that makes many clients appear to come from the same address. If you are making use of workstation rules to limit an account or role's access to privileges, and you are using a VTScada Internet Server to enable remote access, the servers should be included as permitted workstations.

Related Information:

...Example: Managing Complex Security

...Protect Pages and Output Tags – Application privileges reference and instructions.

...Context Tags, See the VTScada Developer's Guide – Organizing tags into hierarchies.

...Accounts and Roles – Creating accounts and roles.

Example: Managing Complex Security

A city has three water treatment facilities – each of which is represented by a large number of tags.

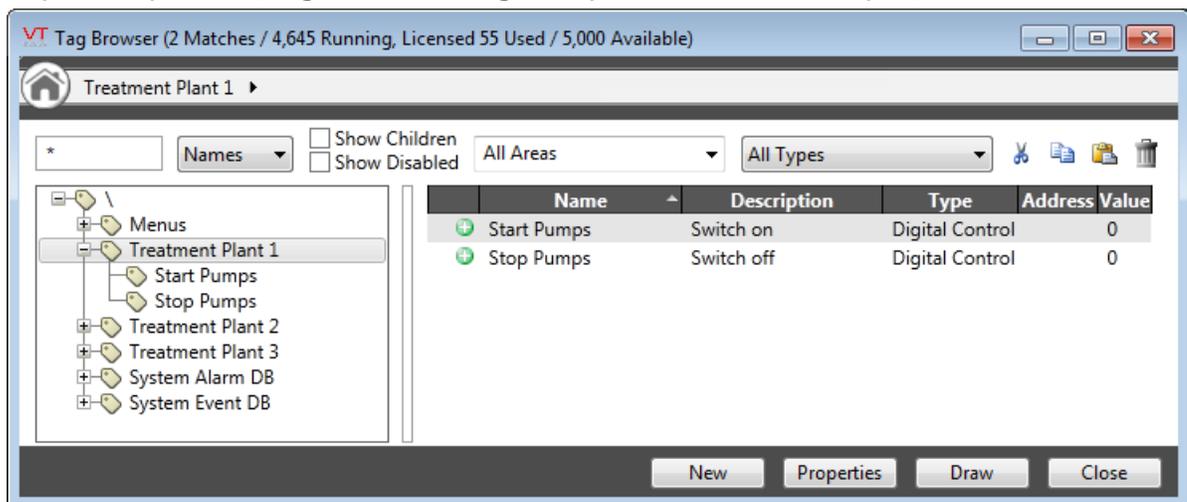


Many operators are employed at each plant. Some are responsible for operations at more than one plant. Others are responsible for only a single plant, but from time to time an operator will transfer from one plant to another.

Any given operator may use only the controls for their assigned treatment plant.

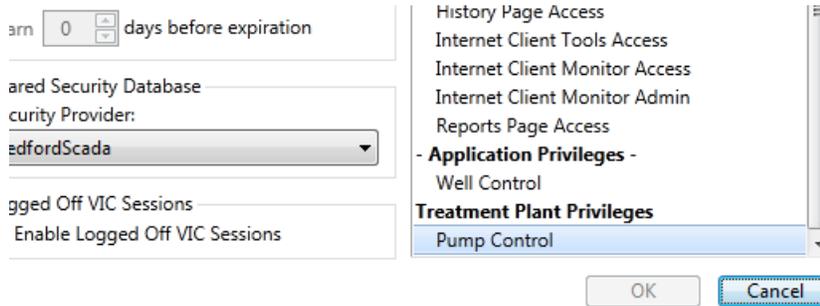
Security for this complex and ever-changing application can be managed as follows:

1. Organize the tags for the three treatment plants into three hierarchies: Plant 1, Plant 2 and Plant 3. All of the tags for each plant will be children of their respective parent. (Tag browser image simplified for this example.)

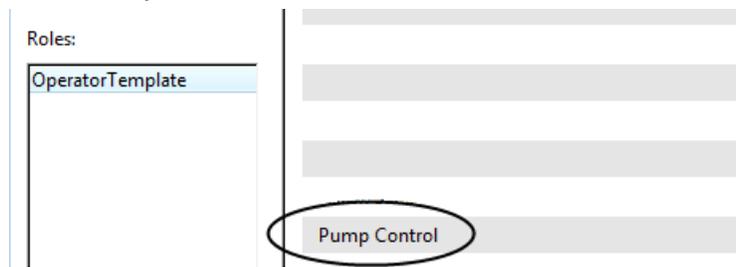


2. Create an application privilege and apply it to all the output tags in all three plants.

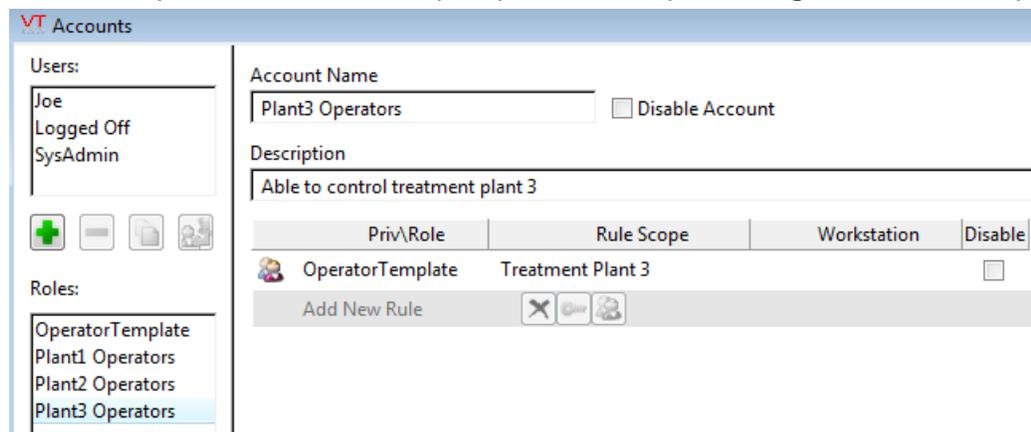
If there are sub-processes within a plant that are controlled by different classes of operators, then more application privileges will be required. The point is that there is no need to create a separate set of application privileges for each plant.



3. Create a generic security role that is assigned the application privilege(s) created in step 2.



4. Create three more roles. Each will be assigned one rule as follows: The generic security role, limited in scope by one of the parent tags created in step 1.



5. Create a user account for each employee.
6. Assign to each employee the role or roles that match their working location.

If an employee transfers from one treatment station to another, you need only change their assigned role. If there is a change in policy granting all operators increased or reduced privileges, you need only change the template security role, thereby instantly updating the privileges of all employees.

Note: Warning: Rule Scope should be applied only to application privileges or to the tag-related system privileges, Questionable and Manual Data. Limiting a system privilege by a rule scope is the same as denying the privilege.

Related Information:

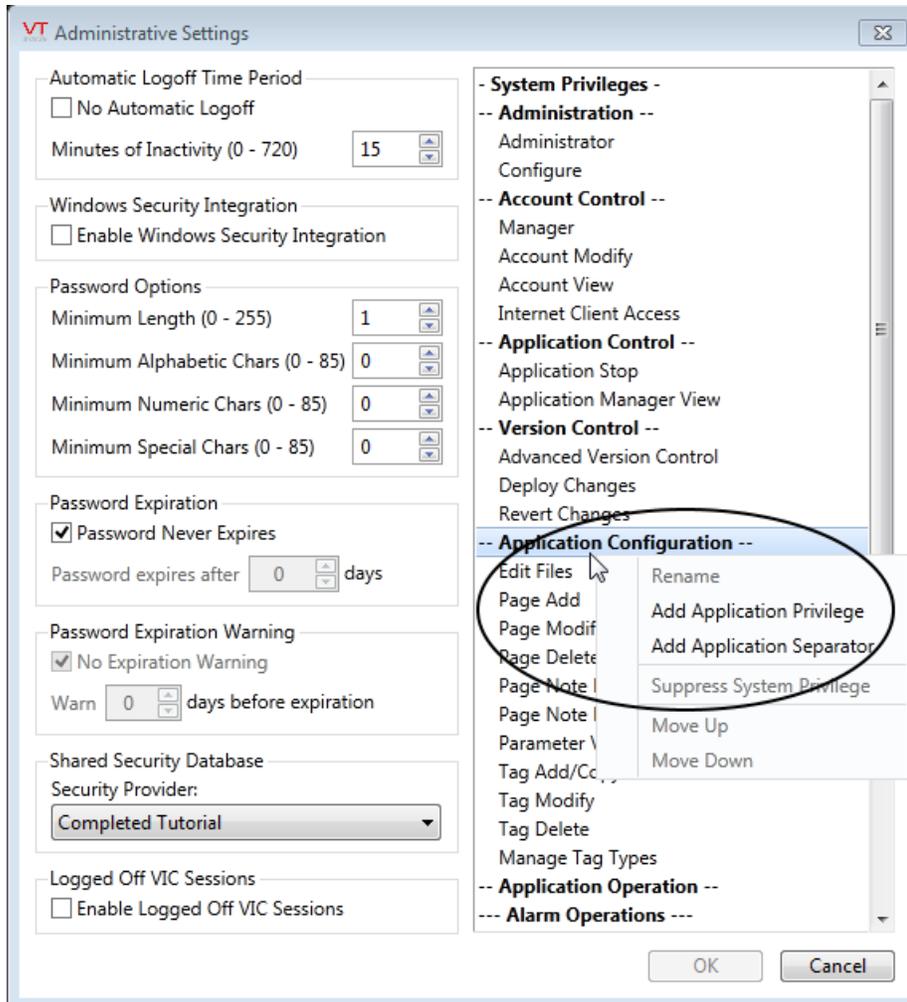
...Protect Pages and Output Tags – Application privileges reference and instructions.

...Context Tags, See the VTScada Developer's Guide – Organizing tags into hierarchies.

...Accounts and Roles – Creating accounts and roles.

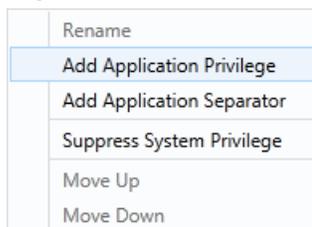
Options for Security Settings

Accounts that possess the Administrator privilege can control options such as minimum password length, automatic log-off time and more. These controls can be found within the Administrative Settings dialog.



This panel is used to control security configuration options that apply to all accounts. It is also where you can create and manage application privileges for your output tags and application pages.

Of particular note is the privilege list. In addition to showing the system privileges, this is where you define new application privileges. You can right-click on this list to open a menu of options:



Only application privileges can be renamed. The rename option is disabled if you right-clicked on a system privilege. Also, only application privileges may be moved up or down the list.

Privileges can be hidden from the view of managers (suppressed). This enables administrators to limit the range of privileges that managers are able to assign.

The automatic lock-out feature, where users are locked out of their accounts for a period of time after N failed password attempts, is not configured in the user interface. Instead, you must add two application properties.

If it is your intention to share security between applications by selecting an OEM layer to provide the security configuration, do that before spending time configuring accounts and other security options.

The Logged Off VIC Sessions option is used for VTScada Internet Client connections. When checked, a remote user can log off, but retain a connection to the VTS Internet Server. This makes it slightly faster for the user to log back in, but at the cost of a client connection that is not freed for use by others.

Related Information:

...Automatic Log-off Time Period – Log users off when the application has been left idle.

...Password Options – Define the required strength of passwords.

...Confirm Change to Password Options – Dialog reference.

...Security-Related Settings – Control via properties in Settings.Dynamic

... MaxFailedLoginAttempts, AccountLockoutTime, MaxRateFailedLoginAttempts– Logon-attempt limiting options.

...Shared Security Between Applications – Applications that are based on a common OEM layer can share a security database.

Related Tasks:

...Suppress or Reveal Privileges

Automatic Log-off Time Period

VTScada can log users off when the application has been left idle for a defined period of time. The setting in the Administrative Options dialog will apply to all users, but you may also set a unique log-off time for each user in the Accounts dialog.

The default time period is 15 minutes. The period can be set from 0 (no automatic log-off) to 720 minutes (12 hours). You may also disable this feature by checking the No Automatic Log-off option.

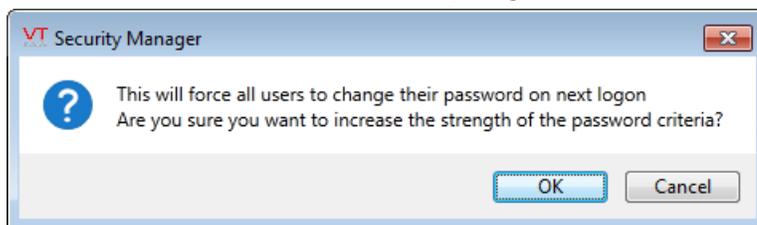
Related Information:

...Options for Security Settings – Dialog where these controls are found.

... AutoLogOff, AutoLogOffMin , and AutoLogOffMax – Application properties

Password Options

These four spin boxes define the required strength of passwords. Password strength is a measure of how difficult it is to guess the word. In general, passwords that can be found in a dictionary are easily guessed by a hacker. Words that include a mix of letters, numbers and symbols are more difficult. When these values are changed, all users must reset their passwords the next time they log in.



Note: When you change any of these values, all existing users will be required to change their password on their next log-on.

Minimum Length – Sets the overall minimum number of characters. It ranges from 0 characters (no restriction) to 255 characters. The minimum password length will always be at least the sum of the other 3 minimum values.

If anyone attempts to set a password shorter than this length, a warning dialog will be displayed.

Minimum Alphabetic Characters – Sets how many letters must be included in the password.

Minimum Numeric Characters – Can be set to a number greater than 0 if you want to require passwords to contain numbers.

Minimum Special Characters – Can be set to a value greater than 0 if you want to require passwords that contain symbols such as @#\$%, etc.

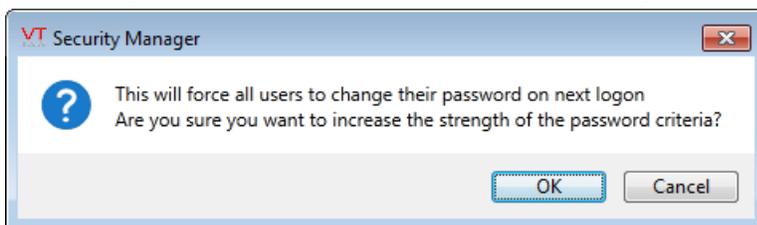
If an attempt is made to set a password that does not have the required number of any type of character, a warning dialog will be displayed. This will also tell the user how many of each required type of character must be used.

Related Information:

...Options for Security Settings – Dialog where these controls are found.

Confirm Change to Password Options

If you have changed the Password Options in the Administrative Settings dialog to increase the required password strength, all existing users will be forced to change their passwords on their next logon. The following dialog will be displayed before you can close the Settings dialog, to remind you of this fact and confirm that you wish to proceed.



Click OK to acknowledge the dialog and proceed with increasing the password security strength. Click cancel to return to the Administrative Settings dialog.

Password Expiration Warning

If password expiration is enabled, you can also provide users with a warning that will appear each time they log-on, for X days before the next

expiration of their password. This option is available only if the Password Never Expires box is *not* checked. You cannot set the number of days in warning period to be larger than those in the expiration period.

Related Information:

...Password Options – Define the required strength of passwords.

Suppress or Reveal Privileges

System privileges can be suppressed from view using the Administrative Settings dialog. This will prevent managers from granting a privilege as well as preventing users from knowing that the privilege exists.

To suppress system privileges using the Administrative Settings dialog:

1. Select the system privilege you wish to suppress from the System Privilege Suppression list.
2. Click the Suppress button.
The Suppress button becomes disabled while the Reveal button becomes enabled when the suppressed privilege is selected in the list.

To reveal suppressed system privileges using the Administrative Settings dialog:

1. Select the system privilege you wish to reveal from the System Privilege Suppression list.
The Reveal button will become enabled if the privilege has been suppressed, whereas the Suppress button will become enabled if the privilege has been revealed.
2. Click the Reveal button.
The Reveal button becomes disabled while the Suppress button becomes enabled. This indicates that the privilege is now revealed.

Related Information:

...Options for Security Settings – Dialog where these controls are found.

Shared Security Between Applications

Applications that are based on a common OEM layer can share a security database. This means that managers can configure one set of users, who

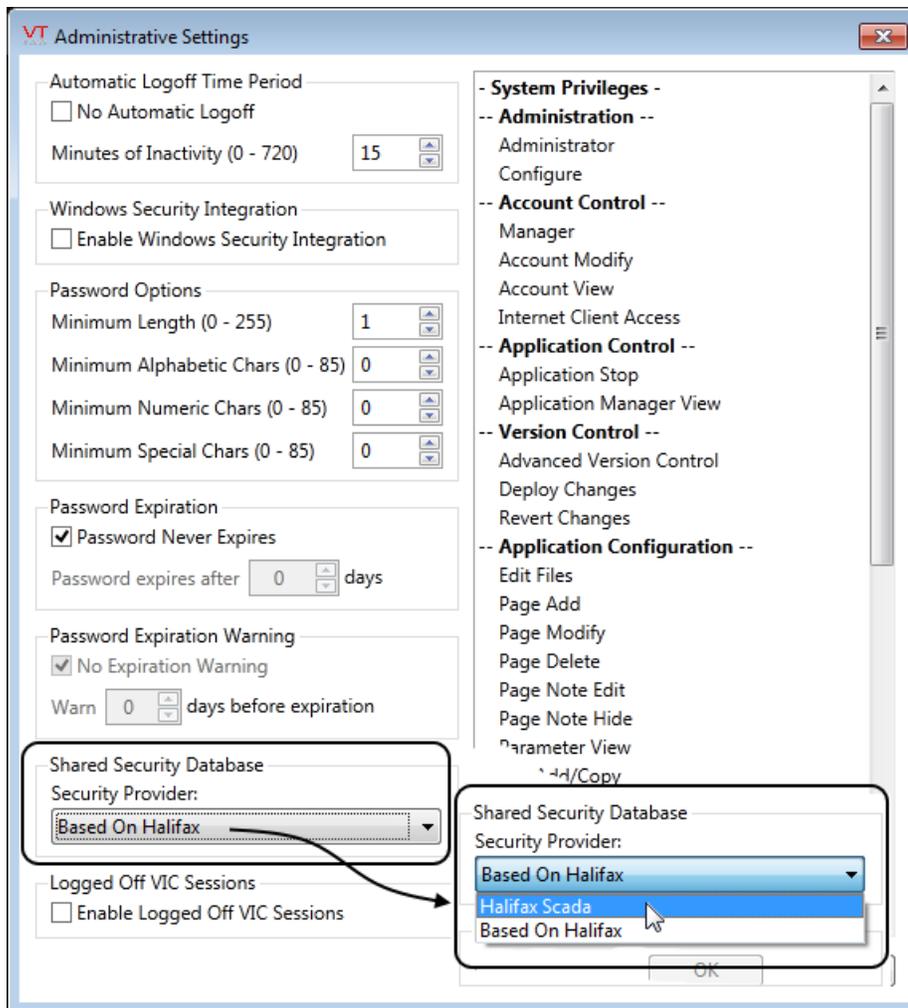
will have the same logon name, password and privileges for all the applications that use the same security database.

Shared security can be enabled at any time in the application layer by selecting the OEM layer that is to provide security. The OEM layer need not be secured at the time that you select it as the security provider, but you are strongly advised to secure it first.

At least one security account will exist in the dependent application, since only accounts with the Administrator privilege can access the Administrative Settings dialog. When an OEM layer is selected to act as the security provider, all accounts and other security settings in the current application will cease to function, in favor of accounts and settings configured in the security provider layer.

To enable Shared security, log in to your application with an account that has the Administrator privilege and open the Administrative Settings dialog. In the following example image, the shared security section has been highlighted.

The default security provider is the current application – in this example, "BasedOnHalifax".



Shared Security is enabled as soon as you select an OEM layer to be the security provider (in this example, Halifax Scada).

Note: VTScada (not just the current application) must be re-started on all machines in order to complete the process. This should be done immediately after configuring shared security.

Until you re-start the VTScada and the application, the account you used to make this configuration change will still operate within the application. If you are working with security through the Application Properties dialog of an application that is not running, the Application Properties dialog will need to be closed and re-opened to achieve the same effect. After the application has re-started, all accounts and other security settings in the application will stop working, replaced by those in the selected security provider. You may still use the security dialogs within the

application, but rather than working with the current application's security database, you will be working with the security provider's database. To disable Shared Security, change the security provider back to the current application and re-start. Accounts and other security settings that had previously been created within the application will resume.

Read-Only Workstations

You can configure a workstation to have read-only access to an application, regardless of the privileges assigned to the logged-in user at that workstation. This may be especially useful for workstations located in unsecured areas or for VTScada Internet Client access.

The read-only workstation privilege takes precedence over all other security privileges. If set for a particular workstation, then all I/O write access will be denied. Attempts to operate any control will result in the Access Denied dialog box being displayed.

To configure a workstation as read-only, add the following line to the [System] section of that computer's Workstation.Dynamic file, and import the file into the application's working set.

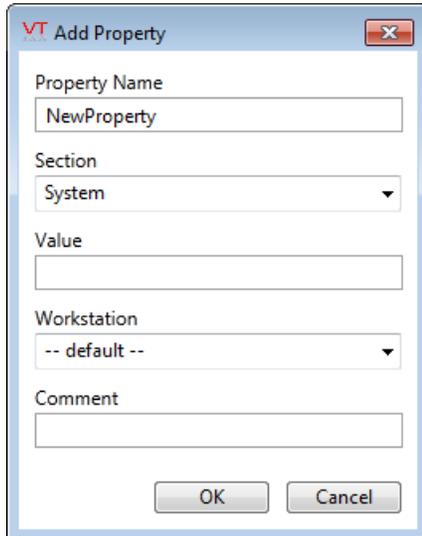
```
[System]
ReadOnlyStation = 1
```

Note: a Workstation.Dynamic file is not named "Workstation.Dynamic". Substitute the name of the computer to which the configuration variables should apply, for the word "workstation". You can have a different workstation. dynamic file for each workstation in your network.

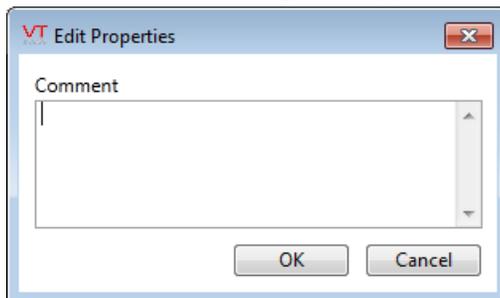
If the workstation configured to be read-only is also a VTScada Internet Server, then all VTScada Internet Client connections to that server will have read-only access. Note that if you are running a multi-server environment, the read-only server should be configured in Legacy mode to prevent automatic fail-over to a server that is not read-only.

Steps to define a read-only workstation:

1. Open the Application Configuration dialog.
2. Click on the Insert button
The Add Property dialog will open.



3. Set the property name to "ReadOnlyStation".
4. The section should remain as "System".
5. Set the value to 1.
6. Select the workstation that is to be flagged as Read-Only.
7. Enter a comment, describing the new property.
Comments will be stored on the line below the property in the Workstation.Dynamic file.
8. Click OK
The dialog closes. Note that the new property will not be saved until you apply your changes.
9. Click Apply.
The Comment dialog will appear.



10. Type a comment into the Comments dialog and click OK.

This comment is for the VTScada version control system and should explain why the new property is being added, unlike the earlier comment that explains what the property does.

Note that you can also modify security rules so that they are in effect only at named workstations.

SSL Certificates for Internet Security

An SSL certificate is a digitally-signed authentication that fulfills the following requirements:

- Identifies a host computer, organization, or individual, carrying with it an assurance (warranted by a Certification Authority (CA)) that the host computer, organization, or individual is whom they represent themselves to be, and providing an electronic means of verifying that a communication came from that individual, and not from someone else posing as them.
- Contains a public key and provides assurance that the key has not been tampered with.

An SSL authentication certificate, digitally-signed by a CA can be trusted on the basis that a CA will not digitally sign a certificate unless they have adequate proof that the host computer or individual has a right to represent itself by that information.

Account name and password authentication is all that protects access to the VTScada Internet Server, unless you use other security mechanisms, such as a virtual private network (VPN)). The web or mobile browser needs to be sure that it is communicating with a legitimate VTS/IS before transmitting a name and password. To protect these authentication credentials, SSL is used, with the VTScada server providing an SSL certificate to the web browser or VIC.

Note: "SSL" is the acronym for the Secure Sockets Layer security protocol. SSL enables you to securely transmit private data over the Internet by creating a secure connection between a client and a server. SSL is an older technology and the term has become the de-facto name for

internet security. While the term "SSL" is used here by convention, VTScada does use the more modern Transport Layer Security.

An SSL certificate carries with it a public key that is secure and has not been tampered with. This public key is half of a pair of an asymmetric set of keys. One key is called the private key, while its mate is called the public key. Data encrypted using the private key can only be decrypted using the public key, and data encrypted using the public key can only be decrypted using the private key.

The private key is held securely by the organization that owns the SSL certificate containing the public key (e.g. your organization). No one, not even the CA who issues the SSL certificates knows the private key; rather, the CA knows only the public key, and digitally signs the SSL certificate to provide assurance that the public key it holds is the mate to the private key held by the party receiving the certificate.

Note: You must safeguard and keep backups of the private key, as well as the SSL certificate.

VTScada makes it easy for you to generate a request for an SSL certificate from a Certification Authority (such as VeriSign) using the SSL Certificate tab of the VTScada Internet Client/Server Setup dialog. This request is formed and deposited on your Windows® operating system clipboard. You may then send this request to the CA, either by email, or using an online form (if provided by the CA at their web site). The request is persistently lodged in VTS/IS¹ request store, and when the reply arrives from the CA, the VTScada Internet Client/Server Setup dialog must be used again to process the reply from the clipboard into the VTS/IS' store. This processing phase removes the request from the request store and places the SSL certificate into the VTS/IS' certificate store, binding it to the correct private key.

Note: It is highly recommended that you use the Microsoft Management Console (MMC) to backup the certificate and private key. If the registry

¹VTScada Internet Server

has to be restored or is lost, the private key will be permanently lost as well. If you do not have a backup of your private key, there is no way to re-generate it. If you irretrievably lose your private key, you will have to purchase a new SSL certificate. Therefore, you should ensure that you store your certificate request and subsequent certificate in PKCS #12 (.PFX) format, and include the private key in the backup.

It is recommended that the certificate request be made on the same PC that will be the VTS/IS. After you've done so, you may back up the SSL certificate and copy it to the PC for which the request was made. It is also important that the certificate be processed using an account with administrative privileges.

The key will be encrypted to protect it during the backup process; you will therefore be required to enter a password.

Next Steps:

...Generate a Request for an SSL Certificate

...Process an SSL Certificate

...Configure a VTS Internet Server – See the VTScada Developer's Guide – Configuring a VTScada Internet Server? Go back to the generalized steps.

Related Information:

...Redundant SSL-Protected Servers

Generate a Request for an SSL Certificate

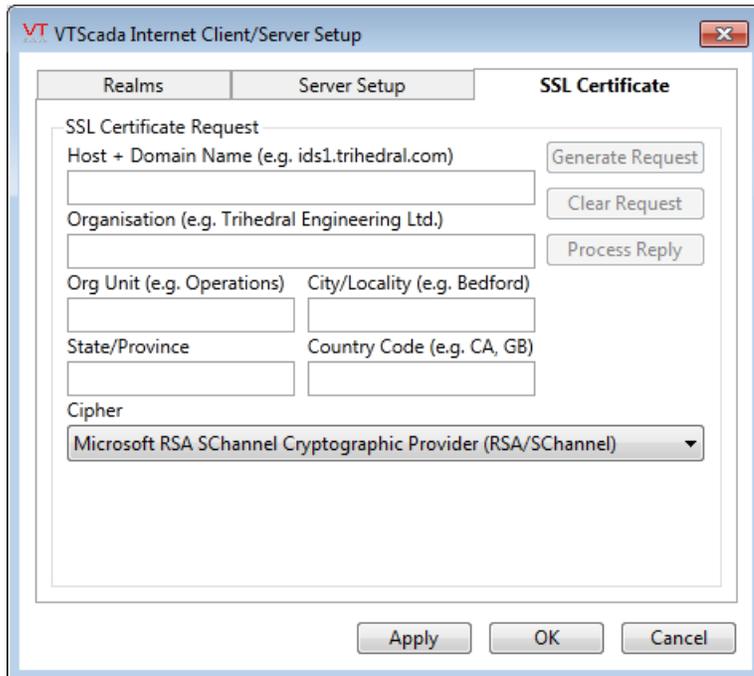
The SSL tab of the VTScada Internet Client/Server Setup dialog is used to request new SSL certificates for your VTS/IS.

Note: The process will fail unless the following conditions are met:
You must be using the same account as VTScada will use when running as a VTS/IS
As the same user, you must then export the SSL certificate and its private key from the user certificate store to a file.

After requesting the certificate, you must then import the SSL certificate and its private key into the computer certificate store. You must be

logged into your computer (not VTS) as a user with administrative rights in order to do this.

1. Ensure that VTScada is running using the same user account that it will use when running as a VTS/IS.
2. Open the VTScada Application Manager (VAM)
3. Click the Internet Client button.
The VTScada Internet Client/Server Setup dialog opens.
4. Click the SSL Certificate tab. The dialog appears as shown.



The screenshot shows the 'VTScada Internet Client/Server Setup' dialog box with the 'SSL Certificate' tab selected. The dialog contains the following fields and controls:

- Host + Domain Name (e.g. ids1.trihedral.com):** A text input field with a 'Generate Request' button to its right.
- Organisation (e.g. Trihedral Engineering Ltd.):** A text input field with a 'Clear Request' button to its right.
- Org Unit (e.g. Operations):** A text input field.
- City/Locality (e.g. Bedford):** A text input field.
- State/Province:** A text input field.
- Country Code (e.g. CA, GB):** A text input field.
- Cipher:** A dropdown menu currently showing 'Microsoft RSA SChannel Cryptographic Provider (RSA/SChannel)'.
- Buttons:** 'Apply', 'OK', and 'Cancel' buttons are located at the bottom of the dialog.

5. Enter the host and domain name in the Host + Domain Name field. The name you supply must exactly match the host + domain name supplied in the URL used to access the VTS/IS. For example:

`myserver.trihedral.com`

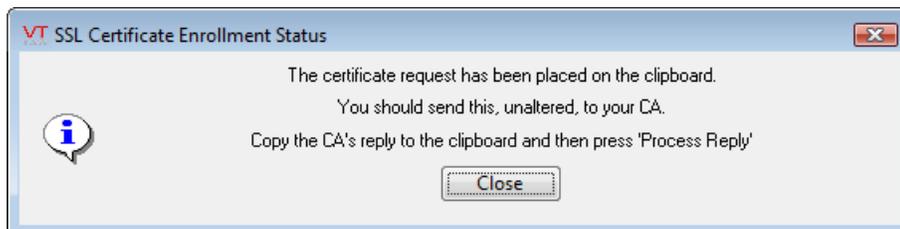
Where, "myserver.trihedral.com" is the host + domain name, "myserver" being the host, and "trihedral.com" being the domain name.

6. Enter the name of your organization in the Organization field.
7. Fill in the remaining identifying fields.
8. Select the cipher you wish to use for cryptography from the Cipher drop-down list.

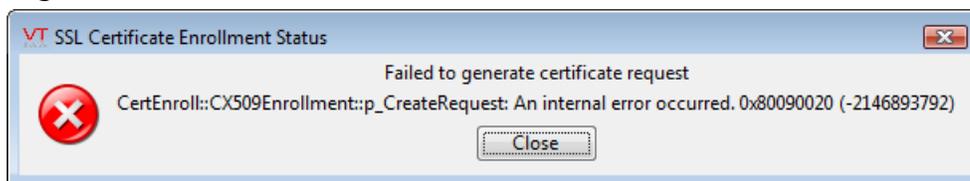
Note that there is normally only one cipher ("Microsoft RSA SChannel Cryptographic Provider (RSA/SChannel)") available for selection, unless you have installed a custom cryptographic package.

Once all fields have been entered, the Generate Request button becomes enabled.

9. Click the Generate Request button. VTScada compiles the data you've entered and displays the following dialog:



If the request failed, the Enrollment Status dialog will display an error message:



10. Open the text editor of your choice (Notepad, UltraEdit), or paste (Ctrl + V) the clipboard contents into your CA's online form (if available).
11. Select Edit | Paste (or press Ctrl + V) to paste the certificate request into your text editor. The pasted request begins with "-----BEGIN CERTIFICATE REQUEST-----" and ends with "-----END CERTIFICATE REQUEST-----".
12. Save the text file.
13. Send the text file to your Certificate Authority (such as Thawte or VeriSign). It is not essential to perform the certificate request on the same PC for which the request is being made. You can request a certificate for any PC; however, the CA's reply must be processed into the store of the PC on which the request was made.

Note: When VTScada generates the certificate request, a matching public/private key pair is generated. The public key is encoded into the certificate request and is sent to the CA. The private key is placed in a secure, encrypted key store. If you do not take a backup of your private key, a system restore operation or catastrophic computer failure will

cause loss of the private key. This will require that you generate a new key and a new request. Therefore, it is highly recommended that you use the Microsoft Management Console (MMC) to backup the certificate request and private key. Once you receive your SSL certificate and subsequently process it, you should again do a backup using MMC.

Next Steps:

...Process an SSL Certificate – Use the certificate you have generated.

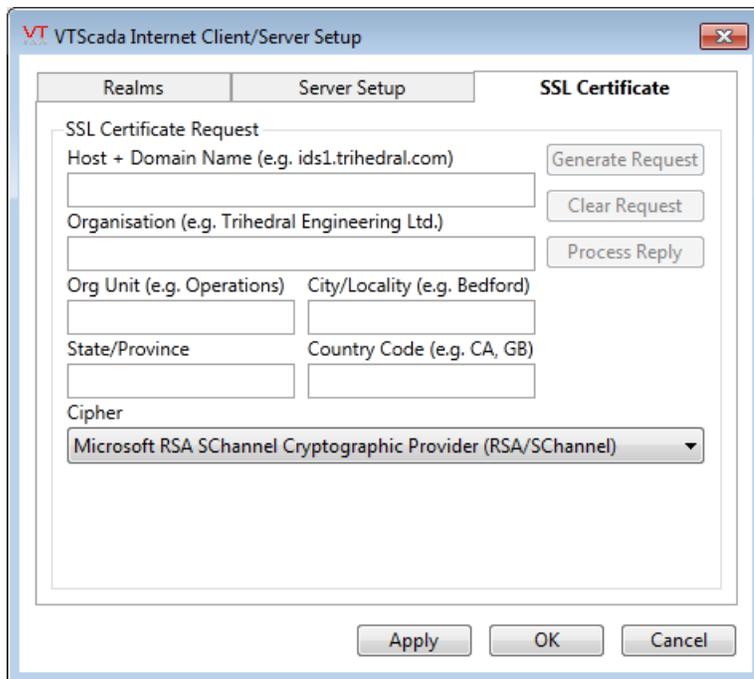
Process an SSL Certificate

Once you have sent an SSL certificate request to a Certificate Authority and the CA has validated your request, you will receive a reply containing the certificate. To process this information, use the following steps.

The SSL certificate will be generated in the certificate store for the logged in user (which should be the same account that the VTS/IS will use). After processing the certificate reply, the certificate (and its private key) must be exported from the user's certificate store and imported into the local computer's certificate store using the Microsoft Management Console and an account that has administrative rights.

For further information on importing and exporting certificates, please refer to Microsoft's Website: <http://windowshelp.microsoft.com/Windows>

1. Copy the CA's reply to the Windows clipboard by selecting the certificate including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines, and pressing Ctrl + C.
2. Open the SSL Certificate tab of the VTScada Internet Client/Server Setup dialog.



3. Click the Process Reply button.

Note: VTScada processes the reply by removing the request from the request store and placing the SSL certificate into the VTS/IS' certificate store, binding it to the correct private key. The CA's reply must be processed into the store of the PC on which the request was made. After you've done so, you should back up the SSL certificate and copy it to the PC for which the request was made.

4. Run the Microsoft Management Console (MMC) under the user account that VTScada is running in.
 - a. From the File menu, add the Certificates snap-in for "My user account".
 - b. In the tree on the left, expand "Certificates - Current User"
 - c. Expand "Personal" and click "Certificates".
 - d. In the right-hand pane you will see the SSL certificate.
 - e. Right-click on the SSL certificate and from the "All Tasks" sub-menu, select "Export".
 - f. Follow the Wizard, selecting to export the private key and to delete the private key if the export is successful.
 - g. Complete the wizard, exporting the certificate to a *.PFX file.

- h. If the export is successful, right-click the SSL certificate in the right-hand pane of MMC and select Delete to delete the certificate from the user account certificate store.
5. Stop VTScada and log out from your Windows account.
6. Log into Windows using an account that has administrative privileges.
7. Run the Microsoft Management Console (MMC).
 - a. From the File menu, add the Certificates snap-in for "Computer account".
 - b. In the tree on the left of the MMC, expand "Certificates - Current User" then right-click on "Personal".
 - c. From the "All Tasks" sub-menu, select "Import".
 - d. Follow the wizard selecting the certificate file that you saved earlier.
8. Locate the newly added certificate in Personal\Certificates, right-click it and pick Manage Private Keys... from the All Tasks sub-menu.
9. Click Add and add the user account you will be running VTScada as to the security list, granting Read access.
10. Run REGEDIT as administrator.
11. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates\MY.
12. Right-click the tree-node and select Permissions... from the menu.
13. Click Add and add the user account you will be running VTScada as to the security list, granting Full Control access.
14. Locate the Subject field of the certificate, noting the line: CN = YourServer.Name.Com.
15. Edit the VTScada SETUP.INI file. In the [SYSTEM] section, add *SSLCertName = YourServer.Name.Com* where YourServer.Name.Com should be replaced by the actual text from your certificate.
16. Reboot the workstation. (This step may not be required in all situations.)
17. Start VTScada and configure a secure realm.

As an alternative to setting permissions to a specific user account in MMC and REGEDIT, you can set them for a group, such as Domain Users. VTScada will now be able to access the SSL certificates and run HTTPS connections for VICs, once configured

Note: It is highly recommended that you use the Microsoft Management Console (MMC) to backup the certificate and private key. If the registry has to be restored or is lost, the private key will be permanently lost as well. The key will be encrypted to protect it during the backup process; you will therefore be required to enter a password.

Related Information:

...Configure a VTS Internet Server – See the VTScada Developer's Guide – Configuring a VTScada Internet Server? Go back to the generalized steps.

...Redundant SSL-Protected Servers

Redundant SSL-Protected Servers

If you want redundant SSL-protected VIC servers, you can use one of the following options:

- One certificate per server, in the case that each server uses a different URL. For example, if you had two servers named vtscada1.countyscada.com and vtscada2.countyscada.com, then you will need one SSL certificate per server name. Each server has its own SSL certificate installed and the server list contains both server names.
- You can use a wildcard SSL certificate (which costs more) and install the same certificate on both servers. Do this if you need to increase the number of servers, while continuing to use the same certificate.
- One certificate installed on multiple servers, in the case that the URL resolves to a networking device and that networking device automatically detects failure of one server and port forwards new connections to the other server or contains some sort of load balancer.

Related Tasks:

...Generate a Request for an SSL Certificate

...Process an SSL Certificate

Technical Reference for Security

Technical details for various features of the security system are provided in the following topics.

...Proximity Card Readers – Configuration details

...System Privilege Reference for Developers – Formatted to match the user interface.

...Enabled Features of a Secured Application – Features available when nobody is logged on.

...Storage of Security Data and Configuration – Files holding security-related information.

...Security-Related Settings – Configuration settings that are found in, or may be added to, Settings.Dynamic.

...Security Manager – See the VTScada Programmer's Guide. Scripting language features for security.

Proximity Card Readers

Proximity card readers are RF (Radio Frequency) devices, commonly issued to employees in order to permit access to a secured area by swiping or holding the card near a detector.

You can attach a proximity card reader to your workstations, then associate an employee's account to their card. Users can then log into their VTScada account by simply swiping their card by a reader.

USB – connected devices are supported. Install and configure your device according to the manufacturer's instructions.

Set the application property `pcProxEnable` to 1 so that VTScada can recognize the device.

Once this property is set, VTScada will begin scanning all ports between those identified by the properties `pcProxPortScanLow` (3) and `pcProxPortScanHigh` (16), excluding those on which a modem has previously been detected. When the device has been found, VTScada will create a connection to it.

Following this, all that remains is to associate each user's account with their card by opening the security accounts dialog, then swiping their card by the reader. While an account is loaded in the accounts dialog, VTScada will interpret the identification coming from the reader with that account.

Close the accounts dialog. From this point onwards, the user can log in to their account by allowing the device to detect their card.

Note: At the time of writing, only proximity cards from RF Ideas are supported by VTScada.

Related Information:

...pcProxEnable – Application property setting to enable a proximity sensor.

Related Tasks:

...Create Accounts

...Configure Alternate Identification

System Privilege Reference for Developers

Related Information:

...Add Privileges to Accounts – The process to add privileges to roles, then roles to accounts.

For programmers: Every application privilege will have an index number, starting at 16. Also, every application privilege is enumerated in the configuration file, Settings.Dynamic with values starting at zero. When writing expressions that check privileges, add 16 to the enumerated value in Settings.Dynamic.

Advanced Version Control Privilege

Scope	Application Configuration
If Granted	Enables operators to use the Version Control dialog to change or revert versions. Note that Version Control is only available if your VTScada license includes it.

Related Privileges Deploy Changes Privilege
Revert Changes Privilege

Account Modify Privilege

Scope Security-related

If Granted Enables operators to change their own passwords using the Accounts dialog.

Notes When you configure your operator accounts, you may choose to enter a temporary, generic password (such as the operator's first name), and grant the Account Modify privilege to these accounts. Operators may then logon to their accounts and modify their temporary password to one that is secure.
This privilege is not needed when operators are required to change an expiring password.

Account View Privilege

Scope Security-related

If Granted Enables operators to view (but not modify) their own privileges using the Accounts dialog.

Notes The Account View privilege provides read-only access to a list of the user's privileges.

Administrator Privilege

Scope Security-related

If Granted Provides operators the ability to change the application-wide administrative security settings using the Administrative Settings dialog.
Required for operations that modify Roles.

Notes Administrative settings that may be modified by operators granted the Administrator privilege include:

- Change the auto-logout time period. All operators will

automatically be logged off of their user account if the application has been left idle for the amount of time specified;

- Change the minimum length permissible for passwords;
- Suppress and reveal system privileges in all other security dialogs; and
- Add and modify application privileges.

Alarm Operation Privileges:

Alarm Acknowledge Privilege

Scope	Alarm Management
If Granted	Enables operators to acknowledge alarms while silencing the sounding audio alarm siren by clicking the Ack or Ack All buttons in the Actions button panel on the Alarm page.
Notes	Without the Alarm Acknowledge privilege, the Ack and Ack All buttons in the Actions panel on the Alarm page are disabled.
Related Privileges	Alarm Mute Alarm Silence

Alarm Disable Privilege

Scope	Alarm Management
If Granted	Enables operators to disable alarms in the event that equipment needs to be disconnected, or must undergo maintenance.
Notes	Disabling an alarm results in the suspension of any alarm signals from the selected equipment until the alarm is enabled. As a result, you should grant the Alarm Disable privilege with caution, and instruct operators on the proper method of disabling and enabling alarms.

Related Privileges Tag Modify Privilege

Alarm Mute Privilege

Scope Alarm Management

If Granted Enables operators to mute alarm sounds by clicking the Mute button on the Alarm page.

Notes Without the Alarm Mute privilege, the Mute button in the Actions panel on the Alarm page is disabled.

Related Privileges Alarm Acknowledge
Alarm Silence
Alarm Shelve

Alarm Page Access Privilege

Scope Application Operation

If Granted Enables operators to access the default VTScada Alarm page.

Related Privileges History Page Access Privilege
Reports Page Access

Alarm Shelve Privilege

Scope Alarm Management

If Granted Enables operators to shelve alarms, leaving them enabled but deactivating all notifications.

Notes A shelved alarm will still be triggered and logged, but will not be shown in the list of current alarms and will not activate any notification features.

Related Privileges Alarm Silence
Alarm Mute

Alarm Silence Privilege

Scope Alarm Management

If Granted	Enables operators to silence alarm sounds by clicking the Silence button on the Alarm page.
Notes	Without the Alarm Silence privilege, the Silence button in the Actions panel on the Alarm page is disabled.
Related Privileges	Alarm Acknowledge Alarm Mute Alarm Shelve

Application Stop Privilege

Scope	Application Operation
If Granted	Enables operators to stop an application.
Notes	VTS will not shut down while an application is running.

Application Manager View

Scope	Application Configuration
If Granted	When the property HideWAM is true, only accounts that possess this privilege may view the VTScada Application Manager.
Notes	Has no effect until HideWAM (HideVAM) is set to true.

Configure Privilege

Scope	Application Configuration
If Granted	Enables access to the Application Configuration dialog. Enables access to the Import File Changes button in the VAM. Enables access to the Remove button in the VAM.
Notes	Even with configuration privileges, an operator will not have full access to the tools in the dialogs noted. See the following list of related privileges that are required for full

configuration rights.

Related Privileges	Tag Add/Copy Privilege Tag Modify Privilege Tag Delete Privilege Edit Files Privilege Deploy Changes Privilege Revert Changes Privilege Page Add Privilege Page Delete Privilege Page Modify Privilege
---------------------------	--

Deploy Changes Privilege

Scope	Application Configuration
If Granted	Determines whether local changes can be made part of the application's working set of files. Additionally, deployed changes are distributed to all workstations running the application.
Notes	The Deploy Changes dialog is found in the Application Configuration dialog. If the Auto-Deploy option is selected, as it is by default, then the Deploy Changes button is not used.
Related Privileges	Configure Privilege Advanced Version Control Privilege Edit Files Privilege Revert Changes Privilege

Edit Files Privilege

Scope	Application Configuration
If Granted	Enables operators to use the Import File Changes dialog, and to manage files in the File Manifest.
Notes	Files that have been changed outside of the VTScada user interface must be imported to become part of the set of

working files. The File Manifest enables users to add or remove files that are not mandatory parts of an application.

Related Privileges Configure Privilege
Revert Changes Privilege
Deploy Changes Privilege

Group Delete Privilege

Scope Application Operation

If Granted Enables operators to delete pen groups from the Historical Data Viewer page.
Must also have the Group Modify privilege.

Related Privileges History Page Access Privilege
Group Save Privilege
Pen Modify Privilege

Group Modify Privilege

Scope Application Operation

If Granted Enables users to modify pen groups from the Historical Data Viewer page.

Related Privileges History Page Access Privilege
Group Delete Privilege
Group Save Privilege
Note Add

Group Save Privilege

Scope Application Operation

If Granted Enables operators to save new pen groups from the Historical Data Viewer page.
Must also have the Group Modify privilege.

Related Privileges History Page Access Privilege
Group Modify Privilege

Note Add
Pen Modify Privilege

History Page Access Privilege

Scope	Application Operation
If Granted	Enables operators to access the default VTScada Historical Data Viewer page.
Related Privileges	Alarm Page Access Privilege Note Add Pen Modify Privilege Reports Page Access Privilege Group Delete Privilege Group Modify Privilege Group Save Privilege

Internet Client Access Privilege

Scope	VTScada Internet Client
If Granted	Enables remote users without VTScada installed to access a VTScada application running on a VTScada Internet Server.
Notes	The Internet Client privilege is only pertinent to those VTScada installations that have also purchased a view-only or control-capable VTScada Internet Server license.

Internet Client Tools Access Privilege

Scope	VTScada Internet Client Connections
If Granted	Enables advanced users to access the various debugging and analysis tools included with VTScada over an Internet connection.
Notes	The Internet Client Tools Access privilege applies to VTScada Internet connections only.
Related Privileges	The Internet Client Access Privilege

Internet Client Monitor Access Privilege

Scope	VTScada Internet Client Connections
If Granted	Enables advanced users to view the Internet Client Monitor page within an application, if present.
Notes	The Internet Client Monitor Access privilege applies to VTScada Internet connections only. Do not confuse with the Internet Client Monitor application.
Related Privileges	The Internet Client Access Privilege

Internet Client Monitor Admin Privilege

Scope	VTScada Internet Client Connections
If Granted	Enables advanced users to view and operate the Internet Client Monitor page within an application, if present.
Notes	The Internet Client Monitor Admin privilege applies to VTScada Internet connections only.
Related Privileges	The Internet Client Access Privilege

Manager Privilege

Scope	Security-related
If Granted	Enables operators to add, copy, modify, and delete user accounts, and manage privileges for these user accounts.
Notes	Your application must always include at least one account with the Manager privilege for the purposes of maintaining security accounts for your application. If you wish to modify Roles, you must possess the Administrator privilege in addition to the Manager privilege.

Manage Tag Types

Scope	Application Development
If Granted	Enables developers to use the Redefine Type button in the Tag Browser and use the Manage Types dialog in the

	Application Configuration dialog.
Notes	The Redefine Type button can be extremely dangerous when used for a built-in VTScada tag. This privilege should be granted only to experienced developers.

Manual Data Privilege

Scope	Application Operation
If Granted	Enables operators who do not have the Tag Modify privilege to enter manual data for input and status tags, to override the value being reported for the tag from the I/O device.
Notes	Does nothing if the operator has the Tag Modify privilege.
Related Privileges	Tag Modify Privilege Parameter View Questionable Privilege

Note Add Privilege

Scope	Application Operation
If Granted	Enables operators to add notes to selected notebooks from the Historical Data Viewer page.
Related Privileges	History Page Access Privilege Pen Modify Privilege Group Delete Privilege Group Save Privilege

Page Add Privilege

Scope	Application Configuration
If Granted	Enables users to create new pages and widgets using the Idea Studio.
Notes	Granting the Page Add privilege enables the Add button in the Pages context menu.

Related Privileges Page Delete Privilege
Page Modify Privilege

Page Delete Privilege

Scope Application Configuration

If Granted Gives users the ability to delete pages and widgets using the Idea Studio.

Notes Granting the Page Delete privilege enables the Idea Studio's page or widget delete button.

Related Privileges Page Add Privilege
Page Modify Privilege

Page Modify Privilege

Scope Application Configuration

If Granted Allows a user to modify existing pages using the Idea Studio.

Notes This privilege must be granted before a user may open the Idea Studio.

Related Privileges Page Add Privilege
Page Delete Privilege

Page Note Edit Privilege

Scope Application Operation

If Granted Enables operators to add, modify and delete page notes.

Notes Granting this privilege enables the Page Notes button at the top of every page. No other configuration privileges need be granted for an operator to add or edit page notes.

Related Privileges Page Note Hide Privilege

Page Note Hide Privilege

Scope Application Operation

If Granted	Enables operators to hide or display existing page notes.
Notes	Granting this privilege enables the Page Note Display button at the top of every page.
Related Privileges	Page Note Edit Privilege

Parameter View Privilege

Scope	Application Operation
If Granted	Enables operators who do not have the Tag Modify privilege to view the properties of tags. Operators can right-click any basic I/O tag's widget, and select the Properties shortcut menu item. The tag properties folder will open.
Notes	Does nothing if the operator has the Tag Modify privilege.
Related Privileges	Tag Modify

Pen Modify Privilege

Scope	Application Operation
If Granted	Enables operators to modify the attributes of the pens plotting data on the Historical Data Viewer page.
Related Privileges	History Page Access Privilege Group Delete Privilege Group Modify Privilege Group Save Privilege

Questionable Privilege

Scope	Application Operation
If Granted	Enables operators who do not have the Tag Modify privilege to change the questionable flag on any tag.
Notes	Does nothing if the operator has the Tag Modify privilege.
Related Privileges	Alarm Disable

Manual Data Privilege

Reports Page Access Privilege

- Scope** Application Operation
- If Granted** Enables operators to access the default VTScada Reports page.
- Related Privileges** Alarm Page Access privilege
History Page Access Privilege

Revert Changes Privilege

- Scope** Application Configuration
- If Granted** Enables operators to roll back changes that have not been deployed.
- Related Privileges** Configure Privilege – The Application Configuration dialog cannot be accessed without the Configure privilege; therefore, the Configure privilege and the Revert Changes privilege must be granted together.
Advanced Version Control Privilege
Edit Files Privilege
Deploy Changes Privilege – If the Auto-Deploy option is selected, as it is by default, then there will be no undeployed local changes to revert.

Tag Add/Copy Privilege

- Scope** Application Configuration
- If Granted** Enables operators to add new tags or copy existing tags using the Tag Browser.
- Related Privileges** Tag Modify Privilege – Operators must also have the Tag Modify privilege in order to configure the new tag they are adding.
Tag Delete Privilege – If you wish users to have the ability to remove tags from your application, you may addi-

tionally grant the Tag Delete privilege.

Tag Delete Privilege

Scope	Remote Application Configuration
If Granted	Enables operators to delete tags using the Tag Browser.
Related Privileges	Tag Add/Copy Privilege Tag Modify Privilege

Tag Modify Privilege

Scope	Remote Application Configuration
If Granted	Enables operators to modify the properties of new and existing tags using the Tag Browser.
Related Privileges	Tag Add/Copy Privilege Tag Delete Privilege

Enabled Features of a Secured Application

It should be noted that in the case of secured applications, certain features will be available to users who have not logged on or do not have a user account, unless those features are protected from use by the creation of application privileges.

The following table identifies the features available to users of secured applications who have not logged on, and where possible, suggests a way to protect these features. Note that it is possible, (although not recommended,) to grant privileges to the Logged Off role.

Feature	Description	Suggested Protection
Viewing Operator Notes	Users who are not logged on may view the Operator Notes page.	
Viewing the Callout List	Users who are not logged on to a secured application are able to view the Callout list page	

Page Changes	Users who are not logged on to a secured application still have the ability to change pages in the application using the menu, hotboxes or page buttons.	Configure an application privilege and assign it to the system pages you wish to protect.
Sending Output Values to Equipment	Users who are not logged on to a secured application still have the ability to change the value of analog and Digital Output tags whose widgets are output control related (such as a command button, or entry field), even though you may have denied the Tag Modify privilege or the Manual Data privilege.	Configure an application privilege and assign it to the tags you wish to protect from data entry by selecting it from the tag's Privilege dropdown list in the tag properties folder.

Storage of Security Data and Configuration

Security-related information is stored in two separate files, each having a specific function. Details for each file follow the list.

- **Settings.Dynamic** (formerly, SecurityManager.ini was used)
Stores security-related administrative settings for the application.
- **Accounts.Dynamic**
Stores user account information (i.e. username, password, and privileges).

Settings.Dynamic

Changes to this file will not take effect until they are imported into an application using the Import File Edits feature of the Application Configuration dialog. In a secured application this action can only be performed by a user with configuration and file modification rights.

Unauthorized users cannot change security settings by tampering with application properties.

Application properties related to security can be used to configure:

- The default automatic log off time period. This is the amount of idle time after which the logged on user will automatically be logged off by the system. Each user may be given their own automatic log off time.
- The minimum length for user passwords.
- Suppressed privileges (see: Suppression of System Privileges).
- Default application privileges.

Accounts.Dynamic

The Accounts.Dynamic data file is used by the Security Manager to store user account data. This file is automatically generated by VTScada when you create your application.

Password hashing uses a salted, key-stretched, SHA2-512 algorithm. An AES-256 block cipher is used to encrypt account data. In addition, every user account has its own generated key. The only means of adding, copying, modifying, and deleting user accounts and their related passwords and privileges is by using the security dialogs provided by VTScada.

Information taken from one application's Accounts.Dynamic file will not be valid in another.

Security-Related Settings

Certain configuration settings related to security are stored in the file, Settings.Dynamic. Many of these variables can be changed only by directly editing this file in your application's root directory, and then importing the edited file using the Application Configuration dialog. Only authorized accounts may import a file that has been edited.

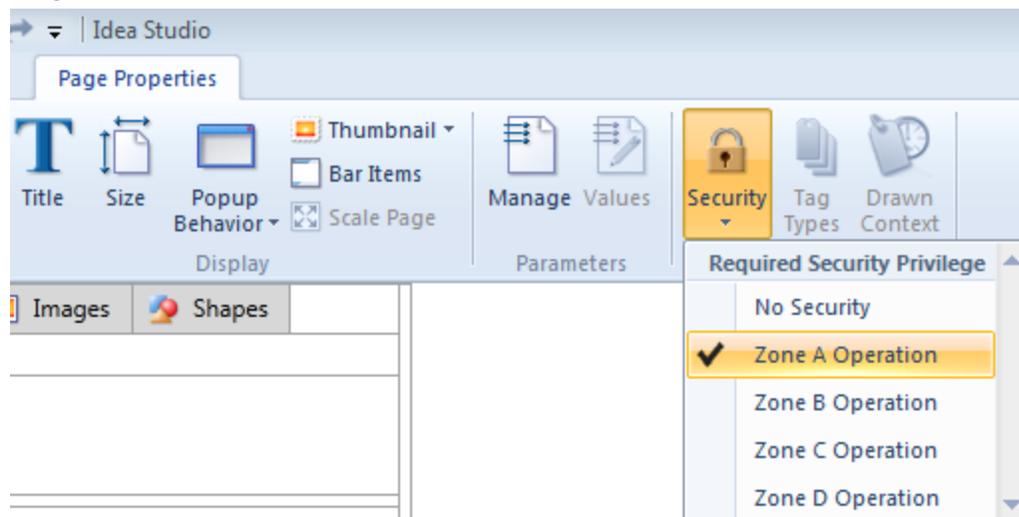
All application privileges that you create in an application are named according to the pattern PrivDescN where N is a number starting at 0. For example, if you have added 4 custom application privileges to your application, they would appear as follows:

```
<SECURITYMANAGER-PRIVAPP>
PrivBitsTotal = 4
PrivDesc0 = Zone A Operation,0
PrivDesc1 = Zone B Operation,1
```

Secure Your Application

```
PrivDesc2 = Zone C Operation,2  
PrivDesc3 = Zone D Operation,3
```

The label is used for display purposes, including the selection drop-down in each output tag's Merit tab and the security property of each page.



The number following the property sets its value, which is to be used in code. Note that this value is an offset from 16. Referring to the preceding example, where the page has been protected with the application privilege "Zone A Operation", the first few lines of the source code of that page will look like the following:

```
[  
  Title = "Overview";  
  Color = "<FFFFFFF";  
  SecBit = 16;  
]
```

PrivDes0, having number 0 in the list above, means that its actual value to be used in code is $16 + 0 = 16$.

Note: For the following list, take careful note of each property's section. Three distinct sections are used for security-related properties. A property will be ignored if it is associated with the wrong section.

... AccountLockoutTime

...AccountRateWindow

...ADGroupPrefix

...ADRefreshPeriod
...AutoAddADUsers
... AutoLogOff
... AutoLogOffMax
... AutoLogOffMin
...ForcePasswordAltIdSync
... GroupLogin
...IdleWebSessionTimeout
... MaxFailedLoginAttempts
...MaxRateFailedLoginAttempts
... NamespaceDelimiter
... OEMEncryptKey
... PasswordDisplay
... PasswordMinLen
... PasswordTimeLimit
... PasswordWarningTime
...pcProxBaudRate
...pcProxConnectCheckTO
...pcProxDatabits
...Security-Related Settings
...pcProxExcludePortx
...pcProxParity
...pcProxPortNum
...PcProxPortScanHigh
...pcProxPortScanLow
...pcProxStopBits
... PrivBitsTotal
... PrivDescX

- ... PromptForBadAltID
- ... ReadOnlyStation
- ...RootNamespace
- ... SecurityAlarmArea
- ... SharedContexts
- ... SharedSecurity
- ... SysPrivDefault
- ... SysPrivSuppress
- ... UserName

AccountLockoutTime

Indicates the minutes (or fractions of a minute) for which the user will be locked out after supplying an incorrect password MaxFailedLoginAttempts times, or MaxRateFailedLoginAttempts within the AccountRateWindow time frame.

Section: SecurityManager-Admin

Default: AccountLockoutTime = 1

Application restart required before changes will take effect.

Related Information:

- ...AccountRateWindow
- ... MaxFailedLoginAttempts
- ...MaxRateFailedLoginAttempts

AccountRateWindow

The window of time, measured in seconds, used to distinguish between logon attempts made by a person and those made by an automated attack.

If the number of consecutive unsuccessful logon attempts set by MaxRateFailedLoginAttempts are made within this time period, the account is locked.

If there are MaxFailedLoginAttempts consecutive failed attempts within any time frame, the account will be locked.

Section: SecurityManager-Admin

Default: AccountRateWindow = 15

Application restart required before changes will take effect.

Related Information:

AccountLockoutTime

MaxFailedLoginAttempts

MaxRateFailedLoginAttempts

ADGroupPrefix

The prefix to be added to a VTScada role name for the equivalent Active Directory Security Group.

Default: ADGroupPrefix = VTScada-

Section: <SecurityManager-Admin>

ADRefreshPeriod

The interval in seconds between checks for changes to the accounts in the Active Directory for the logged-on users.

Default: ADRefreshPeriod = 900

Section: <SecurityManager-Admin>

AutoAddADUsers

Controls whether authorized Windows accounts are automatically added to the VTScada Security Manager upon initial successful logon.

Must be added to the application's Settings.Dynamic file.

Default: FALSE

Section: <SecurityManager-Admin>

AutoLogOff

Indicates the minutes (or fractions of a minute) of inactivity after which the logged on user is logged off.

Section: SecurityManager-Admin

Default: AutoLogOff = 15

AutoLogOffMax

Indicates the highest amount of time that can be selected for the AutoLogOff variable.

This variable represents the maximum value that can be selected from the Minutes of Inactivity spinbox in the Administrative Settings Security Manager dialog.

Section: SecurityManager-Admin

Default: AutoLogOffMax = 720

AutoLogOffMin

Indicates the lowest amount of time that can be selected for the AutoLogOff variable.

This variable represents the minimum value that can be selected from the Minutes of Inactivity spinbox in the Administrative Settings Security Manager dialog.

Section: SecurityManager-Admin

Default = 0

ForcePasswordAltIdSync

By default, SecurityManager keeps encrypted passwords and alternate ids in sync during user update, but only if they were in sync to begin with. If this variable is 1, it will always keep them in sync.

If you intend to use an alternate ID for purposes other than for alarm dialler support, this value should be set to FALSE. See also: AlphaNumericXFormScheme

Section: SecurityManager-Admin

Default: Set to 1 in all new applications by the application template.

GroupLogin

Enables the group name field in the Please Logon dialog that is launched when the Logon button in the Display Manager's title bar is clicked. Accounts that have been assigned a group name will be able to enter it in that field.

The NameSpaceDelimiter property is also part of security group configuration, and must be specified before you can assign group names to accounts.

Section: System⁽¹⁾

Default = 0

⁽¹⁾In legacy applications, this property was defined in the <SecurityManager-Admin> section. It will work in either section, but the System definition takes precedence.

Related Information:

... NameSpaceDelimiter

MaxFailedLoginAttempts

Sets the number of times in a row that a user may attempt to log on with an incorrect password before being locked out of the system for AccountLockoutTime minutes. Defaults to twenty-five (25) consecutive attempts will result in the account being locked.

Note: Attempts made within a user-defined time span are subject to a lower threshold before lockout. See related information.

Section: SecurityManager-Admin

Default: MaxFailedLoginAttempts = 25

Application restart required before changes will take effect.

Related Information:

... AccountLockoutTime

...AccountRateWindow

...MaxRateFailedLoginAttempts

MaxRateFailedLoginAttempts

Sets the number of times in a row that a user may attempt to log on with an incorrect password, and within the time span defined by AccountRateWindow, before being locked out of the system for AccountLockoutTime minutes. This value is lower than MaxFailedLoginAttempts on the assumption that an automated attack will make repeated attempts much faster than would a person.

Defaults to three (3)

Section: SecurityManager-Admin

Default: MaxRateFailedLoginAttempts = 3

Application restart required before changes will take effect.

Related Information:

...AccountRateWindow

... AccountLockoutTime

... MaxFailedLoginAttempts

NameSpaceDelimiter

Required in order to specify the characters that will be used to separate security groups from account names. If NameSpaceDelimiter has a valid value, then group security accounts are enabled for your application (see "Security Namespaces").

Security groups enable the subdivision of the user base into "super users" and "group users,". The primary application is for realm-area filtering.

The GroupLogin property is also part of security group configuration, and must be enabled before users will be able to enter a group name while logging on.

Section: System⁽¹⁾

Default =

⁽¹⁾In legacy applications, this property was defined in the <SecurityManager-Admin> section. It will work in either section, but the System definition takes precedence.

Related Information:

... GroupLogin

OEMEncryptKey

Enables you to enter an encryption key for this application.

If left invalid (as it is by default), then no encryption key is required.

Section: SecurityManager-Admin

Default: OEMEncryptKey =

PasswordDisplay

Indicates the display that users view when entering their passwords in the Please Log on dialog (that appears when the Logon button is clicked) to help protect password entries from detection.

This variable can be set to one of three values:

Value	Description
0	Displays the characters in the password as they are entered by the user.
1	Displays asterisks equal to the password length as the characters are entered by the user (default).
2	Displays a number of asterisks that vary in length as the password is entered by the user.

Section: SecurityManager-Admin

Default: PasswordDisplay = 1

PasswordMinLen

Indicates the minimum number of characters that can appear in any user's password.

Section: SecurityManager-Admin

Default: PasswordMinLen = 1

PasswordTimeLimit

If the application is configured for automatic expiration of passwords, this variable stores the number of days that passwords will be valid for.

For each user, the time of their last password reset is stored within SecMgr.DAT.

Section: SecurityManager-Admin

PasswordWarningTime

This variable stores the number of days prior to password expiration during which the user will be warned upon login.

This feature applies only if the application is configured for automatic expiration of passwords, and also to provide a warning prior to password expiration.

Section: SecurityManager-Admin

pcProxBaudRate

The default baud rate for communication with the proximity card reader connection.

Default: pcProxBaudRate = 9600

Section: System

pcProxConnectCheckTO

Period at which the connection to the proximity card reader should be re-checked. Disabled when set to zero (the default).

Default: pcProxConnectCheckTO = 0

Section: System

pcProxDatabits

The default data bit setting for communication with the proximity card reader connection.

Default: pcProxDatabits = 8

Section: System

pcProxEnable

Controls whether ports will be scanned for a proximity card reader.

Defaults to off (0). Scanning will begin from the last port used.

Default: pcProxEnable = 0

Section: System

Related Information:

pcProxExcludePortx

pcProxPortNum

PcProxPortScanHigh

pcProxPortScanLow

pcProxExcludePortx

If it is known that devices other than a proximity card are on various ports, you should exclude those port numbers.

"x" should be replaced by the port to be excluded from scanning, and the value of the property should then be set to 1 to exclude that port.

For example, if an auxiliary input device is installed on port 3, you would set:

pcProxExcludePort3 = 1

Ports that are associated with modems are automatically excluded from scanning.

Default: no defaults.

Section: System

All port numbers from pcProxPortScanLow to PcProxPortScanHigh will be scanned, excepting those associated with modems, if pcProxEnable is set to true.

Related Information:

pcProxExcludePortx

pcProxPortNum

PcProxPortScanHigh

pcProxPortScanLow

pcProxParity

The default parity bit setting for communication with the proximity card reader connection.

Default: pcProxParity = 0

Section: System

pcProxPortNum

Set this value if you know the port number to which the proximity card reader will be attached. Not set by default.

Use with caution: the port number may change if the USB device is unplugged temporarily. In general, it is better to allow VTScada to search for the device.

Default: pcProxPortNum =

Section: System

Related Information:

pcProxPortNum

pcProxExcludePortx

PcProxPortScanHigh

pcProxPortScanLow

PcProxPortScanHigh

Specifies the highest port number to scan for a proximity card reader.

Defaults to 16.

Default: PcProxPortScanHigh = 16

Section: System

Related Information:

PcProxPortScanHigh

pcProxExcludePortx

pcProxPortNum

pcProxPortScanLow

pcProxPortScanLow

Specifies the lowest port number to scan for a proximity card reader.

Defaults to 3.

Default: pcProxPortScanLow = 3

Section: System

Related Information:

pcProxPortScanLow
pcProxExcludePortx
pcProxPortNum
PcProxPortScanHigh

pcProxStopBits

The default stop bit setting for communication with the proximity card reader connection.

Default: pcProxStopBits = 1

Section: System

PrivBitsTotal

Indicates the total number of application privileges that have been configured for this application.

PrivBitsTotal should not be set to invalid, or errors will occur in your application. If there are no application privileges for your application, you should set PrivBitsTotal to 0, as it is by default.

Each time you add a new application privilege using the PrivDescX variables (that is PrivDesc0 through to PrivDesc239), you must remember to increment PrivBitsTotal by 1. For example, if you've specified 5 application privileges using the PrivDesc0 through to PrivDesc4 variables, then you should set PrivBitsTotal to 5. It should be noted that this process is only necessary if you are manually adding application privileges. If you use the Administrative Settings dialog to add application privileges, VTScada automatically updates the PrivBitsTotal and PrivDescX variables.

Section: SecurityManager-PrivApp

Default: PrivBitsTotal = 0

PrivDescX

Where "X" is the number of the privilege starting at 0. Each PrivDescX variable is set equal to the name of the privilege.

If no application privileges have been added to your application, the PrivDescX variables are invalid.

Related Variables: The PrivBitsTotal variable represents a running total of the application privileges you have configured. PrivBitsTotal must always have a value matching the number of PrivDescX variables present for your application.

Section: SecurityManager-PrivApp

Default = Invalid

Note that when referred to by code, application privilege numbers are offset by 16. 0 -> 16, 1 -> 17, etc.

Example:

```
<SECURITYMANAGER-PrivApp>
PrivBitsTotal = 2
AppPrivDefault =
PrivDesc0 = Station 1 Access,0
PrivDesc1 = Station 2 Access,1
```

PromptForBadAltID

Indicates whether or not users should be prompted if validation of their alternate ID fails during user management. The purpose is to avoid passwords that will be the same on touchtone keypads.

If set to 1 (default), prompt user if validation of their alternate ID fails during user management. Duplicate passwords are disallowed.

If set to 0, do not prompt user if validation of their alternate ID fails during user management. Duplicate passwords are allowed

Section: SecurityManager-Admin

Default: PromptForBadAltID = 1

ReadOnlyStation

When set to true (1), tag write operations on the named workstation will be prevented.

Intended for use with named workstations, therefore this property should be added to a Workstation.Dynamic file rather than Settings.Dynamic.

Section: System

Default: ReadOnlyStation = 0

RootNamespace

If your applications makes use of realm-area filtering and if you allow remote access to the VTScada Internet Server (VIC or MIC) then you must define a realm for super-user access and declare it in the RootNamespace property. Accounts that are not part of any security group (super-users) will not have access to any realm otherwise.

Default: RootNamespace =

Section: System

SecurityAlarmArea

Indicates the area to display in the alarm list for security-related alarms.

Section: System

Default: SecurityAlarmArea = Security

SharedContexts

Matches the field "Enable Shared User Logins" of the security manager's Administrative Options dialog. When set, a user need only log in once on a workstation for all application contexts that share a security database. This applies to applications that share security with an OEM layer and to the separate contexts of the application and its control buttons in the VAM.

Section: SecurityManager-Admin

Default: SharedContexts = 1

SharedSecurity

Matches the field, "Enable Shared Security" of the security manager's Administrative Options dialog. Enables shared security if set to 1 in an OEM layer.

Section: SecurityManager-Admin

Default: SharedSecurity = 0

SysPrivDefault

Indicates the default system privileges available to those users who are not logged on to the application. The defined system privileges will also be granted to newly-created user accounts by default.

Related Privileges: AppPrivDefault

You may also define default application-specific privileges to those users who are not logged on to the application. The defined application privileges will also be granted to newly-created user accounts by default.

Section: SecurityManager-Admin

Default: SysPrivDefault =

SysPrivSuppress

Indicates whether system privileges have been suppressed or revealed. Each digit following the SysPrivSuppress variable represents a system privilege, each of which can be turned on or off using a "0", a "1", or a "2" respectively. Digits have meaning according to their placement counting from the right. Leading zeros are not required

If set to "0", the associated system privilege is revealed.

If set to "1", the associated system privilege is suppressed in all security dialogs, except the Administrative Settings dialog.

If set to "2", the associated system privilege is suppressed in all security dialogs, including the Administrative Settings dialog.

By default, all system privileges are revealed in all security dialogs. A table showing the index of each system privilege in the SysPrivSuppress variable can be found in: Suppress and Reveal System Privileges Using the SysPrivSuppress Variable.

Section: SecurityManager-Admin

Default: SysPrivSuppress = 000000000000000000000000000000000000

UserName

Indicates the registered username of the logged on user. If no user is logged on to the application, UserName will be invalid.

Section: n/a

Default = Invalid

Troubleshooting

Each new version of VTScada is rigorously tested before it is released to the market. Trihedral has customers who have been running their applications for more than 20 years without interruption. Nonetheless, problems can sometimes occur. The following list may help you through some of them.

If you experience a difficulty and need to call Trihedral's technical support line (1-800-463-2783), or email at support@Trihedral.com, you may be asked to create a crash dump so that VTScada engineers can trace the source of the problem.

A crash dump is a file that captures the state of the system when a problem occurs. The engineers at Trihedral are able to use this file to determine what caused the problem to occur, and therefore what can be done to fix it.

There are several ways to create a crash dump each of which is described in the following sections:

- You can use the Source Debugger application to generate a snapshot of a running process on command. This snapshot is referred to as a crash dump, even though the process is has not actually terminated.
- You can use the Problem Reports and Solutions tool in Windows Vista™, Windows 7 and Windows 8 to retrieve the crash dump file that was generated when an application fails.

Related Information:

...Tooltips Do Not Appear

...Add Scroll Bars to a Page – If viewing on a smaller screen

Related Tasks:

...Generate a Crash Dump from the Source Debugger

...Generate a Crash Dump from Windows Vista

...Generate a Crash Dump with Windows 7 or Later

Tooltips Do Not Appear

There are two reasons for why tooltips may fail to appear:

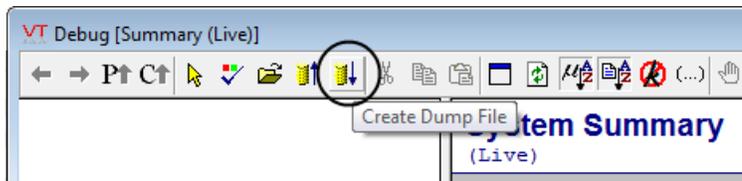
- Tooltip visibility in VTScada is controlled by an application property, ShowTip. Ensure that the value for this property is set to one (1).
- Tooltip visibility in general is controlled by a Windows™ registry setting. Ensure that the following registry key is set to one (as a dword, 00000001).
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"EnableBalloonTips"=dword:00000001

Generate a Crash Dump from the Source Debugger

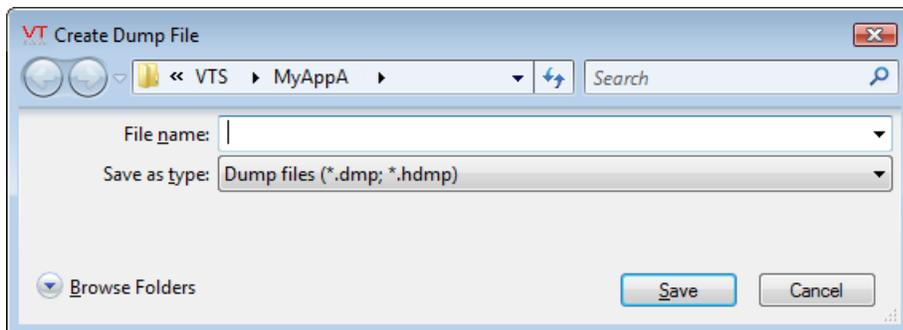
The Source Debugger is a script application that is included with every copy of VTScada. If you do not see it listed in the VAM, you will need to add it to the application list.

Note: Dump files created by the Source Debugger will typically be between 150 and 200 megabytes in size.

1. To start, run the Source Debugger.
2. Ensure that your application is also running.
3. Click on the Create Dump File button in the Source Debugger.



4. Browse to the location where you wish to save the dump file. You can expand the dialog box to show the folders and files by using the Browse Folders button in the lower left corner of the dialog box.



5. Enter a name for the dump file in the File Name field.
6. Click the Save button. The dump file will be generated and saved in the specified location.
7. Contact Trihedral Technical Support for instructions on where to send the dump file.

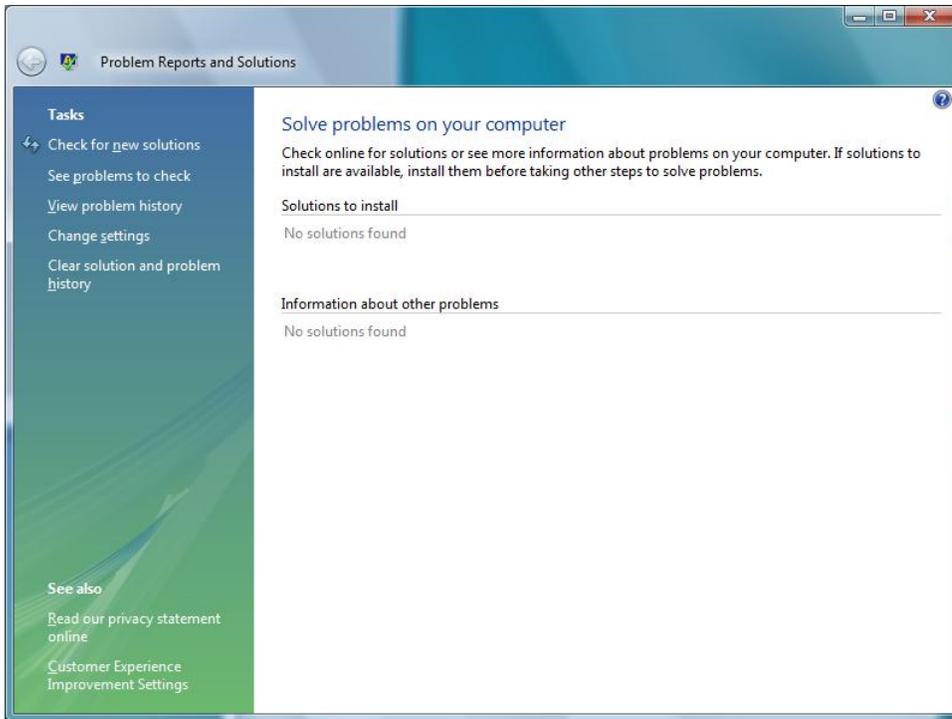
Generate a Crash Dump from Windows Vista

If your computer uses Windows Vista, you can follow these steps to collect an automatic crash dump.

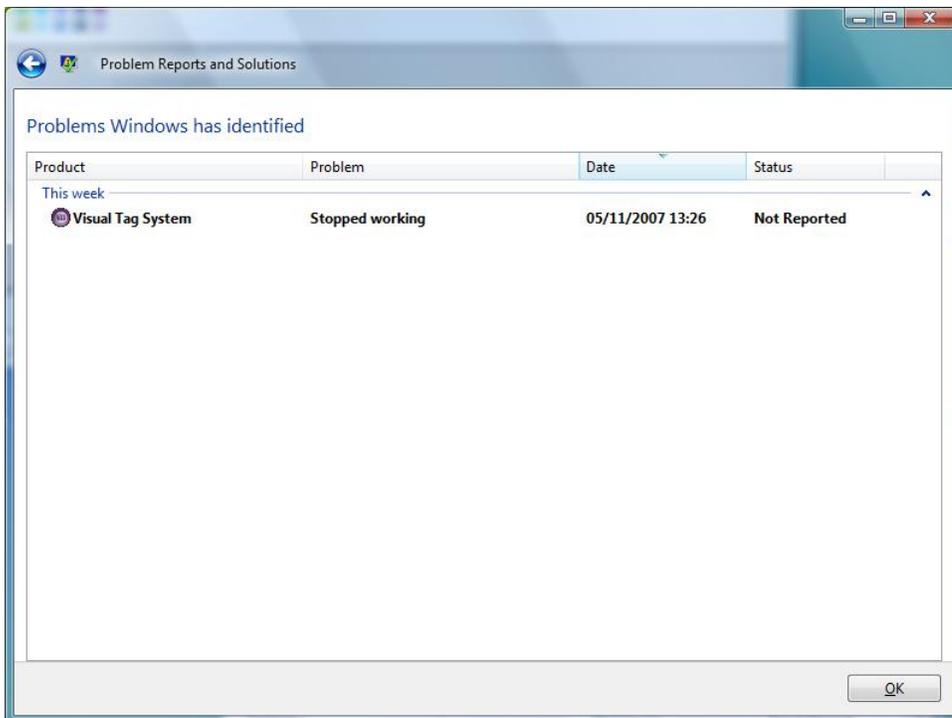
Note: The UserDump program included on the VTScada program CD (DumpTools\Setup.exe) , is supported only by operating systems prior to Windows Vista. Attempting to use it under Vista or later Windows versions may cause a system crash.

As an alternative, use the Task Manager to generate a dump file via a right-click on the process. This will output to the task manager's default location, as set by the Windows variable, %TEMP%.

1. From Control Panel, double-click Problem Reports and Solutions. You will see a window like this:

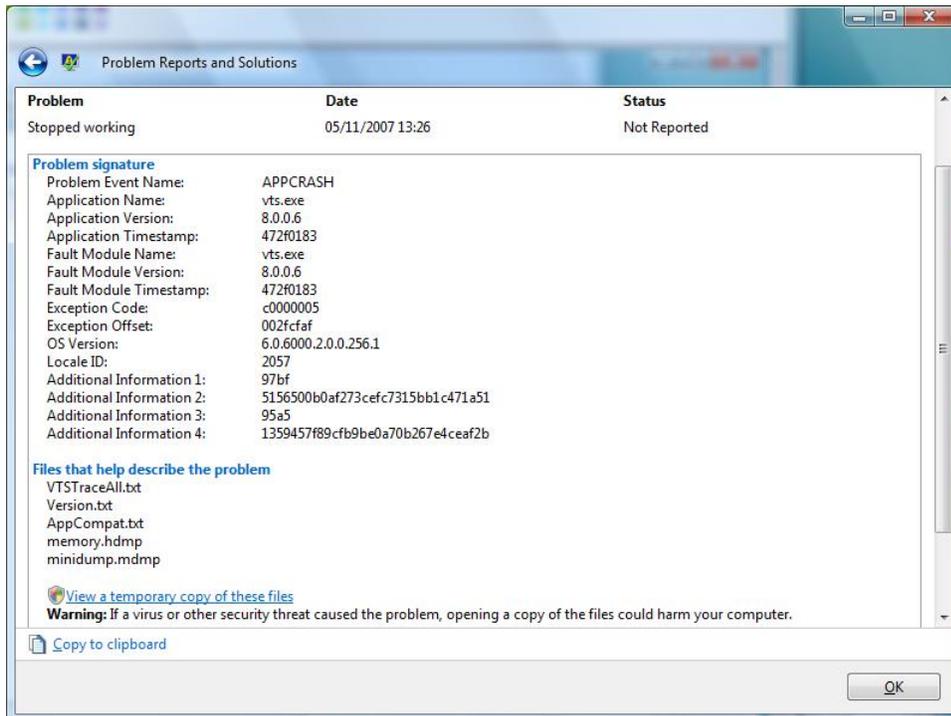


2. In the left pane, click View problem history.
 You will see a window that lists all known problem reports Windows has a record of, like this:

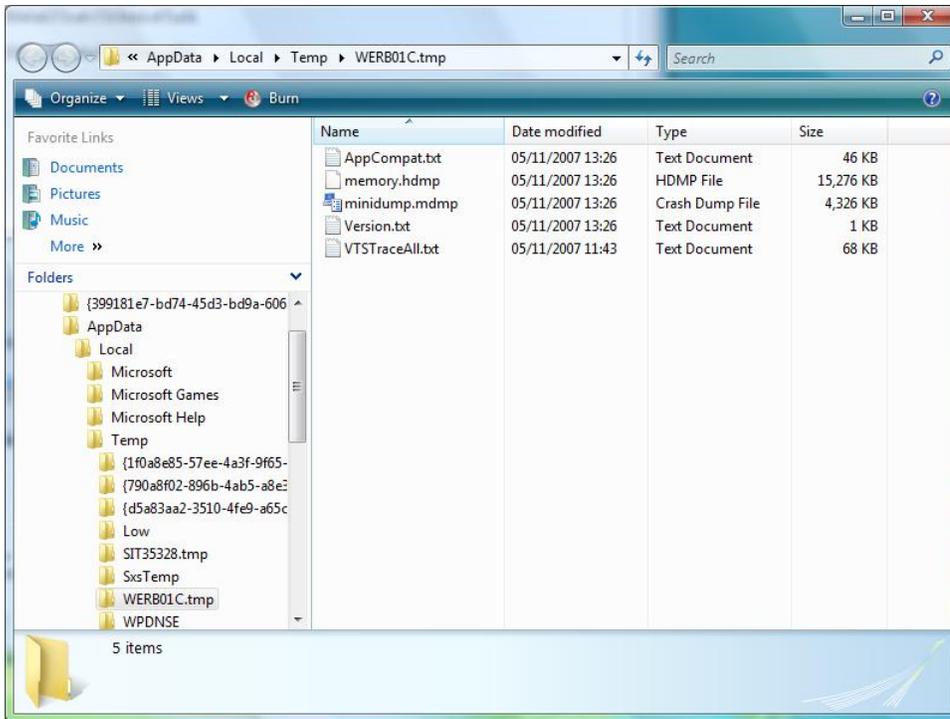


3. Locate the problem report you are interested in and double-click it.

You will see a window that lists a summary (signature) of the problem like this:



Near the bottom of the window is a link "View a temporary copy of these files". If you want to access the dump file automatically created when the problem occurred, click that link. A copy of Windows Explorer will open displaying the files that Windows archived (and compressed) when the problem occurred. The set of files is as listed in the above dialog. Note that VTSTraceAll.txt is also archived at the point of the crash.



The explorer window shows these files. memory.hdmp is the full user-mode dump file that you can open with VTS's Source Debugger. Do not worry about tidying up the temporary files. They will be automatically removed when you close the Problem Solutions and Reports dialog window.

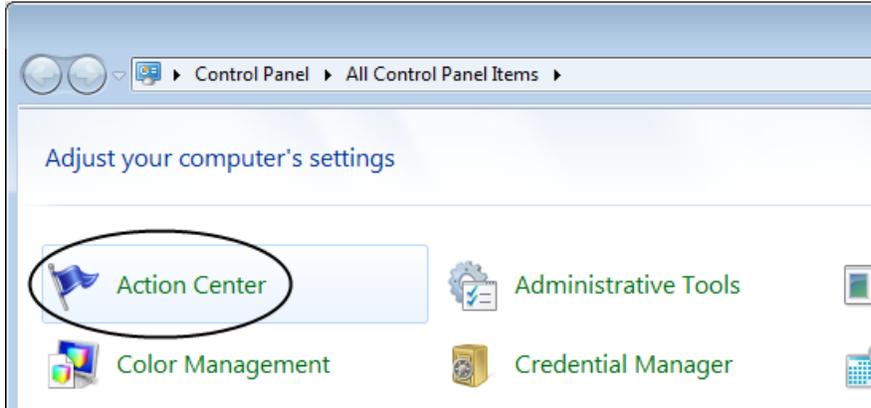
Note: If you need to keep the dump file (perhaps for sending to Tri-hedral technical support), ensure that in the problem reports control panel, the settings are configured to "Ask me to check if a problem occurs". Selecting "Check for solutions automatically" will result in the "temporary" dump files being deleted.

Generate a Crash Dump with Windows 7 or Later

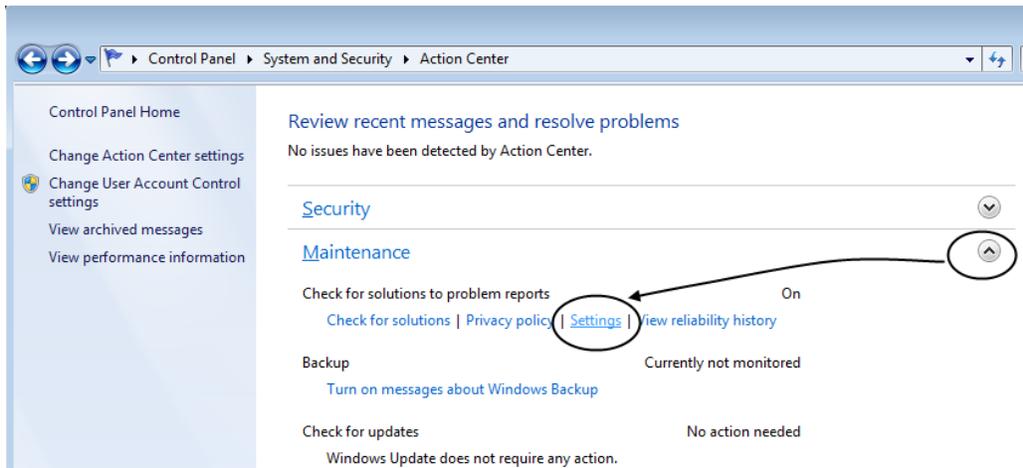
Note: In Windows 8 and later, the "Problem Reports and Solutions" utility has moved to Control Panel >> Action Center >> Maintenance >> View Reliability History.

Troubleshooting

1. Open the Windows Control Panel.
2. Open the Action Center application.



3. Expand the Maintenance section, and then click Settings.



4. Ensure that the third option is selected, "Each time a problem occurs, ask me before checking for solutions".

Choose when to check for solutions to problem reports

When you send problem reports to Microsoft, you will receive solutions when they are available. You can adjust how much information is sent.
[What information is sent?](#)

- Automatically check for solutions (recommended)
- Automatically check for solutions and send additional report data, if needed
- Each time a problem occurs, ask me before checking for solutions
- Never check for solutions (not recommended)

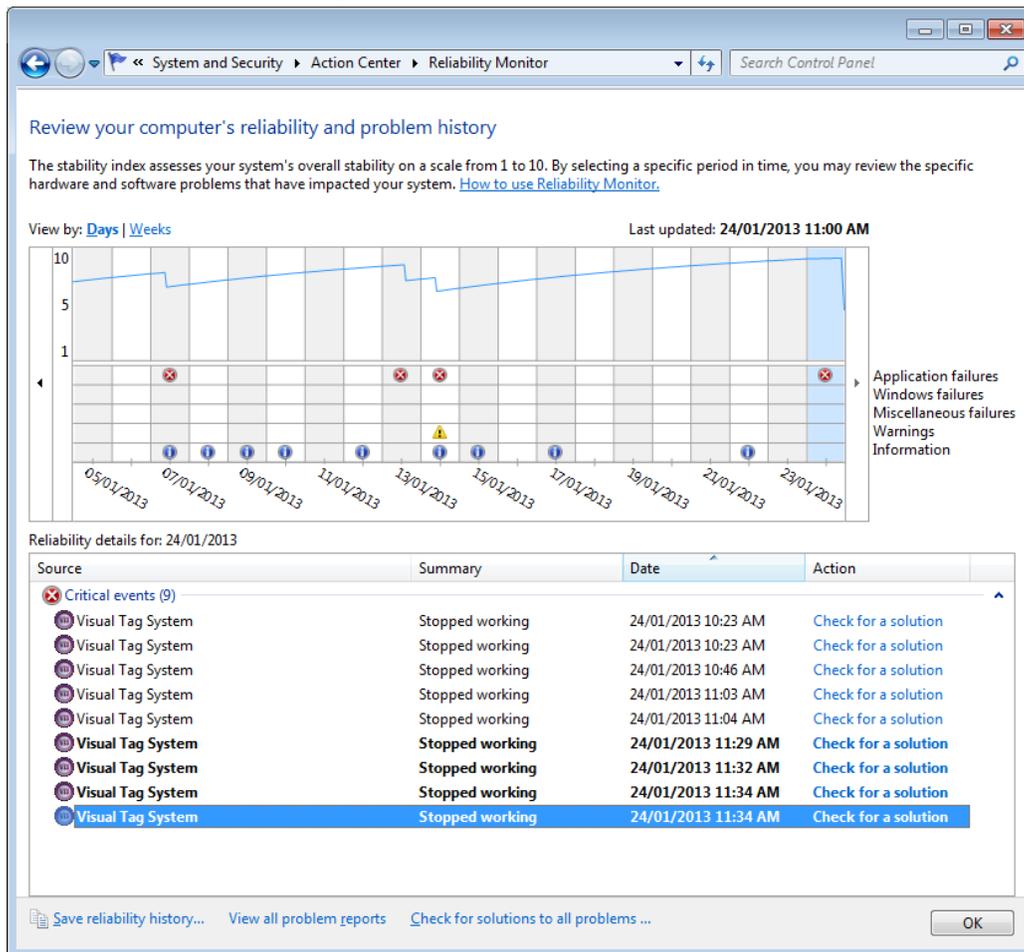
[Change report settings for all users](#)
[Select programs to exclude from reporting](#)
[Read the Windows Error Reporting privacy statement online](#)

To view error reports and crash dumps:

The dump file will be stored to %PROGRAMDATA%\Trihedral\WER.

1. Open the Windows Control Panel.
2. Open the Action Center application.
3. Expand the Maintenance section.
4. Click View Reliability history.

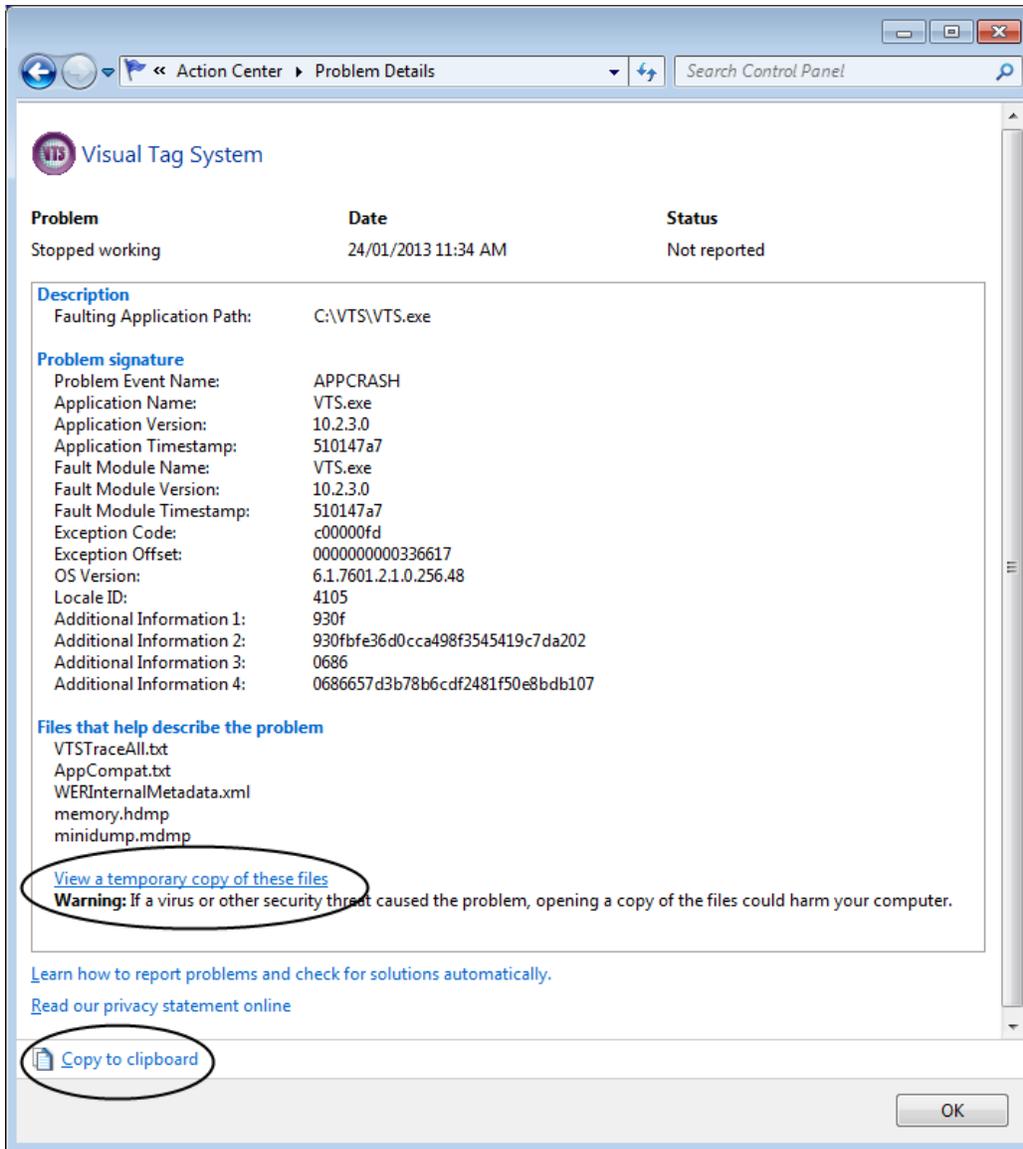
This will give a list of the problems. You can view problems from a given day by clicking in the graph. You can view all problems using the link at the bottom of the page.



(Illustration created using a copy of VTScada that was designed to produce errors for the benefit of these instructions.)

Do not click on "Check for a solution". Doing so will send a problem report to Microsoft. No solution will be found there.

5. Find the entry you want and double-click it or right-click and choose View Technical Details.



6. You may copy the displayed details to the Windows clipboard, and then include them in an email to Trihedral Technical Support. (support@trihedral.com)
7. A full crash dump can be found by clicking the link, "View a temporary copy of these files". These are the files that should be sent if the technical support team asks for a copy of the crash dump.

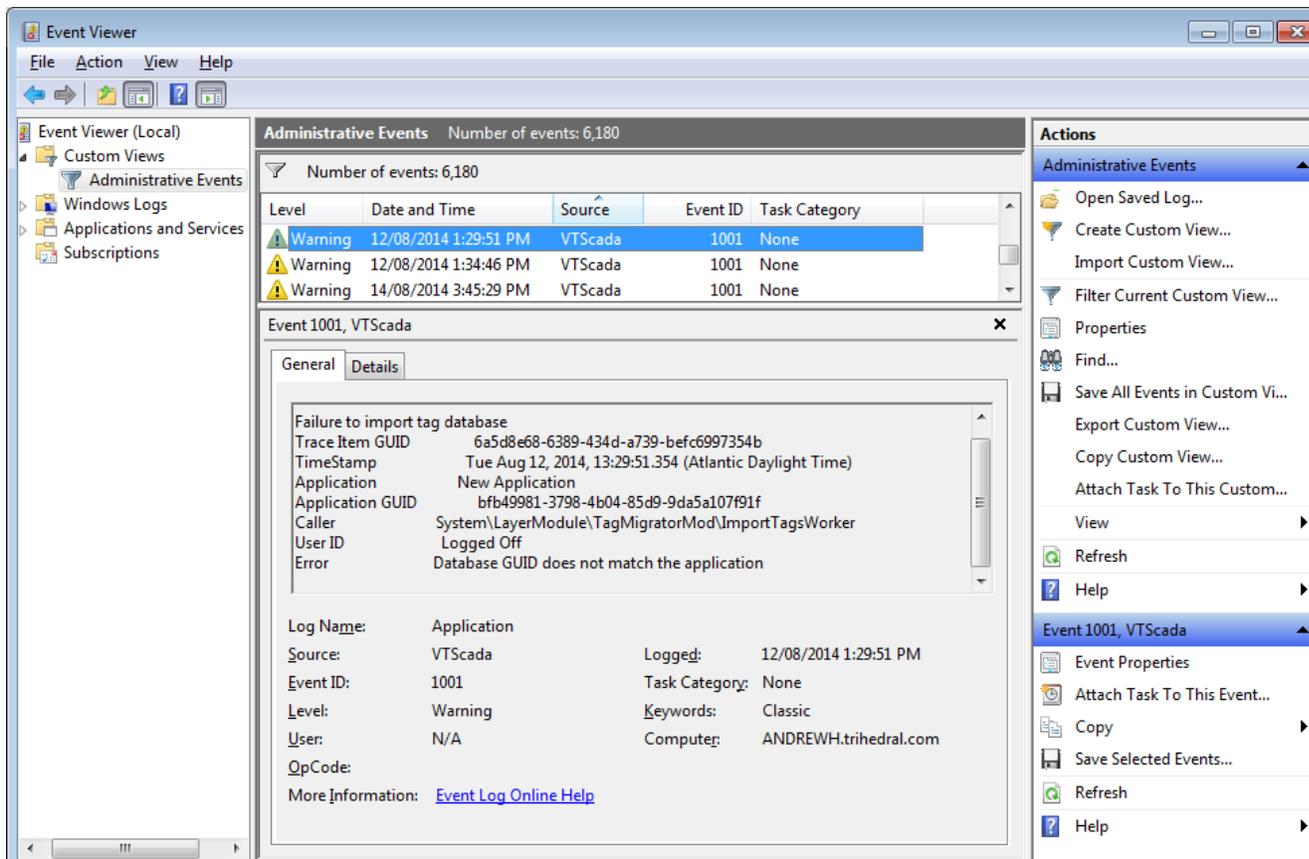
Use the Windows® Event Viewer

The Windows Event Viewer® maintains a record of VTScada notifications and error messages. This may be useful in the event that you wish to review a message after closing the dialog.

Note to VTScada programmers: You can also add your own messages to the Windows Event Viewer using the function LogNTEvent in your scripting code.

Find your VTScada event messages as follows:

1. Open the Windows Control Panel.
2. Open the Administrative Tools group.
3. Open the Event Viewer program.
The Event Viewer starts with an overview of event logs to choose from.
4. Using the panel on the left of the Event Viewer window, expand Event Viewer (Local)
5. Expand Custom Views.
6. Select Administrative Events.
The Administrative Events list opens in the center panel.
7. Sort the list by Source.
Within each source, events are sorted by date and time.
8. Scroll to find the VTScada events.
9. Scroll within the VTScada events to find one with a timestamp closest to the event you wish to review.



Note: The Event Log Online Help is a Microsoft® data store. If this is a purely VTScada message, the Event Log Online Help will not be useful.

Related Functions:

LogNTEvent in the VTScada Programmer's Guide

Adjusting the Virtual Address Space

32-bit operating systems are capable of addressing 4 GB of virtual address space, however access to this memory is divided evenly between applications and the operating system. On a server with 4GB of RAM installed, and running a 32-bit operating system, only 2GB of address space will be available to applications.

You can direct the operating system to make 3GB of the address space available to applications if you find that VTS requires more than the 2GB

of memory that would normally be available. This is likely to occur only in very large applications.

Note: Follow the instructions in this section only if all of the following are true:

- You are running the 32-bit version of VTS.
- Your server has 4GB of RAM installed
- Your server is running a 32-bit operating system.
- You have an application that is using more than 1GB of memory.

You can determine the memory in use by opening the About VTS box from the VTS Application Manager.

The 32-bit version of VTS, running on a server with a 64-bit operating system can address 4GB without changes to the system configuration. The 64-bit version of VTS, running on a server with a 64-bit operating system can address up to 8096GB of memory.

Adjusting the Address Space in Windows XP:

1. Open the Boot.ini file for editing as follows:
 - a. Right-click My Computer, and then click Properties.
 - or-
 - b. Click Start, click Run, type sysdm.cpl, and then click OK.
 - c. On the Advanced tab, click Settings under Startup and Recovery.
 - d. Under System Startup, click Edit.
2. Add the /3G switch to the operating system partition as shown in the following example: (the space marked by "???" in this example, will display your operating system version).

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="???" /3GB
```

3. Re-boot your computer.

Further information may be found on Microsoft's website at:

<http://www.->

microsoft.com/whdc/system/platform/server/PAE/PAEmem.msp

Adjusting the Address Space in Windows Vista, Windows 7 and Windows 8:

1. Type the following at a Windows command prompt that has been opened with Administrative privileges.

```
BCDEDIT /Set IncreaseUserVa 3072
```

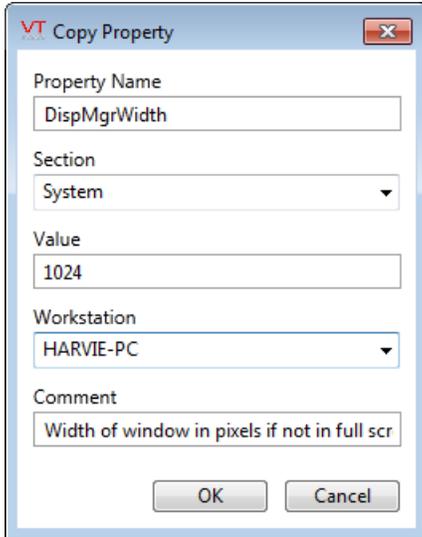
2. Re-boot your computer.

Add Scroll Bars to a Page

You may need to add scroll bars to the VTScada display if you are attempting to edit an application while using a monitor that is smaller than the one that the application was created on. This can be done in a way that affects only your workstation. To force scroll bars (when a page is larger than your monitor) set the width and height (DispMgrWidth and DispMgrHeight) to match your current screen size.

Step by step:

1. Open the Application Configuration dialog.
2. Select the Edit Properties page.
3. Find and select the property DispMgrWidth.
4. Click Copy.
5. Set the width value to match your display.
6. Enter your workstation name in the space provided. (You may be able to select it using the drop-down list.)



7. Repeat for DispMgrHeight.
8. Click Apply.
9. Provide a comment in the dialog that opens and click OK.
10. Click OK to acknowledge that the application must be restarted before the changes will go into effect.
11. Re-start the application on your workstation.

Hardware Device Limited License – Cannot Connect to Device

If your VTScada license requires that a hardware device (also known as a "dongle") be installed, and if VTScada is unable to communicate with the device, then problem is most likely to be related to the driver. The Sentinel driver, required by the device, was included when you purchased VTScada.

Note: Do not remove the hardware device. If the device is required as part of your license, then VTScada will stop immediately if the device is removed.

Troubleshooting steps:

1. Ensure that the device is firmly inserted into a USB port of your computer.
2. Ensure that the Sentinel\Drivers folder exists within your VTScada installation.
3. Re-run Setup.EXE from that folder.
4. Select "Modify" in the menu that will open.
5. Ensure that Sentinel Protection Server is selected.
6. Complete the setup program.

If problems remain, then the following may help:

- Uninstall the Sentinel Software and re-install it. Re-start VTScada. If there are still issues, send a screen capture of the VTScada information window to Trihedral Technical Support.
- Open a web browser on the VTScada workstation. Navigate to <http://YourComputerName:6002> replacing "YourComputerName" with the name of your computer. This should display a list of dongles attached to your computer. Send this to Trihedral Technical Support.

Cloning a VTScada Workstation

Note: Do not clone a VTScada workstation.

Cloning a VTScada workstation, for installation on a new computer, will also clone the unique machine identifier (UMID), which VTScada generates for each workstation. Running two machines with the same UMID will cause corruption of the configuration repository.

In newer VTScada installations, any attempt to run two VTScada workstations with the same UMID will be detected and prevented.

Recommended practice to avoid this situation is to install VTScada on the new machine and use the Get From Workstation tool in the VTScada Application Manager to transfer the application to that machine from another workstation.

If you have cloned a workstation, the existing UMID must be deleted from the registry before running VTScada on that machine. Contact Tri-hedral Technical Support before proceeding.

Related Information:

Backups

VTScada as a Windows® Service

VTScada can be installed to run as a Windows® service. Once installed, it can be stopped and then re-started as either a service or as an interactive program.

Note: User interface items may differ in appearance when rendered within a Windows service. In particular, Windows control buttons will differ in appearance when viewed on a mobile client. Certain third-party applications may have limited interaction with the service.

If you have been running VTScada as an interactive program, it is necessary to install the service objects before the program can be run as a service. This can be done using command line switches, or you may choose to repeat the full installation, selecting the service option.

Note: Use caution if switching VTScada between running as a service and running as an interactive program. It is likely that the account you log in with will be different from the account used by VTScada when running as a service. If file permissions do not match, then fundamental operations such as updates to repository files, history (data and alarms) and more may fail to work properly.

Once installed, the service will automatically start when Windows® starts. Note that a delayed start is configured by default. It may be stopped and started through the Windows® Service Control Manager or using the command line, which is the recommended option.

```
vtsc.exe /s=start
```

```
vtsc.exe /s=stop
```

VTScada security permissions are not required in order to stop the service.

Note: Your Windows account must have administrative privileges (and, if using the command line, the console must be run with administrator privileges) in order to issue service commands.

The application that will be available through your VTScada service must exist on the server, and be configured to auto-start. Since VTScada cannot run as a service and as an interactive program at the same time on the same workstation, the following procedure is suggested.

1. Install VTScada and run as an interactive program.
2. Create or install the application.
3. Configure the VTScada Internet Server, to allow VTScada Internet Client connections.
4. Configure the application to auto-start.
The application can be stopped only by stopping the service.
5. Stop the interactive VTScada session.
6. Run VTScada as a service, re-installing to add the service components if this was not done earlier.
The command-line syntax is recommended.
7. Start the VTScada service.

When VTScada is running as a service, all operational access to your application will be done through other workstations where VTScada is installed and running as an interactive program, or through VTScada Internet Client or Mobile Client connections. Ensure that your VTScada license permits the maximum number of simultaneous Internet Client connections that you expect. System messages that would otherwise have been shown on the interactive console will be directed to a VIC connection. Error messages will be directed to the Windows® event log. Tag configuration may be done using a VIC connection.

Further development work that involves pages and graphics can be done using any of the following methods:

- Install VTScada on a second server and configure your server list. Use Get From Server to install the application on the second workstation. Configuration changes will be deployed from one to the other.
- ChangeSets, created on a non-networked workstation, can be copied to the server, then applied using the VIC. The identical application must be installed on the second workstation.

- Stop the service and re-start as an interactive session. Ensure that you are logged into Windows using an account that has permissions that match those being used by the service, so that file changes can be saved. Perform the development work. Re-start VTScada as a service.

Plan for Troubleshooting

Note: If you plan to allow programmers and developers to access diagnostic applications such as the Source Debugger or TraceViewer over an Internet connection, then you must add those applications to the realm configured for your VTScada application.

These diagnostic applications do not store user accounts, therefore to be accessed over a VTScada Internet Connection, they must share a realm with at least one secured application that has a user account with the Internet Client privilege. That account can be used to connect to diagnostic applications in the same realm.

Related Information:

...Internet Realms

...See also: "Internet Realms" in the VTScada Developer's Guide

...Service Installation – Steps for installing the service

...Accounts and Permissions – Considerations for selecting the Windows account for the VTScada service.

...Service Command Line Reference

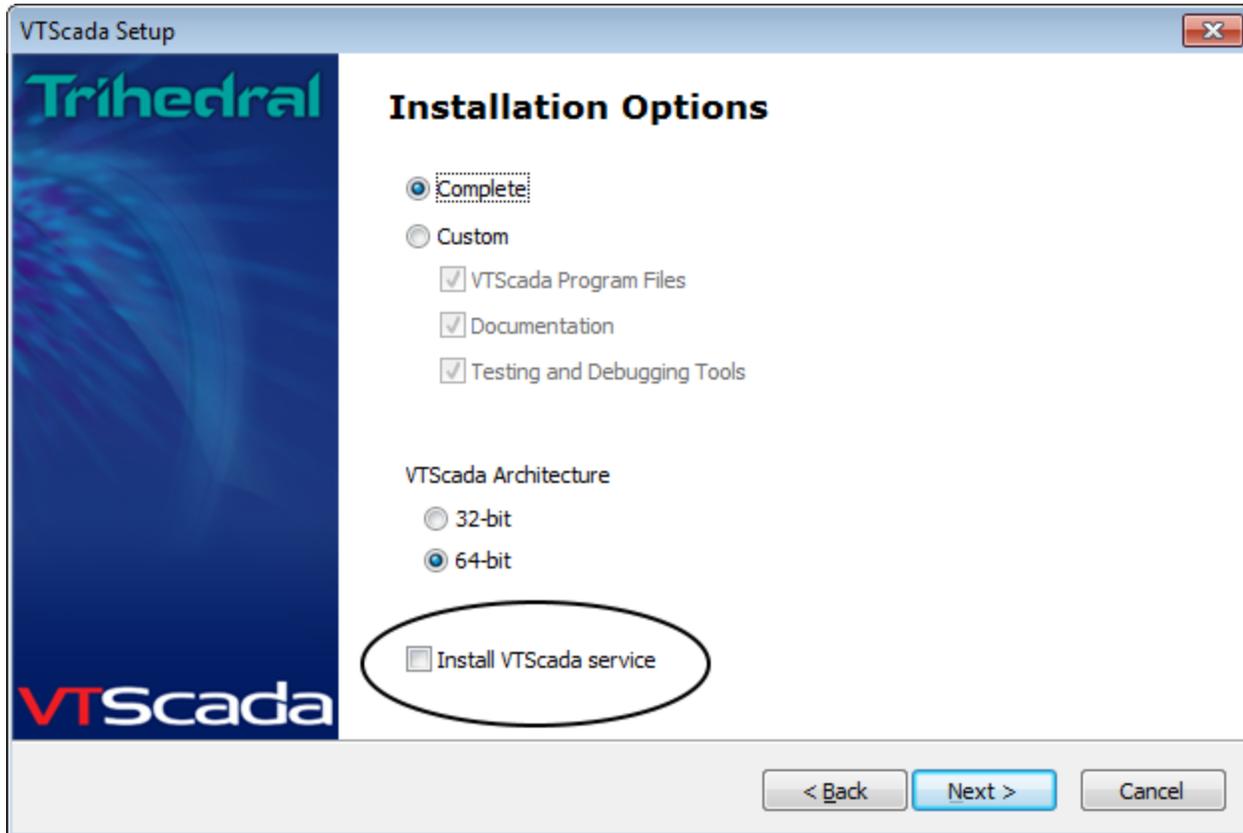
...Service Error Dialogs

Service Installation

There are two ways to install VTScada to run as a service:

Note: Your Windows account must have administrative privileges (and, if using the command line, the console must be run with administrator privileges) in order to issue service commands.

- Choose the Install VTScada Service option during the standard installation.

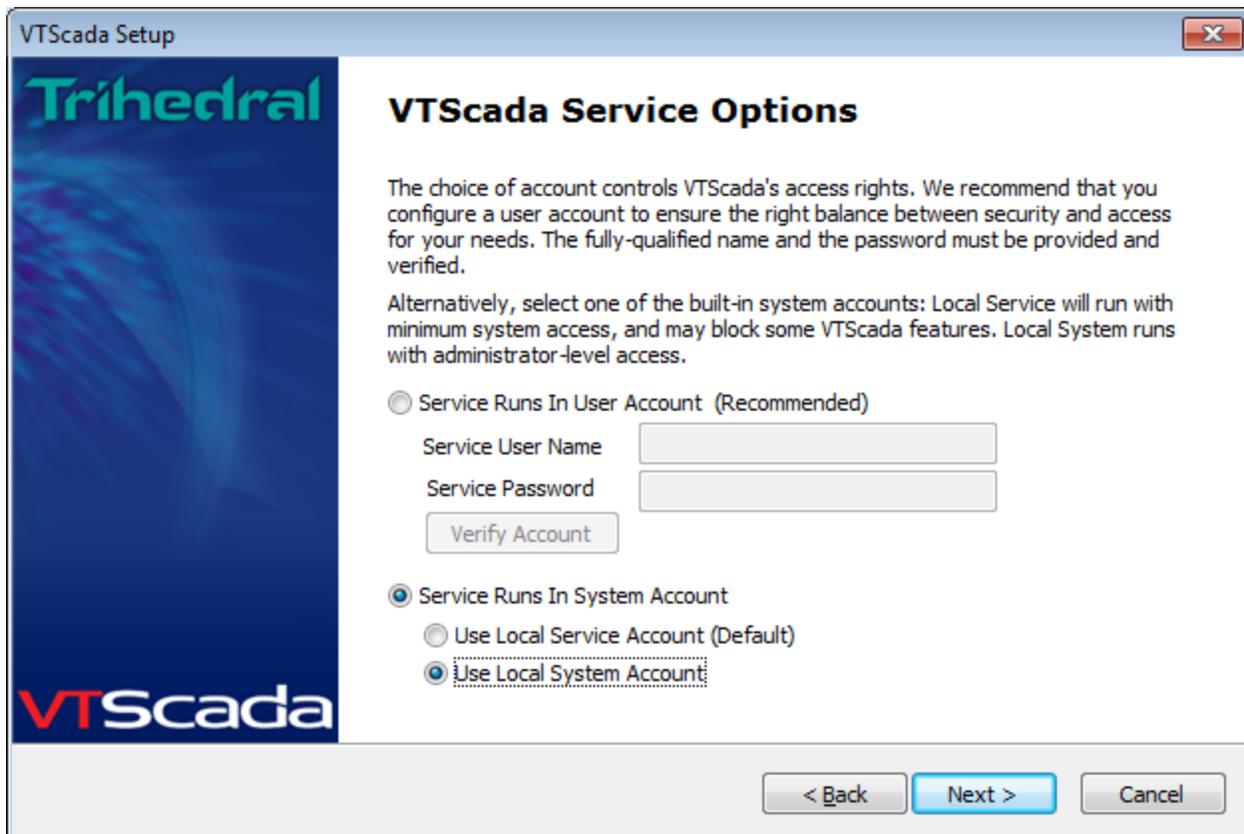


- On a workstation where VTScada version 11.1 or later has been installed, stop the program, then run the executable from the command line, using the /s switch.

In either case, you must provide the account credentials that VTScada will use when running as a service. Your options are:

- Use the Local Service account
Has minimal permissions, therefore the highest security. Certain VTScada features may not be allowed to run.
- Use the Local System account
Has maximum permissions, thereby ensuring that all VTScada features can run.
- Use an account and password that you have created for use by the service.
You can tailor the account permissions to balance security with functionality.
You must know and understand Windows security configuration.

If running the standard installation, you will select the account to use and enter the credentials in a dialog:



If installing from the command line, you will enter the account selection and credentials as part of the command switch:

- Install the VTScada service with a fully-qualified user name and password:

```
vts.exe /s=install [username] [password]
```

- Install the VTScada service using the Local *Service* account:

```
vts.exe /s=install [NT AUTHORITY\LocalService]
```

- Install the VTScada service using the Local *System* account:

```
vts.exe /s=install
```

Related Information:

...Accounts and Permissions – Further details to help you select the account to use.

...Service Command Line Reference

Accounts and Permissions

If running VTScada as a service, it is important to understand Windows® account permissions.

Note: Your Windows account must have administrative privileges (and, if using the command line, the console must be run with administrator privileges) in order to issue service commands.

Note: Windows Security Integration can be used when VTScada is run as a service, but the account that the service is run under must allow the COM operations required for the AD queries. The "Local Service" account may not have sufficient permissions. In most cases, the "Local System" account will.

Examples:

- If the VTScada service uses the built-in Local Service account, you may find that certain VTScada actions cannot run since they do not have sufficient privileges.
- Running the VTScada service using the built-in Local System account will ensure that all required system access is available since this is an administrator account. But, some IT departments may object to the use of an administrator account by a service.
- If the VTScada service is shut down, and VTScada restarted as an interactive program, then it will use your account while in interactive mode. This might not have access to logged data, alarm history and other files written using the service account, and therefore VTScada will be unable to perform required file operations during the interactive session.
- Certain components (DCOM objects in particular) must grant the user attached to the VTScada Service permissions beyond those given to the administrator by default. For the OPC service, VTScada does this automatically.

Service Command Line Reference

The following command line options are recognized:

<code>vts.exe /s=install</code>	Install VTScada as a service using the Windows® operating system account, "Local System". Reinstalls if previously installed.
<code>vts.exe /s=install[NT AUTHORITY\LocalService]</code>	Install VTScada as a service using the Windows account, "Local Service". Reinstalls if previously installed.
<code>vts.exe /s=install[user-name][password]</code>	Install VTScada as a service using an account of your choice. Reinstalls if previously installed.
<code>vts.exe</code>	Run VTScada as an application. (requires administrator privileges). Fails if the service is not stopped.
<code>vts.exe /s=start</code>	Run the VTScada service, installing it first if not present.
<code>vts.exe /s=stop</code>	Stops the service if it is running but leaves it installed.
<code>vts.exe /s=uninstall</code>	Uninstall the service. Will fail if the service is running.
<code>vts.exe /s=disable</code>	Disable the VTScada service, this leaves the service installed but prevents it from starting.
<code>vts.exe /s=enable</code>	Enable the VTScada service if it was previously disabled. This restores the ability to start the service.

Service Error Dialogs

Server-side dialogs will be redirected to a VTScada Internet Client if one is available. By default, this will be the connection that has been running for the longest time, since that connection is most likely to be in a control room.

You can set the preference for which VTScada Internet Client will receive the message by adding a configuration section to your Setup.INI file, found in the VTScada installation folder. Note that VTScada must be restarted before any changes to that file will take effect.

Client selection done by checking the account name logged in at each VTScada internet client connection. Thus, the list is titled "Default-User-Sessions" and will contain the account names. All VIC connections will

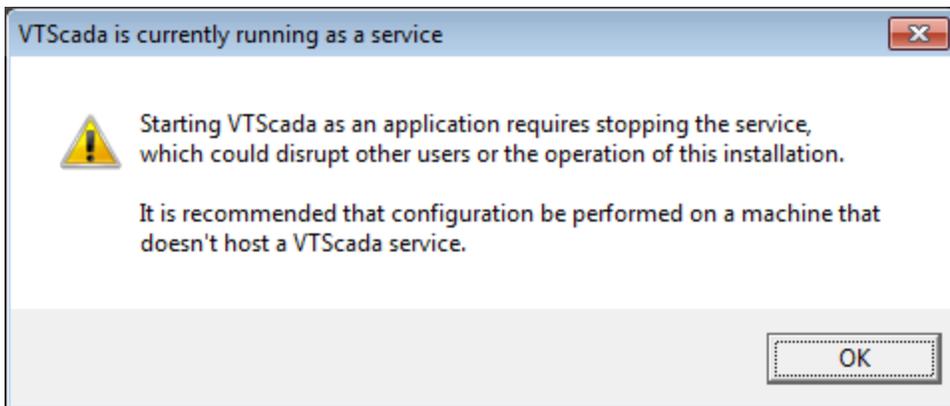
checked for each account listed in order. The messages will go to that client connection.

```
[Default-User-Sessions]
Joe
Bob
Mary
```

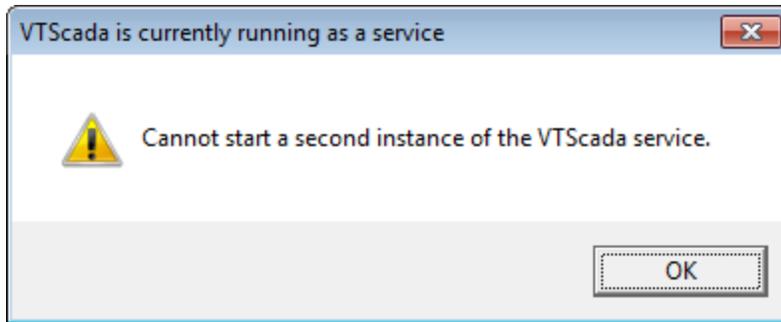
If you are running more than one application, you can have server messages go to the first client connection where a given application is running. For example, if one of the applications is named "Demo" and you would like server messages to go to whichever client connection is running that application (if available), then the list might be written as follows:

```
[Default-User-Sessions]
Demo
Joe
Bob
Mary
```

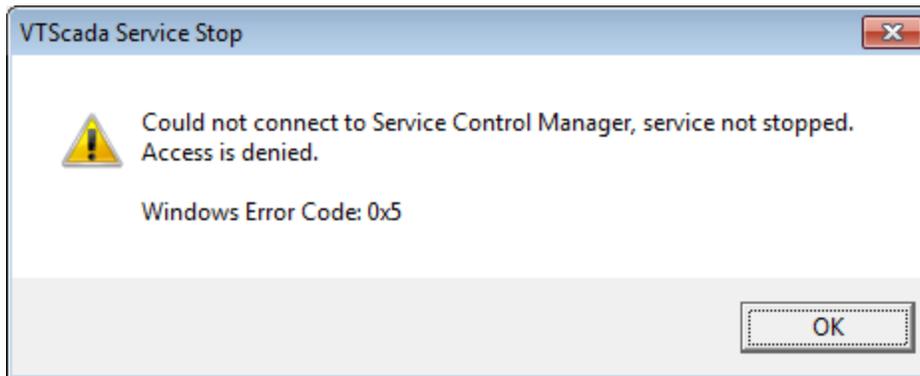
In the event that two clients match the given criteria, then the messages will go to the one that has been running for the longest time.



Displayed when someone attempts to start an interactive VTScada session on a workstation where the VTScada service is running.



Displayed when someone attempts to start VTScada as a service on a workstation where it is already running.



Displayed if you attempt to stop the VTScada service using the command line if the console is not running with administrative privileges, or while logged in on an account that does not have sufficient permissions.

Index

A

ABSharedRPC 378
Account Modify Privilege 570
Account View Privilege 570
AccountLockoutTime 386, 587
AccountRateWindow 386, 587
Accounts 518
AccountsChangeDlgWait 456
AckAllRequiresConfirmation 245
ActivateProgressDelay 456
ActiveAlarmFlash 246
ActiveCommColor 246
ActiveFlashRate 246
ADGroupPrefix 387, 588
administrator options 549
Administrator Privilege 570
ADRefreshPeriod 387, 588
Advanced Version Control Privilege 569
AITrendEnable 420
Alarm-Manager – property section 210
Alarm Acknowledge Privilege 571
Alarm Disable Privilege 571
Alarm Mute Privilege 572
alarm notification properties 217
Alarm Page Access Privilege 572
alarm properties 241
Alarm Shelve Privilege 572
Alarm Silence Privilege 572
ALARM_MANAGER 209

AlarmAutoNavEnable 246
AlarmAutoNavHold 247
AlarmAutoNavTimeout 247
AlarmAutoNavWindowed 248
AlarmCheckMail 219, 248
AlarmCheckMailFastPoll 219, 249
AlarmColor 249
AlarmDatabaseGroups 249
AlarmDatabasePurgeDelay 250
AlarmDatabasePurgeEnable 251
AlarmDatabasePurgeRate 251
AlarmDialerStatusTemplate 219
AlarmDialerTemplate 220
AlarmDisplayDateFormat 251
AlarmDisplayTimeFormat 251
AlarmEditEmailAck 220
AlarmEmailAckSubjectTemplate 220
AlarmEmailAckTemplate 221
AlarmEmailStatusTemplate 222
AlarmEmailSubjectTemplate 223
AlarmEmailTemplate 224
AlarmEventDesc0 252
AlarmEventDesc1 252
AlarmEventDesc10 252
AlarmEventDesc11 252
AlarmEventDesc12 253
AlarmEventDesc13 253
AlarmEventDesc14 253
AlarmEventDesc15 253
AlarmEventDesc16 253
AlarmEventDesc17 253

AlarmEventDesc18 253
AlarmEventDesc19 253
AlarmEventDesc2 252
AlarmEventDesc20 253
AlarmEventDesc21 253
AlarmEventDesc3 252
AlarmEventDesc4 252
AlarmEventDesc5 252
AlarmEventDesc6 252
AlarmEventDesc7 252
AlarmEventDesc8 252
AlarmEventDesc9 252
AlarmEventDescWidth 252
AlarmEventDescX 252
AlarmFlashTime 253
AlarmFlashTitleBar 253
AlarmFlashTitleBarOnVIC 254
AlarmIndDisable 254
AlarmIndDisableOnVIC 254
AlarmKeySize 255
AlarmManager.INI 108, 199
AlarmMaxPriority 255
AlarmMinPriority 255
AlarmNotifyEmailAcknowledge 225
AlarmNotifySMSAcknowledge 226
AlarmOperatorVarName 255
AlarmPageHistoryRecordHardLimit 256
AlarmPageHistoryRecordLimit 256
AlarmPagerTemplate 227
AlarmPopupsEnable 257
AlarmPrintDateFormat 257

AlarmPrintPort 257
AlarmPriorityDescWidth 257
AlarmPriorityIndicatorShowNormalUnacked 228
AlarmRevUnack 258
AlarmRPCEnable 258
AlarmSeparatorString 258
AlarmSMSAckTemplate 228
AlarmSMSStatusTemplate 229
AlarmSMSTemplate 230
AlarmSnapshotCount 259
AlarmSoundDisable 259
AlarmSpeechEnable 259
AlarmSpeechInit 259
AlarmSpeechQuality 260
AlarmSpeechTemplate 261
AlarmSpeechVoice 262
AlarmStateDesc0 262
AlarmStatRange0 262
AlarmStatRange0Label 264
AlarmStatRange1 262
AlarmStatRange1Label 264
AlarmStatRange2 262
AlarmStatRange2Label 264
AlarmStatRange3 262
AlarmStatRange3Label 264
AlarmStatusDesc0 267
AlarmStatusDesc1 267
AlarmStatusDesc2 267
AlarmStatusDesc3 267
AlarmStatusDesc4 267
AlarmStatusDesc5 267

AlarmStatusDescWidth 267
AlarmStatusField 267
AlarmTemplateDateFmt 268
AlarmTemplateTimeFmt 268
AlarmTimeStampField 268
AlarmTxtColClear 268
AlarmTxtColDisable 269
AllowIP 451
AlmColumn1 269
AlmColumn2 269
AlmColumn3 269
AlmColumn4 270
AlmColumn5 270
AlmColumn6 270
AlmColumn7 271
AlmDBArea 271
AlmDBHPUnits 271
AlmDBHPValue 271
AlmDBMessage 272
AlmDBOperator 272
AlmDBPointName 272
AlmDBPriority 272
AlmDBStatus 273
AlmDBTimeStamp 273
AlmDBType 273
AlmHdg1 273
AlmHdg2 273
AlmHdg3 274
AlmHdg4 274
AlmHdg5 274
AlmHdg6 274

AlmHdg7 275
AlmListTextColor 275
AlmPgLineStyle 275
AlmPgStartList 275
AlmTagsOnly 277
AlphaNumericXFormScheme 231
Alternate identification 531
AnalogControlName 403
AnalogInputWidth 364
AnalogScaledMaxDefault 403
AnalogScaledMinDefault 404
AnalogStatusName 404
AnalogSummaryReportTimeUnits 373
AnalogUnscaledMaxDefault 404
AnalogUnscaledMinDefault 404
AnswerCalls 344
Application 209
APPLICATION 209
Application Information 154
application manager 149
Application Manager View 573
application privileges 538
application properties 160
application property definitions 205
Application Stop Privilege 573
ApplyMuteSilencePerComputer 276
ApplyMuteSilencePerUser 277
APPS – setup.ini section 438
Area-REALMAREAS 216
AreaExclude 404
AreaFilter 405

Areas 209
attempts (login) 389, 590
auto start 441
AutoActivate 330
AutoAddADUsers 387, 588
AutoExportToUCDelay 442
AutoExportToUserCopy 443
AutoLogOff 387, 589
AutoLogOffMax 388, 589
AutoLogOffMin 388, 589
AutoLogon 456
automatic log-off 552
AutomaticDeploy 443
AutoOpenIdeaStudio 313
AutoRecover 443

B

BackupAlarmPriority 278
Backups 470
BackupSwitchCount 299
BadQualityColor 286, 299
BitmapDirExt 314
BMPPath 314
BrowserHeight 333
BrowserWidth 333
BrowserX 334
BrowserY 334
ButtonFace 286
ButtonHighlight 286
ButtonShadow 287
ButtonTextColor 287

C

CallInterval1 344
CallInterval10 344
CallInterval2 344
CallInterval3 344
CallInterval4 344
CallInterval5 344
CallInterval6 344
CallInterval7 344
CallInterval8 344
CallInterval9 344
CallOutDelay1 232, 345
CallOutPriority 233, 345
CanRedefineOEMType 405
ChangeSet 472
CIPENIPSharedRPC 378
CIPTimeoutMultiplier 300
ClientAlarmSoundOn 278
ClientCabPath 450
cloning 470
color properties 284
command line options – service 623
CommFailColor 301
CommStatsQualityFactor 301
CommStatsUpdateRate 302
communication driver properties 297
Compile 491
CompileProgressDelay 457
Config.DB 108
Config.INI 108
ConfigListBroadcastWait 443

configuration dialog – opening 153
configuration files 160
configuration variables 160
Configure Privilege 573
Configurer 533
ContainerTerm 358
ConvertProgressDelay 457
crash dump 601
CycleDelay 346
CycleLength 346
Cycles 278

D

DataFlowModuleName 302
DataFlowStationName 302
DataIdleTime 346
DataLines 299
DataradioSharedRPC 378
date format codes 155, 158
DbTraceDaysToPreserve 457
DbTraceFileSize 457
DDESharedRPC 378
deactivate security 517
debugging properties 327
DefaultAnalogDeadbandFractionOfFullScale 405
DefaultBGColor 287
DefaultCalculationDeadbandFractionOfFullScale 406
DefaultEmailSubject 373
DefaultPage 364
DefGraphicBColor 288
DefGraphicPColor 288
DemoMode 303

Deploy Changes Privilege 574
DFSimulateOn 303
DialCancelOnAck 233
DialCancelOnNormal 233
DialerAckIndividualAlarms 238
DialerConnectDelay 234
DialerLocation 234
DialerPort 234
DialerSpeechInit 235
DialerVoice 235
DialInControl 235
DialogBGColor 288, 364
DialogMoveTime 314
DialogServiceFailoutTime 458
DialOnActive 235
DialOnClear 236
DialResetTime 346
DialWaitTime 347
DigitalControlName 406
DigitalIndicator0Color 288
DigitalIndicatorInvalidColor 289
DigitalInputWidth 365
DigitalStatusName 406
DisableCommStats 303
DisableGoToPage 330
DisableUSDialog 365
DiskFreeSpaceCheck 336
DiskFreeSpaceDrives 336
DiskPcentLogRestart 336
DiskPcentLogStop 336
display manager properties 312

DisplayManagerTitle 314
DispMgrAspectRatio 315
DispMgrBitmap 315
DispMgrBMPMarginBottom 315
DispMgrBMPMarginLeft 316
DispMgrBMPMarginRight 316
DispMgrBMPMarginsWin 316
DispMgrBMPMarginTop 316
DispMgrDateFormat 316
DispMgrFullScreen 317
DispMgrHeight 317
DispMgrHidden 318
DispMgrHoriz 319
DispMgrMinHeight 319
DispMgrMinMaxDisabled 319
DispMgrMinWidth 320
DispMgrPageStyle 320
DispMgrResizable 321
DispMgrTimeFormat 322
DispMgrTitleBorder 322
DispMgrVert 322
DispMgrWidth 323
DispMgrWPageStyle 323
DispMgrX 324
DispMgrY 325
DITrendEnable 420
DNP3DataInvalidOnFail 304
DNP3DelayedResponseTimeout 304
DNP3FailoverCount 304
DNP3MaxFileSize 304
DNP3SharedRPC 304, 379

dongle 614
DoNotStart 330
DontLogTrendPens 420
DOWidth 365
DriverRPCOptimization 305
DriverSetupDelay 379

E

EchoPhoneThroughSpeaker 236
Edit Files Privilege 574
edit properties 200
EmailServer 373
EmailSubject 373
EnableLexiconDialog 236
EnableMobileMaps 358
EnableShowHide 458
ErrorLogFileName 458
ExcludeIP 452

F

FastPollCommColor 305
FastPollDuration 305
FastPollRate 305
FieldHighlight 289
FieldShadow 290
File Manifest 482
FileListMax 337
FilterCount 212
FilterName 212
FlashUnackedAlarmsOnServer 278
FlashUnackedAlarmsOnVIC 279
ForcePasswordAltIdSync 388, 589

G

GDI.WIF 108
GiveUpCallTimeout 237
grant privileges 528
GrayedText 290
GridColor 290, 399
GridDense 400
GridShiftX 400
GridShiftY 400
GridVis 400
Group Delete Privilege 575
Group Modify Privilege 575
group name 534
Group Save Privilege 575
GroupLogin 388, 590
GuardTone 347

H

HangUpDelay 347
hashing algorithm 584
HDV properties 417
HDVAnalogAlarmsVisibility 421
HDVAnalogLegendAverage 421
HDVAnalogLegendDescription 421
HDVAnalogLegendHighScaleValue 422
HDVAnalogLegendLowScaleValue 422
HDVAnalogLegendMax 422
HDVAnalogLegendMin 422
HDVAnalogLegendValue 423
HDVAnalogPenAverageVisibility 423
HDVAnalogPenMinMaxVisibility 423

HDVAnalogPenScale 424
HDVAnalogPenStyle 424
HDVAnalogPenVisibility 424
HDVAnalogPenWidth 425
HDVAnalogScalesVisibility 425
HDVDataRetrievalMsg 425
HDVDataRetrievalMsgColor 425
HDVDataRetrievalWaitTime 425
HDVDateFormat1 426
HDVDateFormat2 426
HDVDigitalGridColor 426
HDVDigitalLegendAverage 426
HDVDigitalLegendDescription 427
HDVDigitalLegendHighScaleValue 427
HDVDigitalLegendLowScaleValue 427
HDVDigitalLegendMax 427
HDVDigitalLegendMin 428
HDVDigitalLegendNumberOfStarts 428
HDVDigitalLegendOnTime 428
HDVDigitalLegendValue 429
HDVDigitalPenStyle 429
HDVDigitalPenVisibility 429
HDVDigitalPenWidth 430
HDVDigitalScalesVisibility 430
HDVDisplayTimeSelectionScrollBar 430
HDVDisplayToolbar 430
HDVGridCellColor 431
HDVGridLineColor 431
HDVGridViewColor 431
HDVGridViewSortOrder 431
HDVHorizontalGridColor 431

HDVLayoutBGColor 432
HDVLegendVisible 432
HDVMaxNoteWindows 432
HDVNotesLegendDescription 433
HDVNotesLineVisibility 433
HDVNotesPenStyle 433
HDVNotesPenVisibility 434
HDVNotesPenWidth 434
HDVPlotBGColor 434
HDVPlotViewColor 434
HDVShowAllScales 434
HDVShowTimeScales 435
HDVSimpleLegend 435
HDVTimeCursorColor 435
HDVTimeFormat1 435
HDVTimeFormat2 435
HDVVerticalGridColor 436
HelloPacketLength 347
HelpFile 407
HelpServerPath 458
HideFromVAM 331
HideMenuOnOutgoing 237
HideWam 447
HighlightUnackedAlarms 279
HistorianBroadcastMaxSize 337
HistorianBroadcastMinInterval 337
HistorianConnectionRetryDelay 337
HistorianDataAgeSweepIntervalDivisor 337
HistorianDefaultArchiveInterval 337
HistorianFailoverInterval 338
HistorianWriteBufferMaxLength 338

HistorianWriteBufferMaxTimeDiff 338
History Page Access Privilege 576
HTTPAllow 459
HTTPODeny 459
HTTPServerMaxHeaderLength 450
HTTPServerMaxHeaders 450
HTTPServerThreads 451

I

IdleWebSessionTimeout 358
Import File Changes 489
import file edits 202
Import New Files 490
Import/Export Files 486
InactiveCommColor 305
IncomingCallSection 237
InitialDataDelay 348
InitModemsDisabled 348
Internet Client Access Privilege 576
Internet Client Monitor 492
Internet Client Monitor Access Privilege 577
Internet Client Monitor Admin Privilege 577
Internet Client Tools Access Privilege 576
Internet logging 496
InvalidColor 290
InvalidText 407
IODrawGap 365
IODrawHeight 366

K

KeyCount 211
KeyName 211

L

LABELS 209
Labels – property section 213
LABELS setup.ini section 438
LABELS, config section 213
Language 328
LDAP 509
legacy applications 88
LegacyHistoryPath 338
LINKTOLERANCE – setup.ini section 439
LocalScopeSyntax 331
lockout time 386, 587
log and historian properties 335
Logged-Off Role 532
Logged Off VIC Sessions 551
LogOffUponHide 460
LogPath 338
LowBatteryPercent 460
LowBatteryTime 460

M

Manage Tag Types 577
Manager Privilege 577
Manual Data Privilege 578
ManualVICServerLists 451
marquee properties 360
MarqueeDashColor 360
MarqueeSolidColor 360
MarqueeSpeed 360
MaxCallAlarmPriorityReported 237
MaxFailedLoginAttempts 389, 590

MaxHandOffCount 348
MaxMuteDuration 279
MaxPagerBaudRate 238
MaxRateFailedLoginAttempts 389, 591
MaxShelveDuration 280
MaxWinPage 366
MDSSharedRPC 379
Menu.TXT 109
MenuBgnd 291
MenuRepeatMax 238
MenuTextColor 291
MinAltIDLength 461
MinModemsFree 348
MinMuteDuration 280
MinShelveDuration 280
MMCycleTime 349
MMLogDateFormat 349
MMLogLevel 349
MMLogTimeFormat 350
MMMaxQTime 350
MMRPCTimeout 350
MMUnAvailRetry 350
mobile browser properties 358
MobileBrowserAutoRefreshPeriod 359
MobileBrowserDisablePageGraphics 359
MobileBrowserSnapshotRefreshPeriod 359
MobilePageMaxRenderTime 359
MobileSlippyMapTilesSource1 461
modem properties 342
ModemAlarm 351
ModemAutoReset 351

ModemManagerLogSize 351
ModemMmaster 351
ModemName
 Device 352
 Disabled 352
ModemRetries 352
ModemSpeechTO 352
ModemTCPIPPort 353
ModiconPortSharedRPC 379
ModiconSharedRPC 381
ModiconVTSTMaxBlocka 306
MuteAlarms 280

N

NameSpaceDelimiter 390, 591
new features 31
NoBalloonTips 415
NoIconFile 443
NoInitialDriverDial 306
NoModal 328
NoOpChangeDialog 329
NormalColor 292
NoSoftDriverFailure 306
NoSplash 448
Note Add Privilege 578
NoteAddRequiresAuthentication 391
NoteMinLengthForAck 280
NoteMinLengthForShelve 281
NoteMinLengthForUnshelve 281
NoteRequiredForAck 282
NoteRequiredForShelve 282
NoteRequiredForUnshelve 283

NumHistoryItems 325
NVShowCheckFilesDlgCount 329
NVShowDialogs 329

O

ODBC Show Stats widget 498
OEM – setup.ini section 439
OEMEncryptKey 391, 592
OEMHelp 448
OEMPath 448
OEMRestrict 449
OEMVersionNum 449
OffColor 292
OmronSharedRPC 382
OnColor 292
OnTop 329
OpaqueBackground 292, 366
OPCClientSharedRPC 382
Operator 532
operator logging properties 360
OperatorLogArea 361
OperatorLogging 361
OperatorLogName 362
OperatorLogTemplate 362
options (security dialog) 513
OrderlyShutdown 461

P

Page 366
Page Add Privilege 578
Page Delete Privilege 579
Page Modify Privilege 579

Page Note Edit Privilege 579
Page Note Hide Privilege 579
page properties 363
PageButtonToolTipBalloonStyle 367
PageButtonToolTipDelay 367
PageButtonToolTipEnable 367
PageButtonToolTipFont 368
PageSnapshotCacheThresholdCount 368
PageSnapshotCacheThresholdPct 368
PageSnapshotsMaxInMemory 369
PageToolTipLabel 369
Parameter View Privilege 580
ParmChangedColor 408
ParmInfoCreatedByLabel 408
ParmInfoCreatedOnLabel 408
ParmInfoHistoryEnabled 408
ParmInfoLastModByLabel 409
ParmInfoLastModOnLabel 409
ParmInfoTimeFormat 409
ParmOverrideColor 410
password options 552
PasswordDisplay 391, 592
PasswordMinLen 392, 592
PasswordTimeLimit 392, 592
PasswordWarningTime 392, 593
pcProxBaudRate 392, 593
pcProxConnectCheckTO 392, 593
pcProxDatabits 393, 593
pcProxEnable 393, 593
pcProxExcludePortx 393, 594
pcProxParity 394, 594

pcProxPortNum 394, 595
PcProxPortScanHigh 395, 595
pcProxPortScanLow 395, 595
pcProxStopBits 395, 596
Pen Modify Privilege 580
PhoneKeyFeedback 238
PINRetries 238
PINTimeOut 239
Points.MDB 109
PollDisabledColor 293
PopupCloseOnPageClose 369
PopupLimitAction 370
port properties 355
PrintWidth 462
Prioritized 453
PrivBitsTotal 395, 596
PrivDescX 396, 597
privilege reference 569
ProgSpawnTitle 371
PromptForBadAltID 397, 597
properties 160
Properties 160
Proximity card readers 568
PulseInName 409

Q

Questionable Privilege 580
QuickAddTypeGUID 462

R

RateOfChangeRPCThreshold 410
RateOfChangeTagRPCInterval 410

read-only workstation 557
ReadOnlyStation 397, 597
realm area filtering configuration 214
RealmAreas – application properties 215
RealmAreasExcludeInvalid 334
ReceiveColor 293
RefreshRate 451
ReloadWCProgressDelay 462
RemCfgTransLog 382
RememberLoginDuration 462
RememberNewTagParameters 410
REMOTE – setup.ini section 439
rename privileges 541
RepeatMenuTime 239
RepoClashWait 462
report properties 372
ReportBrowseDir 373
ReportDateFormat 374
ReportOutputDir 374
Reports Page Access Privilege 581
ReportTempDir 374
ReportTemplateDir 374
ReportTimeZoneAware 374
ReportXPos 375
ReportXSize 375
ReportYPos 376
ReportYSize 376
RepositoryCommentDisable 443
RepositoryCommentMinLen 444
RepositoryShowCloneHistory 444, 473
restrict access 543

Revert Changes Privilege 581
revision files 473
role privileges 532
Roles 519
RootNamespace 335, 397, 598
RosterDelay 239
Round-robin 453
RPC properties 377
RPCMANAGER-EXCLUDEIP – setup.ini section 439
RPCMANAGER-NETPRIORITY – setup.ini section 439
RPCManager-AllowIP 451
RPCManager-ExcludeIP 452
rule scope 544

S

ScaleDisplayContent 325
ScreenReportsInExcel 376
ScriptIconFile 444
scroll bars – adding 613
SCT.MDB 109
security 500
security-group 534
security privileges 569
security properties 383, 584
security rules 544
SecurityAlarmArea 283, 598
SecurityManager-Admin 209
SecurityManager-PrivSys 210
SecurityManager.INI 109, 199
SelectedBGnd 293
SelectedText 294
SerialShareSemaphore 355

SerPortDisconnectDelay 356
service accounts 622
service errors 624
service installation 619
service, running VTScada 617
Settings 160
settings files – rules for editing 206
Settings.Dynamic 199
Settings.Startup 199
Shared Security 554
SharedContexts 397, 598
SharedSecurity 398, 599
ShowTip 415
ShowUnlinkedIndicators 326
ShutdownOnLowBattery 464
SiemensS7PortSharedRPC 382
SiemensS7SharedRPC 383
SiteDetailsWindowed 326
SiteRetries 353
SiteToolsQueryChange 411
SkipLogonDialout 239
SlippyMapRemoteTileSource1 464
SMTPPort 240
Snap/Grid properties 399
SnapOn 401
Snapshot ChangeSet 472
SNMPAgentEnable 307
SNMPAgentInformRetryInterval 307
SNMPAgentInformRetryLimit 307
SNMPAgentIPListener 308
SNMPAgentMaxTCPSize 308

SNMPAgentReadCommunity 308
SNMPAgentSessionTimeout 309
SNMPAgentTagNotifyMode 309
SNMPAgentTrapCommunity 309
SNMPAgentTrapHost 310
SNMPAgentTrapPort 310
SNMPAgentWriteCommunity 310
SNMPAgentWriteEnable 310
SoapServicesRealmName 339
splash screen 448
SQLDataQueryDriverDefaultDBType 311
SQLDataQueryDriverDefaultTableName 311
SQLLoggerDefaultLogInterval 411
SQLLoggerDefaultMaxDataAge 411
SQLLoggerDefaultTagDataTableName 411
SQLLoggerDefaultTagIdTableName 411
SQLLoggerDeleteInterval 412
SQLLoggerDeleteOffset 412
SQLLoggerGroupSharedRPC 412
SQLLoggerLogInvalids 412
SQLQueryDriverMaxTagsPerQuery 312
SQLQueryHideLegacyTables 340
SQLQueryTableTPPs 341
SquelchDetectDelay 353
SquelchIdleTime 354
SquelchPacketLength 354
SSL certificate 559
StandardServerLists 210
start, splash animation 448
StartOfWeek 377
startup animation 448

State0DefColor 294
State1DefColor 294
State2DefColor 295
State3DefColor 295
StorageLocation 341
StorageType 342
StretchBackground 371
SuperUser 533
suppress privileges 554
Sync.WIF 109
SyncOEMLayers 332
SyncServAuditDeferTime 444
SyncServConnectTimeout 444
SyncServSyncTimeout 445
SysPrivDefault 398, 599
SysPrivSuppress 398, 599
SYSTEM 210
SYSTEM – setup.ini section 439
SystemAlarmAreas 210

T

Tag Add/Copy Privilege 581
Tag Delete Privilege 582
Tag Modify Privilege 582
tag properties 402
TagField1Name 412
TagField2Name 413
TagField3Name 413
TagNameDelimiter 464
TCPIPPortMaxRcvLen 357
TCPIPPortMaxXmtLen 357
Template ChangeSet 472

timesync properties 413
TimeSyncEnable 414
TimeSyncMicroAdjust 414
TimeSyncRPCQMax 414
TimeSyncUpdtltrl 414
TipBack 415
TipFore 416
TipOff 417
TipOn 417
TitleLogoTarget 326
ToolBoxOn 327
ToolBoxTranslucent 327
tooltip properties 415
tooltip visibility 602
TPPath 371
TRACE – setup.ini section 440
TraceBrowser 466
TraceCM 466
TraceDispMgr 466
TraceDlg 467
TraceELM 467
TraceMenuEd 467
TraceModem 467
TraceNav 467
TracePageMgr 467
TracePLimit 468
TraceRamRecs 468
TraceRPC 468
TraceSQL 468
TraceSS 468
TraceTagCfg 468

TraceToFile 468
TraceTool 469
TraceUserConfigActions 342
TraceVAM 469
TransmitColor 296
trending properties 417
TrendOnTop 436
troubleshooting 601

U

UnackAlarmFlash 283
UnackFlashRate 283
UnselectedBgnd 296
UnselectedText 296
updating applications 88
upgrade notes 88
UPS Configuration 461
UseLegacyHistoryPriorTo 342
UseOldSiteDialog 372
UseOldSpeechEngine 240
user groups 534
UserName 399, 600
UseSerialAreaInModemCall 354, 357
UseSMTPOverTLS 241
UseUnimodem 355
UseXPCompatibleFont 465

V

VAM 149
VAMIcon 332
VIC properties 333
VICAutoAddDebugTools 465

VICMonitorLogFileName 451
VICMonitorPageInfo 495
virtual address space 611
VTSDriverClearDataOnServerLossDelay 311

W

WavAmplitude 284
WAVType 284
WelcomeToTheLabel 437
WindowBgnd 297
WindowFrame 297
Wizard properties 436
WizardFinishText1 436
WizardFinishText2 437
WizardFinishText3 437
WizardFinishTitle 437
workstation.dynamic 207
Workstation.INI 109
workstation.startup 207
WorkstationSettings 208
WSI 509

X

XGrid 401

Y

YGrid 401